

»Ein rundum gelungenes und
beeindruckendes Werk!« Java Magazin



ernst TIEMEYER (Hrsg.)

HANDBUCH IT-MANAGEMENT

KONZEPTE, METHODEN, LÖSUNGEN UND
ARBEITSHILFEN FÜR DIE PRAXIS

4. Auflage



EXTRA: Mit kostenlosem E-Book



Neu: Mit Kapiteln zu IT-Compliance
und IT-Lizenzmanagement

HANSER

Tiemeyer (Hrsg.)
Handbuch IT-Management



Bleiben Sie einfach auf dem Laufenden:

www.hanser.de/newsletter

Sofort anmelden und Monat für Monat
die neuesten Infos und Updates erhalten.

Handbuch IT-Management

Konzepte, Methoden, Lösungen
und Arbeitshilfen für die Praxis

Herausgegeben von
Ernst Tiemeyer

Mit Beiträgen von

Werner Bachmann, Robert Bergmann, Torsten Groll, Michael Klotz,
Dietmar Kopperger, Helmut Krcmar, Jörg Kunsmann, Andreas Nehfort,
Klaus Schmidt, Andreas Roland Schwertsik, Ernst Tiemeyer,
Anette Weisbecker, Walter Wintersteiger

4., überarbeitete und erweiterte Auflage

HANSER

Alle in diesem Buch enthaltenen Informationen, Verfahren und Darstellungen wurden nach bestem Wissen zusammengestellt und mit Sorgfalt getestet. Dennoch sind Fehler nicht ganz auszuschließen. Aus diesem Grund sind die im vorliegenden Buch enthaltenen Informationen mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Herausgeber, Autoren und Verlag übernehmen infolgedessen keine juristische Verantwortung und werden keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieser Informationen – oder Teilen davon – entsteht.

Ebenso übernehmen Herausgeber, Autoren und Verlag keine Gewähr dafür, dass beschriebene Verfahren usw. frei von Schutzrechten Dritter sind. Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Buch berechtigt deshalb auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Dieses Werk ist urheberrechtlich geschützt.

Alle Rechte, auch die der Übersetzung, des Nachdruckes und der Vervielfältigung des Buches, oder Teilen daraus, vorbehalten. Kein Teil des Werkes darf ohne schriftliche Genehmigung des Verlages in irgendeiner Form (Fotokopie, Mikrofilm oder ein anderes Verfahren) – auch nicht für Zwecke der Unterrichtsgestaltung – reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

© 2011 Carl Hanser Verlag München, www.hanser.de

Lektorat: Margarete Metzger, Stefanie Gerhards

Herstellung: Irene Weihart

Copy editing: Manfred Sommer, München

Umschlagdesign: Marc Müller-Bremer, www.rebranding.de, München

Umschlagrealisation: Stephan Rönigk

Gesamtherstellung: Kösel, Krugzell

Ausstattung patentrechtlich geschützt. Kösel FD 351, Patent-Nr. 0748702

Printed in Germany

print-ISBN: 978-3-446-42751-8

e-book-ISBN: 978-3-446-43048-8

Inhalt

1	IT-Management – Herausforderungen und Rollenverständnis heute	1
	<i>Ernst Tiemeyer</i>	
1.1	Managementtätigkeit im Gesamtkontext von Unternehmen und Verwaltung	2
1.1.1	Visionen, Leitbilder und Zielsysteme von Unternehmen	3
1.1.2	Vom Denken in Funktionen zum Denken in Prozessen	6
1.1.3	Strategische versus operative Managementfunktionen	7
1.2	Die IT im Unternehmensumfeld – Entwicklungstrends und Konsequenzen	8
1.2.1	Informations- und Kommunikationstechnologien im Wandel der Zeit	8
1.2.2	Der Wandel der IT zum kundenorientierten Dienstleister	10
1.2.3	Beitrag der IT zum Unternehmenserfolg	11
1.2.4	Die Integration der IT in die Unternehmensstrategie	13
1.3	IT-Management – Rollenverständnis und Kernaufgaben	15
1.3.1	Positionierung des IT-Managements im Unternehmen	15
1.3.2	Partner für das IT-Management und die Rolle der IT	15
1.3.3	Strategisches und operatives IT-Management	17
1.4	Typische Aufgaben und Anforderungen an das IT-Management	18
1.5	IT-Management – Orientierungen für die Zukunft	35
1.6	Literatur	40
2	IT-Strategien entwickeln und umsetzen	41
	<i>Walter Wintersteiger, Ernst Tiemeyer</i>	
2.1	Rahmenbedingungen für die IT-Strategieentwicklung	42
2.1.1	Strategische Unternehmensführung	42
2.1.2	Zweck und Grundsätze der IT-Strategieentwicklung	44
2.1.3	Inhalte einer IT-Strategie	46
2.1.4	Einschlägige Methoden und Techniken	48
2.2	IT-Strategien entwickeln – Wesentliche Teilschritte	50
2.2.1	Analyse der Unternehmensstrategie und Ermittlung der strategischen Erfolgsfaktoren	52
2.2.2	Situationsanalysen	54
2.2.3	Umfeldanalyse	59
2.2.4	Zielfindung	60
2.2.5	Strategische Grundsätze zur IT-Ausrichtung	62
2.2.6	IT-Teilstrategien definieren	63
2.2.7	IT-Applikations-Architektur planen	65
2.2.8	Soll-Daten-Architektur dokumentieren	66

2.2.9	Soll-Technologie-Architektur entwickeln	67
2.2.10	Sicherheitsarchitektur	67
2.2.11	IT-Prozesse vereinbaren und IT-Prozesslandschaft weiterentwickeln	68
2.2.12	Ausrichtung und Gestaltung der IT-Organisation	69
2.2.13	Vorhabensplanung aus IT-Strategien ableiten	71
2.2.14	Projektportfolio ableiten und im IT-Masterplan dokumentieren	73
2.3	Eine IT-Strategie umsetzen	74
2.3.1	IT-Strategie kommunizieren	74
2.3.2	(IT-)Projekte realisieren	75
2.3.3	Sonstige IT-Entwicklungsmaßnahmen umsetzen	75
2.3.4	Umsetzung der IT-Strategie prüfen	75
2.4	Literatur	83
3	Enterprise Architecture Management (EAM) – IT-Architekturen erfolgreich planen und steuern	85
	<i>Ernst Tiemeyer</i>	
3.1	Ausgangssituation und Herausforderungen	86
3.2	Ordnungsrahmen und Grundausrichtungen für das Architekturmanagement	91
3.2.1	Grundelemente einer Enterprise- bzw. IT-Architektur	92
3.2.2	Zielsetzungen und Handlungsprinzipien für das IT-Architekturmanagement	94
3.3	Dokumentation der Architekturen – Beschreibungsmodelle und Praxisbeispiele	97
3.3.1	Dokumentationsformen für IT-Architekturen	99
3.3.2	Technologie-Architektur	100
3.3.3	Applikations-Architektur	102
3.3.4	Geschäftsarchitektur	103
3.3.5	Datenarchitektur	104
3.4	IT-Architekturen planen und ausgestalten	105
3.4.1	Generelle Vorgehensweise zur Architekturplanung	106
3.4.2	Architekturlandschaften bewerten	110
3.4.3	Soll-IT-Architekturlandschaft entwickeln und darstellen	111
3.5	Organisation der Einführung und Optimierung von Enterprise Architecture Management (EAM)	113
3.5.1	Aufgaben und Rollenkonzept im Architekturmanagement	113
3.5.2	Prozesse im Architekturmanagement	116
3.6	Projektierungen von IT-Landschaften – IT-Konsolidierungsprojekte	123
3.6.1	Hardware-Konsolidierung	124
3.6.2	Software-Konsolidierung (Applikationskonsolidierung)	128
3.6.3	Datenkonsolidierung	130
3.6.4	Projektmäßige Umsetzung von IT-Konsolidierungen	130
3.7	Projektbeispiel „SOA-Einführung“	132
3.8	Framework TOGAF im Architekturmanagement nutzen	134
3.9	Nutzen eines IT-Architekturmanagements	136
3.10	Literatur	138

4	IT-Servicemanagement	139
	<i>Dietmar Kopperger, Jörg Kunsmann, Anette Weisbecker</i>	
4.1	Effizientes IT-Servicemanagement – eine permanente Herausforderung	139
4.1.1	IT-Servicemanagement – begriffliche Orientierung	140
4.1.2	Grundlagen eines professionellen IT-Servicemanagements	141
4.1.3	IT-Servicequalität definieren – ein wichtiger Produktivitätsfaktor	143
4.1.4	Erfolge durch professionelles Management der IT und ihrer Services	144
4.2	IT-Servicemanagement – Konzepte und Standards	145
4.2.1	Die Vielfalt der Lösungen – Überblick über vorhandene Konzepte	145
4.2.2	Servicemanagement nach ITIL	148
4.3	ITIL unter der Lupe	153
4.3.1	Service-Support-Prozesse	153
4.3.2	Service-Delivery-Prozesse	159
4.3.3	Neue ITIL 3-Prozesse	164
4.4	Fahrplan zu einem optimalen IT-Servicemanagement	170
4.4.1	Kritische Erfolgsfaktoren für die Einführung	170
4.4.2	Einführung von IT-Servicemanagement – eine Vorgehensweise	171
4.4.3	Einführungsaspekte bei ITIL 3	175
4.4.4	Aufbau einer Servicekultur in der IT	178
4.4.5	IT-Servicemanagement in der Praxis	181
4.5	IT Services verrechnen und überwachen	182
4.5.1	IT-Services verrechnen	182
4.5.2	IT-Services überwachen	188
4.5.3	IT-Servicemanagement und Wirtschaftlichkeit	192
4.6	Toolauswahl für das IT-Servicemanagement	194
4.6.1	Die richtigen Werkzeuge wählen – eine Vorgehensweise	194
4.6.2	Funktionsvielfalt und Produktkategorisierung	200
4.7	Literatur	202
5	IT-Projektmanagement	207
	<i>Ernst Tiemeyer</i>	
5.1	Von der Projektinitiative zum Projektantrag	208
5.1.1	IT-Projekttypen und ihre Besonderheiten	208
5.1.2	Auslöser für IT-Projekte	210
5.1.3	Wichtige Voraussetzungen für erfolgreiche Projektarbeit	212
5.1.4	Die Projektskizze	213
5.1.5	Der Projektantrag	214
5.2	Vereinbarung eines Projektauftrages	218
5.2.1	Bewertungskriterien für IT-Projekte und Priorisierungsverfahren	218
5.2.2	Wirtschaftlichkeitsbeurteilung von IT-Projekten	221
5.2.3	Der Projektauftrag als Grundlage für die Projektarbeit	223
5.2.4	Projektaufträge erfolgreich umsetzen	223
5.3	IT-Projekte starten	225
5.3.1	Start-up-Workshop/Kick-off-Meeting	225
5.3.2	Projekt-Visionen entwickeln	226

5.3.3	Stakeholderanalyse und Stakeholdermanagement	228
5.3.4	Projektziele präzisieren	231
5.3.5	Phasengliederung und Meilensteine festlegen	231
5.4	Projektbeteiligte und Projektorganisation	234
5.4.1	Der IT-Projektleiter – Aufgaben, Anforderungen und Befugnisse	235
5.4.2	Das Projektteam – Rollenkonzept und Teambildung	236
5.4.3	Projekt-Auftraggeber und unterstützende Gremien	238
5.4.4	Kooperation mit externen Fachkräften	242
5.5	Planungsaufgaben in IT-Projekten	243
5.5.1	Rahmenbedingungen moderner Projektplanung	243
5.5.2	Projektstrukturplan und Arbeitspakete	246
5.5.3	Projektablauf- und Terminplanung	250
5.5.4	Ressourcenbedarfsplan und Ressourceneinsatzplan	256
5.5.5	Projekt-Kostenplanung	259
5.5.6	Projekt-Qualitätsplanung	261
5.5.7	Projekt-Risikoplanung	264
5.5.8	Nutzung von Projektmanagement-Software für die Projektplanung	266
5.6	Kontrolle und Steuerung von IT-Projekten	267
5.6.1	Varianten der Projektüberwachung	268
5.6.2	Statuserfassung für Projektvorgänge	269
5.6.3	Plan-Ist-Vergleiche und Reviews	272
5.6.4	Kostencontrolling in Projekten	273
5.6.5	Projektreporting	274
5.6.6	Claim-Management	275
5.6.7	Projekt-Marketing	277
5.6.8	Nutzung von Projektmanagement-Software für die Projektsteuerung	278
5.7	Multiprojektmanagement und Projektportfoliomanagement	280
5.7.1	Zielsetzungen und Erfolgsfaktoren im Multi-Projektmanagement	281
5.7.2	Projektauswahl mittels IT-Portfolioanalyse	283
5.7.3	Planungsaktivitäten im Multiprojektmanagement	284
5.7.4	Steuerung des IT-Projekt-Portfolios	285
5.8	IT-Projekte abschließen	286
5.8.1	Projektabnahme und Produktübergabe	287
5.8.2	Projektabschlussanalyse durchführen – Evaluierung und Auswertung der Projektarbeit	288
5.8.3	Projekt-Abschlussbericht und Projekt-Gesamtdokumentation erstellen	289
5.8.4	Projekterfahrungen sichern	290
5.9	Literatur	293
6	Organisation und Führung im IT-Bereich	295
	<i>Ernst Tiemeyer</i>	
6.1	Organisation und Führung – Basis für den Erfolg der IT-Abteilung	295
6.2	Elemente und Einflussfaktoren moderner IT-Organisation	296
6.3	Grundausrichtung und Konzepte zur Organisation der IT	299
6.3.1	Gestaltung und Optimierung der IT-Prozesslandschaft	299
6.3.2	Aufbauorganisatorische Ausrichtung	301

6.4	Rollen und Aufgabenstellungen im IT-Bereich	303
6.4.1	Typische Rollen im IT-Bereich	304
6.4.2	Stellenbildung und Personalbemessung	310
6.5	Outsourcing von IT-Leistungen	312
6.5.1	Entscheidung über IT-Outsourcing	312
6.5.2	Projektierung von IT-Outsourcing	315
6.6	Information und Kommunikation mittels Kennzahlen und Reporting	317
6.6.1	Informationsbedarf der IT-Führung	317
6.6.2	Reporting im IT-Bereich	318
6.7	Führung im IT-Bereich als Herausforderung	320
6.7.1	Führungsaufgaben – Einordnung und Teilaktivitäten	322
6.7.2	Führungsstile	325
6.7.3	Ausgewählte Führungsinstrumente	328
6.8	Führung von Teams – Teambildung und Teammanagement	332
6.8.1	Teamentwicklungsprozesse identifizieren	332
6.8.2	Teamkultur aufbauen und zielorientiert weiterentwickeln	335
6.9	Literatur	338
7	IT-Controlling	339
	<i>Helmut Krcmar, Andreas Roland Schwertsik</i>	
7.1	Begriff des IT-Controllings und konzeptionelle Aspekte	339
7.1.1	Funktionsbegriff und Institutionenbegriff	340
7.1.2	Organisatorische Einbindung des IT-Controllings	341
7.2	Ziele, Objekte und Aufgaben des IT-Controllings	344
7.2.1	Ziele und Objekte für ein IT-Controlling	344
7.2.2	Aufgaben im IT-Controlling	345
7.3	Methoden, Instrumente und Werkzeuge im IT-Controlling	354
7.3.1	IT-Balanced Scorecard	355
7.3.2	IT-Kennzahlensysteme	356
7.3.3	Benchmarking	359
7.3.4	Service-Level-Agreements (SLA)	360
7.3.5	Leistungsverrechnung	363
7.4	Umsetzung von IT-Controlling	368
7.5	Literatur	371
8	Herausforderung Lizenzmanagement – vom Risiko zum Wert	373
	<i>Torsten Groll</i>	
8.1	Potenzial und Nutzen des Lizenzmanagements	373
8.2	Was ist eine Softwarelizenz?	378
8.3	Der Software-Life-Cycle-Prozess und seine Bestandteile	383
8.4	Der Lizenzmanager und verwandte Rollen	386
8.5	Welche Daten sind für das Lizenzmanagement erforderlich?	388
8.6	Komplexitätstreiber im Lizenzmanagement	392
8.7	Der Einfluss der IT-Architektur auf das Lizenzmanagement	394

8.8	Auswahl des Lizenzmanagement-Tools	396
8.9	Einführung einer Lizenzmanagement-Lösung	400
8.10	Literatur und weiteres Informationsmaterial	402

9 Qualitätsmanagement für IT-Lösungen 403

Andreas Nehfort

9.1	Begründungen und Ansätze für umfassende Qualitätsmanagement-Lösungen	403
9.1.1	Warum ist Qualitätssicherung bzw. Qualitätsmanagement im IT-Bereich so wichtig?	403
9.1.2	Wie funktioniert Qualitätsmanagement?	405
9.1.3	Das Dilemma des Qualitätsmanagements	405
9.2	Grundlagen und Begriffe des IT-Qualitätsmanagements	406
9.2.1	Qualität	407
9.2.2	Qualitätsverbesserung	409
9.2.3	Qualitätsmanagement und Qualitätssicherung als Teil eines Managementsystems	410
9.2.4	Konsequenzen für den Aufbau von Qualitätsmanagement-Systemen	411
9.3	Sequenzielle versus iterative Entwicklungsmodelle: Risiko-Strategie	413
9.3.1	Sequenzielle Entwicklung: das V-Modell	414
9.3.2	Iterative Entwicklung	416
9.3.3	Schlussfolgerungen zum Vorgehensmodell in der Software-Entwicklung unter Qualitätsaspekten	420
9.4	Qualität von Produkten	422
9.4.1	Brauchbarkeit und Wartbarkeit	422
9.4.2	Qualität der Anforderungen	424
9.4.3	Qualität der Lösung	427
9.5	Qualität des Projekts	429
9.5.1	Qualität in der Projektplanung	429
9.5.2	Qualität in der Projektleitung	433
9.6	Qualität der Prozesse	434
9.6.1	Prozessmodellierung	434
9.6.2	Referenz-Prozessmodelle	434
9.6.3	Prozessreifegrad-Modelle	436
9.6.4	Prozessqualität in agilen Prozessen	439
9.7	Qualitätssicherung	441
9.7.1	Organisatorische Qualitätsmaßnahmen	441
9.7.2	Konstruktive Qualitätsmaßnahmen	441
9.7.3	Analytische Qualitätsmaßnahmen	442
9.7.4	Reviews	444
9.8	Relevante Qualitätsmanagement-Standards	448
9.8.1	Die Normenreihe ISO 9000ff	448
9.8.2	Standards für Software-Produktqualität	450
9.8.3	Prozessreifegrad-Modelle (CMMI & SPICE/ISO15504)	454
9.8.4	Referenz-Prozessmodelle in der IT	458
9.9	Literatur	461

10	IT-Governance	463
	<i>Robert Bergmann, Ernst Tiemeyer</i>	
10.1	Merkmale und Bedeutung von IT-Governance	464
10.1.1	Zielsetzungen und Rahmenbedingungen für eine erfolgreiche IT-Governance	465
10.1.2	IT-Governance-Prozesse und Corporate Governance	468
10.2	Kern-Aufgabenbereiche zentraler IT-Steuerung	470
10.2.1	Ganzheitliche IT-Strategieentwicklung	472
10.2.2	IT-Anforderungsmanagement	474
10.2.3	IT-Architekturmanagement und Enterprise Architecture Management	477
10.2.4	Multiprojektsteuerung für IT-Projekte	482
10.2.5	IT-Risikomanagement	484
10.2.6	Compliance Management	486
10.2.7	IT-Investitionsmanagement und Value-Management	487
10.3	Zentrale IT-Governance einführen	490
10.3.1	Die Ansätze	490
10.3.2	Vorgehen	492
10.4	Performance Management für IT-Governance	494
10.5	Fazit	496
10.6	Literatur	499
11	IT-Security-Management	501
	<i>Klaus Schmidt</i>	
11.1	Ausgangssituation und Bedeutung von IT-Security-Management	502
11.1.1	Problemlage	502
11.1.2	Ermittlung der Sicherheitsrelevanz	503
11.1.3	IT-Security-Management als Erfolgsfaktor	505
11.1.4	Rechtlicher Rahmen für die IT-Security	506
11.1.5	Anforderungen an ein hochwertiges IT-Security-Management	511
11.2	Sicherheitsorganisation für die IT-Security	514
11.2.1	Möglichkeiten für die Einordnung in die Organisation	514
11.2.2	Rollen im IT-Security-Management	516
11.2.3	Organisationsmodelle	518
11.2.4	Zusammenspiel mit anderen Sicherheitsbereichen	521
11.3	Aufbau des IT-Security-Managements	522
11.3.1	Sicherheitsrichtlinien	523
11.3.2	Schutzbedarfsanalyse	523
11.3.3	Sicherheitskonzepte und Sicherheitslösungen	524
11.3.4	IT-Security Reporting	524
11.3.5	Information Security Circle	527
11.3.6	Notfallmanagement	528
11.4	Einsatz von Sicherheitsstandards	528
11.4.1	ISO/IEC 2700x (International)	529
11.4.2	IT-Grundschutz (Deutschland)	530
11.4.3	Informationssicherheitshandbuch (Österreich)	530
11.4.4	Informatiksicherheit in der Bundesverwaltung (Schweiz)	531

11.5	Sicherheit als Sollzustand vorgeben	531
11.5.1	IT-Sicherheitskriterien	531
11.5.2	Sicherheitsgrad und Sicherheitsklassen	535
11.5.3	Sicherheitsstrategien	536
11.5.4	Sicherheitspolitik und Corporate IT-Security Policy	537
11.5.5	Security Policy Management	540
11.5.6	IT-Security Auditing	541
11.5.7	Sicherheit in externen Partnerschaften	542
11.6	Literatur	545
12	IT-Risikomanagement	547
	<i>Klaus Schmidt</i>	
12.1	Risiko und Gefahr	548
12.1.1	Der Gefahrenbegriff	548
12.1.2	Der Risikobegriff	548
12.1.3	Risikowahrnehmung	551
12.2	Entstehung von Risiken und Risiko-Identifikation	552
12.2.1	Schwachstelle	552
12.2.2	Angriffspfad	553
12.2.3	Auslöser	554
12.2.4	Bedrohung	554
12.3	Risikoszenario	555
12.3.1	Sicherheitsrelevantes Ereignis	555
12.3.2	Wirkungsszenario	556
12.4	IT-Risikoanalyse	557
12.4.1	Kernbestandteile der IT-Risikoanalyse	557
12.4.2	Arten von IT-Risikoanalysen	557
12.4.3	IST-Aufnahme	558
12.4.4	Schwachstellenanalyse	560
12.4.5	Bedrohungsanalyse	561
12.4.6	Risikofeststellung und -bewertung	562
12.4.7	Risikodarstellung und Risikodokumentation	568
12.5	Risikoentscheidung	573
12.5.1	Risikotragfähigkeit	574
12.5.2	Risikobereitschaft	574
12.5.3	Risikoakzeptanz	574
12.5.4	Risikopriorisierung	575
12.5.5	Risikobewältigungsstrategien	575
12.5.6	Restrisikodeklaration	577
12.6	IT-Risikosituation managen	578
12.6.1	Risikokorridor	578
12.6.2	Risikofrüherkennung	580
12.6.3	IT-Risikomanagementprozess	580
12.7	Literatur	583

13	IT-Compliance	585
	<i>Michael Klotz</i>	
13.1	Begriff und Aktualität von Compliance	585
13.1.1	Begriffliche Grundlagen	586
13.1.2	Beispiele von Compliance-Verstößen	589
13.2	IT-Compliance	591
13.2.1	Begriffliche Grundlagen	591
13.2.2	IT-Compliance als Verhalten	594
13.2.3	Compliance der IT-Funktion vs. IT-gestützte Corporate Compliance	595
13.2.4	„Governance – Risk – Compliance“ und IT-Compliance	598
13.3	IT-Compliance nach COBIT	600
13.3.1	COBIT als IT-Governance Framework	600
13.3.2	Compliance als allgemeine Geschäftsanforderung	601
13.3.3	Der COBIT-Prozess zur Sicherstellung von Compliance	603
13.4	Nutzen von IT-Compliance	605
13.5	Beteiligte und Interessenlagen	608
13.6	IT-relevante Regelwerke	610
13.6.1	Klassifikation der Regelwerke	610
13.6.2	Rechtliche Vorgaben	612
13.6.3	Verträge	615
13.6.4	Unternehmensexterne Regelwerke	615
13.6.5	Unternehmensinterne Regelwerke	618
13.7	Kernbereiche der Legal IT-Compliance	619
13.7.1	Buchführung und steuerliche Anforderungen	619
13.7.2	Dokumentenmanagement	621
13.7.3	Datenschutz	623
13.7.4	Webpräsenz	624
13.7.5	Personalwesen	627
13.7.6	IT-Beschaffung	628
13.8	Management der IT-Compliance	629
13.9	Organisatorische Verankerung von IT-Compliance	633
13.10	Literatur	638
14	Rechtliche Rahmenbedingungen für das IT-Management	641
	<i>Werner Bachmann</i>	
14.1	IT-Governance und IT-Compliance	642
14.1.1	Vorsorge gegen Gesetzesverstöße und Risikomanagement	642
14.1.2	Reporting	645
14.1.3	Persönliche Haftung des Managements	645
14.1.4	Strafrechtliche Verantwortung des Compliance Officer und anderer Funktionsträger mit besonderen Aufgaben	651
14.1.5	Unterstützung der Corporate Compliance durch die IT-Organisation	651
14.2	IT-Beschaffung	654
14.2.1	Ausschreibung von Beschaffungsvorhaben	654

14.2.2	Voraussetzungen für die Ausschreibungspflicht	657
14.2.3	Weitere Fragestellungen	658
14.3	Allgemeine Geschäftsbedingungen	661
14.3.1	Grundlagen	661
14.3.2	Weitere Fragestellungen	663
14.4	Mängel und Garantie beim Hardwarekauf	667
14.4.1	Rechte bei Mängeln	667
14.4.2	Vorgehen in der Praxis	668
14.4.3	Weitere Fragestellungen	668
14.5	Software-Lizenzierung	670
14.5.1	Grundlagen	670
14.5.2	Das sollten Sie beachten	671
14.5.3	Weitere Fragestellungen	672
14.6	Das Lizenzaudit	676
14.7	Externe Software-Entwicklung	677
14.8	Software aus der Eigenentwicklung	679
14.9	Verträge in der Vorbereitung eines IT-Projekts	680
14.10	Verträge für schlüsselfertige IT-Systeme	682
14.10.1	Grundlagen	683
14.10.2	Vorgehen in der Praxis	684
14.11	Verträge über Cloud Services	686
14.12	Literatur	690
Die Autoren		691
Index		695

Vorwort

Mittlerweile ist unbestritten, dass Erfolg oder Misserfolg der Unternehmenstätigkeit zunehmend von einem funktionierenden Einsatz moderner Informations- und Kommunikationstechnologien abhängen. Dies hat natürlich zur Konsequenz, dass die Anforderungen an ein gutes IT-Management in den letzten Jahren gestiegen sind und IT-Manager in vielen Organisationen zunehmend eine Schlüsselposition einnehmen. Die Bedeutung der IT wird auch weiterhin noch wachsen, das ist beispielsweise an Diskussionen um das Thema IT-Governance sowie der zunehmenden Abhängigkeit der Geschäftsprozesse von effizienter und sicherer IT-Unterstützung zu erkennen. Proportional zur Bedeutung der IT steigen aber auch die Risiken: Als Beispiele seien hier ein Systemausfall durch zu hohe Komplexität der IT-Systeme genannt oder Angriffe auf IT-Systeme von innen und außen. All diese Aspekte sind durch ein hochleistungsfähiges IT-Management nicht nur zu koordinieren und zu optimieren, sondern auch zu verantworten, was nicht zuletzt in Diskussionen um IT-Compliance deutlich geworden ist.

Erfolgreiches IT-Management – so zeigen unabhängige Untersuchungen – ist zwischenzeitlich also zu einem der wichtigsten Erfolgsfaktoren eines jeden Unternehmens geworden und die IT somit zum unverzichtbaren Enabler von Geschäftsprozessen. Deshalb sind fundiertes Fach- und Methoden-Wissen zu verschiedenen Managementthemen, Kompetenzen zur Wahrnehmung von Führungsfunktionen sowie Kenntnisse und Fähigkeiten zur Anwendungs- und Systementwicklung von Informations- und Kommunikationstechnologien für im IT-Bereich tätige Personen mit Management- und Führungsaufgaben inzwischen unverzichtbar. Dazu gehören insbesondere: die Fähigkeit zur Entwicklung von IT-Strategien, die nachhaltige Konzipierung von leistungsfähigen Enterprise Architekturen, technisches Know-how der IT-Architekturen, fundiertes Anwendungswissen zu verschiedenen Managementthemen (Projektmanagement, IT-Servicemanagement, Qualitätsmanagement, Risiko- und Sicherheitsmanagement), Führungs- und Controllingkompetenz sowie Kenntnisse zu den IT-Anwendungsfeldern (Geschäftsprozess-Wissen als Basis eines erfolgreichen Business-IT-Alignments) und zu wichtigen Rechtsgebieten (IT-Compliance, IT-Recht).

Obwohl einzelne technische Komponenten billiger werden, ist eine steigende Kostentendenz bei IT-Produkten, IT-Services und IT-Projekten insgesamt zu beobachten. Management und Führung von IT-Bereichen sind heute damit konfrontiert, komplexere Aufgaben in kürzerer Zeit unter Beachtung von strengen Wirtschaftlichkeitsvorgaben wahrnehmen zu müssen. Eine effiziente Erfüllung dieser Aufgaben macht einen aktuellen Stand der Kenntnisse in den wichtigsten Themenbereichen des IT-Managements notwendig.

Das Ziel dieses umfassenden Handbuchs IT-Management ist, Ihnen in systematischer Form das nötige Wissen zu den verschiedenen Handlungs- und Kompetenzfeldern des IT-Managements praxisnah und anschaulich aufbereitet zu vermitteln. Insbesondere sollen Sie – ausgehend von vorhandenem Basiswissen und Erfahrungen im IT-Bereich – die für ein erfolgreiches IT-Management notwendigen Methoden und Instrumente sowie relevante Frameworks kennenlernen und auf Ihre Praxissituationen transferieren können. 13 Experten aus der

Industrie, von Consulting-Unternehmen und Universitäten stellen in den einzelnen Kapiteln die folgenden Themen vor und geben hilfreiche Tipps für die Umsetzung in der Praxis:

- IT-Strategien entwickeln und umsetzen
- Enterprise Architecture Management/IT-Architekturen
- IT-Servicemanagement
- IT-Projektmanagement
- Organisation und Führung im IT-Bereich
- IT-Controlling
- Herausforderung Lizenzmanagement
- Qualitätsmanagement für IT-Lösungen
- IT-Governance
- IT-Security-Management
- IT-Risikomanagement
- IT-Compliance
- Rechtliche Rahmenbedingungen für das IT-Management

Dieses umfangreiche Handbuch möchte einen wesentlichen Beitrag leisten, um allen im IT-Bereich tätigen Fach- und Führungskräften die für erfolgreiches IT-Management notwendigen Methoden und Techniken zu vermitteln:

- Nach Durcharbeiten des Buches besitzen Sie das fachliche und methodische Know-how, um IT-Managementaufgaben erfolgreich wahrzunehmen.
- Gleichzeitig erweitern Sie mit dem Lesen des Buches integrativ Ihre sozialen und personalen Kompetenzen, die Ihnen beim Entwickeln, bei der Entscheidungsfindung und der Durchsetzung von IT-Lösungen zugute kommen.
- Das Durcharbeiten des Buches soll Ihnen außerdem helfen, die Herausforderungen und Strukturen Ihres Handelns im IT-Bereich zu erkennen, zu analysieren und so umzusetzen, dass Sie erfolgreich in Planungs-, Entscheidungs- und Controllingfunktionen tätig sein können.
- Insgesamt liefert Ihnen das Buch ein umfangreiches Repertoire an Vorgehensweisen, Praxistipps und Methoden im IT-Bereich. Welche der vorgestellten und angebotenen Werkzeuge und Methoden Sie in der Praxis jeweils auswählen und wie Sie diese nutzen, das hängt natürlich von Ihrem konkreten Tätigkeitsbereich, dem Unternehmensumfeld und von Ihnen selbst ab.

Das Buch richtet sich an Fach- und Führungskräfte im IT-Bereich; beispielsweise

- IT-Leiter (CTOs)
- Chief-Information-Officer (CIOs)
- Leiter von IT-Kompetenzzentren (Shared Service Center für IT-Lösungen)
- IT-Management verschiedener Schwerpunktbereiche; z.B. Leitung System- und Anwendungsentwicklung, Leiter Rechenzentrum und Systemmanagement, Leitung Architekturmanagement etc.
- Projektleiter für IT-Projekte, Multiprojektmanager

- IT-Architekten/Enterprise Architekten
- Leitung IT-Servicemanagement
- IT-Prozess-Verantwortliche (IT-Process-Owner)
- IT-System- und Produktverantwortliche
- Qualitätsmanager in der IT
- IT-Controller und IT-Revisoren
- IT-Compliance-Manager
- IT-Consultants
- Organisatoren, deren Arbeitsfeld auch IT-Aufgaben umfasst
- Informationsmanager und Unternehmensberater

Nicht zuletzt dürfte das Handbuch für alle Studierenden beispielsweise der Wirtschaftsinformatik oder anderer angewandter Informatik-Studiengänge an Fachhochschulen und Universitäten höchst interessant und lesenswert sein. Gerade von künftigen Fach- und Führungskräften der Informations- und Kommunikationstechnik wird ein immer komplexeres Management-Know-how erwartet, wollen sie den Herausforderungen der Praxis gerecht werden und ihnen übertragene Aufgaben erfolgreich wahrnehmen.

Ich freue mich sehr, dass das Handbuch aufgrund der hohen Nachfrage nach so kurzer Zeit bereits in der vierten Auflage erscheinen kann und eine Neubearbeitung seitens des Verlages ermöglicht wurde. Dies gab mir als Herausgeber und allen Autoren die Möglichkeit, einerseits die bereits vorliegenden Beiträge auf einen aktuellen Stand zu bringen und eine mehr oder weniger intensive Bearbeitung der Beiträge vorzunehmen. Gleichzeitig konnten wir sich aktuell herauskristallisierende Management-Themen neu in diese Auflage des Handbuchs aufnehmen: Beispiele sind die Beiträge zum IT-Lizenzmanagement sowie zur IT-Compliance-Thematik.

Ich hoffe jedenfalls, dass es mir und meinen Autoren, denen ich für ihre äußerst engagierte und qualifizierte Arbeit an ihrem jeweiligen Beitrag ausdrücklich danken möchte, auch in der vierten Auflage wieder gelungen ist, Ihnen ein Handbuch zu präsentieren, das interessante, umfassende sowie auf alle Fälle für die berufliche Tätigkeit hilfreiche Einblicke und Handlungshilfen gibt.

Danken möchte ich auch dem Hanser Verlag (hier insbesondere Frau Stefanie Gerhards und Frau Margarete Metzger für ihr umfassendes Controlling und für zahlreiche weiterführende Hinweise), der die Herausgabe des Handbuchs in der neuen Auflage ermöglicht hat, für die professionelle Umsetzung sowie für die Geduld und vielfältige Unterstützung während der Erstellung.

Ich wünsche Ihnen viel Spaß beim Lesen der Beiträge in diesem Handbuch sowie Ideen zur Umsetzung des Gelesenen in Ihre Praxis. Über Anregungen zur Verbesserung und Weiterentwicklung des Buches aus dem Kreis der Leserinnen und Leser würde ich mich freuen.

Hamminkeln, im September 2011

Ernst Tiemeyer

ETiemeyer@t-online.de

IT-Management – Herausforderungen und Rollenverständnis heute

Ernst Tiemeyer



Fragen, die in diesem Kapitel beantwortet werden:

- Welche Konsequenzen haben die rapiden Veränderungen in Wirtschaft und Gesellschaft sowie sich daraus ergebende Neuausrichtungen von Unternehmen auf die Tätigkeitsfelder im IT-Management?
- Welchen Herausforderungen muss sich das IT-Management heute stellen?
- Welche Bedeutung hat die Unterscheidung von strategischem und operativem Management für die optimale Organisation und Führung im IT-Bereich?
- Welche wichtigen Entwicklungstrends sind im IT-Umfeld zu berücksichtigen, wenn es um nachhaltige Organisation und Etablierung von IT-Managementaufgaben geht?
- Wie sieht das Rollenverständnis im IT-Management aus, und welche Kernaufgaben fallen im Managementbereich von IT-Abteilungen bzw. IT-Organisationen an?
- Welche Kompetenzen benötigt das IT-Management heute und morgen?

Insbesondere die Entwicklung neuer Technologien sowie die Globalisierung, Internationalisierung und Liberalisierung des Weltmarktes stellen Unternehmen und Verwaltung vor immer größere Herausforderungen. Intensivierung des Wettbewerbs, zunehmende Dezentralisierung, kürzere Time-to-Market-Zyklen, steigende Kundenanforderungen und die Beschleunigung des technologischen Wandels sind nur einige dieser Problembereiche, denen sich die Unternehmensführung stellen muss. Auch die öffentliche Verwaltung muss zunehmend wirtschaftlich organisiert und durch neue Technologien effizient unterstützt werden.

Die Arbeitswelt – dies gilt insbesondere für die im IT-Bereich tätigen Personen – befindet sich nach wie vor in einem permanenten Umbruch. Um die geänderten und gewachsenen Herausforderungen erfolgreich zu meistern, sind als Folge davon neue Konzepte und Vorgehensweisen im IT-Management sowie besondere Anstrengungen zur Kompetenzentwicklung notwendig.

In diesem Handbuch werden dazu entsprechend detaillierte und handlungsorientierte Informationen gegeben, um die vielfältigen Anforderungen und Herausforderungen im IT-Bereich erfolgreicher bewältigen zu können:

- Das Handbuch liefert angehenden und erfahrenen IT-Managern umfassendes, aktuelles und in der Praxis notwendiges Wissen aus allen wesentlichen Bereichen des IT-Managements. Dazu zählen sowohl das strategische IT-Management (Strategieentwicklung, Enterprise Architecture Management, IT-Governance etc.) als auch operative Managementthemen wie etwa das IT-Servicemanagement, IT-Projektmanagement und IT-Qualitätsmanagement.

- Im Mittelpunkt der Ausführungen stehen vielfach unmittelbar anwendbare Lösungsansätze, die Anregungen und Antworten für typische Fragen und Problemstellungen im Kontext des IT-Managements geben. So stehen für viele Bereiche bereits umfassende Tools und Frameworks zur Verfügung, die ebenso wie bewährte Vorgehensmodelle und Konzepte in diesem Handbuch systematisch und problemlösungsorientiert dargestellt werden.

Dieses erste Kapitel des Handbuchs ist als Einstieg in die vielfältige Thematik des IT-Management sowie als Überblick und Einordnung für die nachfolgenden Kapitel gedacht. Dazu werden zunächst wesentliche Aufgaben und Handlungsfelder skizziert, die im Management- und Führungsbereich generell (unabhängig vom Aufgabenbereich) wahrzunehmen sind. Darauf bezogen werden dann die Bedeutung und die Rolle der IT in Unternehmen und Verwaltung analysiert und die notwendigen Konsequenzen für das IT-Management diskutiert. Schließlich finden Sie in diesem Kapitel eine systematische Beschreibung der wesentlichen Aufgaben und Handlungsfelder im IT-Management sowie Hinweise, wie das IT-Management in der Unternehmenspraxis positioniert und organisatorisch verankert sein muss, um einen hohen Wertbeitrag der IT-Leistungen zum Unternehmenserfolg sicherzustellen. Damit lässt sich dann integriert aufzeigen, über welche Managementkompetenzen das IT-Führungspersonal verfügen sollte.

■ 1.1 Managementtätigkeit im Gesamtkontext von Unternehmen und Verwaltung

Im Mittelpunkt jeder **Managementtätigkeit** stehen heute die übergreifende Koordination von Leistungsprozessen, die in Unternehmen und Verwaltung anfallen. Dabei sind verschiedene Einzelaktivitäten notwendig, die immer auf ein gemeinsames Ziel auszurichten sind. Die Teilaktivitäten im Management können durch den so genannten **Managementprozess** beschrieben werden:

- Ziele setzen,
- Planen,
- Entscheiden,
- Realisieren und
- Kontrollieren.

Managen, Führen und Organisieren ist grundsätzlich nichts anderes als Problemlösung. Bei der Lösung von Management- und Organisationsproblemen ist die Komplexität allerdings häufig sehr groß. Jedes „vernünftige“ Handeln stößt an die Grenzen dieser Komplexität. Erfolgreiche Problemlösungen sind daher ohne Einsatz geeigneter Techniken nicht denkbar. Bekannte Techniken wie etwa Management by Objectives (Managen durch Zielvorgabe) sowie Management by Exception (Managen nach dem Ausnahmeprinzip; d. h. weitgehende Eigenverantwortung der Mitarbeiter, Eingriff nur im Ausnahmefall) sind bereits seit Jahrzehnte bewährt und werden heute in der Praxis in unterschiedlichen Ausprägungsformen erfolgreich genutzt.

Die Auswahl einer geeigneten Handlungsalternative ist in der betrieblichen Praxis eine wichtige, häufig wiederkehrende Aufgabe. Typische Entscheidungsprobleme sind: Preisvergleiche, Beschaffungsplanungen, Investitionsplanung, Personaldisposition, Lieferantenauswahl, Wahl zwischen Eigenfertigung und Fremdbezug, Standortwahl sowie Entscheidungen über Hard- und Software. In allen Fällen sind die wahrscheinlichen Wirkungen der alternativen Lösungen in Bezug auf die verfolgten Gestaltungsziele zu beurteilen.

Unabhängig vom Entscheidungsproblem ist im Regelfall ein systematisches Vorgehen „angesagt“. Vermieden werden sollte in den meisten Situationen, sich allein von subjektiven Überlegungen leiten zu lassen. Transparent und nachvollziehbar werden Bewertungs- und Auswahlprozesse allerdings erst dann, wenn die subjektiven Bewertungsvorgänge in formalisierte Bewertungsverfahren eingebettet werden.

Jeder Entscheidungsprozess kann als ein Informationsverarbeitungsprozess bezeichnet werden. In ihm sind tatsächliche und bewertete Komponenten wirksam, die miteinander in Einklang zu bringen sind:

- Tatsächliche Entscheidungskomponenten:
 - Situation (Realität, Umweltzustände)
 - Mögliche Aktionen (alternative Handlungen)
 - Erwartete Ergebnisse (Konsequenzen) der Aktionen
- Wertende Entscheidungskomponenten:
 - Ziele (mit unterschiedlichen Präferenzen)
 - Nutzen der Ergebnisse der Aktionen (unter Berücksichtigung der Ziele)

1.1.1 Visionen, Leitbilder und Zielsysteme von Unternehmen

Eine wesentliche Aufgabe des General-Managements besteht darin, eigene Visionen für die Unternehmensentwicklung zu formulieren und zu kommunizieren. Dabei kommt es darauf an, „realistische Visionen“ zu fixieren und andere (etwa die betroffenen Mitarbeiter und Mitarbeiterinnen sowie die Stakeholder) dafür zu begeistern.

Dabei gilt es zu beachten: **Chancen für die Zukunftsfähigkeit von Unternehmen** liegen nicht primär in der Realisierung weiterer Prozessautomatisierungen oder des „Aufkaufens“ anderer Unternehmen, sondern vielmehr

- in einem effizienten Einsatz von Ressourcen durch Einsatz moderner Informationstechnologien,
- in der optimalen Gestaltung überbetrieblicher Vernetzungen unter Nutzung von Kommunikationstechnologien und
- in der Kompetenzentwicklung der Beschäftigten.

Diese Herausforderungen bedeuten insbesondere erhebliche Anstrengungen für das Innovations- und Technologiemanagement sowie für die Personalentwicklung in Wirtschaft und Verwaltung. Dem Personal muss unter diesen Perspektiven eine Zukunftsorientierung und eine entsprechende Sicherheit gegeben werden, die gleichzeitig eine hohe Effizienz und Effektivität ermöglicht.

Bei der **Formulierung der Vision** gilt es zu beachten, dass das Engagement, das Wissen und die Flexibilität der Mitarbeiter die Basis für die Verwirklichung der Visionen und der Werte bilden. Unternehmen müssen ihre Mitarbeiterinnen und Mitarbeiter als das wichtigste Kapital für eine erfolgreiche Zukunft ansehen und daher auf kontinuierliches Lernen setzen. In Zeiten permanenten Wandels ist Lernen von zentraler Bedeutung, um sowohl die Leistungs- und Wettbewerbsfähigkeit von Unternehmen als auch die Entwicklungs- und Beschäftigungsfähigkeit der Mitarbeiter langfristig zu sichern.

Aus der Vision heraus sind entsprechende **Leitbilder** zu entwickeln. Leitbilder von Unternehmen und praktisches Handeln in den Unternehmen sind – natürlich – unterschiedlich geprägt von Branchen und Betriebsgrößen. Liegt unabhängig davon eine klare Orientierung an einem zukunftsorientierten Leitbild vor, dann bedeutet eine solche Veränderung natürlich auch eine Auswirkung auf nahezu alle beruflichen Tätigkeiten in diesem Unternehmen bzw. in dieser Branche.

**Beachten Sie:**

Aufgrund der vielfältigen Herausforderungen ist für nahezu alle Branchen ein umfassendes und aktuelles Bereitstellen von Informationen wichtig, beispielsweise über Marktentwicklungen, Wettbewerber, Kunden (bisherige und künftige Zielgruppen), Kaufverhalten sowie Gesetze, Normen und Technologien. Nur so können auch der Unternehmensführung nachgeordnete Bereiche optimal handeln.

Aus der Vision und dem Leitbild heraus müssen konkrete **Unternehmensziele (Systemziele)** abgeleitet und permanent fortgeschrieben werden. Um Ziele zu konkretisieren, wird heute sehr häufig der **Balanced Scorecard-Ansatz** verfolgt. Es handelt sich hierbei um einen methodischen Ansatz zur strategischen Steuerung von Organisationen. Als konkretes Ergebnis wird darüber hinaus der Vorschlag eines umfassenden Kennzahlenkanons unterbreitet.

Dabei werden finanzielle Kennzahlen natürlich auch als notwendig angesehen. Allein sind sie jedoch nicht geeignet, um zukünftige Werte durch Investitionen in Kunden, Zulieferer, Mitarbeiter, Prozesse, Technologien und Innovationen zu schaffen. Die Balanced Scorecard (kurz BSC) ergänzt deshalb finanzielle Kennzahlen vergangener Leistungen um die treibenden Faktoren zukünftiger Leistungen. Die **Ziele und Kennzahlen**, die aus der Vision und Strategie des Unternehmens abgeleitet werden, fokussieren die Unternehmensleistung aus vier Perspektiven:

- aus der finanziellen Perspektive,
- aus der Kundenperspektive,
- aus der Perspektive der internen Geschäftsprozesse sowie
- aus der Personal- und Innovationsperspektive (Lernen und Entwicklung).

Diese vier Perspektiven schaffen den Rahmen für die Balanced Scorecard. In Abbildung 1.1 werden sie illustriert.

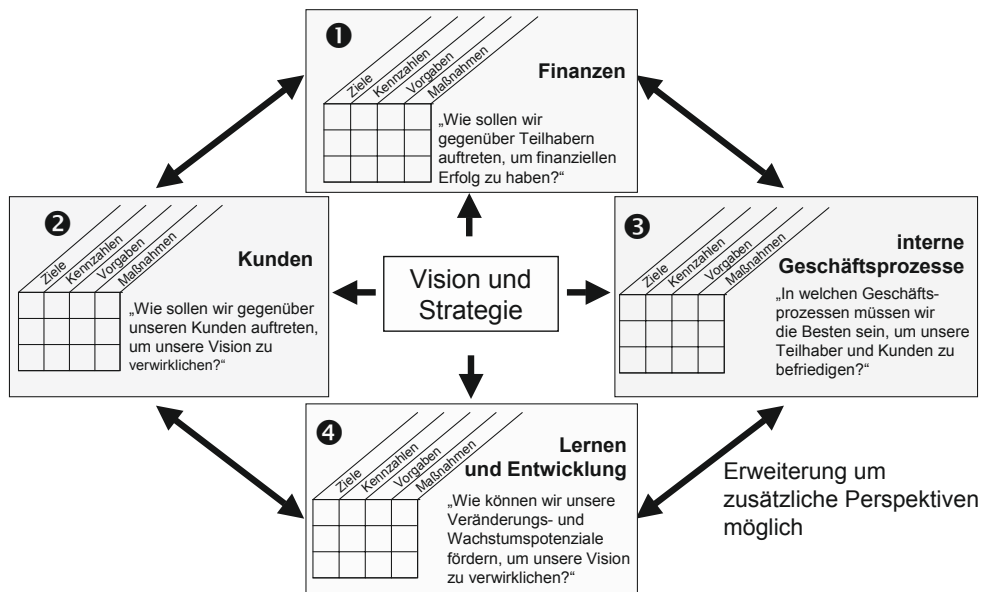


ABBILDUNG 1.1 Die Perspektiven der Balanced Scorecard (nach [KaNo01])

Grundsätzlich bietet sich das Herunterbrechen der Unternehmens-BSC auf den IT-Bereich an; im Ergebnis wird heute der Aufbau einer IT-BSC empfohlen. Der Vorteil liegt darin, dass das IT-Management nun messen kann, inwieweit der IT-Bereich für gegenwärtige und zukünftige Kunden wertschöpfend arbeitet und inwieweit interne Möglichkeiten und Investitionen in Personal, Systeme und Abläufe aufrechterhalten werden müssen, um in Zukunft die IT-Leistungen noch zu steigern.

Die Balanced Scorecard erfasst die kritischen Wertschöpfungsaktivitäten, die durch ausgebildete, motivierte Mitarbeiter geschaffen werden. Während sie durch die finanzielle Perspektive das Interesse an kurzfristig orientierter Leistung aufrechterhält, offenbart sie die Werttreiber für wichtige, langfristige und wettbewerbsfähige Leistungen.

Die Ziele und Kennzahlen der Balanced Scorecard sind mehr als eine Ad-hoc-Sammlung von finanziellen und nicht finanziellen Leistungsmessern. Sie werden aus einem Top-down-Prozess hergeleitet, dessen Mission und Strategie der Geschäftseinheit der treibende Faktor ist. Die Balanced Scorecard sollte die Mission und Strategie einer Geschäftseinheit in materielle Ziele und Kennzahlen übersetzen können. Wie sich aus Vision und Strategien die Perspektiven und Kennzahlen ergeben, illustriert Abbildung 1.2 (nächste Seite).

Die Kennzahlen sind eine Balance zwischen den Messgrößen der Ergebnisse vergangener Tätigkeiten und den Kennzahlen, die zu künftigen Leistungen antreiben. Und die Scorecard ist ausgewogen in Bezug auf objektive, leicht zu quantifizierende Ergebniskennzahlen und subjektive, urteilsabhängige Leistungstreiber der Ergebniskennzahlen.

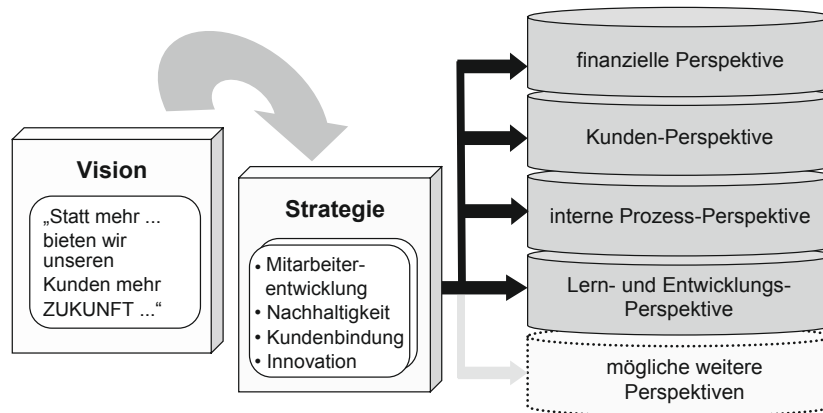


ABBILDUNG 1.2 Die Ableitung der Balanced Scorecard (als Prozess); vgl. [KaNo01]



Die Balanced Scorecard ist mehr als ein taktisches oder operatives Messsystem. Innovative Unternehmen verwenden sie als ein strategisches Managementsystem, um ihre Strategie langfristig verfolgen zu können.

1.1.2 Vom Denken in Funktionen zum Denken in Prozessen

Unternehmensorganisationen waren klassischerweise durch eine Aufgliederung in funktionale Einheiten (Abteilungen) gekennzeichnet. In jüngster Zeit hat sich das „Denken in Funktionen“ zu einem „Denken und Handeln in Prozessen“ gewandelt.

Blickt man auf ein Unternehmen, so gibt es eine Vielzahl möglicher Kriterien, Unternehmensprozesse zu gliedern. Allgemein ist die Unterscheidung in Kern-, Management- und Unterstützungsprozesse akzeptiert. Dabei wird von einem Geschäftsprozess gesprochen, wenn Zwecke Dritter (Kunden, Patienten, Bürger etc.) erfüllt werden sollen und diese Dritten daher zu Prozess-„Beteiligten“ gemacht werden. Wesentliche **Merkmale eines Geschäftsprozesses** sind:

- **Kundenorientierung:** Ein Geschäftsprozess wird durch konkrete Anforderungen der Kunden bestimmt und weiterentwickelt.
- **Wertschöpfungseffekt:** Ein Geschäftsprozess ruft sowohl beim Kunden als auch bei der leistungserstellenden Organisation einen Nutzen hervor.
- **Bereichsübergreifender Verlauf:** Ein Geschäftsprozess ist typischerweise nicht auf eine Organisationseinheit beschränkt.

Bei der Einführung eines professionellen Prozessmanagements empfiehlt sich eine Orientierung an drei grundlegenden Phasen, wie sie nachfolgend skizziert werden:

- **Phase 1:** In der Einführungsphase wird die Idee des Prozessmanagements den Betroffenen nahegebracht und ein Prozessverantwortlicher benannt.
- **Phase 2:** Durch kontinuierliche Verbesserung soll ein optimales Prozessergebnis erreicht werden.

- **Phase 3:** Der Prozess soll so beherrscht werden, dass er auch unter sich ändernden Bedingungen die an ihn gestellten Anforderungen erfüllt.

Um nun die Geschäftsprozesse zu beherrschen, ist heute unbestritten, dass Informationen nicht nur zur erfolgreichen Aufgabenbewältigung vieler Mitarbeiter erforderlich sind, sondern dass sie auch einen wesentlichen Beitrag zum Unternehmenserfolg leisten. Als Beispiele für die Vielzahl neuer Herausforderungen, denen sich Unternehmen unter diesem Aspekt heute gegenübersehen, seien erwähnt:

- Das Marktgeschehen ist durch eine immer stärkere Internationalisierung gekennzeichnet, auf die sich viele Unternehmen vorbereiten müssen, wollen sie am Markt langfristig bestehen.
- Die Mitkonkurrenten weisen eine zunehmende Flexibilität auf. Wettbewerbsvorteile sind daher heute nur noch temporär realisierbar.
- Die Wissensmenge nimmt rasant zu. Das macht die ständig zunehmende und komplexer werdende Informationsflut deutlich: Alle 2,5 Jahre haben wir eine Verdoppelung des wirtschaftlich und technisch relevanten Wissens zu verzeichnen. Zur Erledigung ihrer Arbeiten müssen sich Fach- und Führungskräfte immer wieder neue und immer mehr Informationen beschaffen und sie verarbeiten.

1.1.3 Strategische versus operative Managementfunktionen

Zur Sicherung des langfristigen Unternehmenserfolgs wird vom Management in jedem Fall ein Denken in strategischen Dimensionen erwartet. Gleichzeitig sind für die Erledigung des Tagesgeschäftes aber auch kurzfristige operative Entscheidungen notwendig. Aufgrund der unterschiedlichen Reichweite und Bedeutung von Managemententscheidungen im Unternehmen hat sich in der Praxis deshalb als ein Hauptkriterium zur **Klassifizierung der Managementaufgaben** die Unterscheidung in strategisches und operatives Management durchgesetzt.

Das **strategische Management** dient dem Erkennen und Beachten von zukünftigen Chancen und Risiken. Es verfolgt das Ziel, eine möglichst gute Adaption des Unternehmens in seine Umwelt zu erreichen.

Im strategischen Management geht es vor allem um die Frage: **Machen wir die richtigen Dinge?** Letztlich geht es um die Entwicklung zukünftiger und die optimale Nutzung vorhandener Erfolgspotenziale. Wichtig ist dabei die Beeinflussung der Effektivität des unternehmerischen Handelns. Jedes Unternehmen hat eine spezifische Ausprägung und ist in eine konkrete wirtschaftliche, technische und soziale Umwelt eingebunden. Daraus leiten sich die Möglichkeiten seiner Entwicklung ab. Durch die Definition der strategischen Ziele entscheidet sich das Unternehmen bewusst, einen Teil dieser Möglichkeiten wahrzunehmen.

Operatives Management zielt im Gegensatz zum strategischen Management primär auf die Beeinflussung der Effizienz des unternehmerischen Handelns. Im Mittelpunkt steht die Frage: **Machen wir die Dinge richtig?** Die Zielgrößen des operativen Managements sind der Erfolg bzw. der Gewinn des Unternehmens, seine Liquidität sowie die Rentabilität der Geschäftsprozesse.

Der Schwerpunkt des operativen Managements liegt in der Gewinnsteuerung. Das operative Management richtet die Geschäftsprozesse des Unternehmens auf eine kurz- bis mittelfristige

Gewinnerzielung bei gleichzeitigem Erhalt der Liquidität aus. Bei gegebener Liquidität steht die Gewinnmaximierung im Vordergrund. Die zeitliche Dimension des operativen Managements liegt im kurz- bis mittelfristigen Bereich.

**Zusammenfassend lässt sich festhalten:**

1. Strategisches und operatives Management haben eine unterschiedliche zeitliche Orientierung (Zukunftsorientierung versus aktueller Handlungsbedarf)
2. Die Reichweite und Auswirkung von Entscheidungen ist unterschiedlich im Unternehmen (Gesamtauswirkung versus Einfluss auf Teilbereiche).
3. Das strategische Management ist durch mehr Freiheitsgrade gekennzeichnet als das operative Management.

■ 1.2 Die IT im Unternehmensumfeld – Entwicklungstrends und Konsequenzen

Die Bedeutung der IT für das Unternehmen hat in den letzten Jahren einen Wandel erfahren. Während IT in der Anfangszeit primär als Rationalisierungsinstrument gesehen wurde, wird sie zunehmend auch als wichtiger Wettbewerbsfaktor betrachtet. Ergänzend wird heute der Wertbeitrag der IT zum Unternehmenserfolg diskutiert (Stichwort „IT-Governance“). Mit der veränderten Rolle der IT im Unternehmen ergeben sich natürlich entsprechende Veränderungen hinsichtlich der Anforderungen an ein modernes IT-Management. Deshalb sollen nachfolgend diese Änderungen genauer betrachtet werden.

1.2.1 Informations- und Kommunikationstechnologien im Wandel der Zeit

Der Fokus der IT ist im Verlauf der Nutzung der Informationstechnologien durch folgende Entwicklungsströme gekennzeichnet:

- Ursprünglich (bis in die 1970er Jahre) orientierte man sich sehr stark an der Rationalisierung der Informationsverarbeitung im Unternehmen. Letztlich wurde damit deutlich, dass durch den Einsatz von IT die Leistungserbringung (= Kernprozesse des Unternehmens) sowie die Verwaltungsarbeit (= Unterstützungsprozesse) erheblich wirtschaftlicher erbracht werden können.
- In den 1980er Jahren setzte sich die Erkenntnis durch, dass die IT das Geschäft unterstützt (z. B. durch Differenzierung). Produkt- und Dienstleistungsqualität konnten mit IT-Unterstützung verbessert und damit höhere wirtschaftliche Erfolge realisiert werden.
- Seit den 1990er Jahren wird die IT primär als Enabler eingeschätzt. Bestimmte Geschäftsprozesse lassen sich mit den neuen Möglichkeiten der Informations- und Kommunikationstechnologie überhaupt erst realisieren.

- Seit der Verfügbarkeit des Internet setzt sich für viele Bereiche ergänzend die Erkenntnis durch, dass die IT Teil des Geschäfts ist. So können etwa durch Online-Geschäfte ganz neue Zielgruppen erschlossen und Kundengruppen intensiver gebunden werden.
- Heute geht die Aufgabenorientierung stärker in Richtung Produktivitäts- und Qualitätssteigerung. Gleichzeitig rückt die Unterstützung und Optimierung von Geschäftsprozessen, die auch übergreifender Natur sind, in den Mittelpunkt. Im Zentrum der IT-Investitionen stehen innerbetriebliche Anwendungen, seien es betriebswirtschaftliche Applikationen (wie Auftragsabwicklung, Controlling, Materialwirtschaft, PPS etc.) oder technische Applikationen wie CAD, CAM, NC und Simulation. Außerdem sind die Investitionen stärker zwischenbetrieblich orientiert: Beispiele sind IT-Infrastrukturen zur Kommunikation mit Kunden (wie CRM, E-Business, E-Learning, E-Government, Collaboration Tools, ...) sowie zur Kommunikation mit Lieferanten (wie SCM, E-Procurement, ...).

Eine Orientierung darüber, wie Investitionen in neue Informations- und Kommunikationstechnologien einzuschätzen sind und welche Zielrichtungen dabei im Mittelpunkt stehen, gibt Abbildung 1.3.



ABBILDUNG 1.3

Der IT-Fokus im Wandel
(insbesondere aus Sicht
der Geschäftsprozesse)

Die Unternehmen müssen sich diesen neuen Herausforderungen der IT stellen, wenn sie auch zukünftig im Wettbewerb bestehen wollen. Das Spannungsfeld verdeutlicht Abbildung 1.4.

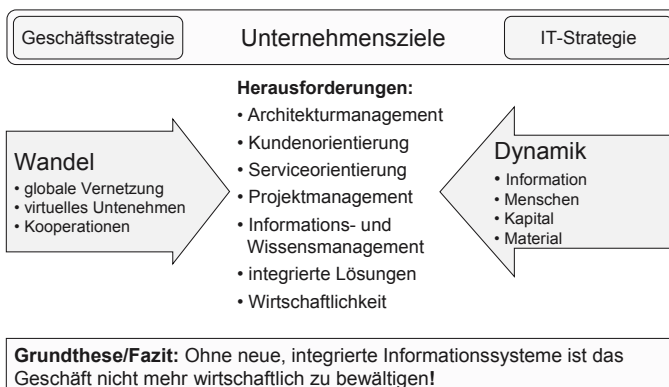


ABBILDUNG 1.4

IT-Herausforderungen
im Spannungsfeld von
Geschäftsstrategie und
IT-Strategie

1.2.2 Der Wandel der IT zum kundenorientierten Dienstleister

Die Unternehmen, die auf die Zeichen der Zeit reagieren und sich auf neue Situationen und neue Technologien „offensiv“ einstellen, werden heute von Beratern, Organisatoren, Wissenschaftlern und sonstigen Fachleuten mit guten Ratschlägen nur so überhäuft. Ein besonders beeindruckendes Beispiel ist die rasant verlaufende Entwicklung im Internet-Umfeld. Kaum eine Technologieveränderung hat in den letzten Jahren so weitreichende Auswirkungen innerhalb der Volkswirtschaft wie auch in der Gesellschaft insgesamt nach sich gezogen.

Der Trend zur Informations- und Wissensgesellschaft ist unaufhaltsam. Dies hat zur Folge, dass die Informations- und Kommunikationstechnologie auch weiterhin eine hohe und steigende Bedeutung für Wirtschaft und Verwaltung haben wird. So werden Produktion, Handel und Dienstleistungen immer mehr von der effizienten Nutzung moderner Informations- und Kommunikationstechnologien abhängig. Entsprechende Geschäftsprozesse in den genannten Bereichen lassen sich ohne Unterstützung durch die IT gar nicht mehr bzw. bei weitem nicht so effizient abwickeln.

Für die Mehrzahl der Unternehmen ist der Einsatz moderner Informationstechnologien (IT) inzwischen eine unabdingbare Grundvoraussetzung ihrer Geschäftstätigkeit. Banken und Versicherungen können zum Beispiel ohne zuverlässige und hochverfügbare IT-Systeme nicht mehr im Wettbewerb bestehen.

Wichtig ist in jedem Fall eine klare Kundenorientierung für das Handeln im IT-Bereich; also eine Sichtweise auf die Fachabteilung als sog. internen Kunden. Damit verbunden ist die Notwendigkeit einer umfassenden Serviceorientierung (etwa auch durch Bereitstellung von IT-Produkt- und Leistungskatalogen, die Vereinbarung von Service Level Agreements sowie die Einrichtung eines leistungsfähigen Service-Desks).

Der IT-Bereich muss sich als Dienstleister organisieren, eine wichtige Aufgabe des IT-Managements besteht in der Koordination der IT-Leistungsprozesse. IT-Leistungsprozesse erzeugen für einen Kunden die gewünschten IT-Produkte. Der Kunde möchte durch das Einsetzen der IT in seinen Leistungsprozessen bestimmte Effekte erzielen. Insofern tritt neben die nach innen gerichteten Managementaufgaben auch ein Stakeholder-Management nach außen.

In einer erweiterten Sichtweise kann die IT jedoch auch als wesentlicher Enabler von Geschäftsprozessen gesehen werden. Abbildung 1.5 verdeutlicht, inwieweit moderne IT-Technologie als Enabler gesehen werden kann.

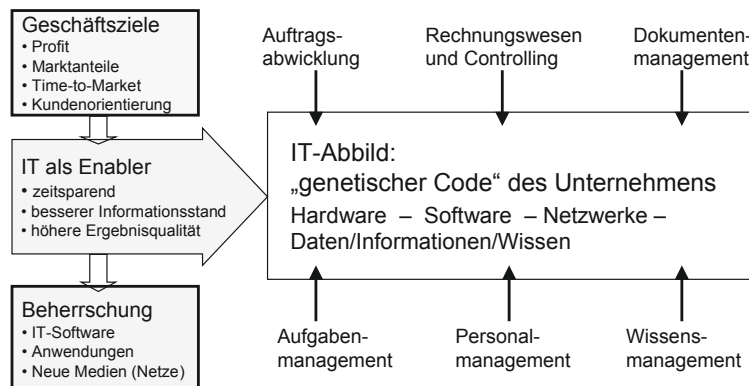


ABBILDUNG 1.5
Informationstechnologien als Enabler



Die Informationstechnologie (IT) leistet einen wesentlichen und unverzichtbaren Beitrag zur Bewältigung der Herausforderungen des Informationszeitalters. Sie stellt die Summe der technischen und organisatorischen Mittel (Hardware, Software, Services) zur Unterstützung der Geschäftsprozesse sowie der verschiedenen informationellen Prozesse (der Beschaffung, Verarbeitung, Speicherung, Übertragung und Bereitstellung von Informationen) dar.

1.2.3 Beitrag der IT zum Unternehmenserfolg

Für die Mehrzahl der Unternehmen ist der Einsatz moderner Informationstechnologien (IT) inzwischen eine unabdingbare Grundvoraussetzung ihrer Geschäftstätigkeit. Banken und Versicherungen können zum Beispiel ohne zuverlässige und hochverfügbare IT-Systeme nicht mehr im Wettbewerb bestehen.

Die Informationstechnologie (IT) leistet einen wesentlichen und unverzichtbaren Beitrag zur Bewältigung der Herausforderungen des Informationszeitalters. Sie stellt die Summe der technischen und organisatorischen Mittel (Hardware, Software, Services) zur Unterstützung der Geschäftsprozesse sowie der verschiedenen informationellen Prozesse (der Beschaffung, Verarbeitung, Speicherung, Übertragung und Bereitstellung von Informationen) dar.

Beachten Sie: Auch in der Literatur wird die IT mittlerweile nicht mehr nur als Kostenfaktor und Dienstleister, sondern zum Beispiel als „Value Center“ oder Werttreiber gesehen, der durch seine Orientierung am langfristigen Erfolg ein Unternehmen auch zu besseren und neuen Leistungen befähigen und sich durch seine Marktorientierung sogar als „Profit Center“ profilieren kann. Im Grunde wird also – in der Theorie wie in der Praxis – die IT zunehmend als eine Art Unternehmen im Unternehmen betrachtet, das Kundenbedürfnisse befriedigen, profitabel im Markt agieren, kostenbewusst arbeiten und zukunftsfähig handeln muss.

Die Möglichkeiten und Chancen der IT, den Erfolg zu beeinflussen, liegen unter anderem in der Kostensenkung. Die positive Beeinflussung der Erlössituation ist sicherlich auch durch eine Steigerung der Erlöse möglich, leichter und prozentual gewichtiger aber durch Kostensenkung erreichbar. Durch eine effiziente betriebliche IT können Bestandskosten und Gemeinkosten nachhaltig gesenkt werden. Wichtig ist es aber auch, den anfallenden Kosten den Wertzuwachs gegenüberzustellen, der durch die Anwendung von Informations- und Kommunikationstechnologien realisiert werden kann.

Möchte man den Beitrag eines Informationssystems zur Wertschöpfung eines Unternehmens genauer untersuchen, gilt es zunächst einmal, bestimmte Wertkategorien abzugrenzen sowie die Nutzenvorteile herauszuarbeiten:

- **Erhöhte Wirtschaftlichkeit:**

Mit dem Einsatz neuer Informations- und Kommunikationstechnologien wird generell ein Beitrag zur erhöhten Wirtschaftlichkeit geleistet. So können etwa kostenintensive Medienbrüche vermieden werden, wenn Workflow-Applikationen über ein einheitliches Technologiesystem realisiert werden. Des Weiteren lassen sich viel Redundanz und hohe Kosten durch Mehrfachspeicherungen vermeiden.

- **Abwicklung von Arbeits- und Geschäftsprozessen mit hoher Wertschöpfung:**

Zahlreiche Arbeits- und Geschäftsprozesse lassen sich mit IT-Unterstützung bei überschaubarem Input und einem qualitativ hohem Output realisieren, wobei gleichzeitig der Aufwand insgesamt minimiert werden kann. Kaum ein Unternehmen kann seine Geschäftsprozesse noch reibungslos und performant abwickeln, wenn die Unterstützung der IT nicht oder nur eingeschränkt gegeben ist.

- **Bessere Informationsversorgung führt zu Wettbewerbsvorteilen:**

Ein entscheidender Vorteil, der immer wieder herausgestellt wird, ist die bessere Informationsversorgung. Da die mit einem IT-System abrufbaren Zahlen wesentlich genauer und aktueller sind, erfüllen viele Informationssysteme die Funktion eines Frühwarnsystems. Gerade im Hinblick auf die zunehmende internationale Verflechtung der Wirtschaft ist für Fach- und Führungskräfte auch ein schneller Zugriff auf unternehmungsexterne Informationsquellen (z. B. Marktinformationen) von besonderer Bedeutung.

- **Unterstützung der Entscheidungsfindung:**

Fach- und Führungskräfte verwenden einen großen Teil ihrer Zeit für strategische und dispositive Entscheidungen. IT-Anwendungen bieten die Möglichkeit, übersichtliche und aussagefähige Entscheidungsunterlagen direkt zu erzeugen. Bei professioneller Einrichtung wird mehr als nur ein traditionelles Berichtswesen bereitgestellt. Die für Entscheidungen verfügbare Zeitspanne wird immer kürzer. Grundsätzlich gilt: Eine IT-unterstützte Entscheidungsvorbereitung ermöglicht gegenüber der konventionellen (bei gleichem Entscheidungszeitpunkt) einen höheren Sicherheitsgrad oder (bei gleichem Sicherheitsgrad) eine frühzeitigere Entscheidung.

- **Schnellere Reaktionsfähigkeit der Unternehmensführung:**

Ein entscheidender Wettbewerbsvorteil, der durch moderne IT-Anwendungen erzielt werden kann, liegt in dem für alle Führungsebenen transparenten und umfassenden Informationsvorsprung. Die Unternehmensführung kann nun schneller reagieren, da Detailinformationen bei Bedarf unmittelbar zur Verfügung stehen. Nur durch die Möglichkeit einer elektronischen Verwaltung von Daten und Dokumenten ist ein schnelles Auffinden von relevanten Informationen gewährleistet.

- **Zielgerichtete Planungsmöglichkeiten als strategische Unterstützung:**

Eine wichtige Führungsfunktion ist generell das Setzen von Zielen und das Ausarbeiten von Planungen. Dies kann die globale Unternehmensplanung sein; es können aber auch Teilplanungen sein wie beispielsweise die Finanzplanung sowie Produkt- und Absatzplanungen. Bei Nutzung einer IT-Lösung können nun auf einfache Weise Prognosen, Simulationen oder Szenarien entworfen und in allen erdenklichen Varianten durchgerechnet werden. So lassen sich z. B. schnell und problemlos individuelle Analysen aus vorhandenen Daten vornehmen, Kennzahlen ableiten und bewerten sowie Prognosemodelle aufstellen. Die Multidimensionalität der Märkte, Unternehmen und Unternehmensaufgaben kann man deshalb nur mit modernen, computergestützten Methoden in den Griff bekommen.



Gerade die nächsten Jahre werden für zahlreiche Unternehmen die Notwendigkeit bringen, sich stärker als bisher mit der Ressource Information auseinander zu setzen, was auch eine aktive Mitwirkung von Fach- und Führungskräften einschließt. Informationssysteme werden zur strategischen Waffe erfolgreicher Unternehmensführung, das Management wird zum Gestalter und Nutzer derartiger Systeme. Viele IT-Verantwortliche haben mittlerweile die Herausforderungen erkannt und sehen zunehmend die Notwendigkeit, dass sie die IT anhand von Leistungskennzahlen steuern müssen. Dazu zählen etwa ein optimiertes Managen und Steuern der IT-Services und eine verbesserte Kundenbindung, um so auch den IT-Beitrag zur Wertschöpfung des Unternehmens ermitteln und kommunizieren zu können.

1.2.4 Die Integration der IT in die Unternehmensstrategie

Für einen nachhaltigen Erfolg der IT wird es heute als wesentlich angesehen, dass Entscheidungen und IT-Lösungen in enger Kooperation mit den Fachbereichen (den Kunden) im Unternehmen abgestimmt werden. Dabei sollte gleichzeitig eine Einbettung in strategische Überlegungen erfolgen.

Die Erarbeitung einer IT-Strategie kann als eine wesentliche Voraussetzung angesehen werden, um optimale IT-Services unter Beachtung von wirtschaftlichen Aspekten bereitzustellen. Hauptzielsetzungen sind daher die Sicherung der Betriebs- und Lieferfähigkeit der eigenen Organisation sowie der Verbesserung der Leistungsfähigkeit der IT, was sich auch auf die Wettbewerbsfähigkeit des Unternehmens positiv auswirkt.

Der erste Schritt ist immer eine **Analyse der Unternehmensstrategie** und der sich daraus ergebenden Auswirkungen auf die IT-Strategie. Die wesentlichen Treiber für die IT-Strategie werden festgehalten: abgeleitet aus der IT-Position des Unternehmens sowie der strategischen Rolle der IT in der Branche. Danach werden die daraus abgeleiteten Informationsbedürfnisse aufgezeigt. Zweck der **Erfolgsfaktorenanalyse** ist die Beschaffung von Information für die strategische IT-Planung, insbesondere die strategische Maßnahmenplanung.

Die permanenten Leistungssteigerungen bei den Informationstechnologien erlauben es den Unternehmen, immer intensiver alle Phasen ihrer Wertschöpfungsprozesse zu unterstützen. In den vergangenen Jahren entstandene funktionsorientierte Insellösungen werden heute von integrativen, **ganzheitlichen Systemlösungen** abgelöst, die dem neuen Ansatz einer prozessorientierten Unternehmensorganisation besser gerecht werden. Dennoch stellen sich zahlreiche Fragen, für die das Management Unterstützung benötigt (vgl. [Ge02]):

- Inwiefern werden die Unternehmensziele durch die eingesetzten IT-Produkte optimal unterstützt, und welchen Wertbeitrag leistet die IT für das Unternehmen?
- Wann sollte welches IT-Produkt zum Einsatz kommen?
- Welches der zur Auswahl stehenden IT-Produkte (Hardware, Applikationen, Netze, Speichersysteme u. a.) weist jeweils das beste Kosten-Nutzen-Verhältnis auf?
- Ist die IT „zur Genüge“ strategisch aufgestellt, oder beschränkt sie sich zu sehr auf operative Aktivitäten?
- Wann ist der richtige Zeitpunkt, um auf eine neue innovative Technologie zu migrieren?

- Wie sehen die grundlegenden IT-Architekturen aus, die eingeführt und fortentwickelt werden sollen?
- Welche IT-Prozesse sind identifiziert, und wie lassen sich diese optimieren?
- Wann werden eher zentrale, wann eher dezentrale IT-Systeme eingesetzt?
- Welches Vorgehen ist in den anstehenden IT-Projekten (etwa zur Realisierung eines neuen Anwendungssystems) zweckmäßig und zielführend?
- Wie kann die IT übergreifend geplant, überwacht und nachhaltig gesteuert werden?
- Welche rechtlichen Besonderheiten sind bei einer IT-Einführung bzw. bei einer vorhandenen IT-Lösung zu beachten?
- Welches Personal wird für die Realisierung von IT-Aufgaben und IT-Prozessen benötigt? Über welche Skills sollte das IT-Personal verfügen?

Dies sind nur einige Fragen, mit denen sich IT-Manager heute unter Beachtung strategischer Aspekte konfrontiert sehen. IT-Manager tragen die Verantwortung unter anderem für die Auswahl, die Einführung und den störungsfreien Betrieb geeigneter IT-Systeme. Die eingesetzten Technologien und Produkte sollen die Geschäftsprozesse des Unternehmens optimal unterstützen. Dabei sind die Interessen des einzelnen Anwenders genauso zu berücksichtigen wie die strategischen Ziele des Unternehmens insgesamt. IT-Manager müssen die Balance zwischen den begrenzten Ressourcen des Unternehmens und den vielfältigen Möglichkeiten, die die modernen Informationstechnologien heute eröffnen, täglich neu finden. Gleichzeitig müssen sie in der Lage sein, im Team aus der Unternehmensstrategie auch geeignete IT-Strategien für ihr Unternehmen abzuleiten.

Der strategische Einsatz von Informationssystemen wird durch innovative Anwendungen realisiert, die zur Erlangung von Wettbewerbsvorteilen beitragen. Ist das Informationssystem in entsprechender Weise auf die Unternehmensstrategie ausgerichtet, so kann die Technologie mithelfen,

- die Branchenstrukturen zu verändern;
- Eintrittsbarrieren gegenüber neuen Mitbewerbern aufzubauen;
- neue Märkte zu schaffen;
- die kritischen Erfolgsfaktoren des Unternehmens zu fördern.

Es gibt mehrere Lösungswege, die das IT-Management gezielt angehen sollte:

- Unter dem Motto „Betroffene zu Beteiligten machen“ ist die Erstellung und Umsetzung der IT-Strategie nicht nur Aufgabe der Leitung des IT-Bereichs, vielmehr müssen alle Führungskräfte des gesamten Unternehmens in den Prozess eingebunden werden.
- Die gemeinsame Erarbeitung einer IT-Strategie ist Chance und Verpflichtung zu einem Stück Organisationsentwicklung im Sinne eines umfassenden Gestaltungs- und Lernprozesses auf der Metaebene.
- Unterschiedliche Sichten und Erwartungen der Beteiligten prallen auf diese Weise frühzeitig aufeinander, und die Erkenntnisse aus einschlägigen Diskussionen – vielleicht auch Konflikten – können entsprechend genutzt werden.
- Gerade für den IT-Bereich als Dienstleister ist die Kooperation mit den Kunden sowie zur Unternehmensführung von besonderer Bedeutung. Wichtig ist ein optimales Beziehungsmanagement zu allen Kooperationspartnern.

Erfahrungen der Praxis zeigen: IT-Verantwortliche, IT-Projektleiter oder IT-Service-Manager sind zunehmend gefordert, ein professionelles Anforderungsmanagement zu etablieren. Nur so können IT-Lösungen mit hoher Akzeptanz implementiert, eine hohe Qualität der IT-Services gewährleistet und gleichzeitig die IT-Kosten „im Griff“ gehalten werden. Gleichzeitig sind aber auch die Fachbereiche stärker gefordert, die Potenziale von IT-Lösungen kompetent zu eruieren und in adäquate Anforderungen umzusetzen.

■ 1.3 IT-Management – Rollenverständnis und Kernaufgaben

1.3.1 Positionierung des IT-Managements im Unternehmen

Das Top-Management Ihrer Organisation schätzt die Leistungen der IT, die Benutzer Ihrer Anwendungen sind motiviert und hochzufrieden mit dem IT-Bereich, die Kooperation funktioniert bestens. Stellen Sie sich vor, diese „heile Welt“ wäre für Sie möglich! Stellen Sie sich vor, dass das General Management sowie Ihre Anwender Ihre Leistungen, die bereitgestellten IT-Produkte sowie die Ergebnisse Ihrer IT-Projekte tatsächlich in hohem Maße anerkennen und honorieren.

Es liegt auf der Hand, dass die zunehmende Bedeutung der IT für die Unternehmenspraxis und den Unternehmenserfolg es erforderlich macht, dass sich auch das General Management eines Unternehmens mit den Kernfragen der Auswahl und Nutzung der IT-Systeme im Unternehmen befassen muss. Dies bedingt gleichzeitig verschiedene **Aufgaben für die Entscheidungsträger** im Unternehmen. So ist es unabdingbar, dass das General Management

- über die Rolle der IT innerhalb des Unternehmens informiert sein muss,
- Zuständigkeiten (etwa auch bezüglich der Kooperation von IT und Fachbereich) festsetzt,
- die Performance der IT misst und ggf. steuernde Maßnahmen überlegt und ergreift,
- IT-Risiken managt und
- Vertrauen für die IT und ihre Services in der Organisation schafft.

1.3.2 Partner für das IT-Management und die Rolle der IT

Verstand man in den letzten Jahrzehnten unter der IT-Abteilung häufig einen Teil des Unternehmens, der „lediglich“ technische Komponenten und eine Infrastruktur zur Verfügung stellt, so wird die IT zunehmend als aktiver Partner für diverse andere Bestandteile eines Unternehmens gesehen, etwa:

- als Unterstützung für Fachabteilungen
- als zentraler Anlaufpunkt für Mitarbeiter und Kunden bei technische Fragen und Problemen
- als Geschäftspartner für externe und interne Lieferanten, Outsourcing-Firmen oder für externe Consultants

Aus diesem neuen Rollenverständnis, als Partner für unterschiedlichste Stakeholder, ergibt sich, dass an die IT verschiedenste neue Anforderungen gestellt werden. Neben den „klassischen“ Anforderungen an die IT wie Benutzerfreundlichkeit, Performance, Sicherheit, Funktionalität, Support werden Aspekte wie

- Know-how-Transfer zwischen Abteilungen,
- wirtschaftliche Bereitstellung von IT-Produkten (Hardware, Applikationen),
- qualitativ hochwertige IT-Services oder
- konsequente Unterstützung der Geschäftsprozesse

immer wichtiger. Wie einleitend dargestellt, spielt IT heute in allen Bereichen eines Unternehmens eine zunehmend wichtigere Rolle. Untersucht man diese Rolle weiter, lassen sich vier verschiedene Partner herausarbeiten, jeweils gekennzeichnet durch eine spezifische Sicht auf die IT und, daraus abgeleitet, unterschiedlichen Ansprüchen an die IT:

- Unternehmensführung
- Anwender
- Geschäftspartner (Lieferanten, externe Consultants)

Im vorherigen Abschnitt wurde bereits darauf hingewiesen, dass die **Unternehmensführung** sich intensiv mit der strategischen Positionierung der IT im Unternehmen beschäftigen muss. Um langfristig die Existenz des Unternehmens zu sichern, verfolgt die Unternehmensführung vielfach das Ziel, alle Ressourcen des Unternehmens und die damit mögliche Leistungsfähigkeit der IT optimal auf die Erreichung der strategischen Unternehmensziele auszurichten. Für die Unternehmensführung stehen langfristige Aspekte des Einsatzes und der Bereitstellung von Informationstechnologien im Vordergrund. Sie trägt die Gesamtverantwortung für die Effektivität und Effizienz der IT im Unternehmen. Sie verfolgt eigene strategische Interessen mit der Etablierung von IT im Unternehmen.

Die **Anwender** in den verschiedenen Geschäftsbereichen nutzen die IT in unterschiedlicher Ausprägung zur Erledigung ihrer Aufgaben. Sie wünschen sich eine funktionstüchtige, preisgünstige und termingerechte IT, die ihre Aufgaben effektiv und effizient unterstützt. Entsprechend ihrem jeweiligen Aufgabenumfeld stellen sie vielfältige Anforderungen hinsichtlich Funktionalität, Benutzerfreundlichkeit, Performance, Verfügbarkeit, Support etc.



Beachten Sie:

IT-Anforderungen zu spezifizieren und zu managen, ist eine Herausforderung, deren Optimierung sich die IT-Abteilung einer jeden Organisation stellen muss. Erst eine Optimierung ermöglicht der IT zufriedene (interne) Kunden und die Erbringung qualitativ hochwertiger Produkte und leistungsfähiger IT-Services.

Die mit dieser gewünschten IT-Unterstützung verbundenen IT-Systeme müssen konzipiert, realisiert, in Betrieb genommen und betrieben werden. Je nachdem, wie das Unternehmen aufgestellt ist, kann dies durch einen unternehmensinternen IT-Bereich oder externe IT-Dienstleister erfolgen. Der **IT-Lieferant** verfolgt das Ziel, seine Leistungsprozesse effektiv und effizient zu gestalten. Dabei bewegt er sich im Spannungsfeld zwischen langfristiger und kurzfristiger Erfolgsorientierung. Langfristiges, zukunftsorientiertes Denken führt nicht immer zu schnellen, preisgünstigen Lösungen. Kurzfristig ausgerichtete Lösungen bringen

vorübergehend den einen schnellen Erfolgseffekt, rächen sich aber oft in der späteren Betriebs- und Wartungsphase.

Jede dieser Gruppen verfolgt ihre **eigenen Ziele**. Interessenskonflikte können hier leicht entstehen, wie die folgenden Beispiele zur **Sichtweise der Anwender** verdeutlichen (vgl. auch [Ge02]).

Der **Anwender** möchte ein funktionierendes, sicheres und kostengünstiges System. Ständige Neuheiten stören ihn eher. IT-Entwickler wünschen sich ein fortschrittliches und technologisch anspruchsvolles System. Modernste Technologien sind ihnen wichtig. Kosten treten für sie oft in den Hintergrund. Die Bereitstellung von 100%-Leistung bringt jedoch keinen Vorteil, wenn der Anwender nur eine 30%-Leistung bestellt, also keine „Cartier-Lösung“ will, wenn die „Swatch-Lösung“ ausreicht.

Auf der anderen Seite ist dem Anwender die Art und Weise, wie die IT-Unterstützung realisiert wird, völlig gleich. Er stellt seine Anforderungen und erwartet eine qualitäts-, termin- und kostengerechte Umsetzung. Seine Wünsche können mitunter hohe Aufwände bei der Bereitstellung, z. B. in der Programmierung oder im Service, hervorrufen, ohne dass ihm dies bewusst ist. Aus Sicht des Unternehmens soll die Bereitstellung möglichst wirtschaftlich erfolgen. Hier muss der Anwender mitunter gebremst werden.

In vielen Fällen erweist es sich auch als sinnvoll, die Wünsche der Anwender zu bündeln, sodass nur ein Anwendungssystem entwickelt, implementiert und gewartet werden muss. Es ist zum Beispiel ausreichend, im Unternehmen ein Bestellsystem zur Verfügung zu stellen, auch wenn mehrere Geschäftsprozesse dieses benötigen und zum Teil unterschiedliche Anforderungen an den Funktionsumfang stellen. Das Ausbalancieren dieser verschiedenen Zielvorstellungen gehört zu den täglichen Aufgaben des IT-Managers.

1.3.3 Strategisches und operatives IT-Management

Es wurde bereits dargelegt, dass die gegenwärtige Entwicklung der IT durch eine hohe Komplexität und immer kürzer werdende Innovationszyklen gekennzeichnet ist. Die zunehmende Dynamik der Umweltveränderungen fordert von Unternehmen ein immer früheres Erkennen von Chancen und Risiken. Andererseits sollten sich die IT-Lösungen in den Unternehmen jedoch auch durch Stabilität und Kontinuität auszeichnen. Dies zeigt, dass neben dem operativen Handeln auch strategisches Denken benötigt wird.

Strategisches IT-Management stellt die Synchronisierung der Unternehmensziele mit der Informationssystem-Strategie in den Mittelpunkt. Dazu muss es die Entwicklung der Unternehmensziele kontinuierlich reflektieren und geeignete IT-Ziele und Strategien für die operative Umsetzung in den IT-Leistungsprozessen ableiten. Die Effektivität des IT-Systems und der IT-Leistungsprozesse werden kontinuierlich verbessert. Dabei geht es auch um die Initiierung und Planung von IT-Vorhaben und die Priorisierung dieser Vorhaben, mit dem Ziel der Verbesserung der strategischen Position der Organisation durch die implementierten Informationssysteme.

Das Hauptaugenmerk des **operativen IT-Managements** liegt auf der wirtschaftlichen Nutzung der IT-Ressourcen. Es stellt die wirtschaftliche Durchführung der IT-Leistungsprozesse im Unternehmen sicher. Beim operativen IT-Management geht es letztlich um die effektive Entwicklung von IT-Lösungen, den reibungslosen IT-Betrieb sowie die Weiterentwicklung und

Wartung von Informationssystemen. Ausgehend von Kosten- und Leistungsdaten erfolgt eine Steuerung der Prozesse und Produkte über konkrete Kennzahlen und ein angepasstes Berichtswesen.

„Ein Ausdruck für den Grad der Zielerreichung ist die Wirksamkeit des IT-Systems. Um Aussagen über die **Wirksamkeit der IT** zu erhalten, wird unter anderem untersucht:

- der Einfluss, den die IT auf Produkt- und Servicequalität des Unternehmens hat
- ob IT in den richtigen Bereichen eingesetzt wird
- inwieweit mit dem vorhandenen System die Bedürfnisse der Anwender befriedigt werden (quantitative und qualitative Bewertung)
- die Qualität der IT-Dienstleistungen (Service, Consulting, Training, Wartung)
- die Qualität der IT-Infrastruktur und der IT-Anwendungen.“ [Ge02]

Neben der Wirksamkeit des IT-Systems bestimmt auch seine **Wirtschaftlichkeit** den Grad der Zielerreichung. Diese lässt sich unter anderem anhand der folgenden Aspekte einschätzen:

- Einzelinvestitionen
- Kosten/Nutzen-Verhältnis der IT
- wirtschaftlichere Alternativen zur bisherigen Bereitstellung der IT (Ersatzinvestitionen)



Das IT-Management „sollte immer beiden Aspekten gleichermaßen gerecht werden, um sowohl kurzfristige Erfolge der verschiedenen Geschäftseinheiten als auch den langfristigen Erhalt des Unternehmens zu sichern“. [Ge02]

■ 1.4 Typische Aufgaben und Anforderungen an das IT-Management

Es ist sicher unbestritten, dass die IT einen wesentlichen Beitrag zur Wirtschaftlichkeit in Unternehmen und Verwaltung leistet und sie gleichzeitig zunehmend auch zum Unternehmenserfolg und zur unmittelbaren Wertschöpfung von Unternehmen beiträgt. Um die IT-Potenziale auch erfolgreich auszuschöpfen, sind jedoch eine leistungsfähige organisatorische Positionierung der IT im Unternehmen sowie hochqualifiziertes IT-Personal unverzichtbar.

Neben den oben genannten generellen Veränderungen in Unternehmen und Verwaltung, die Einfluss auf die IT-Leistungen haben, lassen sich auch spezifische **Änderungen im IT-Bereich** feststellen, die zu neuen **Herausforderungen** führen (siehe Tabelle 1.1).

TABELLE 1.1 Herausforderungen für IT-Verantwortliche

Phänomene in der IT-Welt	Herausforderungen für IT-Verantwortliche
Höhere Anforderungen an die IT-Abteilungen durch Fachabteilungen und Unternehmensführung (bei Wunsch nach hoher Effizienz und Effektivität)	IT-Strategieentwicklungen optimieren und Kundenorientierung in der IT forcieren
Historisch gewachsene IT-Landschaften, steigende Komplexität der eingesetzten IT-Technologien	IT-Architekturen zielorientiert planen und managen (IT-Architekturmanagement, Enterprise Architecture Management); betrifft unter anderem die IT-Infrastrukturen/Technologie-Architektur, IT-Applikationen, die damit verbundenen Geschäftsprozesse und IT-Services.
Steigende Benutzerzahlen, die IT-Support benötigen	Unterstützung für die Endbenutzer verbessern (Optimierung der Benutzerverwaltung, automatisierter Support etc.) und IT-Services umfassend managen
Modularisierung der Software und Standards (umfangreiches Angebot an Standardsoftware)	Koordination der Einführung von Software-Applikationen, Notwendigkeit der Integration von Standard-Lösungen forcieren
Sinkende oder gleichbleibende IT-Budgets	IT-Budgetierung und interne Kosten- und Leistungsverrechnung in der IT einführen; Kennzahlensystem aufbauen/nutzen sowie Benchmarking in der IT durchführen
Extrem hohe Fluktuation bei den im IT-Bereich Beschäftigten	Personalmanagement in der IT ausbauen (Mitarbeiterzufriedenheit steigern, Personalentwicklung fördern)
Zunehmende Anzahl kritischer IT-Anwendungen (immer mehr „mission-critical“-Applikationen)	Umfassende IT-Serviceleistungen anbieten und IT-Security-Lösungen entwickeln
Zahlreiche Einflussfaktoren und Vorgaben von Rahmenbedingungen (Gesetze, Verordnungen etc.)	Risikomanagement in der IT und IT-Compliance (Einhaltung von gesetzlichen Regeln und Verordnungen) sicherstellen

Eine effiziente Erfüllung der sich aus den skizzierten Anforderungen ergebenden Aufgaben im IT-Management setzt umfassende Kenntnisse und vielfältige (persönliche und soziale) Handlungskompetenzen in den skizzierten Themenbereichen des IT-Managements voraus. Insbesondere sollte das IT-Management in der Lage sein,

- die IT im Unternehmen erfolgreich zu etablieren und dabei zukunftssträchtige IT-Strategiekonzepte zu entwickeln;
- IT-Architekturen (IT-Infrastrukturen, Applikationen, Daten-Architekturen sowie Geschäftsarchitekturen) nachhaltig zu planen und zielorientiert zu steuern;
- die „richtigen“ IT-Projekte erfolgreich zu initiieren, diese Projekte sorgfältig zu planen und effizient zu kontrollen sowie als Projektleiter erfolgreich zu führen;
- IT-Services zu definieren, IT-Produkte zu beschreiben und ein Service-Level-Management aufzubauen;

- eine leistungsstarke IT-Organisation für eine Unternehmung/Behörde aufzubauen und dabei Methoden und Techniken für die tägliche Arbeit gezielt einzusetzen (z. B. Führungstechniken, Problemlösungs- und Moderationstechniken);
- für die IT ein professionelles Anforderungsmanagement im Unternehmen erfolgreich zu etablieren und dabei zukunftssträchtige IT-Lösungen zu entwickeln;
- Sourcing- und Beschaffungslösungen zu konzipieren und entsprechende Entscheidungsprozesse kompetent zu begleiten;
- ein leistungsstarkes IT-Qualitätsmanagement für eine Unternehmung/Behörde aufzubauen und dabei geeignete Methoden und Techniken für die Qualitätssicherung gezielt einzusetzen;
- IT-Systemmanagement sowie IT-Sicherheitsmanagement systematisch zu realisieren;
- Kosten- und Leistungstransparenz in der IT zu schaffen, ein effizientes IT-Controlling zu realisieren sowie geeignete IT-Kennzahlen zu nutzen;
- Software-Einführungsentscheidungen methodengestützt vorzunehmen und die wesentlichen Konzepte der Software-Entwicklung sowie der Auswahl und Implementierung von Standardsoftware anzuwenden;
- typische Rechtsfragen im IT-Bereich zu analysieren und sachgerecht zu bewerten.

Aus den vorangegangenen Ausführungen wurde deutlich, dass die IT in modernen Unternehmen eine immer wichtigere Rolle spielt. Weiterhin wurde festgestellt, dass die Anforderungen an das IT-Management gestiegen sind und daher vom IT-Management neue Vorgehensweisen verlangt werden. Was bedeutet dies konkret?

- Es ist zu prüfen, welchen Zielen und Aktivitäten (Aufgaben) beim IT-Management besondere Bedeutung zukommt.
- Es ist zu bestimmen und zu konkretisieren, in welchen Rollen das IT-Management agieren sollte.
- Es ist zu erheben, in welchem situativen Umfeld bzw. unter welchen Rahmenbedingungen das IT-Management agiert.

Genauere Ausführungen dazu finden Sie in verschiedenen Kapiteln dieses Handbuches. Abbildung 1.6 gibt Ihnen einen Überblick über Ziele, Aufgaben und typische Rollen sowie übliche Rahmenbedingungen (typische Situationen), die sich aus den Anforderungen an ein modernes IT-Management ergeben.

Bezüglich der Zielorientierung muss das IT-Management immer wieder die nötige Balance finden, wie dies in Abbildung 1.7 illustriert wird.

Die notwendigen Fähigkeiten des IT-Personals lassen sich am besten aus den Aufgaben ableiten. Vielfältige Erfahrungen zeigen, dass die IT-Mitarbeiter vor allem für Management-Aufgaben befähigt sein müssen. Dazu zählen insbesondere:

- das Entwickeln von IT-Strategien;
- das Planen und Steuern von IT-Landschaften (Informationssystem-Architekturen, Geschäftsarchitekturen);
- das Planen und Bereitstellen von IT-Infrastrukturen und Lizenzen;
- das Managen hochwertiger IT-Services;
- das Managen von IT-Projekten und das Führen von Projektteams;
- die Übernahme von Organisationsaufgaben im IT-Bereich;

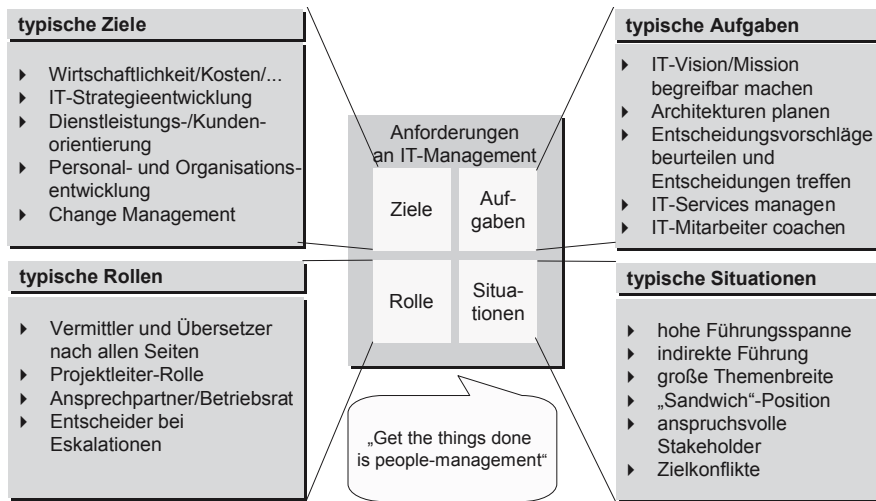


ABBILDUNG 1.6 Anforderungen und ihre Realisierung im IT-Management

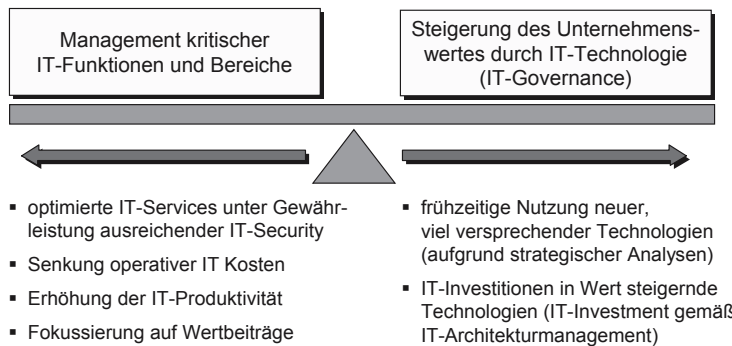


ABBILDUNG 1.7

Die Balance aufgrund von Anforderungen finden

- das Führen und Coachen von IT-Mitarbeitern und Teams;
- das Managen von Software-Entwicklungen und Software-Einführungen (Software-Lizenzen) sowie von Software-Qualität;
- das Treffen von Investitions- bzw. Sourcing-Entscheidungen im IT-Bereich;
- das Budgeting der IT-Abteilung und der IT-Produkte sowie der IT-Beschaffungen;
- das Controlling der IT-Kosten, IT-Services und IT-Produkte (mittels Kennzahlen- und Reporting-Systemen);
- Entwickeln und Umsetzen von Konzepten für das IT-Risiko- und IT-Sicherheitsmanagement;
- Maßnahmen zur Sicherstellung des Einhaltens von Richtlinien und rechtlichen Erfordernissen (IT-Compliance-Aufgaben).

Von der Unternehmensstrategie zur IT-Strategie

Die strategische Ausrichtung der IT ist in jüngster Zeit Thema vieler Untersuchungen. Dabei zeigen sich interessante Ergebnisse:

- Gartner-Analysten fordern vehement, dass die IT als ein wesentliches Instrument für wirtschaftliches und erfolgreiches Agieren der Unternehmen gesehen wird. Nachteilig für eine solche Positionierung im Unternehmen sei allerdings die vielfach rein technologische Sichtweise vieler IT-Führungskräfte. So müssen sich IT-Verantwortliche unbedingt der Herausforderung stellen, die Entscheidungsträger davon zu überzeugen, dass veraltete und teure Soft- und Hardware dem Firmenerfolg wenig dienlich sind. Wichtig ist es, die IT klar als Schlüssel-Infrastruktur zu positionieren.
- Einer Umfrage der Marktforscher von Dynamic Markets zufolge sehen mittlerweile ca. 89 Prozent der befragten IT-Manager ihre Rolle im Unternehmen zunehmend strategisch. Dies ist durchaus erfreulich, aber wie sieht die Realität aus? Nach Auswertung derselben Studie zeigt sich, dass die IT-Manager im Alltag vorwiegend administrative Tätigkeiten ausüben. Hier gilt es, anzusetzen und Veränderungen zu initiieren.

Eine entscheidende Konsequenz aus allen bekannten Studien sollte sein: Die Aktivitäten im IT-Bereich müssen – unabhängig von der Unternehmensgröße – stärker strategisch geplant und daran orientiert konsequent zu einer Umsetzung „geführt“ werden. Dies setzt bei den Verantwortlichen sowohl ein Kenntnis der Anforderungen des Unternehmens an die IT sowie ein Wissen um die aktuellen IT-Trends voraus.

Die IT-Strategie beschreibt ausgehend vom Ist-Zustand der IT im Unternehmen, den Anforderungen des Unternehmens an die IT sowie den Möglichkeiten auf dem Gebiete der Informations- und Kommunikationstechnologie

- die Vision, die Mission, die Ziele und Wege, wie die IT einerseits in Zukunft in einem Unternehmen genutzt und
- andererseits als Instrument und durch moderne Architekturen gestaltet werden sollen.

In einer Handlungsanleitung von Gartner für IT-Entscheider wird festgestellt, dass unter anderem die strategische Ausrichtung der IT zunehmend eine wichtige Rolle spielen wird. Gleichzeitig ist die Strategieorientierung in der IT in der Praxis viel zu wenig verbreitet (erst 20 Prozent der Unternehmen verfügen laut Studien über eine ausgereifte IT-Strategie). Zahlreiche Nachteile und Probleme können die Folge sein. So lässt sich insbesondere das Ziel, zukunftsfähige IT-Infrastrukturen zu schaffen und dauerhaft bereitzustellen, nur schwer ohne ein integriertes strategisches Vorgehen erreichen. Laut einer Studie der Meta Group sollte man sich **fünf Todsünden der IT-Strategie** (siehe Tabelle 1.2) vergegenwärtigen, wenn eine IT-Strategieorientierung aufgesetzt werden soll.

TABELLE 1.2 Todsünden der IT-Strategie

Todsünden der IT-Strategie	Begründung/Erläuterung
Keine systematische Vorgehensweise	Sofern auf eine abgestimmte methodische Vorgehensweise bei der Strategieentwicklung verzichtet wird, ist die Erarbeitung einer IT-Strategie und der darauf aufbauenden IT-Architektur zum Scheitern verurteilt.

Todsünden der IT-Strategie	Begründung/Erläuterung
Produktstandards als Ausgangspunkt	Die Festlegung von Produktstandards (etwa eines Servertyps) sollte gemäß der IT-Strategie gewählt und nicht zum Ausgangspunkt gemacht werden.
Fehlende Business-Vision	Ohne eine von der Unternehmensführung entwickelten Business-Vision besteht die Gefahr, dass die IT-Strategie nur wenig Bezug zu den eigentlichen Anforderungen hat.
Kein gemeinsames Verständnis über die Rolle der IT	Die Unternehmensführung sollte die IT-Organisation als strategisches Potenzial schätzen.
Das Projekt „IT-Strategie“	IT-Strategien lassen sich auf Dauer nicht im Projekt ermitteln, sondern sollten als iterative Prozesse gesehen und etabliert werden (wichtig: Prozessbeschreibung nötig).

Aus den Schwachstellen vieler Organisationen wird deutlich, dass das IT-Management sich für die kontinuierliche Entwicklung von IT-Strategien verantwortlich zeigen muss. Im Ergebnis ist ein „Vorgehen“ zu realisieren, das

- die Erarbeitung einer an den Unternehmenszielen ausgerichteten IT-Strategie ermöglicht,
- aus der IT-Strategie heraus die Qualitätsziele für das jeweilig Jahr ableitet,
- eine darauf aufbauende technische Architektur und Infrastruktur sowie
- die Darstellung und Vermarktung des daraus resultierenden Werts für die Kunden des IT-Bereichs realisiert.

Die Konsequenz lautet: IT-Verantwortliche sind zunehmend gefordert, eine IT-Strategie zu implementieren und diese fortzuschreiben. Damit verbunden ist die Etablierung eines professionellen IT-Architekturmanagements, damit auf diese Weise die Qualität der IT-Services gewährleistet und gleichzeitig die IT-Kosten langfristig gesenkt werden können.

Unter Berücksichtigung der vorgenannten Punkte ist die IT-Strategie, die es in fast allen Unternehmen als jährliche Ausarbeitung gibt, eigentlich als Leitfaden für die Entwicklung der Schwerpunkte zu sehen. Sie stellt also eine Verbindung zwischen den Unternehmenszielen und den „notwendigen Ausprägungen“ in der IT-Organisation dar. Außerdem sollte die IT-Strategie dazu dienen, die internen Projekte der IT abzuleiten und zu begründen. Es bietet sich daher an, die Konsequenzen aus der Strategiebetrachtung direkt im Projektportfolio zu integrieren und zu konkretisieren.



Kapitel 2 dieses Handbuchs vermittelt Ihnen kompaktes Know-how zur Entwicklung und praktischen Umsetzung von IT-Strategien. Sie erfahren anhand von praktischen Beispielen, wie Sie die IT Ihrer Organisation zukunftsorientiert positionieren können und welche IT-Innovationen nötig sind. Damit machen Sie Ihre IT-Landschaften fit für die Zukunft. Gleichzeitig können Sie ein optimales Enterprise Architecture Management realisieren.

Komplexität beherrschen – IT-Architekturen planen und managen

Ein weiterer Kernprozess im IT-Management ist daher die **Entwicklung, Auswahl und Umsetzung von IT-Architekturen**. Die IT-Architektur leistet durch die Definition von grundlegenden Gestaltungsprinzipien, Konzepten und Leitlinien sowie das Treffen von Systementscheidungen und die Auswahl von strategischen Technologien und Produkten die Grundlage für eine effektive und effiziente Bereitstellung der von den Fachabteilungen geforderten IT-Unterstützung. Sie dient allen Stakeholdern als Orientierungsrahmen.

Das IT-Management muss hierfür ein tragfähiges Gesamtbild der IT-Entwicklung als Orientierungsrahmen bieten: die Zielarchitektur von Infrastruktur und Anwendungslandschaft. Dazu sind Gestaltungsprinzipien und Systementscheidungen zu formulieren, ebenso wie „strategische“ Technologien und Produkte definiert und sodann kommuniziert werden sollten. Im Sinne des Strategic Alignment muss daraus auch die Konzeption von Zukunftsszenarien oder verbindlichen „Roadmaps“ für die weitere IT-Entwicklung ableitbar sein, ebenso wie jegliche Erarbeitung konkreter Vorgaben und Standards.

Die Forderung von Unternehmen, grundlegende und strategische Geschäftsprozesse schnell umzusetzen, wird dabei durch die Reaktionsfähigkeit der Informationstechnologie bestimmt. Häufig wird eine Unternehmensarchitektur durch vier Bausteine beschrieben:

- Technologiearchitektur,
- Anwendungsarchitektur,
- Datenarchitektur und
- Geschäftsarchitektur.

Die Konsequenz: Das IT-Management muss die vier Architekturbausteine beherrschen und in der Lage sein, die dazu notwendigen Entscheidungen für die eigene Organisation auf den Weg zu bringen. Von besonderer Relevanz ist die ganzheitliche Entwicklung und Betrachtung von Architekturen auf Unternehmensebene sowie die Berücksichtigung der Wechselwirkungen zwischen den verschiedenen Bausteinen der Architektur, um zu zukunftsorientierten integrierten Lösungen zu gelangen.



Für große und komplexe IT-Systeme ist es wichtig, die grundlegenden informationstechnischen und organisatorischen Strategien in Form einer übergreifenden IT-Architektur festzuschreiben. Welche Aufgaben sich für das IT-Management in Zusammenhang mit der Planung, Verwaltung und Weiterentwicklung von IT-Architekturen ergeben und wie diese optimal gelöst werden können, erfahren Sie in **Kapitel 3** dieses Handbuchs.

IT-Servicemanagement – durch Prozessorientierung zu einer höheren Servicequalität

Die Geschäftsprozesse einer Organisation lassen sich nur dann erfolgreich realisieren, wenn die erforderlichen IT-Applikationen und IT-Infrastrukturen störungs- und problemfrei arbeiten sowie eine adäquate Funktionalität aufweisen. Um dies sicherzustellen, ergibt sich in der Praxis ein wachsender Bedarf an leistungsfähigen IT-Services.

IT-Servicemanagement umfasst jene Prinzipien und Verfahren, die der Erstellung und Erbringung von zuverlässigen, kundengerechten IT-Dienstleistungen dienen. Neben der Verbesserung der Kundenbeziehungen zielt das IT-Servicemanagement auch auf eine Qualitätsverbesserung und Kostensenkung ab. Diese Ziele ziehen einen Paradigmenwechsel – vom IT-Anwender zum IT-Servicekunden – nach sich und setzen einen kulturellen Wandel in der Organisation voraus.

IT-Services müssen zum richtigen Zeitpunkt, in der richtigen Quantität, mit der richtigen Qualität, am richtigen Ort und zu marktfähigen Preisen für die internen Kunden der IT-Abteilung – also den Fachabteilungen – erbracht werden. Dieses Gleichgewicht ist nur durch eine optimal aufgestellte Serviceorganisation zu erreichen. Dazu müssen die IT-Ressourcen und IT-Architekturen geplant, überwacht und optimal eingesetzt werden. Daraufhin gilt es, die IT-Prozesse auf der Basis von Frameworks (wie ITIL und CobiT) zu unterstützen und zu professionalisieren.

Laut verschiedener Studien kann eine unzureichende Servicequalität labile Abläufe im Betrieb zu Folge haben. Sie führen wiederum zu teuren Produktivitätsverlusten und Unterbrechungen in den Geschäftsprozessen. Die Konsequenzen können sich bis zu den Kunden auswirken und den Ruf der Firma schädigen.

IT Servicemanagement zählt zu den jungen Managementdisziplinen, seine Bedeutung in Unternehmen wächst zunehmend. Schließlich bildet eine funktionierende IT heute in Unternehmen und Verwaltungen gewissermaßen das Rückgrat für die Geschäftsprozesse. Ausfälle führen zu erheblichen Konsequenzen und wirtschaftlichen Schäden, die nicht zuletzt auch ein gutes Image gefährden.

IT Servicemanagement stellt nach unserem Selbstverständnis einen ganzheitlichen Ansatz dar, der auf der einen Seite Prozesse und Abläufe analysiert und neu definiert, andererseits die Menschen und ihre Motivation einbezieht. Darauf gehen wir in unseren Assessments, Schulungen und Beratungen ausführlich ein.

In Kapitel 4 dieses Buches

- erhalten Sie eine Einordnung, wie IT-Services in einer modernen IT-Organisation zu „positionieren“ sind;
- gewinnen Sie einen Einblick in die wichtigsten IT-Serviceprozesse (orientiert am ITIL-Standard);
- erfahren Sie, wie IT-Serviceprozesse erfasst, beschrieben und optimiert werden können;
- lernen Sie kennen, welche Methodik sich für ein zeitgemäßes IT-Servicemanagement bewährt hat;
- erfahren Sie, welche organisatorischen Vorarbeiten für die Anwendung moderner IT-Servicemanagement-Lösungen erforderlich sind;
- eignen Sie sich ein fundiertes Wissen über die Vorgehensweisen im IT-Servicemanagement an, und gewinnen Sie einen Überblick über relevante Tools;
- lernen Sie, wie Sie IT-Servicemanagement zur professionellen Steuerung Ihrer IT-Abteilung nutzen sowie die IT-Ressourcen planen, überwachen und optimal einsetzen.



Die stetig wachsende Bedeutung des IT-Servicemanagements wird offensichtlich, wenn man sich vergegenwärtigt, dass eine funktionierende IT heute in Unternehmen und Verwaltungen gewissermaßen das Rückgrat für die Unternehmensprozesse bildet. Ausfälle von IT-Systemen führen zu erheblichen Konsequenzen und wirtschaftlichen Schäden, die nicht zuletzt auch das Image der IT und des Unternehmens insgesamt gefährden. Erfahrungen der Praxis zeigen es: IT-Verantwortliche oder IT-Servicemanager sind zunehmend gefordert, ein professionelles IT-Servicemanagement zu etablieren.

In **Kapitel 4** erfahren Sie, wie eine umfassende Qualität der IT-Services gewährleistet und gleichzeitig die IT-Kosten langfristig gesenkt werden können.

IT-Projekte erfolgreich managen

Neue Systeme oder Erweiterungen vorhandener Systeme werden in der Regel innerhalb von Projekten erstellt. Projekte stellen eine besondere Form der Arbeitsorganisation dar. Die Arbeit des IT-Bereiches ist weitgehend durch das Arbeiten in Projekten gekennzeichnet. Daher widmen wir auch dem Projektmanagement ein eigenständiges Kapitel.

Oft müssen eine Vielzahl von Projekten gleichzeitig realisiert werden. IT-Projekte – gleich welcher Art – können aber nur dann erfolgreich abgewickelt werden, wenn ein entsprechendes Projektmanagement und geeignete Rahmenbedingungen vorhanden sind.

Dazu ist es wichtig, dass das IT-Management bewährte Methoden, Techniken, Vorgehensweisen und Hilfsmittel kennt, die helfen, mögliche Probleme in IT-Projekten zu erkennen, zu analysieren, zu lösen und künftig zu vermeiden.

Besonderes Augenmerk ist im Rahmen der IT-Projektorganisation auf die Installation eines Multi-Projektmanagements bzw. strategischen Projektmanagements und der Nutzung von IT-Projektportfolios zu richten (zuweilen auch als Enterprise Project Management bezeichnet). Es dient der integrierten und ganzheitlichen Planung, Steuerung und Kontrolle einer Vielzahl von Projekten. Ansonsten laufen IT-Projekte Gefahr, intransparent und zu komplex für eine effiziente Koordination zu werden. Ohne Multiprojektmanagement erweisen sich Gremien und Ausschüsse (beispielsweise Lenkungsausschüsse) häufig überfordert, als Mittler zwischen Projekt und Linie zu agieren.

In Kapitel 5 erfahren Sie:

- wie das IT-Projekt durch effiziente Projektsteuerung auf Erfolgskurs bleibt;
- wie Leistungen, Termine und vor allem die Kosten eines IT-Projektes zu überwachen sind;
- wie man die Kosten und Qualität eines IT-Projektes in den Griff bekommt;
- wie eine realistische Projektfortschrittskontrolle und Risikosteuerung in IT-Projekten eingebaut werden kann;
- welche Werkzeuge und Tools für ein erfolgreiches IT-Projektcontrolling geeignet sind;
- wie durch die Entwicklung und Nutzung von Kennzahlen geeignete Führungsinformationen für ein IT-Projektcontrolling bereitgestellt werden;
- welche Berichtsarten für ein Reporting zu IT-Projekten sinnvoll sind und
- wie ein zukunftsorientiertes Projektcontrolling aufgebaut werden kann.



Eine notwendige Konsequenz: Das IT-Management muss die für ein erfolgreiches Projektmanagement erforderlichen Methoden, Techniken, Vorgangsweisen und Hilfsmittel kennen und beherrschen. Dazu zählen Konzepte und Verfahren zum Erarbeiten von Projektvisionen und Projektanträgen, Projektplanungstechniken sowie die eigentliche Durchführung der Projektarbeit. Doch nicht nur methodisches Know-how ist wichtig, auch soziale Kompetenzen sind für eine erfolgreiche Projektarbeit unverzichtbar (Führungsaufgaben, Teamarbeit etc.). Hinzu kommen neue Herausforderungen im IT-Projektmanagement; als Beispiele seien das Projekt-Risikomanagement, Claim-Management, Change-Management sowie Qualitätsmanagement in IT-Projekten genannt. **Kapitel 5** liefert Ihnen dazu wichtige Informationen.

Organisation und Führung im IT-Bereich – ein möglicher Erfolgsfaktor

Grundsätzlich ist die IT-Leitung für die Bereitstellung der IT im Unternehmen verantwortlich. Eingeschlossen sind alle IT-Leistungsprozesse. Die Sicherstellung des effektiven und effizienten Einsatzes der bereitgestellten IT-Produkte in den Geschäftsprozessen des Unternehmens liegt in der Verantwortung der Fachbereiche und ist keine Aufgabe des IT-Bereiches. Daher sollte es eine eigenständige Instanz in jedem Geschäftsbereich geben, die sich für den ordnungsgemäßen Einsatz der IT in den Geschäftsprozessen des Unternehmens verantwortlich fühlt. Nur bei kleinen Unternehmen kann diese Rolle gleichzeitig von der Geschäftsführung wahrgenommen werden.

Die IT-Bereitstellung (Lieferant) kann als Unternehmen im Unternehmen mit den üblichen Funktionen Beschaffung, Produktion und Absatz aufgefasst werden. Ist im Unternehmen ein eigener IT-Bereich eingerichtet, so ist diese Analogie noch zutreffender. Die Bereitstellung der IT-Leistungen kann auch durch externe IT-Dienstleister erfolgen. Ein interner IT-Bereich im Unternehmen ist in der Regel nur bei gegebener Unternehmensgröße anzutreffen. Kleinere Unternehmen beziehen die IT-Leistungen in der Regel extern. In Kapitel 6 erfahren Sie, welche organisatorischen Optionen sich für den IT-Bereich stellen und wie diese zu bewerten sind.

Ohne ausgefeilte Führungstechniken und ausgeprägtes Teamverhalten ist heute eine moderne IT nicht mehr vorstellbar. Wie alle Führungsaufgaben im Unternehmen ist auch die Führung des IT-Bereichs den Einflüssen aus den Veränderungen der allgemeinen Wirtschaftslage sowie den Veränderungen der Aktivitäten innerhalb der Unternehmensorganisation unterworfen. Zu beachten ist auch, dass Veränderungen bei den Anforderungen und Rahmenbedingungen fester Bestandteil des IT-Umfelds sind (Beispiel: es müssen immer wieder neue Projektteams gebildet werden).

Im Einzelnen lernen Sie in Kapitel 6:

- wie Sie Ihre vielfältigen Rollen als IT-Verantwortlicher erfolgreich meistern;
- wie Sie Motivationen im IT-Bereich „freisetzen“;
- Zielvereinbarungen als Basis der Zusammenarbeit kennen;
- mit Mitarbeitern im Team erfolgreich kommunizieren;
- für den IT-Bereich eine erfolgreiche Personalentwicklung zu initiieren und umzusetzen,

- wie man durch ein bestimmtes Führungsverhalten Widerständen in IT-Teams begegnet (Konfliktmanagement).



Die erfolgreiche Wahrnehmung von Führungsaufgaben stellt für das IT-Management eine echte Herausforderung dar. Der Erfolgsfaktor „Personal“ sollte keinesfalls unterschätzt werden, wenn es um die Optimierung des IT-Bereichs und der Bereitstellung hochwertiger IT-Produkte geht. Nur so können die Mitarbeiter ihre Leistungsfähigkeit voll entfalten und Teams erfolgreich arbeiten. Letztlich ergibt sich damit auch eine hohe Qualität der IT-Services, der entwickelten IT-Produkte (Applikationen) sowie der Projektergebnisse. **Kapitel 6** widmet sich diesem Thema ausführlich.

IT-Controlling – Kosten und Leistungen der IT nachhaltig managen

Die Notwendigkeit, auch genauere Kosten- und Leistungsbetrachtungen im IT-Bereich herzustellen und entsprechende Transparenz zu schaffen, wird immer mehr eingesehen. Ein Grund dafür sind zahlreiche Studien, die anhand konkreter Beispiele zeigen, dass vielfach regelrecht Kostenverschwendungen in der IT vorliegen:

- Jährlich werden ca. 20% des IT-Budgets in den Unternehmen verschwendet (Studie der Gartner-Group).
- Anwender setzen ca. 12% ihrer IT-Budgets auf Grund falscher oder unzureichender Abläufe in der Beschaffung von Computer-Equipment in den Sand (Studie der META Group).
- 190 Milliarden Dollar beträgt das Over-Investment im Bereich der Informationstechnologien allein in den USA für das Jahr 2000 (Studie der Credit Suisse First Boston).
- Weniger als 5% der „Global 2000-Firmen“ haben finanzielle Aspekte der IT in ihre Strategien, Pläne und ihr operatives Geschäft einbezogen. CIO's, die das getan haben, erhalten einen durchschnittlichen ROI ihrer IT-Investitionen von mehr als 100% – weitaus mehr als die traditionellen 35–55% der typischen IT-Anwender (Jonathan Poe, Vice President, Executive Directions, META Group).
- Durch Softwarefehler entstehen jährlich Kosten in Höhe von 170 Milliarden US-Dollar (Studie von Accenture).
- Über 52% aller europäischen Unternehmen verzeichnen mindestens einmal pro Quartal einen Systemausfall, der mit erheblichen Folgekosten verbunden ist (MacArthur Stroud International).

Diese Studien und die dabei vorgelegten Zahlen legen es nahe, nach Möglichkeiten zu suchen, wie eine Minimierung von IT-Kostenverschwendungen erreicht werden kann. Das bedeutet unter anderem, dass Investitionen in die IT immer stärker unter Wirtschaftlichkeitsgesichtspunkten geprüft werden müssen. Letztlich muss es darum gehen, in der IT eine Optimierung der Leistungen zu erreichen und dabei die Kostenseite gleichzeitig „im Griff“ zu haben. Für das Erreichen dieser Zielsetzungen bietet sich die Einrichtung eines speziellen IT-Controllings an. Das steigende Bedürfnis, den Erfolg des Einsatzes moderner Informations- und Kommunikationslösungen zu überwachen, verstärkt außerdem den Wunsch nach einem **effizienten Controlling der Informationsverarbeitung** im Unternehmen. Deshalb sollte das IT-Management auch die dazu notwendigen Methoden und Instrumente kennen und anwenden. Dazu zählen beispielsweise

- Methoden und Vorgehensweisen zur Kostenermittlung in der IT,
- Instrumente zur Erstellung von IT-Leistungskatalogen sowie zur Definition von IT-Leistungen (beispielsweise SLAs),
- Möglichkeiten einer internen Verrechnung von IT-Kosten und Leistungen,
- sachgerechte Entscheidung über IT-Outsourcing-Optionen,
- Kennzahlen zur Steuerung der Wirtschaftlichkeit und Qualität der IT sowie
- Instrumente für ein umfassendes operatives und strategisches IT-Controlling.

Auf diese Fragenkreise wird in Kapitel 7 dieses Handbuches ausführlich eingegangen.

IT-Controller sollen letztlich dafür sorgen, dass das Management (Unternehmensführung, Management der Fachbereiche, IT-Management) die „richtigen“ Entscheidungen treffen kann. Sie sichern und optimieren die Informationsversorgung der Manager. Neben der Beschaffung und Aufbereitung der entscheidungsrelevanten Daten klären und präzisieren sie, wo IT-Entscheidungen nicht mehr durch Fakten abgesichert werden können und welche Risiken die Entscheidungsträger eingehen (müssen).

Im Einzelnen lassen sich folgende Kernaufgaben für das IT-Controlling unterscheiden:

- IT-Controller sorgen für Strategie-, Ergebnis-, Finanz- und Prozesstransparenz in der IT und tragen somit zu höherer Wirtschaftlichkeit bei.
- IT-Controller koordinieren Teilziele und Teilpläne ganzheitlich (etwa für IT-Projekte oder IT-Services) und organisieren das Berichtswesen.
- IT-Controller moderieren und gestalten den Managementprozess der Zielfindung, der Planung und der Steuerung in der IT so, dass jeder Entscheidungsträger zielorientiert handeln kann. Dies betrifft etwa Informationen bezüglich der Beschaffung von IT-Produkten.
- IT-Controller leisten den erforderlichen Service der betriebswirtschaftlichen Daten- und Informationsversorgung für die IT-Beschäftigten.
- IT-Controller gestalten und pflegen die IT-Controlling-Systeme.



Zur Erfüllung der Aufgaben im IT-Controlling sind entsprechende Prozesse zu definieren, zu dokumentieren und in der Praxis permanent zu optimieren. Die Controlling-Prozesse lassen sich aus den Geschäftsprozessen im IT-Bereich ableiten. Vorgeschlagen wird nach einer Prozessidentifikation eine Dokumentation in Form von Prozessbeschreibungen. Ausführlich widmet sich **Kapitel 7** diesen Themen.

IT-Asset- und Lizenzmanagement – vielfältige Potenziale nutzen

Das Thema „IT-Asset- und Lizenzmanagement“ hat in den letzten Jahren immer mehr an Relevanz gewonnen. Dabei ist festzuhalten, dass hier verschiedene wichtige Ziele und Teilgebiete angesprochen werden, die es zu berücksichtigen gilt:

- strategische IT-Aspekte (IT-Investitionen, IT-Produktlebenszyklen),
- optimale IT-Serviceerbringung und verstärkte Kundenorientierung,
- wirtschaftliche/finanzielle Fragestellungen sowie
- rechtliche/vertragliche Dimensionen (IT-Compliance-Fragen).

Die Auflistung zeigt, dass es für IT-Organisationen aller Art und Größe sowie für das dort tätige IT-Management gleichzeitig wichtig und notwendig ist, sich mit diesem Themenbereich zu beschäftigen und die notwendigen Kompetenzen zum optimalen Handeln in den genannten Bereichen zu erwerben. Leider wird IT-Asset- und Lizenzmanagement von manchen noch oft als eine lästige Pflichtaufgabe betrachtet. Dies sollte nicht so sein; denn durch ein consequentes IT-Asset- und Lizenzmanagement

- kann den Anforderungen von IT-Auditierungen und IT-Revisionssicherheit in hohem Maße Rechnung getragen werden,
- lassen sich mitunter erhebliche Kosteneinsparungen realisieren,
- können Entscheidungen im Rahmen eines abgestimmten IT-Produkt-Lebenszyklusmanagement auf einer fundierten Basis getroffen werden sowie
- IT-Prozesse verschiedener Art optimiert realisiert werden.

Im Kern gibt es also mehrere Gründe für die zunehmende Bedeutung von IT-Asset- und Lizenzmanagement:

- immer komplexer werdende IT-Bebauungslandschaft (Applikationen, vielfältige Infrastrukturkomponenten, Vernetzungen);
- zunehmender Erwerb von Standardsoftware (mit entsprechender Lizenzierung bei unterschiedlichsten Lizenzmodellen) führt zu höherer Bedeutung von Lizenzmanagement;
- intransparenter und „vermuteter“ hoher Finanzaufwand für IT-Produkte und IT-Services;
- Entscheidungsunsicherheit bzgl. nötiger IT-Investitionen und Beschaffungen: Über die Einführung neuer Technologien oder Produkte kann nur „richtig“ entschieden werden, wenn ausreichend Bestands- und Wert-Informationen vorliegen (Unterstützung des IT-Purchasing, gezieltes Produktlebenszyklusmanagement). Business Case-Ermittlungen werden unverzichtbar;
- zunehmende IT-Risiken mit der Notwendigkeit der Implementation eines IT-Risikomanagement,
- vielfältige rechtliche Vorgaben (Gesetze, Richtlinien, Normen): Handeln unter Rechtssicherheit gewinnt für das IT-Management immer mehr an Gewicht (Gesetze, Verträge, Vorschriften einhalten!).



Wie die Aufgaben und Herausforderungen des IT-Asset- und Lizenzmanagement im Kontext der IT-Prozesse, neuer IT-Technologien und von Compliance-Anforderungen einzuordnen sind, ist Gegenstand von **Kapitel 8** dieses Handbuchs. Gleichzeitig soll in dem Beitrag deutlich werden, welche Optimierungsansätze für das IT-Management heute gegeben sind.

IT-Qualitätsmanagement als Herausforderung

Qualitätsmanagement ist in den letzten Jahren in vielen Firmen zu einem wichtigen Bereich geworden. Es wurden Qualitätsmanagement-Projekte initiiert, Mitarbeiter eingestellt und eigene Gruppen bzw. Abteilungen für das Qualitätsmanagement eingerichtet. Das Wesentliche wurde gemäß ISO 9000 ff. in Qualitätshandbüchern niedergeschrieben, und viele Unternehmen wurden zertifiziert. So auch in vielen IT-Abteilungen. Zur Aufgabenerledigung werden zum Teil eigene Stellen (IT-Quality-Manager) geschaffen.

Hilfreich ist die Unterscheidung zwischen verschiedenen Qualitätsdimensionen, die auch für den IT-Bereich tragbar ist:

- Produktqualität (technische Qualität eines Produktes/Hardwareproduktes, Softwarequalität, Design- und Anmutungsqualität von Soft- und Hardware);
- Kontaktqualität (Qualität der IT-Services, Qualität der Kundenberatung, Kommunikationsqualität);
- Interne Prozessqualität (Organisationsqualität, Kooperations- und Koordinationsqualität).

Die Ausführungen verdeutlichen: Ein wichtiges Aufgabenfeld des IT-Managements betrifft heute das konsequente Qualitätsmanagement für IT-Produkte, IT-Projekte und IT-Prozesse.



Kapitel 9 hält für Sie eine Vielzahl an Informationen zum Thema IT-Qualitätsmanagement bereit. Es macht Sie mit den grundlegenden Aktivitäten vertraut, reflektiert den aktuellen Stand von Vorgehensmodellen, Methoden und Werkzeugen und analysiert diese in Hinblick auf Qualitätsmerkmale.

IT-Governance

Als Antwort auf die vielfältigen technologischen und organisatorischen Herausforderungen im IT-Bereich hat sich mittlerweile der Begriff „IT-Governance“ etabliert. Durch die Schaffung von zentralen Strukturen zur Organisation, Steuerung und Kontrolle der IT eines Unternehmens – kurz IT-Governance – finden sich heute wesentliche Ansätze und vielfältige Handlungsfelder, um die IT-Leistungen und IT-Produkte in Unternehmen mit hoher Qualität und Sicherheit kundenorientiert bereitzustellen. Haupt-Stoßrichtung dieses Ansatzes ist die konsequente Ausrichtung der IT-Prozesse und IT-Produkte an der Unternehmensstrategie. Diese zentrale Steuerung (engl. „Governance“) der IT mit expliziter Unterstützung die Unternehmensführung wird als dringend notwendig angesehen, weil

- die IT-Prozesse – insbesondere die Serviceprozesse – in vielen Unternehmen eine zunehmend wichtige Rolle spielen und somit
- ihr reibungsloser Ablauf und ihre konsequente Verbesserung wesentliche Erfolgsfaktoren für die Unternehmen und Verwaltungen darstellen.

Was sind die primären Zielsetzungen? Die IT-Governance soll sicherstellen, dass die Umsetzung der IT-Strategie im Sinne der Verantwortungsträger – also der Unternehmensführung – erfolgt. Insbesondere können folgende Anforderungen und Zielsetzungen formuliert werden:

- IT-Governance soll die Sicherheit (Integrität, Verfügbarkeit, Vertraulichkeit) und Verlässlichkeit (Einhaltung externer Anforderungen) der Informationen bzw. der IT-Systeme sicherstellen.
- Es soll ein effizienter Einsatz der IT-Ressourcen bei gleichzeitiger Ausrichtung der IT auf die Unternehmensziele hergestellt werden (IT-Strategie als integraler Bestandteil der Business-Strategie eines Unternehmens).
- Durch die Schaffung von Transparenz (etwa die strategische und betriebswirtschaftliche Bewertung von IT-Projekten unter Berücksichtigung von Aspekten des Risikomanagements) soll auch ein Beitrag zur Kostensenkung im Bereich der IT geleistet werden.

- Durch klare, revisionssichere Strukturierung der IT-Organisation, Prozesse und Projekte nach allgemeinen Standards (z.B. ITIL, SPICE) wird ein Beitrag zur optimalen IT-Organisation geschaffen.
- Es kann die Erfüllung gesetzlicher Vorgaben (z. B. Ableitung von Sicherheitsanforderungen aus der IT-Risikoanalyse) gewährleistet werden.

Dabei sind im Rahmen der Organisation zweckmäßige und funktionsbezogene Planungs- und Kontrollsysteme einzurichten und weiterzuentwickeln.



Kapitel 10 behandelt und beschreibt insbesondere die wesentlichen Handlungsfelder zentraler IT-Governance: Unternehmensweite IT-Strategieentwicklung, unternehmensweites IT-Demand-Management, IT-Architekturmanagement, IT-Portfoliomanagement (Multiprojektmanagement) sowie IT-Investitions- und IT-Risikomanagement. Diese Kernbereiche stehen in einem engen Zusammenhang und müssen deshalb integrativ und ganzheitlich implementiert werden. Der Beitrag skizziert ergänzend die Rahmenbedingungen erfolgreicher IT-Governance und entwickelt dabei Empfehlungen als „Fahrplan für die Einführung“ von IT-Governance-Strukturen und -Prozessen.

IT-Security managen – Herausforderungen und Lösungsansätze

Die Bedeutung eines ausgereiften Security Management für ein zukunftsorientiertes IT-Management zeigt eine Studie der Gartner Group. Danach sollte der Anteil von Sicherheitsproblemen als Ursache für Systemausfälle von fünf Prozent im Jahr 2004 auf 15 Prozent bis zum Jahr 2008 steigen. Wesentliche Gründe dafür sind: Wachsende Internet-Aktivität und IT-Komplexität, kombiniert mit der Nutzung vielfältiger Web-Services, drahtlosen Verbindungen (W-LAN etc.) und anderen neuen Techniken. Wenn beispielsweise die Ausfallzeiten der IT-Systeme überhand nehmen, dann wird deutlich, dass bei fehlender IT-Sicherheit mitunter enorme Folgekosten in Kauf genommen werden müssen.

Projekte, Prozesse und Produkte (IT-Infrastrukturen, Software) im IT-Bereich unterliegen – das steht außer Zweifel – immer einem gewissen Sicherheitsrisiko. Eine Vielzahl von Einflussfaktoren kann dazu führen, dass das Erreichen der angestrebten strategischen und operativen IT-Ziele gefährdet oder gar erhebliche negative Folgewirkungen (etwa aus Fehlern der IT-Produkte oder Verzögerungen in der Ausführung der IT-Prozesse oder der IT-Projekte) denkbar sind.

Für die Handhabung von IT-Sicherheitsrisiken sind inzwischen einige hilfreiche und für die Praxis unverzichtbare Lösungsansätze entwickelt worden, die erhebliche Potenziale zur Zukunftssicherung eröffnen können. Sie helfen unter anderem, Gefahrenquellen frühzeitig zu erkennen und – falls notwendig – geeignete Gegenmaßnahmen zu ergreifen. Sicherheitslücken können so erfolgreich beseitigt und Haftungsrisiken minimiert werden.

In jedem Fall müssen sich die IT-Verantwortlichen vergegenwärtigen,

- welche IT-Sicherheitsaspekte bei den IT-Produkten, IT-Prozessen und IT-Projekten zu beachten sind,
- welche Aktivitäten für das IT-Securitymanagement üblich sind,
- wie eine Einordnung dieser Aktivitäten aus operativer und strategischer Sicht erfolgen kann.



In **Kapitel 11** erfahren Sie, wie man IT-Security-Lösungen erfolgreich implementiert und wie ein effektives Management solcher Lösungen möglich ist. Intensiv geht der Autor auch ein auf Fragen zur Sicherheitsorganisation in der IT sowie auf Kriterien für ein hochwertiges IT-Security-Management. Ausführungen zur Sicherheitspolitik und zur Sicherheitsstrategie runden dieses Kapitel ab.

Risikomanagement wird für IT-Produkte, IT-Projekte und IT-Prozesse immer wichtiger

Projekte, Prozesse und Produkte (IT-Infrastrukturen, Software) im IT-Bereich unterliegen – das steht außer Zweifel – immer einem gewissen Risiko. Eine Vielzahl von Einflussfaktoren kann dazu führen, dass das Erreichen der angestrebten Ziele gefährdet oder gar erhebliche negative Folgewirkungen (etwa aus Fehlern der IT-Produkte oder Verzögerungen in der Ausführung der IT-Prozesse oder der IT-Projekte) denkbar sind.

Soll ein Risikomanagement-System für den IT-Bereich neu aufgesetzt oder grundlegend erweitert werden, gilt es also zunächst eine strategische Positionierung vorzunehmen. Im Zuge einer Konzeptentwicklung werden dabei die Abläufe und Werkzeuge des Risiko-Managements bestimmt. Dazu sind vier Schritte erforderlich. Diese müssen immer wieder durchlaufen werden, da neue Risiken hinzukommen oder bestehende sich ändern können:

- **Risiko-Identifikation:** Es sind die IT-Risiken zu identifizieren, etwa durch Meldungen der beteiligten und betroffenen Personen eines IT-Prozesses.
- **Risiko-Analyse:** Die identifizierten Risiken müssen anschließend hinsichtlich der Erreichung der Zielsetzungen einer genauen Analyse unterzogen werden.
- **Risiko-Bewertung:** Der Risikomelder muss schätzen, mit welcher Wahrscheinlichkeit das Risiko eintritt. Dann wird ermittelt, welches Ausmaß das Risiko in Bezug auf Funktion, Zeit und Ressourcen hat. Die Risikokennzahl ergibt sich aus der Kombination von Eintrittswahrscheinlichkeit und Risikoausmaß. Je größer die Kennzahl, desto größer die Wahrscheinlichkeit des Eintritts bzw. des Schadensausmaßes.
- **Maßnahmen zur Risikobehandlung:** Es gilt, Maßnahmen einzuleiten, die den Risiken entgegenwirken. Bei Prozessen zählt dazu beispielsweise die Anpassung von Zielen, Plänen oder Ressourcen. Ist dieses Potenzial ausgeschöpft, können Risiken auch auf Dritte verlagert werden, etwa durch Outsourcing oder die Vereinbarung von Schadensersatz bei Nichterfüllung von Dienstleistungen durch Dritte.

Für die Handhabung von IT-Risiken sind inzwischen einige brauchbare Lösungsansätze entwickelt worden, die erhebliches Potenzial zur Zukunftssicherung eröffnen können. Sie helfen unter anderem, IT-Risiken frühzeitig zu erkennen und – falls notwendig – geeignete Gegenmaßnahmen zu ergreifen. Sicherheitslücken können so erfolgreich beseitigt und Haftungsrisiken minimiert werden.



Kapitel 12 hält für Sie eine Vielzahl an Informationen zur Einführung eines ganzheitlichen IT-Risikomanagements bereit. Ausgehend von aktuellen Herausforderungen des IT-Risikomanagements erfahren Sie, wie IT-Risikoarten identifiziert und bewertet werden. Sie lernen die wesentlichen Instrumente und Praktiken des IT-Risikomanagements sowie deren Umsetzung in die Unternehmenspraxis kennen. Außerdem macht der Beitrag deutlich, warum für IT-Organisationen ein IT-Risikomanagement immer bedeutsamer wird, welche Teilbereiche zu betrachten sind und in welchen Phasen IT-Risikomanagement dabei nutzbringend umgesetzt werden kann. Schließlich werden auch Maßnahmen für das Management von IT-Risiken thematisiert.

IT-Compliance – die Einhaltung von Richtlinien und rechtlichen Erfordernissen sichern

Mit dem Schlagwort „IT-Compliance“, das zunehmend die Runde macht, wird eine neue Herausforderung für das IT-Management deutlich. Das Management des IT-Bereichs ist selbst gefordert – weil hauptverantwortlich –, für die Einhaltung vorliegender Richtlinien und gesetzlicher Vorgaben, die den IT-Bereich betreffen, zu sorgen.

Eines kann vorweg festgestellt werden: IT-Compliance bedeutet für das IT-Management eine Herausforderung, aber auch eine Chance. Der IT-Einsatz im Unternehmen kann durch den besonderen IT-Compliance-Fokus durchaus einen neuen Stellenwert erhalten. Die IT wandelt sich vom Dienstleister für die anderen Unternehmensbereiche zu einem Kernbereich des Unternehmens, der regulatorischen Anforderungen und internen wie externen Prüfern im selben Maß unterworfen ist, wie etwa das Rechnungswesen oder der Personalbereich.

IT-Compliance als Teilbereich der Enterprise-Compliance fokussiert diejenigen Aspekte, welche die IT-Systeme eines Unternehmens aus Compliance-Sicht betreffen. Zu den Compliance-Anforderungen in der IT zählen dabei vor allem das Herstellen von Informationssicherheit und Verfügbarkeit sowie die Berücksichtigung und das Einhalten von Datenschutzregelungen. Unternehmen unterliegen zahlreichen rechtlichen Verpflichtungen, deren Nichteinhaltung zu hohen Geldstrafen und Haftungsverpflichtungen führen kann. EU-Richtlinien, internationale Konventionen, unternehmensinterne Konventionen und Handelsbräuche mit den damit verbundenen Regeln sind ebenfalls zu beachten.

IT-Richtlinien legen die wesentlichen Leitlinien für Informationsqualität, IT-Sicherheit, Schutz der informationellen Ressourcen etc. fest. Sie bilden eine Basis für die Umsetzung strategischer IT-Planungen. Die Wirksamkeit von Richtlinien hängt von ihrer erfolgreichen Kommunikation ab.

Beachten Sie: Unternehmen müssen zwar für Initiativen zur Einhaltung von Compliance-Regularien bezahlen, allerdings kann auch die Nichteinhaltung teuer werden. Darüber hinaus können weitere Kosten aus unterschätzten oder unentdeckten Risiken entstehen.



Das **Kapitel 13** berücksichtigt, dass die Vorgabe von Richtlinien bzw. das Einhalten rechtlicher Anforderungen für Unternehmen einen zunehmenden Stellenwert einnehmen. IT-Compliance beschreibt in der Unternehmensführung die Einhaltung der gesetzlichen, unternehmensinternen und vertraglichen Regelungen im Bereich der IT-Landschaft. Sie erfahren in dem Beitrag, wie es auf nationaler, europäischer und internationaler Ebene ein Anliegen des Gesetzgebers ist, verbindliche Standards für die Risikovorsorge in Unternehmen, für das Etablieren von unternehmensinternen Systemen zur Kontrolle dieser Risiken und für eine interne und externe Berichterstattung über die Wirksamkeit solcher Kontrollsysteme festzulegen.

IT-Recht

Zahlreiche Überlegungen und Entscheidungen im IT-Bereich bedürfen rechtlicher Klärung und Abstimmung. Die Integration von Datenschutzbeauftragten und Betriebsrat soll hier nur als Beispiel dienen.

Auch die personenbezogenen Gesetze wie für behinderte Personen, Mutterschutz, Beschäftigung von Jugendlichen usw. beeinflussen die Organisation der IT. Die unterschiedlichen gesetzlichen Vorschriften der einzelnen Staaten sind ein weiteres Kriterium, das die Organisation und die Führung eines IT-Bereichs beeinflusst. Der IT-Bereich muss sich also auf die verschiedenen Gesetzeslagen vorbereiten und auch sicherstellen, dass hier immer die aktuellen Informationen vorliegen.

Für das IT-Management bedeutet heute die Vielzahl der rechtlichen Vorgaben, die es zu berücksichtigen gilt, letztlich soviel, dass die Einhaltung und Umsetzung von regulatorischen Anforderungen im weitesten Sinne (z.B. Gesetze, Verordnungen) mit dem Ziel eines verantwortungsvollen Umgangs mit allen Aspekten der Informationstechnik (IT) ein wichtiges Handlungsfeld darstellt.



Besondere rechtliche Fragenkreise für IT-Verantwortliche werden in **Kapitel 14** dieses Buches behandelt. Ein Beispiel sind etwa auch gesetzliche Auflagen wie die EU-Richtlinie zum Datenschutz oder Sarbanes-Oxley. Sie stellen IT-Führungskräfte vor große Herausforderungen. Nur mit entsprechenden Kenntnissen im IT-Recht können sie sicherstellen, dass ihre IT-Systeme und Geschäftsprozesse den komplexen gesetzlichen Auflagen entsprechen.

■ 1.5 IT-Management – Orientierungen für die Zukunft

Die Ausführungen in diesem Kapitel haben gezeigt, dass ein erfolgreiches IT-Management eine Vielzahl von Kompetenzen erfordert. Folgende Merkmale sollten heute den modernen IT-Manager kennzeichnen:

- Der IT-Manager denkt und handelt strategisch, er kümmert sich als Manager um die Auswahl und Implementierung von IT-Architekturen, die das Business und die Kunden intern wie extern bestmöglich unterstützen unter Beachtung von Governance, Budget, Risikoabschätzung und Technologie.
- Er führt MitarbeiterInnen leistungs- und zielorientiert, ist ein Teamplayer, der integrativ mit allen Führungslinien im Unternehmen „kann“ und sich als Unterstützer konstruktiv einbringt.
- Er hat eine klare Linie, welche Aufgaben von externen IT-Dienstleistern erbracht werden. Zu diesen ist er partnerschaftlich und fair, managt sie aktiv und verhandelt Verträge sicher zum Wohle seines Unternehmens.
- Er misst ständig die Performance und den Zufriedenheitsgrad der IT, führt Benchmarks mit Peers durch und entwickelt die IT ganzheitlich im Unternehmen weiter.

Wenn Sie künftig vermehrt Führungs- und Managementfunktionen im IT-Bereich übernehmen wollen, sollten Sie sich darauf intensiv vorbereiten. Berücksichtigen Sie dabei, dass die **Anforderungen an das Management im Wandel** begriffen sind:

- Personen mit Führungsaufgaben müssen neu, anders, quer denken.
- Management bedeutet künftig, dass insbesondere Innovationen planmäßig gestaltet und systematisch unterstützt werden.
- Führungskräfte von morgen zeichnen sich durch geistige Flexibilität, Risikobereitschaft und ständige Lernwilligkeit aus.
- Sich selbst führen können, ist eine weitere wichtige Forderung, die Führungskräfte an sich selbst stellen sollten. Die wichtigsten Managementfähigkeiten dazu sind die Delegation von Aufgaben sowie das richtige Setzen von Prioritäten.

Wie sich das IT-Management gewandelt hat, soll die Übersicht in Abbildung 1.8 darlegen.

IT-Manager „alt“	IT-Manager (CIO) „neu“
▪ Technik-orientiert ▪ IT als Inhalt ▪ Technik-qualifiziert ▪ Spezialist ▪ denkt in Kosten ▪ intern orientiert ▪ kennt Technologie	▪ Geschäftsprozess-orientiert ▪ IT als Mittel zum Zweck ▪ führungsqualifiziert ▪ Generalist ▪ denkt in Ergebnissen ▪ extern orientiert ▪ kennt Technik und Geschäft

ABBILDUNG 1.8
IT-Manager – Berufsbild
im Wandel

Immer mehr Unternehmen reagieren auf die größere Bedeutung der IT für das Unternehmen, indem sie neben dem klassischen IT-Leiter die Rolle des Chief Information Officer (CIO) vergeben. Von seiner Stellung her ist der CIO normalerweise Mitglied der Geschäftsleitung oder des Vorstands oder dieser Ebene direkt zugeordnet. Ausschlaggebend hierfür ist die Bedeutung der IT im Unternehmen. Durch den CIO wird technisches Know-How und ein detailliertes Wissen über den momentanen Stand der IT-Abteilung und Infrastruktur in die höchste Führungsebene gebracht. Damit wird der Bedeutung der IT-Abteilung in einem Unternehmen besonders hervorgehoben.

Als typische Aufgabenbereiche eines CIOs werden gesehen:

- Entwicklung und Umsetzung einer IT-Strategie für die Informationstechnik- bzw. das Informationsmanagement.
- Erarbeitung, Festlegung und Durchsetzung von IT-Standards.
- Unterstützung der Fachbereiche bei der Entwicklung und Optimierung von Lösungen für deren Geschäftsprozesse.
- Identifikation und Einführung von so genannten „Best Practices“ für das Unternehmen.
- Förderung des Informationsflusses zwischen allen Gruppen des Unternehmens, die an IT-Lösungen arbeiten bzw. mit diesen arbeiten.
- Planung, Überwachung und Analyse der IT-Budgets und IT-Kosten sowie Initiierung und Überwachung von Kostensenkungsprogrammen in Zusammenarbeit mit dem IT-Controlling.

Eine Trennung zwischen CIO und IT-Leitung ist dann zu sehen, wenn es sich um große Organisationen handelt bzw. eine Trennung zwischen dem Unternehmen und der IT besteht. Dies kann durch Auslagerung als rechtlich selbstständige Einheit festgelegt sein. In diesem Fall ist der CIO auf der Unternehmensseite der Ansprechpartner für den Leiter des IT-Bereichs. Bei integrierten Einheiten in Unternehmen und Verwaltung ist die Aufgabenstellung IT-Leitung und CIO auf eine Person konzentriert.

Auch die Rolle des CIO befindet sich natürlich in einer permanenten Weiterentwicklung. Dies steht in einem engen Zusammenhang mit organisatorischen Veränderungen im IT-Bereich. Dabei kann generell nach wie vor festgestellt werden, dass sich die IT vom reinen technischen „Bereitsteller“ immer mehr zum Business Enabler entwickelt. Dies hat zur Folge, dass neben dem Erbringen von IT-Services das Steuern dieser Services immer stärker in den Vordergrund tritt. Das hat dann etwa für das IT-Management zur Folge, dass die IT künftig Services für das Business definieren muss und dabei standardisierte und modularisierte IT-Lösungen sowie ein Delivery-, Supply- und Sourcing-Konzept etablieren und nutzen muss. Erfolgreich kann dies nur dann gelingen, wenn sich das IT-Management sowohl um das ganzheitliche Management von Business- und IT-Prozessen kümmert, als auch gleichzeitig die Steuerung und Koordination der Entwicklungs- und Betriebsleistungen des IT-Bereichs verantwortet (vgl. auch Ergebnisse einer Detecon-Studie „IT Organisation 2015 – Facelift oder Modellwechsel?“, die in Zusammenarbeit mit dem Branchenverband Bitkom (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien) erschienen ist).

Zu ähnlichen Ergebnissen kommt auch eine aktuelle Studie von Forrester (http://www.forrester.com/rb/Research/whats_driving_demand_for_key_it_roles/q/id/56284/t/2). Als wesentliches Fazit der Studie „What’s Driving Demand For Key IT Roles?“ wird herausgestellt, dass Unternehmen von der Leitung des IT-Bereichs (bzw. den CIOs) erwarten, dass sie für sichere, konsistente und effiziente Prozesse und Services sorgen. Dabei haben die Themen Risiko und Sicherheit nach Einschätzung der Befragten eine besonders hohe Priorität. 40 Prozent der Befragten erwarten eine wachsende Bedeutung von Projekt-Management, 36 Prozent zählen außerdem Business-Analysen zu den immer wichtigeren Aufgaben eines IT-Entscheiders. Schließlich werden auch Fragen der IT-Strategieentwicklung und der IT-Planung als wesentliche Aufgaben und Herausforderungen betont.

Im Wesentlichen raten Forrester-Analysten, dass IT-Leitungen bzw. CIOs ihre Skills in den Bereichen Servicemanagement, Risiko- und Sicherheitsmanagement sowie Enterprise Architecture ausbauen. Darüber hinaus sollten Sie unbedingt Personen in ihre Teams holen,

die sich mit Design und Ausführung von IT-Services und IT-Prozessen auskennen und hier Optimierungen leisten können.

In Tabelle 1.3 finden Sie abschließend einige Thesen und Beispiele, die im Hinblick auf den **künftigen beruflichen Erfolg** gerade auch für im IT-Management tätige Personen diskutiert werden.

TABELLE 1.3 Orientierungshilfen für erfolgreiches IT-Management

Fähigkeiten für den persönlichen Erfolg	Beispiele/Orientierungshilfen
Visionen	Gestalten Sie Ihre eigene Vision! ▪ Vision zur Ausrichtung des IT-Bereichs (als Business-Enabler etc.) ▪ Vision für künftige Technologie- und Personalorientierung ▪ Visionen für die Etablierung der IT-Prozesse und IT-Services ▪ Visionen zur Integration von Business- und IT-Prozess-Verantwortung ▪ Visionen für eigenes Handeln
Prioritäten	Setzen Sie Prioritäten! ▪ Disziplin und Flexibilität in der persönlichen Planung (dringend oder wichtig?) ▪ Richtungsänderung (neues Denken) ▪ Selbstmotivation
Macht	Entwickeln Sie Ihren persönlichen Einfluss! ▪ Wissen ist Macht (lebenslanges Lernen als Grundsatz) ▪ Intuition nicht vernachlässigen ▪ Freunde um sich „scharen“, aber keine Cliquenbildung
Networking	Arbeiten und denken Sie in Netzwerken! ▪ Who knows who? (über die verschiedenen Bereiche des Unternehmens hinweg) ▪ Beteiligung an Communities (offline und online)
Risikobereitschaft	Entwickeln Sie die Fähigkeit, Risiken einzugehen und Verantwortungen zu übernehmen! ▪ Neue Technologien rechtzeitig erproben ▪ Moderne Organisations- und Arbeitsformen einsetzen
Kreatives Denken	Seien Sie kreativ! ▪ Innovationsmanagement in der IT und Trendscouting betreiben ▪ Neuen Ideen gegenüber aufgeschlossen sein. ▪ Kreative Phasen (etwa in Meetings) bewusst einplanen
Serendipity	Nutzen Sie Chancen! ▪ Fragen stellen ▪ Nicht immer „Nein“ sagen ▪ Synergie der 7 Erfolgsfaktoren



„Man kann nicht in die Zukunft schauen, aber man kann den Grund für etwas Zukünftiges legen – denn Zukunft kann man bauen.“

Antoine de Saint-Exupéry



Das Wichtigste – zusammengefasst

- **Um im Management erfolgreich agieren zu können, ist es unumgänglich, die Visionen und Strategien der Unternehmensführung bzw. der Unternehmenseigner (Shareholder) zu kennen.**

Es bietet Vorteile, wenn Sie diese bewährte Handlungsleitlinie auch für das IT-Management umsetzen. Empfohlen wird außerdem eine stärkere Fokussierung der Zusammenarbeit von IT mit den verschiedenen Partnern auf die Nutzengenerierung und Wertorientierung. Ein Beispiel dafür ist etwa ein verstärkter Fokus auf den Wertbeitrag bei den Beziehungen zu externen Lieferanten.

- **Beachten Sie, dass IT-Management sowohl eine strategische Dimension als auch eine operative Ausrichtung haben muss.**

Im strategischen IT-Management muss primär die Frage „Machen wir die richtigen Dinge?“ beantwortet werden. Es sind also beispielsweise die richtigen Projekte auszuwählen (Aufstellen des IT-Masterplans und eines IT-Projektportfolios) oder geeignete Architekturstandards bzw. IT-Services für das Unternehmen zu entwickeln und vorzugeben. Demgegenüber geht es bei der operativen Ausrichtung darum, „die Dinge richtig zu machen“; also beispielsweise die einzelnen IT-Projekte erfolgreich zu managen sowie die IT-Serviceprozesse nachhaltig zu optimieren und optimiert umzusetzen.

- **Prüfen Sie, welche Kern-, Management- und Unterstützungsprozesse für das IT-Management von besonderer Bedeutung sind, und ziehen Sie daraus entsprechende Konsequenzen für die Organisation und die Personalentwicklung!**

Das Systemmanagement, die Anwendungsentwicklung (in der Regel in Projekten), das IT-Servicemanagement sowie die Entwicklung und Etablierung von IT-Architekturen bilden die Kernprozesse der IT-Bereitstellung. Der Definition und Etablierung von Risiko- und Sicherheitsmaßnahmen kommt in allen Bereichen der IT zunehmende Bedeutung zu. Qualitätsmanagement, IT-Controlling, Asset- und Lizenzmanagement, Organisation und IT-Recht sind notwendige querschnittliche Aufgaben und Prozesse. Sie sind in Abhängigkeit von der Größe des Unternehmens unterschiedlich stark ausgeprägt.

- **Stellen Sie für sich – und gegebenenfalls auch für Ihre Mitarbeiterinnen und Mitarbeiter – sicher, dass die in Ihrer IT-Organisation benötigten Managementkompetenzen vorhanden sind! Das IT-Management und die Mitarbeiter sind der wichtigste Erfolgsfaktor für das Erbringen hochwertiger IT-Leistungen.**

■ 1.6 Literatur

- [Ba01] *Baschin, A.*: Die Balanced Scorecard für Ihren Informationstechnologie-Bereich. Ein Leitfaden für Aufbau und Einführung. Campus-Fachbuch 2001
- [BrWi07] *Brenner, W.; Witte, C.*: Erfolgsrezepte für CIOs. Was gute Informationsmanager ausmacht. Hanser, München Wien 2007
- [Br05] *Brugger, R.*: Der IT Business Case. Springer, Berlin 2005
- [Bu05] *Buchta, D.; Eul, M.; Schulte-Croonenberg, H.*: Strategisches IT-Management. Wert steigern, Leistung steuern, Kosten senken. Gabler, Wiesbaden 2005
- [Ge02] *Gernert, Chr.; Ahrend, N.*: IT-Management: System statt Chaos. Ein praxisorientiertes Vorgehensmodell. Oldenbourg, München 2002
- [KaNo01] *Kaplan, R.S.; Norton, D.P.*: Die strategiefokussierte Organisation. Führen mit der Balanced Scorecard. Schäffer-Poeschel, Stuttgart 2001
- [Ti96] *Tiemeyer, E. (unter Mitarbeit von R. Chrobok)*: OrgTools. A für O-Softwareführer für die Organisationsarbeit. Band 1: Geschäftsprozeßorganisation. Schäffer-Poeschel, Stuttgart 1997
- [Ti04] *Tiemeyer, E.*: Projekte im Griff – Tools und Checklisten zum Projektmanagement, m. CD-ROM. WBV Bertelsmann, Bielefeld 2004
- [Ti05a] *Tiemeyer, E.*: IT-Servicemanagement kompakt. Elsevier, Spektrum Akademischer Verlag, Heidelberg 2005
- [Ti05b] *Tiemeyer, E.*: IT-Controlling kompakt. Elsevier, Spektrum Akademischer Verlag, Heidelberg 2005
- [Ti05c] *Tiemeyer, E.; Weiss, Chr.*: IT-Management in Wirtschaft und Verwaltung. In: Monitor, Heft 11/2005, S. 66f.
- [Ti07] *Tiemeyer, E.*: IT-Strategien entwickeln/IT-Architekturen planen. rauscher.Verlag. Haag i. OB 2007. 978-3-940045-02-7
- [Ti10] *Tiemeyer, E. (Hrsg.)*: Handbuch IT-Projektmanagement – Vorgehensmodelle, Managementinstrumente, Good Practices. 714 Seiten, Hanser-Verlag. München 2010

Walter Wintersteiger, Ernst Tiemeyer



Fragen, die in diesem Kapitel beantwortet werden:

- Warum sind strategische Überlegungen für jede IT-Organisation bzw. für jeden IT-Bereich unverzichtbar?
- Welche Vorgehensweisen zur Entwicklung von IT-Strategien haben sich bewährt? Gibt es förderliche Rahmenbedingungen, die es zu beachten gilt?
- Wie lassen sich für die IT-Strategieentwicklung bewährte Methoden wie die Erfolgsfaktorenanalyse, die SWOT-Analyse oder die IT-Diagnosetechnik erfolgreich einsetzen?
- Was sind die wesentlichen IT-Prinzipien (Grundsätze) als Treiber einer IT-Strategieentwicklung?
- Welche Teilstrategien können im IT-Bereich verfolgt werden?
- Welche Ergebnisse werden aufgrund von IT-Strategieentwicklungen erwartet?
- Wie kann durch eine gezielte Vorhabensplanung (IT-Masterplanerstellung) die entwickelte IT-Strategie erfolgreich umgesetzt werden?
- Welche Steuerungsoptionen zur Verfolgung der Strategieumsetzung gibt es?

Die Bedeutung der Informations- und Kommunikationstechnologie für Wirtschaft und Gesellschaft nimmt kontinuierlich zu. Trends wie der steigende Vernetzungsgrad der Unternehmen, die Globalisierung und Dynamisierung des unternehmerischen Umfelds und die wachsende Informationsflut stellen die Unternehmen vor Herausforderungen, die ohne einen verstärkten Einsatz von Informations- und Kommunikations-Technologien kaum noch zu lösen sind. In vielen Branchen hat die IT längst ihre ursprüngliche reine Unterstützungsfunktion verlassen und ist zu einem Treiber des Geschäfts oder sogar zum Geschäft selbst geworden.

„Um erfolgreich zu sein, müssen Flexibilität, Offenheit, Zusammenarbeit und Schnelligkeit zu einem Teil der Unternehmenskultur werden“, erklärt Henning Kagermann, Vorstandssprecher von SAP im Rahmen einer Umfrage der Economist Intelligence Unit, bei der rund 4000 Führungskräfte aus Unternehmen und öffentlichen Verwaltungen in den 23 stärksten Volkswirtschaften befragt wurden. „Unternehmen werden sich zunehmend auf ihre Kernkompetenzen konzentrieren und müssen sich noch stärker auf ein integriertes Netzwerk von Partner- und Zulieferfirmen verlassen, um Kundenerwartungen in Bezug auf Flexibilität und Bequemlichkeit zu erfüllen.“

Erik Brynjolfsson, Professor für Management an der MIT Sloan School und Direktor des Massachusetts Institute of Technology Center für E-Business: „In den nächsten fünf Jahren werden wir wahrscheinlich mehr Innovation durch den Einsatz von IT sehen als jemals zuvor. Diese neue Studie deckt sich mit unseren Erkenntnissen, wonach die IT eine zunehmend wichtige Rolle spielt, um neue Geschäftsmodelle zu entwickeln und stärker auf den Kunden zu fokussieren. In dem Maße, wie die IT-Kosten sinken, steigt das Potenzial für Innovationen, die erst durch IT ermöglicht wird.“

■ 2.1 Rahmenbedingungen für die IT-Strategieentwicklung

Um den stark zunehmenden und komplexen Anforderungen der Unternehmen gerecht zu werden, muss man die IT strategisch planen. Die Erstellung und Umsetzung der IT-Strategie ist einerseits eine wichtige Aufgabe der Leitung des IT-Bereichs, andererseits müssen aber auch alle Führungskräfte des gesamten Unternehmens sowie verschiedene Mitglieder aus dem IT-Managementkreis daran mitwirken.

Nachfolgend soll zunächst deutlich werden, dass das Vorhandensein und die Kenntnis der Unternehmensstrategie eine wesentliche Voraussetzung für eine erfolgreiche IT-Strategieentwicklung bildet. Wichtig sind auch eine Unterstützung durch die Unternehmensführung sowie das Verfolgen klarer Planungsgrundsätze. Eine wichtige Rahmenbedingung stellt darüber hinaus das Anwenden ausgewählter Methoden und Techniken für die Strategieentwicklung dar.

2.1.1 Strategische Unternehmensführung

Bevor wir uns mit der Aufgabe „IT-Strategie entwickeln und umsetzen“ im Detail beschäftigen, wollen wir uns mit einigen grundsätzlichen Überlegungen zur strategischen Unternehmensführung auseinandersetzen.

Der Begriff der „**Strategie**“ fand in den sechziger Jahren Eingang in die amerikanische Managementlehre und entwickelte sich immer mehr zu einem zentralen Begriff der Betriebswirtschaftslehre – auch im deutschsprachigen Raum.

Übernommen wurde er aus der Wahrscheinlichkeits- bzw. Spieltheorie, die nach grundsätzlichen Wegen fragt, unter Berücksichtigung bestimmter Wahrscheinlichkeiten zu einem Zielwert zu kommen, und aus der Lehre der Kriegsführung, die zahlreiche Grundsätze der strategischen Führung entwickelt – so z.B. die Grundsätze Konzentration der Kräfte, Vermeidung von Schwächen bzw. Aufbau von Stärken, Ausnützen von Umweltbedingungen.

Zwei wichtige Vorgaben für die IT-Strategieentwicklung stellen in diesem Zusammenhang das **Unternehmensleitbild** und die **Unternehmensstrategie** dar.

2.1.1.1 Unternehmensleitbild

Im Brockhaus-Lexikon wird „Leitbild“ definiert als eine „idealhafte richtungsweisende Vorstellung, deren Verwirklichung in der Praxis durch entsprechende Grundsätze, Methoden und Einzelziele angestrebt wird“. Demnach ist ein **Unternehmensleitbild** eine schriftliche Darlegung von ideellen Werten, Normen und Überzeugungen eines Unternehmens. Durch ihr Leitbild gibt eine Organisation Auskunft über ihre grundsätzlichen Vorstellungen hinsichtlich der anzustrebenden Zielsetzungen und Verhaltensweisen. So dient ein Leitbild als Orientierungshilfe sowohl für Mitarbeiter als auch für Kunden und sonstige Interessenten.

Tabelle 2.1 zeigt in tabellarischer Form ein Beispiel eines Unternehmensleitbildes.

TABELLE 2.1 Unternehmensleitbild eines Großhandelsunternehmens für technische Produkte

Fragen	Antworten
Welchen Bedarf wollen wir mit unseren Marktleistungen (Produkte, Dienstleistungen) befriedigen?	▪ Arbeitsschutz ▪ Technische Produkte ▪ Bauprodukte
Welchen grundlegenden Anforderungen sollen unsere Marktleistungen entsprechen?	▪ Volles Sortiment ▪ Hochwertige Qualität ▪ Fairer Preis
Welche geografische Reichweite soll unser Unternehmen haben?	▪ Österreich ▪ Schweiz ▪ Ungarn ▪ Tschechien ▪ Kroatien
Welche Marktstellung wollen wir erreichen?	▪ In der Schweiz: Marktführer. ▪ In den anderen Ländern: mind. 10% vom Marktvolumen.
Welchen Grundsätzen soll unser Verhalten gegenüber unseren Marktpartnern entsprechen?	▪ Erstklassiger Service für unsere Kunden. ▪ Partnerschaftliche Kooperation mit den führenden Herstellern.
Welches sind unsere grundsätzlichen Zielvorstellungen bezüglich Gewinnerzielung und Gewinnverwendung?	▪ Steigerung der Umsatzrendite bis zum ... auf 6%. ▪ Einsatz des gesamten Gewinns für die Realisierung unserer Wachstumsziele von 10% pro Jahr.
Welchen Stellenwert haben die Unternehmensressourcen für uns?	▪ Personal: Gut ausgebildete, engagierte und glückliche Mitarbeiter sind das Rückgrat unseres langfristigen Erfolgs. ▪ IT: Wir nutzen bewusst die neuesten Möglichkeiten der IuK-Technologie. ▪ Finanzen: Wir halten fest an dem Prinzip der Firmengründer, unser Unternehmen – auch das Wachstum – zu 75% aus Eigenkapital zu finanzieren.
Welchen Stellenwert hat das Auslandsgeschäft für uns?	Für die Expansion des Auslandsgeschäfts werden weiterhin angemessene Akquisitionen getätigt.

2.1.1.2 Unternehmensstrategie

Eine **Unternehmensstrategie** ist eine umfassende Beschreibung des Entscheidungsverhaltens der Unternehmensführung zur Sicherung zukünftiger Erfolgspotenziale. Obwohl sie sich von einem zukünftigen Erfolg ableitet, gibt sie den Weg vor, wie in der Gegenwart entschieden werden soll.

Die Unternehmensstrategie gibt Antwort auf folgende essenzielle Fragen:

- Wo stehen wir (mit unserem Unternehmen)? (IST-Zustand)
- Wo wollen wir hin? (Ziel, SOLL-Zustand)
- Wie kommen wir dorthin? (Weg zum Ziel)

Beispiele für strategische Unternehmens-Zielsetzungen:

- Persönliche Betreuung der Großkunden durch Mitarbeiter vor Ort
- Erhöhung der Deckungsbeiträge durch Forcierung der Produktgruppen X, Y, Z
- Erschließung neuer Absatzwege (z. B. E-Commerce)
- Optimierung der Lagerverwaltung durch Aufbau einer zentralen Logistik
- Erhöhte Mitarbeitermotivation durch finanzielle Beteiligung der Mitarbeiter am Unternehmenserfolg

Abbildung 2.1 verdeutlicht die wichtigsten Teile einer Strategie.

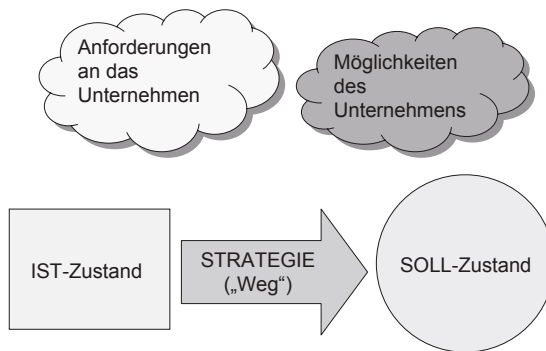


ABBILDUNG 2.1

Die wichtigsten Teile einer Strategie

2.1.2 Zweck und Grundsätze der IT-Strategieentwicklung

Grundsätzlich kann festgestellt werden, dass eine IT-Strategie für Unternehmen aller Größenordnungen notwendig ist, um eine zukunftsorientierte Planung und Steuerung der IT-Services zu gewährleisten. Hinzu kommt: Weil die IT in Unternehmen aller Art eine immer wichtigere Rolle spielt und immer mehr Personen in der Unternehmenspraxis aktiv an der optimalen Gestaltung – nicht nur Nutzung – der IT mitwirken sollen, braucht es eine allgemein gültige – und auch allgemein verständliche – Orientierungshilfe bzw. eine entsprechende **IT-Strategie**.

Welche **Erwartungen** werden an **IT-Strategien** gestellt? Die Erarbeitung einer IT-Strategie stellt eine wesentliche Voraussetzung dar, um optimale IT-Services unter Beachtung wirtschaftlicher Aspekte bereitzustellen. Hauptzielsetzungen sind

- die Sicherung der Betriebs- und Lieferfähigkeit des Anwenderunternehmens sowie
- die Verbesserung der Leistungsfähigkeit der IT, was sich – wie viele Benchmarks zeigen – auch auf die Wettbewerbsfähigkeit des Unternehmens positiv auswirkt.

Ausgehend vom Ist-Zustand der IT im Unternehmen, den Anforderungen des Unternehmens und der Mitarbeiter des Unternehmens an die IT sowie den Möglichkeiten auf dem Gebiete der Informations- und Kommunikations-Technologien sind verschiedene strategische Überlegungen anzustellen. Diese umfassen

- das Festlegen der Vision, der Mission und der strategischen Ziele, wie die IT in Zukunft in einem Unternehmen genutzt werden soll;
- das Skizzieren der Stärken und Schwächen der IT-Organisation und daraufhin das Fixieren wesentlicher IT-Prinzipien und daraus ableitbarer IT-Richtlinien;
- das Beschreiben der dazu notwendigen Soll-IT-Architekturen;
- sowie in einem Masterplan die notwendigen IT-Projekte und organisatorischen Veränderungsnotwendigkeiten.

Die IT-Strategie baut auf dem Unternehmensleitbild bzw. der Unternehmensstrategie auf und wird mitunter als „**funktionale Strategie**“ bezeichnet, weil sie sich mit einer Querschnittsfunktion im Unternehmen beschäftigt – wie zum Beispiel auch die Finanzstrategie (Hinweis: Im Falle eines IT-Unternehmens entspricht die IT-Strategie dann der Unternehmensstrategie).

Die IT-Strategie wird in der Regel unter der Federführung der IT-Abteilung unter Mitwirkung ausgewählter Personen aus allen Fachbereichen eines Unternehmens erarbeitet. Sie wird meist für einen Zeitraum von 3–5 Jahren ausgelegt, es hat sich aber als zweckmäßig erwiesen, die IT-Strategie jährlich zu überprüfen und gegebenenfalls anzupassen. Eigner des Dokuments ist in der Regel die IT-Leitung.



Beachten Sie:

Um die IT strategisch optimal ausrichten zu können, ist eine hohe Wertschätzung der IT im Unternehmen insgesamt von erheblichem Vorteil. Darüber hinaus ist es notwendig und unverzichtbar, die Anforderungen der Fachabteilungen des Unternehmens an die IT sowie die aktuellen IT-Trends zu kennen.

In der Praxis gibt es jedoch – je nach Auslöser – zwei grundsätzlich unterschiedliche **Vorgehensweisen** für einen IT-Strategieprozess:

Top down:

- Die IT-Strategieerstellung ist Teil einer bewährten Unternehmenspraxis und wird aus der Unternehmensstrategie abgeleitet.
- Ein außerordentliches Ereignis im Unternehmen findet statt (Fusion, Filialgründung, neues Geschäftsmodell, neues Produkt/neue Dienstleistung).
- Maßgebliche Intensivierung der Kooperation mit Geschäftspartnern erfordert eine – auch übergreifende – strategische IT-Ausrichtung.
- SWOT-Analyseergebnisse zeigten vor allem Business-IT-Alignment-Notwendigkeiten auf.
- Umfassendes Rightsourcing der IT wird angestrebt.

Bottom up:

- Realisierung eines Großprojekts, dessen Rahmenbedingungen erhoben und/oder neu gestaltet werden sollen.
- Einsatz neuer technologischer Möglichkeiten (z.B. Mobile Lösungen, RFID oder Cloud Computing).
- Unzufriedenheit der IT-Nutzer mit IT-Leistungen und/oder -Kosten.

Die Abhängigkeit des Unternehmenserfolgs von der Wirksamkeit und Wirtschaftlichkeit der IT erfordert eine entsprechende Anpassung der IT an die sich ändernden Rahmenbedingungen. Wesentlich ist deshalb darüber hinaus das Analysieren verschiedener Einfluss- und Erfolgsfaktoren. Die notwendigerweise anzustellenden Grundsatzüberlegungen lassen sich wie folgt zusammenfassen:

- Einbetten der strategischen IT-Planung in die strategische Unternehmensplanung
- Rollierendes Überprüfen und Fortschreiben der strategischen Planung
- Rechtzeitiges Umsetzen von Technologieentwicklungen (durch kontinuierliches Beobachten und Abschätzen der IT-Trends sowie ein Etablieren eines ausgewogenen IT-Life-Cycle-Managements)
- Vergleichen der Planungsergebnisse mit Alternativen
- Anwenden eines ganzheitlichen IT-Planungsinstrumentariums
- Berücksichtigen der bestehenden Architektur [HEI03]

2.1.3 Inhalte einer IT-Strategie

Die schriftliche Fixierung der IT-Strategie kann in der Praxis einen sehr unterschiedlichen Detaillierungsgrad haben:

- Im einfachsten Fall kann es sich um eine Liste von Vereinbarungen und Aktionen handeln, die die IT in Zukunft verfolgen möchte.
- Das Strategiepapier kann aber auch sehr umfassend und komplex sein. Es bezieht sich dann häufig auf einen bestimmten mittel- bis langfristigen Zeithorizont und beschreibt auch verschiedene Teilstrategien. Im Ergebnis wird schließlich eine Vorhabensplanung dargelegt, die ein Masterplan dokumentiert.
- Welchen Umfang und Detaillierungsgrad das Strategiepapier hat, hängt von der Größe der jeweiligen IT-Organisationen ab, für die eine Strategie entwickelt wird. So ist klar, dass das Strategiepapier eines mittelständischen Unternehmens, das sich die IT-Strategie ggf. mit Unterstützung externer Experten erarbeitet, einen anderen Detaillierungsgrad hat als ein größeres Unternehmen oder ein multinationaler Konzern (das IT-Strategiepapier umfasst dann etwa auch strategische Überlegungen der IT-Ausrichtung für die verschiedenen Landesgesellschaften).

Ausgehend vom IST-Zustand der IT im Unternehmen, den Anforderungen des Unternehmens an die IT sowie den Möglichkeiten auf dem Gebiet der Informations- und Kommunikationstechnologie beschreibt eine IT-Strategie grundsätzlich die Vision, Mission, Ziele und Wege, wie die IT einerseits in Zukunft in einem Unternehmen genutzt und andererseits als Instrument gestaltet werden soll.

Im Vordergrund steht die Frage: Wie kann mit Hilfe der IT der Unternehmenserfolg gesichert und möglichst gesteigert werden (Effektivität der IT)? Dann erst folgen die Fragen in Richtung IT-Organisation: Wie lassen sich die IT-Leistungen verbessern und die IT-Kosten senken (Effizienz der IT)?

Abbildung 2.2 zeigt die Hauptstoßrichtungen für eine IT-Strategie.

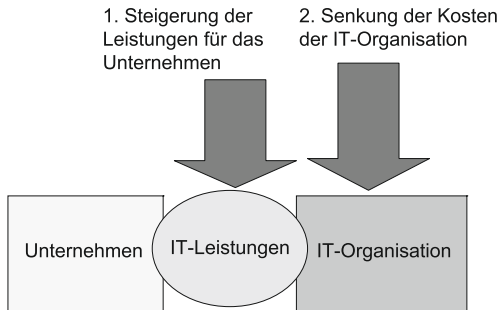


ABBILDUNG 2.2

Die Hauptstoßrichtungen einer IT-Strategie



Beispiel eines Inhaltsverzeichnisses einer IT-Strategie

- 0 Zusammenfassung (Management-Summary)
- 1 Situationsanalyse
 - 1.1 Fachliche Beurteilung
 - 1.2 Technische Beurteilung
 - 1.3 Organisatorische Beurteilung
- 2 Umfeldanalyse
 - 2.1 Interne Aspekte (Geschäftsmodelle, Kundenanalyse, SWOT-Analysen)
 - 2.2 Externe Aspekte (Wettbewerbsanalyse)
 - 2.3 Technologie Aspekte (IT-Trend-Analysen)
- 3 Ziele und Rahmenbedingungen
- 4 Grundsätze der IT (IT-Prinzipien)
- 5 Beschreibung der Teilstrategien – Soll-Konzept und Entscheidungen
 - 5.1 Zulässige Basissysteme der IT
 - 5.2 Organisatorische Positionierung der IT (E-Governance)
 - 5.3 Methoden und Vorgehen im Anforderungsmanagement
 - 5.4 IT-Service-Strategie
 - 5.5 IT-Personalstrategie
 - 5.6 IT-Sourcing-Konzept
 - 5.7 Methodik und Vorgehensmodelle für IT-Projekte
 - 5.8 Konzept für das IT-Qualitätsmanagement und die Qualitätssicherung
 - 5.9 Richtlinien für IT-Security und IT-Risikopolitik

6	Empfehlungen zu den IT-Architekturen (IT-Architekturkonzept)
6.1	Technologiearchitektur
6.2	Daten-Architektur
6.3	Applikationsarchitektur
6.4	Fachliche Architekturen (Fachkonzepte)
6.5	Organisation (Prozesse, Strukturen etc.)
6.6	Sicherheitsarchitektur
7	Vorhabens-Planung
7.1	Projekt-Portfolio
7.2	Wirtschaftlichkeits- und Risikobewertung
7.3	Projekt-Budgetierung
8	Anhang
8.1	Begriffe und Abkürzungen
8.2	Abbildungen und Tabellen
8.3	Formulare/Vorlagen

2.1.4 Einschlägige Methoden und Techniken

Entscheidend für die erfolgreiche Nutzung der IT ist und bleibt die konkrete Umsetzung der IT-Strategie. Die anspruchsvollen Themen und die verschiedenen Sichten der Beteiligten sowie deren unterschiedliche Qualifikation machen diese Aufgabe meist sehr schwierig. Hilfreich dabei ist die Verwendung einschlägiger Methoden und Techniken, namentlich Business Engineering, Projektmanagement sowie gute Praktiken auf dem Gebiet der Kommunikation und Präsentation.

Business Engineering ist eine Managementdisziplin und bezeichnet die methoden- und modellbasierte Konstruktionslehre für Unternehmen des Informationszeitalters. Die Merkmale sind:

- ingenieurmäßiges Vorgehen, wobei Werkzeuge genutzt werden, die eine klare Struktur aufweisen;
- ganzheitliche Sichtweise, die Strategie, Prozess und Informationssystem miteinander verbindet;
- Informationstechnik wird als Enabler der Innovation verstanden;
- der Prozess wird als Schlüssel zur steuerbaren Geschäftsabwicklung angesehen. Dabei löst ein Input verschiedene Aktivitäten aus, die zu einem messbaren Ergebnis führen;
- Prozessverantwortliche, die als Vertreter des Fachmanagements Verantwortung für die Fachprozesse übernehmen;
- operationale Prozessführung ermöglicht ein gezieltes Controlling der Prozesse (Prozess-Monitoring);
- vernetzte Organisation selbstständiger Einheiten.

Für die systematische Erschließung und Umsetzung der Geschäftspotenziale von IT-Innovationen ist es notwendig, dass sich mehr oder weniger große und multifunktionale Teams professionell mit Strategien, Prozessen, IT-Applikationen und Technologien auseinandersetzen. Weil die Transformation komplexe Mensch-Maschine-Systeme betrifft, reicht es nicht aus, sich auf den technischen bzw. fachlichen Aspekt der Veränderung zu beschränken. Zum Instrumentarium des Business Engineers gehören auch Fähigkeiten im Hinblick auf Change Management sowie Einfühlungsvermögen und Verständnis für die menschlichen, kulturellen und politischen Aspekte von Veränderungen. [ÖST 95]

Eine Orientierung gibt Abbildung 2.3.

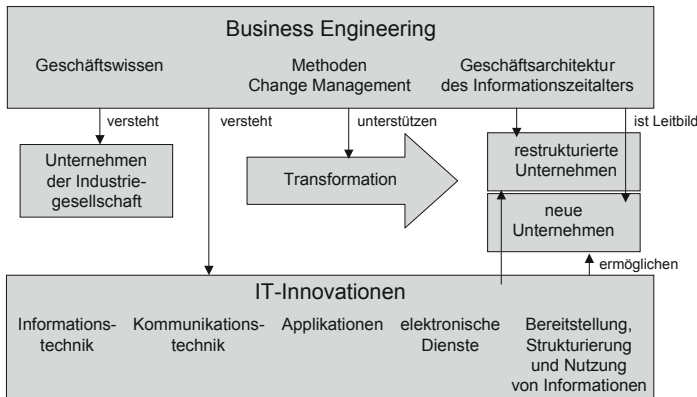


ABBILDUNG 2.3
Business Engineering –
Inhalte und Transforma-
tion

Business Engineering trifft Entscheidungen auf allen Ebenen der Gestaltung eines Unternehmens, namentlich auf den Ebenen Strategie, Prozess, Informationssystem. Dabei ist stets darauf zu achten, dass die wechselseitigen Entsprechungen sichergestellt werden. Das Modell im Überblick zeigt Abbildung 2.4.

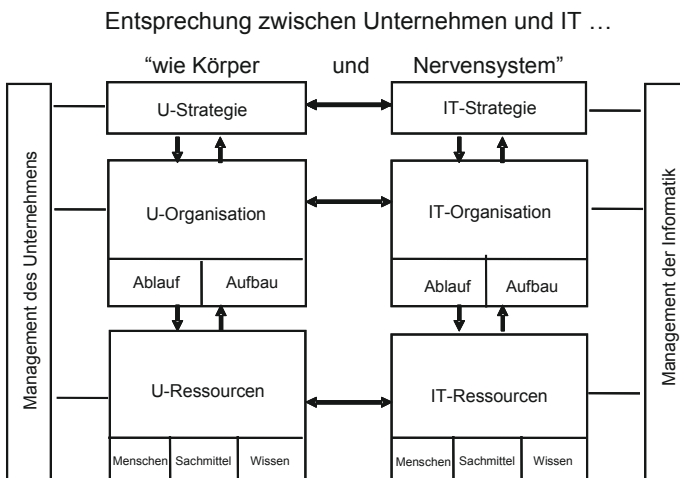


ABBILDUNG 2.4
Business Engineering-
Modell

Das (unternehmensweite Gesamt-) **Informationssystem** muss so gestaltet werden, dass es die Geschäftsprozesse optimal unterstützt.

Die **Geschäftsprozesse** müssen so gestaltet werden, dass die Unternehmensstrategie verwirklicht werden kann.

Gerade in jüngster Zeit wird von vielen Unternehmen in das so genannte „**IT Alignment**“ investiert, das heißt, in die optimale Anpassung der IT an die Anforderungen des Unternehmens als Ganzes und die Geschäftsbereiche bzw. Geschäftsprozesse im Einzelnen.

Dieses Problem soll das folgende Zitat aus „InformationWeek“ verdeutlichen:



“A New Look at the Relationship Between Business and IT”

If you find that the role of technology is still undervalued at your company, it may be a sign that it's not considered as strategic as it should be. To measure the importance that the CEO and other business executives place on technology, consider the following:

Does the CEO insist that business managers commit to savings or revenue growth to cover IT investments?

How interested are the CEO and his/her staff in keeping up with technology advances?

Is the IT executive rewarded for creating bridges with senior business executives?

Does the CEO engage at all with strategic technology suppliers?

Do the CEO and his/her staff utilize appropriate IT themselves?”

■ 2.2 IT-Strategien entwickeln – Wesentliche Teilschritte

Unter dem Motto „**Betroffene beteiligen**“ ist die Erstellung und Umsetzung der IT-Strategie nicht nur Aufgabe der Leitung des IT-Bereichs, vielmehr müssen alle Führungskräfte des Unternehmens in den Prozess eingebunden werden. Die gemeinsame Erarbeitung einer IT-Strategie ist Chance und Verpflichtung zu einem Stück Organisationsentwicklung im Sinne eines umfassenden Gestaltungs- und Lernprozesses auf der Metaebene. Unterschiedliche Sichten und Erwartungen der Beteiligten prallen so frühzeitig aufeinander, und die Erkenntnisse aus einschlägigen Diskussionen – ja, vielleicht auch Konflikten – lassen sich auf diese Weise nutzbringend einsetzen.

Die strategische IT-Planung kann man mit Recht als komplex und risikobeladen bezeichnen; es hat somit alle Attribute eines Vorhabens, das in Form eines eigenen Projekts realisiert werden sollte.

Das Management des **IT-Strategieentwicklungsprozesses** sorgt für eine gute Abwicklung und den Know-how-Transfer an Schlüsselleute in den untersuchten Organisationseinheiten. Die Projektleitung sorgt dafür, dass die Planungsarbeiten nicht „formalistisch“, sondern immer ausgerichtet auf die Zielsetzung – optimale Auslegung der IT-Aktivitäten für die

Organisationseinheit – durchgeführt werden. Sie sorgt mit der Art der Arbeitsorganisation und der Führung des Projektes für die Vernetzung aller Elemente, für eine gezielte Hinterfragung der Erkenntnisse und dafür, dass nicht zu früh vordergründig attraktive Lösungen ins Auge gefasst werden. [Zarnekow2004]

Wichtig ist, dafür zu sorgen, dass der Strategie-Entwicklungsprozess iterativ angelegt wird, weil es immer wieder zwischen den Möglichkeiten und den Grenzen der IT-Gestaltung abzuwägen gilt.

Die Durchlaufzeit eines Vorhabens zur Erstellung oder Totalüberarbeitung der IT-Strategie sollte bei max. 6 Monaten liegen und nahtlos in die Masterplanung zur Umsetzung der IT-Strategie übergehen. Die Teilüberarbeitungen sollten innerhalb von 1-2 Monaten erfolgen.

Folgende Teilschritte sind für die **Entwicklung einer IT-Strategie** üblich und sinnvoll:

Schritt 1: Analyse der Unternehmensstrategie und Ermittlung der strategischen Erfolgsfaktoren

Der erste Schritt muss immer eine **Analyse der Unternehmensstrategie** und der sich daraus ergebenden Auswirkungen für die IT-Strategie sein. Dabei werden die Herausforderungen der Geschäftsprozesse sowie die Informationsbedürfnisse der Fach- und Führungskräfte des Unternehmens sowie der verschiedenen Unternehmensbereiche ermittelt und aufgezeigt.

Um die strategische Ausrichtung der IT-Organisation (des IT-Dienstleisters, der IT-Abteilung etc.) entwickeln und präzisieren zu können, ist in jedem Fall ein Blick auf die Ausgangslage (primär auf das Leistungs- und Kundenportfolio der IT-Organisation) und die Ableitung der wesentlichen Erfolgsbedingungen für die Erbringung von hochwertigen IT-Dienstleistungen in der jeweiligen Branche erforderlich.

Auch sollten die aktuellen Markttrends analysiert und auf ihre Relevanz für das Unternehmen hin untersucht werden. Liegen diese Informationen und Festlegungen vor, kann daraus eine für Fachbereich und IT gemeinsame **Definition der strategischen Anforderungen an den IT-Betrieb des Unternehmens** abgeleitet werden. Die Ergebnisse können in einem **Erfolgsfaktorenmodell** dokumentiert werden. Daraufhin können die Werte der IT erfasst sowie **IT-Mission und IT-Visionen** definiert werden. Auf dieser Basis sind die **strategischen IT-Ziele** zu formulieren. Abgeleitet werden die strategischen Ziele sinnvollerweise aus den typischen Dimensionen Finanzen, Prozesse, Personal, Produkte und Projekte (entsprechend den Perspektiven einer Balanced Scorecard).

Schritt 2: IT-Analysen und IT-Diagnosen durchführen

Die Situation der IT sollte in jedem Fall aus verschiedenen Sichtweisen heraus analysiert werden. Dies betrifft die vorhandenen und genutzten IT-Produkte, die angebotenen IT-Services sowie die Personal- und Finanzsituation des IT-Bereiches. In einer besonderen Analyse (SWOT-Analyse) sind darüber hinaus die Stärken und Schwächen herauszuarbeiten.

Es empfiehlt sich, die IT-Diagnose expertenzentriert durchzuführen (ggf. mit Unterstützung externer Beratung). Der Fokus der IT-Diagnose ist in der Regel darauf gerichtet, den Zustand der IT mit einem Metriksystem zu messen (heute oft in Form einer Balanced Scorecard). Dieses System muss alle für den Unternehmenserfolg bestimmenden Dimensionen der IT umfassen – nicht nur die, welche aus Anwender- und Benutzersicht beurteilt werden können.

Schritt 3: IT-Prinzipien aktualisieren und Teilstrategien formulieren

Unverzichtbar für die Umsetzung einer IT-Strategie ist eine klare Aussage über die strategischen Ziele der IT. Sie sind Ausgangspunkt und Grundlage für die Konzeptentwicklung; etwa die Ableitung von IT-Prinzipien und Teilstrategien. Ausgehend von den strategischen Herausforderungen und den strategischen IT-Zielen, sollten die IT-Verantwortlichen (ggf. unterstützt durch einen neutralen IT-Berater) im Rahmen eines Workshops die strategischen IT-Ziele des Unternehmens entwickeln bzw. anpassen. Diese beschreibt die Rolle der IT im sich ändernden Umfeld und liefert übergeordnete Zielsetzungen für alle Bereiche, von der technischen Architektur über anzustrebende Kooperationen bis hin zum Personaleinsatz und zur Personalentwicklung. Ein weiteres Ergebnis der strategischen Klausur sollten eine eventuell erforderliche Aktualisierung der Q-Policy und die aktuellen Qualitätsziele für das laufende Jahr sein.

Schritt 4: IT-Architekturen festlegen und beschreiben (IT-Bebauungsplanung)

Aufbauend auf den strategischen Anforderungen und den abgeleiteten Teilstrategien wird unter Berücksichtigung der von verschiedenen Stakeholdern eingebrachten Informationen über die aus den Projekten stammenden Anforderungen die konzeptuelle Architektur entwickelt bzw. in späteren Durchläufen adaptiert. Wesentlicher Bestandteil sind **die Architektur-Prinzipien** des Unternehmens. Varianten, auf denen die Prinzipien beruhen können, sind:

- Technologie-Architekturen: IT-Infrastrukturen und ihre Komponenten
- Applikations-Architekturen: Applikations-Landschaften
- Fachliche Architekturen: Geschäftsfelder, Prozesse, Aufgaben, Ziele
- Informations-Architekturen (Daten-Architekturen): Business-Objekte versus Daten-Objekte
- Security-Architekturen

Schritt 5: Vorhabensplanung aufstellen (Projektportfolio, Master- und Migrationsplan)

Aus der Differenz zwischen Soll-Konzepten und Ist-Situation wird die **Vorhabensplanung** für den IT-Bereich abgeleitet. Die Vorhaben werden jeweils auf ihre grundsätzliche Machbarkeit im Sinne einer „Feasibility Study“ geprüft und in einen Mittelfristplan mit einem Planungshorizont von 3–5 Jahren überführt. Die Mittelfristplanung wird in Form einer sog. Masterplanung dokumentiert und bildet die Grundlage für die Erarbeitung der jährlichen Umsetzungsplanung der IT-Strategien.

Die erarbeiteten Architekturpläne werden außerdem mit dem Ist-Zustand abgeglichen und bei entsprechendem Bedarf ein Migrationsplan erstellt. Danach erfolgt die Implementierung der erforderlichen Änderungen. Nach erfolgter Implementierung besteht die Notwendigkeit, die Dokumentation der aktuellen Architekturen entsprechend zu adaptieren, um beim nächsten Durchlauf für den erforderlichen Abgleich zur Verfügung zu stehen.

2.2.1 Analyse der Unternehmensstrategie und Ermittlung der strategischen Erfolgsfaktoren

In der Praxis ist nicht selten zu beobachten, dass es keine bzw. keine ausreichend operationalisierte Unternehmensstrategie gibt bzw. diese dem IT-Management nicht bekannt ist. Im Fall einer zusätzlich unzureichenden Kommunikation zwischen IT und Fachbereich bzw.

Unternehmensführung ist das IT-Management bei der „Ableitung“ der IT-Strategie nicht selten auf sich allein gestellt.

In einem ersten Schritt bietet sich in dieser Situation an, im Rahmen von gezielten Interviews mit der Unternehmensführung die zentralen Parameter für die zu entwickelnde IT-Strategie zu ermitteln und zu dokumentieren. Wichtige Fragen, die adressiert und beantwortet werden sollten, sind beispielsweise:

- Welches sind die Haupt-Geschäftsfelder sowie die wesentlichen Kundensegmente unseres Unternehmens?
- Wie wird die zukünftige Geschäftsentwicklung des Unternehmens in den verschiedenen Geschäftsfeldern eingeschätzt?
- Gibt es aktuell zu berücksichtigende Einflüsse durch Branchentrends und Wettbewerber, die bei der Strategieformulierung zu berücksichtigen sind?
- Welche aktuellen Herausforderungen sind durch rechtliche Regularien (IT-Compliance) zu beachten?

Im Wesentlichen können die notwendigen Informationen bei der Unternehmensführung generiert werden. Darüber hinaus sind auch Interviews mit Leitern aus den Fachabteilungen zu führen. Dies kann in Anlehnung an die oben skizzierten Fragestellungen erfolgen. Allerdings ist hier auch auf die Spezifika der jeweiligen Geschäftseinheit einzugehen. Als Ergebnis der Interviewrunden mit der Unternehmensführung oder Abteilungsleitung sollten sich folgende wesentliche Input-Faktoren für die Entwicklung der IT-Strategie ergeben:

- Strategische Zielsetzungen des Unternehmens (Unternehmensstrategie)
- Abgeleitete strategische Zielsetzungen der Geschäftseinheiten (Teilstrategien)
- Spezielle IT-Trends in den Fachbereichen
- Erwartungen und Zielsetzungen der Unternehmensführung und der Fachbereiche an die IT und die von ihr angebotenen Lösungen und Services

Eine Ermittlung der wesentlichen Erfolgsfaktoren für eine integrierte IT-Strategie, die auch erfolgreich umgesetzt werden kann, ist zu Beginn außerordentlich nützlich. Als kritische Erfolgsfaktoren bezeichnet man dabei im Allgemeinen solche Erfolgsfaktoren, die zwingend oder ganz dringend erfüllt sein müssen, um die gesetzten Ziele erreichen zu können. In der Literatur bezeichnet man die „kritischen Erfolgsfaktoren“ oder „Critical Success Factors“ (CSF) auch anders, z.B. als Schlüsselfaktoren, strategische Variablen oder strategische Prinzipien. Eine besondere Aufgabe besteht darin, aus den vielen Faktoren die relevanten herauszufiltern, weil die Faktoren hinsichtlich der Relevanz unternehmensindividuell sind.

Zweck der **Erfolgsfaktorenanalyse** ist die Beschaffung von Information für die strategische IT-Planung, insbesondere die strategische Maßnahmenplanung. Mit dieser Zwecksetzung ist sie ein Instrument des strategischen IT-Controllings, dessen primäre Aufgabe in der Informationsbeschaffung für das Top-Management gesehen wird. Die für das Verständnis der Methodik wesentlichen Begriffe sind Erfolgsfaktor, Priorität, Leistung und Erfolg; alle weiteren Begriffe leiten sich daraus ab (z.B. Leistungsdifferenz als Differenz zwischen Priorität und Leistung). Im Sinn der strategischen Unternehmensplanung ist die IT ein strategisches Erfolgsobjekt, jede ihrer Komponenten (z.B. Hardware, Anwendungssoftware, Datenhaltung und Personal) ist Teilobjekt. Eine Eigenschaft dieser Objekte bzw. Teilobjekte, die einen Einfluss auf die Schaffung und/oder Erhaltung von Unternehmenserfolg hat, wird als Erfolgsfaktor bezeichnet (genauer gesagt also als IT-Erfolgsfaktor).

Allgemein lässt sich die erfolgreiche **Ausrichtung der IT an den Geschäftszielen** über drei zentrale Fragestellungen treffend charakterisieren:

- Wie kann eine strategische IT-Steuerung das Geschäft des Unternehmens verbessern und somit den Unternehmenswert erhöhen?
- Ist die IT im Unternehmen so positioniert, dass entsprechende Infrastrukturen, Lösungen und Services optimal operieren?
- Sind die eingesetzten IT-Architekturen, die Organisationsformen und die IT-Prozesse an den strategischen Vorgaben ausgerichtet und werden diese „richtig“ und erfolgreich ein- bzw. umgesetzt?

2.2.2 Situationsanalysen

IT-Situationsanalysen liefern eine umfassende Sicht der IT-Situation im Unternehmen aus fachlicher, technischer und organisatorischer Sicht. Dabei wird

- der erreichte Stand skizziert,
- eine Standortbestimmung vorgenommen und
- der Handlungsbedarf aus Sicht der Fachbereiche und der IT Organisation für die Bewältigung der erkannten Herausforderungen der nächsten 3–5 Jahre aufgezeigt.

Hilfreich sind hier übersichtliche Darstellungen des **IST-Zustands des Unternehmens und der IT** zum Beispiel in Form von Verzeichnissen/Tabellen und Beschreibungen für

- Unternehmenspolitik, Unternehmensstrategie
- Managementsysteme
- Kunden, Lieferanten, andere Geschäftspartner
- Produkte und Dienstleistungen
- Geschäftsprozesse
- Unternehmens-Ressourcen
- (derzeitige) IT-Politik und IT-Strategie
- IT-Kunden und sonstige Partner
- IT-Produkte und IT-Dienstleistungen
- IT-Prozesse
- IT-Personal (Anzahl und Qualifikation)
- IT-Ressourcen (Daten, Software, Hardware, Netzwerke)
- IT-Richtlinien
- IT-Projekte in Arbeit
- Kosten, Nutzen, Wirtschaftlichkeit der IT
- Maßnahmenlisten für Verbesserungen aller Art

Nachdem der Ist-Zustand abgeklärt ist und erste Analysen dazu erfolgt sind, können mittels der so genannten SWOT-Analyse alle Gegebenheiten bewertet werden. SWOT steht als Akronym für Strengths, Weaknesses, Opportunities und Threats (auf Deutsch: **Stärken, Schwächen, Chancen, Risiken**):

- Es ist ein bewährtes Werkzeug des strategischen Managements, das sowohl innerbetriebliche Stärken und Schwächen (Strength-Weakness) als auch externe Chancen und Gefahren (Opportunities-Threats) betrachtet.
- Aus der Kombination der Stärken/Schwächen-Analyse und der Chancen/Gefahren-Analyse kann eine ganzheitliche IT-Strategie abgeleitet werden. Die Stärken und Schwächen sind dabei relative Größen und lassen sich erst im Vergleich mit den Zielkriterien beurteilen.

Den Zusammenhang zeigt Abbildung 2.5.

Handlungbedarf bzgl. IT ergibt sich aus ...

- 1) Ausbau von (bestehenden) Stärken
- 2) Abbau von Schwächen
- 3) Nutzen von (künftigen) Chancen
- 4) Bekämpfen von Risiken

und zwar jeweils im Hinblick auf ...

das Unternehmen
(Produkte, Prozesse,
Ressourcen etc.)

die IT
(Produkte, Prozesse,
Ressourcen etc.)

ABBILDUNG 2.5
SWOT-Analyse

Den Kern der SWOT-Analyse bilden Fragen, die auf die Zuordnung der Ergebnisse zu den vier skizzierten Bereichen abzielen. Tabelle 2.2 zeigt diese Fragen in Checklistenform zu den jeweiligen Bereich.

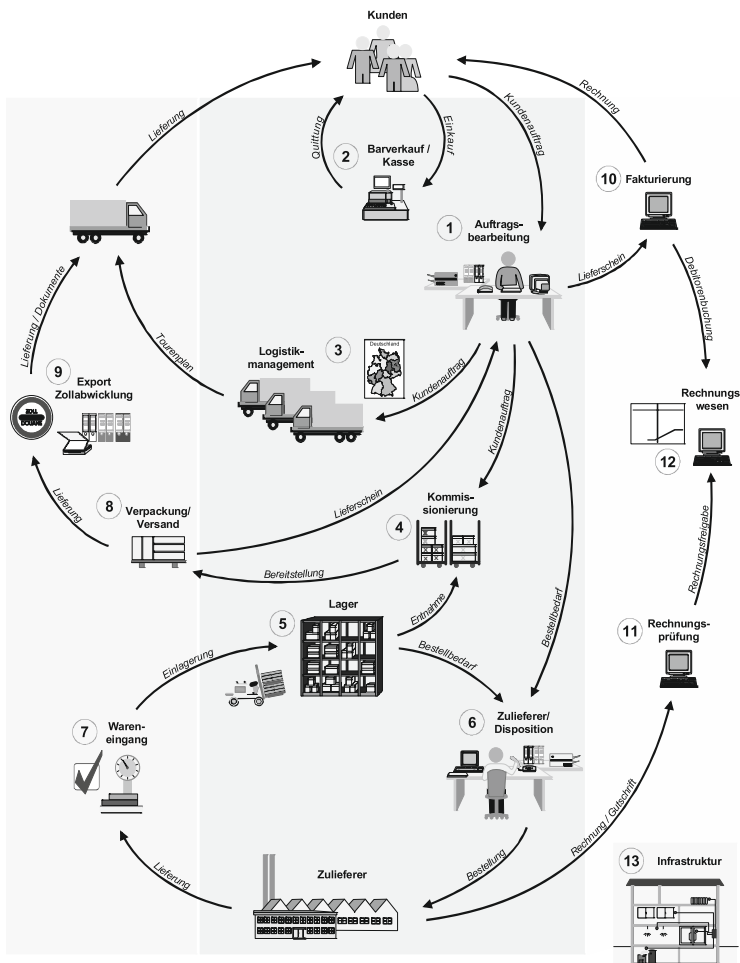
TABELLE 2.2 SWOT-Analyse (Fragen)

S	Strengths Stärken	▪ Gibt es besondere Verfahren und Ergebnisse, die in der vergangenen Periode hervorragend waren (IT-Services, IT-Prozesse, IT-Projekte)? ▪ Was sind unsere Stärken (IT-Produkte, Personal, Organisation)? ▪ Worauf sind wir stolz (Ergebnisse, Qualität)?
W	Weaknesses Schwächen	▪ Was ist/war schwierig? ▪ Wo liegen typische Barrieren, um erfolgreich agieren zu können (Mitarbeiterqualifikation, Finanzen etc.)? ▪ Welche Störungen behinderten in der Vergangenheit die Arbeit im IT-Bereich (personelle Fluktuationen etc.)? ▪ Woran fehlt es aktuell, um erfolgreich IT-Produkte und IT-Services zu erbringen (z. B. fehlende Unterstützung durch Führungskräfte)?
O	Opportunities Chancen	▪ Wo liegen unsere Zukunftschancen (neue Technologien, innovative IT-Projekte)? ▪ Was können wir im IT-Bereich ausbauen (neue Produkte)? ▪ Welche konkreten Verbesserungsansätze werden gesehen (verbesserte IT-Services)?
T	Threats Risiken	▪ Was sind mögliche Risiken/kritische Faktoren beim Einsatz der IT-Produkte und der Umsetzung der IT-Projekte (rechtlich, technisch, wirtschaftlich)? ▪ Womit müssen wir rechnen? ▪ Wo lauern künftig noch Gefahren bzw. Risiken?

**Beachten Sie:**

Für die Beantwortung der Fragen im Rahmen einer SWOT-Analyse bietet sich ein Workshop an. Der Teilnehmerkreis könnte sich aus dem IT-Leiter und den Gruppenleitern oder einem interessierten Kreis von IT-Mitarbeitern zusammensetzen.

Die **fachliche Beurteilung** liefert eine Einschätzung der IT-bezogenen Dienstleistungen und der IT-Ressourcen, bezogen auf den Beitrag zum Erfolg der Gesamtorganisation sowie der Schlüsselanforderungen für die Bewältigung der Herausforderungen an die Organisation. Eine fachliche Beurteilung der Informationssysteme bedingt eine betriebswirtschaftliche Sichtweise. Diese lässt sich nur dann erreichen, wenn die Betrachtungen, Diskussionen, Workshops und Analysen von einem Unternehmensmodell ausgehen. Vorzugsweise wird eine prozessorientierte Darstellung gewählt, die den Untersuchungsbereich und sein Umfeld zeigt. Ein Beispiel für eine übersichtliche Darstellung eines Gesamtprozesses gibt Abbildung 2.6 [SCH03].

**ABBILDUNG 2.6**

Beispiel für eine Prozessübersicht „Handel“

Tabelle 2.3 zeigt beispielhaft die betriebswirtschaftliche Darstellung eines Handels-Unternehmens, basierend auf einem **prozessorientierten Unternehmensmodell**.

TABELLE 2.3 Beispiel für Prozessliste und unterstützende Systeme „Handel“

	Geschäftsprozess	unterstützende Systeme
1	Auftragsbearbeitung	▪ Vertriebsunterstützung, Auftragsbearbeitung ▪ Bestellsannahme über DFÜ vom Kunden ▪ Systeme für Internet-Anbindung/Electronic Commerce ▪ Preisbildung ▪ Bonitätsprüfung
2	Barverkauf/Kasse	▪ POS-Systeme, Kassen, Scanner ▪ Systeme zur Zahlung per Kreditkarte/ec-Karte ▪ Schnittstelle zur Finanzbuchhaltung ▪ Diebstahls-Schutzanlagen
3	Logistikmanagement	▪ Routenplanung ▪ Mobile Bordcomputer, GPS-Systeme ▪ Tankkarten
4	Kommissionierung	▪ Kommissionier-Terminal/Scanner ▪ Lagerzugriffssteuerung
5	Lager	▪ Lagerverwaltungsrechner ▪ elektronische Waagen ▪ Steuerung von Regalfördergeräten/Verteilsystemen ▪ Klimaanlage und Kühlsysteme ▪ Bestandsüberwachung ▪ Inventur ▪ Konsignationslager
6	Zulieferer/Disposition	▪ Bestellabwicklung ▪ Prognosesysteme ▪ Kommunikation per Fax/E-Mail/EDI ▪ Bestellüberwachung
7	Wareneingang	▪ Barcode-Scanner/RFID im Wareneingang ▪ Prüf- und Messeinrichtungen
8	Verpackung/Versand	▪ Versandsteuerung/-unterstützung ▪ Verpackungs-, Frankier- und Etikettier-Systeme ▪ Track & Trace-Systeme
9	Zollabwicklung	Software für die Import-/Export-, Zoll- und Frachtabwicklung
10	Fakturierung	Rechnungsschreibung
11	Rechnungsprüfung	Zahlungsfreigabe
12	Rechnungswesen	▪ Debitorenbuchhaltung ▪ Kreditorenbuchhaltung ▪ automatische Abwicklung des Zahlungsausgangs ▪ Anlagenbuchhaltung

Das Unternehmensmodell dient als „Kommunikationsdrehscheibe“ zum Fachbereich. Es ermöglicht, die Charakteristik des Geschäftes zu diskutieren, Außenbeziehungen darzustellen, Veränderungen zu positionieren und die Unterstützung mit Informatiksystemen zu visualisieren. Durch ein Unternehmensmodell werden die Diskussionen in Interviews und Workshops „kundenorientiert“ und umfassend. Es wird gewährleistet, dass sämtliche (auch aktuell nicht mit Informatik unterstützten) Bereiche besprochen und bewertet werden.

Die **technische Beurteilung** liefert, eingebunden in ein standardisiertes Raster, die technische Beschreibung und Beurteilung der Anwendungslandschaft, des Anwendungs-Designs sowie der technischen Infrastruktur und der betrieblichen Methoden und Hilfsmittel.

Die **organisatorische Beurteilung** der IT liefert eine Analyse sämtlicher Informatik-relevanter Prozesse der Organisation. Sie liefert eine Übersicht und eine Beurteilung der gewählten organisatorischen Lösungen, des erreichten Organisationsgrades, der Mengengerüste und des Ressourceneinsatzes (Personal, Finanzen und kritische Ressourcen).

Hilfreich für das Herausfinden des Handlungsbedarfs sind Aussagen zu folgenden Satzanfängen:

- „Wir wollen weg von ...“

- „Wir wollen hin zu ...“

– und zwar im Hinblick auf die Betrachtungsgegenstände einer IT-Strategie. Ein Beispiel finden Sie in Abbildung 2.7.

Wir wollen weg von ...	Wir wollen hin zu ...
... einer Vielzahl von Individual-Anwendungen (teils extern, meist intern entwickelt)	... einem ERP-System. Damit können wir den klassischen Vorteil eines ERPS, nämlich die starke Integration der Bestandteile, voll ausspielen. Was nicht durch ein ERPS abdeckbar ist, wird durch andere Standardprodukte gelöst.
... einfache Verteilung von Standard Office Produkten	... aus den Standardprodukten einen "Mehrwert" für die Stadt generieren, indem wir maßgeschneiderte Varianten daraus erzeugen (Praxistauglichkeit erhöhen, CD-Vorlagen einarbeiten etc.).

ABBILDUNG 2.7 Beispiele für Handlungsbedarf bzgl. IT

**Beachten Sie:**

Aufgrund der rapide fortschreitende Entwicklungen der Informations- und Kommunikationstechnologien wird von den IT-Verantwortlichen eine hohe Sensibilität für Innovationen (Produkt- und Verfahrensinnovationen) in Bezug auf die Einsetzbarkeit und Zukunftsperspektive der installierten bzw. der möglichen Informations- und Kommunikationstechnologien gefordert. Um diese Herausforderungen bestehen zu können, muss bei der IT-Leitung eine gute Einschätzbarkeit der Bedeutung der Innovationen für das Unternehmen sowie bei den weiteren Beteiligten im IT-Strategieentwicklungsprozess eine gewisse Spezialisierung einzelner Mitarbeiter gegeben sein (etwa eine Spezialisierung auf bestimmte Architekturdomänen oder auf ausgewählte IT-Prozesse und IT-Systeme). Es empfiehlt sich darüber hinaus, ergänzend bei der Entwicklung einer IT-Strategie den Blick auf IT-Trends und generelle Entwicklungen der Branche ebenso zu richten wie auf die aktuell – vor allem zuletzt – eingesetzten Technologien im Unternehmen. Dies erfolgt sinnvollerweise unter Einbeziehung von IT-Experten sowie in Abstimmung aller Teilbereiche der IT-Abteilung.

2.2.3 Umfeldanalyse

Mittels einer Umfeld- und Technologieanalyse werden die möglichen Entwicklungen innerhalb und im Umfeld des Unternehmens betrachtet. Die Umfeldanalyse liefert eine umfassende, vernetzte Analyse der möglichen Veränderungen, die das Unternehmen betreffen. Sie beurteilt sie auf ihre Relevanz, ihre Eintrittswahrscheinlichkeit und die möglichen Auswirkungen aus IT-Sicht. Hauptquellen für die Umfeldanalyse sind Expertenaussagen, Workshops mit dem Management sowie die Ergebnisse der Situationsanalyse. Auch Partner, Kunden und Lieferanten können wertvolle Beiträge leisten. Die identifizierten möglichen Veränderungen (elements of change) werden kategorisiert und bezüglich ihrer Relevanz für die IT-Tätigkeit des Unternehmens beurteilt.

Die **internen Aspekte** beschreiben das Veränderungspotenzial, das aus dem Unternehmen selbst stammt. Es kann sich dabei sowohl um erkannte Entwicklungen (passiv) als auch um mögliche aktive Veränderungen, zum Beispiel Reorganisationen, Veränderungen des Tätigkeitfeldes, Aufbau von neuen Bereichen etc., handeln.

Die **externen Aspekte** beschreiben das Veränderungspotenzial, das außerhalb des Unternehmens liegt, zum Beispiel gesetzliche Veränderungen, Veränderungen der Branche, Verfügbarkeit von Ressourcen – speziell der richtigen Mitarbeiter in Qualität und Quantität – sozial-klimatische Veränderungen etc.

Die **technologischen Aspekte** zeigen die relevanten technologischen Veränderungen, einerseits in Form von „Enablers“, die neue Lösungen ermöglichen, andererseits von Veränderungen, die antizipiert werden müssen.

Ein praktisches Hilfsmittel dabei stellt die so genannte **IT-Landkarte** dar (Abbildung 2.8, nächste Seite).

Die IT-Landkarte fasst die wichtigsten informationstechnologischen Entwicklungen aus der Sicht eines Prozesses zusammen. Sie ist ein Instrument, um die für einzelne Prozesse rele-

vanten Informations- und Kommunikationstechniken zu sammeln, deren Zusammenwirken zu betrachten, die Techniken nach ihrem Entwicklungsstand zeitlich zu positionieren und Schwerpunkte zu erkennen oder zu bilden.

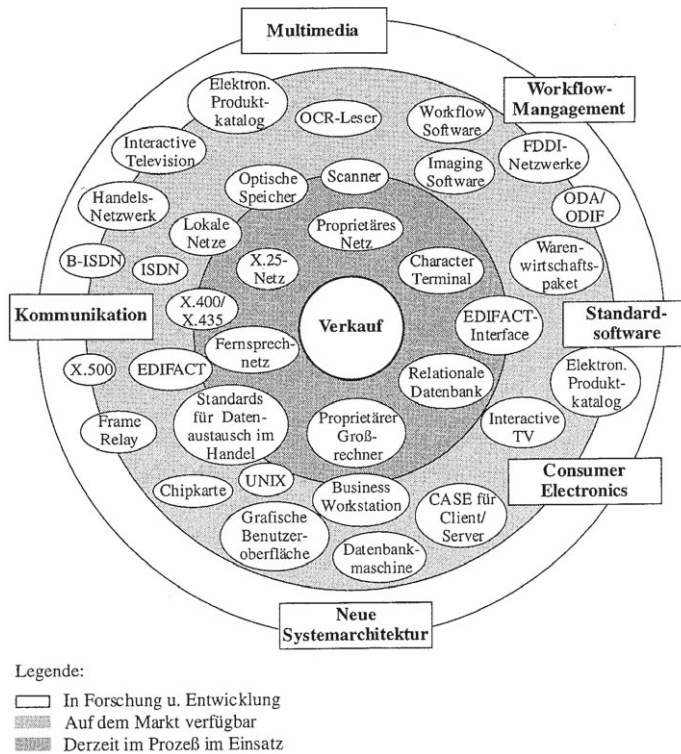


ABBILDUNG 2.8
Beispiel einer IT-Landkarte
für den Prozess „Verkauf“

2.2.4 Zielfindung

Die Ziele und Rahmenbedingungen enthalten die Anforderungen und einzuhaltenden Rahmenbedingungen für die konzeptionelle Ebene. Das Ziel besteht darin, eine gemeinsame, widerspruchsfreie Basis für die Strategiefindung, die Architekturdefinition und die Priorisierung der Projekte zu liefern. Bei den periodischen Überprüfungen der Planungen soll das Zielsystem ermöglichen, mittels einer Abweichungsanalyse wesentliche „Richtungsänderungen“ erkennen zu können. Abbildung 2.9 zeigt die Zusammenhänge, die bei der Analyse und bei der Auswertung der verschiedenen Quellen zu berücksichtigen sind.

Abbildung 2.9 zeigt, dass die Ziele und Rahmenbedingungen der IT aus den Zielen und Rahmenbedingungen des Unternehmens, der Umfeld- und Technologie-Analyse sowie der Situationsanalyse gewonnen werden. Damit wird die führende Rolle der unternehmerischen Zielsetzungen sichergestellt und die Konsistenz des Zielkatalogs gewährleistet.

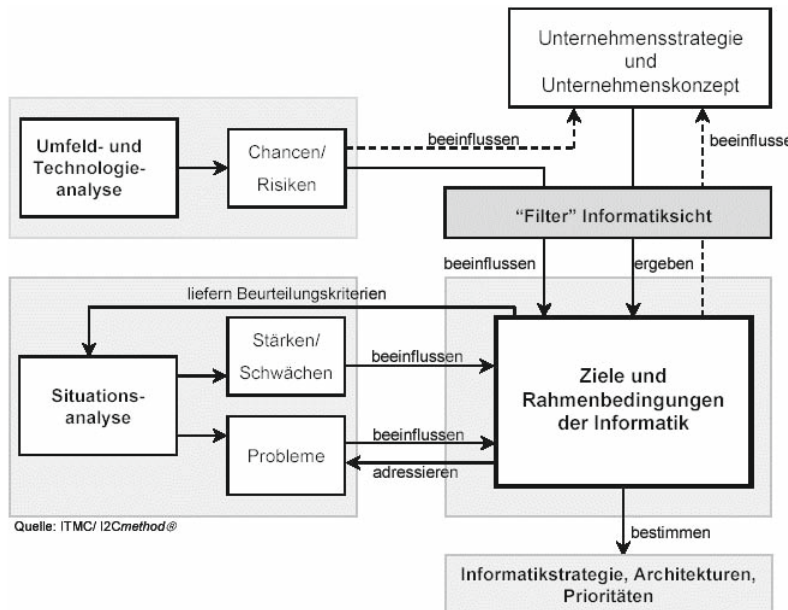


ABBILDUNG 2.9 Zielfindung – Zusammenhänge zwischen den Elementen der strategischen IT-Planung

Ziele können nicht formuliert werden, ohne dass klar ist, ob diese Ziele überhaupt und – insbesondere – wie sie erreichbar sind. Wichtig bei der Formulierung von Zielen ist darüber hinaus die Fähigkeit, die Erreichung der Ziele zu messen. So können eventuelle, zur Erreichung der Ziele eingeleitete Maßnahmen auf ihre Wirkung hin überprüft werden.

Ausgehend von den strategischen Herausforderungen sollten die IT-Verantwortlichen (ggf. unterstützt durch einen neutralen IT-Berater) im Rahmen eines Workshops die strategischen IT-Ziele des Unternehmens entwickeln bzw. anpassen. Ein weiteres Ergebnis des Workshops sind eine eventuell erforderliche Aktualisierung der Qualitäts- und Risikopolitik und die aktuellen Qualitätsziele der IT für das laufende Jahr.

Die Beispiel-Ergebnisse eines entsprechenden strategischen Zielworkshops zeigt die folgende verdichtete Übersicht:

TABELLE 2.4 Strategische IT-Zielsetzungen (nach BSC-Systematik)

Zielbereiche	Zielsetzungen
Finanzielle Ziele	▪ Umsatzrentabilität pro Jahr erzielen (5–6 Prozent) ▪ Leistung- und Kostentransparenz verbessern und Kosten steuerbar machen ▪ Kosteneffizienz halten ▪ Risiko- und Innovationskapital bereitstellen
Kundenziele	▪ Hohe Kundenzufriedenheit herstellen ▪ Kundenbindung erhöhen ▪ Qualität der Anforderungsspezifikation der Kunden verbessern

Zielbereiche	Zielsetzungen
Prozess-Ziele (IT-Service-Ziele)	▪ Reifegrad der IT-Service-Prozesse erhöhen ▪ Nutzungsgrad des Service-Desks erhöhen ▪ Prozesserfolge sichern und dokumentieren (Performance-Management) ▪ Hohe Sicherheit der Prozesse gewährleisten
Personalziele	▪ Mitarbeiterzufriedenheit erhöhen ▪ Kompetenz der Mitarbeiter fördern ▪ IT-Serviceorganisation als attraktiver Arbeitgeber (intern und extern) darstellen
Ziele zu den IT-Produkten	▪ Produkt-Portfolio erweitern ▪ Produktinnovationsgrad erhöhen ▪ IT-Landschaft (Applikationen, Prozesse, Infrastrukturen) mit Augenmaß konsolidieren ▪ Asset-Ownership durch die IT-Organisation übernehmen und erweitern
Ziele zu den IT-Projekten	▪ Projekterfolgsquote erhöhen ▪ Termintreue erhöhen (Erreichung der Meilensteine)

2.2.5 Strategische Grundsätze zur IT-Ausrichtung

Zunächst sollten wir uns daran erinnern, dass die so genannten **allgemeinen strategischen Grundsätze** auch im IT-Bereich nützlich sein können, zum Beispiel:

- Konzentration der Kräfte
- Einfachheit
- Stärken fördern
- Ziele und Mittel abstimmen
- Synergiepotenziale ausnutzen

Dann sollten wir daran gehen, für alle Betroffenen verständliche Strategie-Grundlagen zu formulieren.

Die **Vision der IT** im Unternehmen könnte beispielsweise lauten:

Die IT leistet einen gut sichtbaren, wichtigen Beitrag zum Unternehmenserfolg durch

- Erhöhung der Kundenbindung oder
- Stärkung der Kostenführerschaft oder ...

Daraus könnte zum Beispiel folgende **Mission der IT** abgeleitet werden:

Das IT-Management sorgt auf wirtschaftliche Weise für zufriedene IT-Kunden mittels attraktiver IT-Produkte und effektiver IT-Prozesse, die mittels optimaler IT-Ressourcen in guten Strukturen nachhaltig erbracht werden.

Die Basisstrategie zeigt in knapper, allgemeinverständlicher Form, wie die IT im Unternehmen positioniert ist, wie die Zielsetzungen unter bestmöglicher Nutzung der Chancen und Stärken erreicht sowie die erwarteten Risiken und bestehenden Schwächen beherrscht

werden sollen. Sie definiert die Stoßrichtung zum Aufbau künftiger Erfolgspotenziale mit einem Planungshorizont von 3–5 Jahren.

Die **Steuerung der IT im Unternehmen** soll in erster Linie über betriebswirtschaftliche Steuerungsgrößen erfolgen, namentlich Qualität, Wirtschaftlichkeit, Effektivität und Flexibilität. Abbildung 2.10 zeigt ein Modell der Steuerung der IT. Zu den Aufgaben der strategischen IT-Planung gehört sowohl, darüber nachzudenken, *was* künftig erforderlich ist, als auch darüber, *wie* die Ziele erreichbar sind.

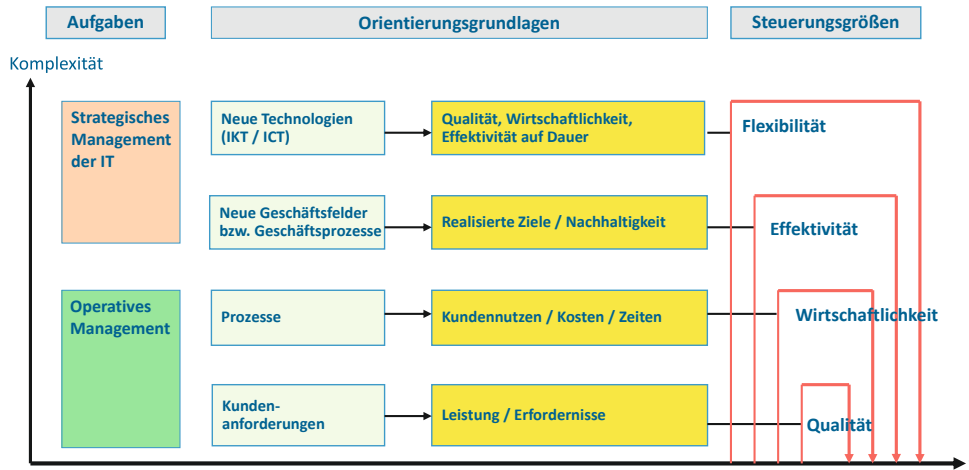


ABBILDUNG 2.10 Modell zur Steuerung der IT in einem Unternehmen



Beachten Sie:

IT-Mission und IT-Vision enthalten die allgemein gültigen Grundsätze über angestrebte Ziele und Verhalten des IT-Bereiches, an denen sich alle IT-bezogenen unternehmerischen Tätigkeiten orientieren sollten. Sie sind die Grundlage für die Entwicklung einer Strategie mit einer klaren und messbaren Zielsetzung. Der Hauptnutzen von IT-Mission und IT-Visionen lässt sich also vor allem darin sehen, Referenzpunkte für die strategische IT-Entwicklung zu liefern. Wichtig ist, dass bereits IT-Mission und IT-Vision auf die Unternehmensstrategie Bezug nimmt und nicht völlig losgelöst von der Unternehmensstrategie entstehen.

2.2.6 IT-Teilstrategien definieren

Je nach Ausrichtung und Organisation des IT-Bereichs ist es sinnvoll, dass präzisere strategische Festlegungen zu bestimmten Bereichen erfolgen. Typische Teilstrategien sind beispielsweise

- **IT-Servicestrategien** (Festlegung der Art und Qualität der IT-Services, Optimierung der Serviceprozesse etc.)

- **IT-Sourcingstrategien** (beispielsweise Grundsatzentscheidungen zum Outsourcing oder strategisches Lieferantenmanagement)
- **IT-Personalstrategien** (insbesondere strategische Personalbeschaffung und Personalentwicklung)

Die stark wachsende Bedeutung des IT-Servicemanagements sowie die Entwicklung der IT-Servicestrategien sind offensichtlich, wenn man sich vergegenwärtigt, dass eine funktionierende IT heute in Unternehmen und Verwaltungen gewissermaßen das Rückgrat für die Geschäftsprozesse bildet. Ausfälle von IT-Systemen führen zu erheblichen Konsequenzen und wirtschaftlichen Schäden, die nicht zuletzt auch das Image der IT und des Unternehmens insgesamt gefährden. Notwendig ist daher eine klare Ausrichtung der IT-Services und die nachhaltige Planung und Steuerung der Prozesse.

Für die Entwicklung des Teilkonzeptes „IT-Servicestrategien“ ist eine Potenzialanalyse mit Reifegradmessung zu den verschiedenen Serviceprozessen nötig, aus dem dann ein Maßnahmenkatalog entwickelt wird. Die Reifegradmessung bewertet die Funktionalität und Qualität des bestehenden IT-Service-Managements sowie seine Bedeutung für die Unterstützung der Kerngeschäftsprozesse im Unternehmen – entsprechend den Empfehlungen des Capability Maturity Model (CMM). Ein Soll-Ist-Vergleich zeigt die Schwachstellen und Optimierungspotenziale für das IT-Service-Management auch in Bezug auf ITIL auf.

Zur Vorbereitung des strategischen Servicekonzeptes empfiehlt es sich, vorab verschiedene Analysen durchzuführen. Diese Analysen sollten sich beziehen auf

- die bestehende Organisationsstruktur,
- eine Analyse der in den IT-Prozessen anfallenden Daten,
- die Struktur und Kompetenz des IT-Personals,
- die vorhandenen IT-Prozesse sowie
- die bestehenden Services und die unterstützende IT-Infrastruktur.

Die Analysen identifizieren auch die Schwachstellen und Anforderungen, um eine Informationsbasis für strategische Festlegungen zu dokumentieren. Im Strategiekonzept zu den IT-Services wird ausgehend von den Analyseergebnissen die grundsätzliche Vorgehensweise auf dem Weg zu einer ITIL-konformen Organisation definiert. Hierbei werden Zeithorizonte, Verfahren und Kosten beschrieben sowie der Return on Investment ermittelt. Der daraus resultierende Maßnahmenkatalog enthält die priorisierten Schritte zur Erweiterung und Neuorganisation der IT, um zum gewünschten Ziel zu gelangen. So wird das Strategie- und Verfahrensmodell (Masterplan) für das IT-Service-Management definiert. Dieser beschreibt primär die Soll-Prozesse und die IT-Organisation. Darüber hinaus werden die Verantwortlichkeiten im IT-Servicebereich nach den unternehmensspezifischen Anforderungen geregelt.

Jeder Prozess – auch jeder Serviceprozess – sollte einer kontinuierlichen Verbesserung unterzogen werden (KVP, kontinuierlicher Verbesserungsprozess), sonst sinkt der Reifegrad schnell wieder ab. Das unabdingbare Ziel der guten Dokumentation und deren fortwährenden Aktualisierung gilt daher nicht nur für die IT, sondern auch und gerade für Prozesse.

**Beachten Sie:**

Als wesentliche Erfolgsfaktoren für die Einführung einer zukunftsorientierten Lösung für das IT-Servicemanagement (also der IT-Service-Strategie) können genannt werden: ausgeprägtes Rollenkonzept, Einsatz umfassender ganzheitlicher Tools (zur Vermeidung von Insellösungen), ganzheitlich ausgerichtete Qualifikation des Personals im IT-Bereich (Schulung ITIL und Rollout) sowie ein entsprechendes Management Commitment und fördernde Unternehmenskultur (Servicekultur).

2.2.7 IT-Applikations-Architektur planen

Die Architekturen liefern für alle relevanten Planungsbereiche der IT konkrete, gegenseitig abgestimmte Konzepte bzw. „Bebauungspläne“ fachlicher und technischer Art, die zeigen, wie die Strategie realisiert werden soll.

In vielen Fällen zeigt sich, dass IT-Management maßgeblich zum Innovationsmanagement im Unternehmen wird. Ziel der IT-Applikations-Architekturgestaltung sind neue geschäftliche Lösungen, die den Kundennutzen erhöhen und/oder die Kosten senken.

Hilfreiche Fragen:

- Wie können wir mit Hilfe der IT neue Wege gehen?
- Wie können wir mit Hilfe der IT alte Aufgaben besser bewältigen?

Auf der Suche nach idealen IT-Applikationen bietet Davenport mit seinen **neun Kategorien von Potenzialen der Informatisierung** interessante Ansatzpunkte:

- *Automational*: Ersatz menschlicher Arbeitskraft durch Computer
- *Informational*: Führung anhand von Prozessgrößen
- *Sequential*: Veränderung der Ablauffolge oder Parallelisierung von Aufgaben
- *Tracking*: Maschinelle Verfolgung von Geschäftsvorfällen
- *Analytical*: Verbesserung der Entscheidungsfindung
- *Geographical*: Koordination von Prozessen über Distanzen
- *Integrational*: Sammlung, Kommunikation und Bereitstellung betrieblichen Wissens zur übergreifenden Integration des im Betrieb vorhandenen Know-hows
- *Intellectual Potential*: Sammlung, Kommunikation und Bereitstellung betrieblichen Wissens im Sinne der betrieblichen Erfahrung
- *Disintermediating*: Ausschalten von Zwischenstufen in Prozessen

So kann man sagen: Investitionen in IT lohnen sich dann, wenn möglichst viele der genannten Punkte möglichst intensiv zum Tragen kommen. So lässt sich auch gut erklären, warum beispielsweise überbetriebliche Prozessoptimierung in Form von Electronic Business Networking besonders attraktiv ist.

Die **Applikationsarchitektur** beschreibt die Konzeption der fachlichen Lösungen und besteht aus den beiden Bausteinen „Funktionalität“ und „System-Design“.

Die **Funktionalität** beschreibt die Soll-Applikations-Landschaft aus zwei Sichten. Die Anwendersicht dient der Darstellung der Soll-Funktionalität der Anwendungen, bezogen auf die Unternehmensprozesse. Die technische Sicht zeigt die Systeme aus IT-Sicht mit ihren Bausteinen, ihrem Zusammenwirken sowie der datenmäßigen Integration.

Das **System-Design** zeigt die Design-Prinzipien und genutzten Standards beim Aufbau der Applikationen, inklusive der Positionierung und Integration eingekaufter Komponenten.

Das **Informationssystem eines Unternehmens** ist die Gesamtheit der Applikationen, Datenbanken und zugehörigen organisatorischen Regeln (siehe Abbildung 2.11). Das Informationssystem dient der Aufnahme, Verarbeitung, Speicherung und Abgabe betrieblich relevanter Informationen zur Unterstützung der Aufgabenausführung im Hinblick auf Zeit, Qualität, Kosten und Flexibilität.

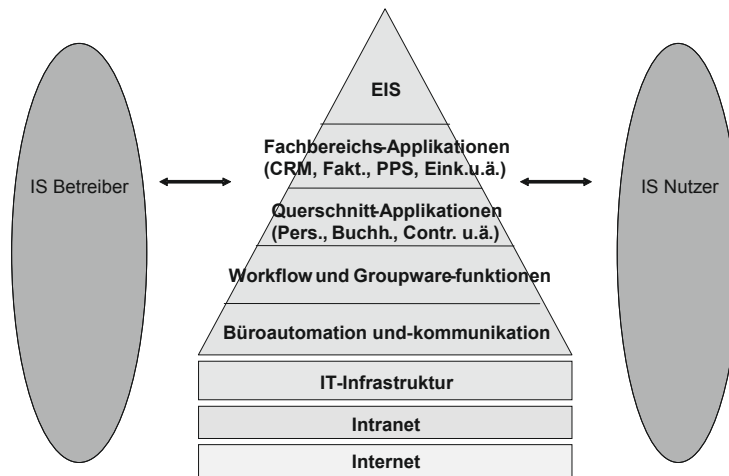


ABBILDUNG 2.11
Modell eines umfassenden Informationssystems

Vom Wunsch, eines Tages ein umfassendes, integriertes, konsistentes und in allen Aspekten einheitliches Informationssystem zu haben, musste man sich im Laufe der Jahre verabschieden. Vielmehr musste und muss man sich auf eine äußerst heterogene Systemlandschaft, bestehend aus unterschiedlichsten Subsystemen verschiedenartigster Herkunft, einstellen, was die Benutzung nicht gerade einfacher macht und den Betrieb und die Weiterentwicklung vielfach vor große Herausforderungen stellt.

2.2.8 Soll-Daten-Architektur dokumentieren

Daten sind der „Rohstoff“ für die Informationsgewinnung. Immense Datenmengen werden erfasst, gespeichert, verarbeitet und übertragen. Neben Schrift gibt es immer mehr Bild und Ton zu berücksichtigen. Da lohnt es sich schon, von Zeit zu Zeit die eigenen Praktiken zu hinterfragen und verbindliche Standards für den Umgang mit Daten festzulegen.

Nachfolgend einige wichtige **Fragen**, die in diesem Zusammenhang zu stellen sind:

- Welchen Umfang haben unsere (gesamten) Daten?
- Gibt es ein Verzeichnis aller Daten (Datenbanken/Datenbestände) des Unternehmens?

- Gibt es eine Klassifikation der Daten nach der Bedeutung für das Unternehmen?
- Ist sichergestellt, dass alle Daten Eigner haben?
- Ist geklärt und schriftlich festgehalten, welche Pflichten/Rechte ein Daten-Eigner hat?
- Ist geklärt und schriftlich festgehalten, wie für die Korrektheit, Vollständigkeit und Redundanzfreiheit der Daten gesorgt wird?
- Wie ist die Datenverwendung geregelt?
- Gibt es Regelungen im Hinblick auf die Datenspeicherung (was, wo, wie, wie lange ...)?
- Was gibt es zum Datenzugriff via Internet zu sagen?
- Welche (IT-)Mittel werden eingesetzt, um den Benutzern einen einfachen und sicheren Zugang zu den Daten/Informationen zu ermöglichen (z.B. Datawarehouse, Portal, Intranet)?

Und anderes mehr.

2.2.9 Soll-Technologie-Architektur entwickeln

Die **Technologie-Architektur** zeigt die Elemente der technischen Basissysteme, die technischen Konzepte, Standards und Produktvorgaben. Die IT-Architektur muss so gestaltet sein, dass sie einerseits den Anforderungen seitens der IT-Nutzer entspricht, andererseits aber auch den Anforderungen der Interoperabilität – intern und extern – sowie den Erfordernissen der Sicherheit und Wirtschaftlichkeit genügt.

Wichtige **Fragen** in diesem Zusammenhang sind beispielsweise:

- Welche Grundsätze sollen hinsichtlich des Innovationsgrades gelten? („Leader“, „Early follower“, „Cheapest“ ...)
- Welcher Zentralisierungs-/Dezentralisierungsgrad wird angestrebt?
- Welches Sourcing wird angestrebt?
- Lease or buy?
- Wie soll mit Einheitlichkeit/Heterogenität umgegangen werden?
- Welcher Integrationsgrad von Informations- und Kommunikationstechnik ist zweckmäßig?
- Welche Reserven sollen vorgehalten werden?

2.2.10 Sicherheitsarchitektur

Die **Sicherheitsarchitektur** zeigt die Sicherheitskonzepte über alle Ebenen des IT-Einsatzes hinweg. Sie stellt ein mit den übrigen Architekturen harmonisiertes Konzept dar.

Wichtige **Fragen**:

- Wie steht es um eine ausformulierte Sicherheitspolitik?
- Welche Bedeutung hat die Informationssicherheit für das Unternehmen?
- Wer sorgt für die Umsetzung der Sicherheitspolitik/-strategie?
- Welches sind die Eckpunkte des Sicherheitskonzepts?

- Welche Bedrohungen sind relevant?
- Welche Technologie löst uns welches Problem?
- Welche Vorkehrungen sind in der Applikation selbst zu treffen?
- Wie lässt sich Sicherheit im Betrieb effizient managen?
- Mit welchen Ausbildungsmaßnahmen unterstützen wir die Mitarbeitenden in dieser Thematik?

Und anderes mehr.

Hinweis: Ausführliche Darlegungen zur Sicherheitsarchitektur von IT-Systemen finden Sie in Kapitel 3 (Enterprise Architecture Management).

2.2.11 IT-Prozesse vereinbaren und IT-Prozesslandschaft weiterentwickeln

Die IT-Prozesse sind aus der Sicht eines Unternehmens „unterstützende Prozesse“. Ziel muss es also sein, die „wertschöpfenden“ Geschäftsprozesse durch die IT-Prozesse optimal zu unterstützen – was eine entsprechende Wirtschaftlichkeit mit einschließt.

Eine effektive und effiziente Organisation der IT erfordert natürlich auch adäquate Abläufe in Form von IT-Geschäftsprozessen. Über ihre Ausgestaltung werden auf der operativen Ebene Möglichkeiten und Grenzen der IT im Hinblick auf Innovationen, Veränderungen, Service-Leistungen, Beziehungen zu Fachabteilungen und zu Lieferanten/Sourcing-Partnern, Skills (Potenziale von IT-Mitarbeitern und IT-Tools) und Administration (z. B. IT-Controlling, Lizenzierung) festgelegt. Im Zusammenhang mit IT-Prozessen bietet sich eine Differenzierung in primäre und sekundäre (unterstützende) IT-Prozesse (analog zur Geschäftsprozessmanagement-Systematik) an. Diese werden im Sinne von übergeordneten (operativen und strategischen) IT-Management-Prozessen koordiniert und gesteuert.

Durch die Prozessorientierung rückt aus organisatorischer Sicht die Betrachtung der gesamten IT-Prozesslandschaft in den Mittelpunkt.

Die **Kernprozesse der IT** sind nach [BR096]:

- Entwicklung und/oder Beschaffung von IT-Applikationen
- Ausbildung und Skill-Management
- IT-Beratung
- IT-Betrieb
- HW-/SW-Management
- Technologie-Management
- Führung (inklusive Qualitätsmanagement, Risikomanagement, Controlling)

Wesentliche **Fragen** in diesem Zusammenhang sind beispielsweise:

- Welche IT-Prozesse haben wir im Unternehmen?
- Wie werden sie dokumentiert und verbessert?
- Wer ist wofür zuständig – im IT-Bereich bzw. in den Fachbereichen?

Kundenorientierung und Qualitätsmanagement seitens der IT-Organisationen haben heute strategische Bedeutung und sind entsprechend zu planen und umzusetzen. In diesem Zusam-

menhang darf der Hinweis auf ITIL respektive das CMMI Framework (vom Software Engineering Institute (SEI)) nicht fehlen.

ITIL ist die Abkürzung für den durch die CCTA (heute OGC) in Norwich (England) im Auftrag der britischen Regierung entwickelten Leitfaden IT Infrastructure Library. ITIL ist heute der weltweite De-facto-Standard im Bereich Service Management und beinhaltet eine umfassende und öffentlich verfügbare fachliche Dokumentation zur Planung, Erbringung und Unterstützung von IT-Serviceleistungen. ITIL bietet die Grundlage zur Verbesserung von Einsatz und Wirkung einer operationell eingesetzten IT-Infrastruktur. ITIL beschreibt ein systematisches, professionelles Vorgehen für das Management von IT-Dienstleistungen. Die Library stellt nachdrücklich die Bedeutung der wirtschaftlichen Erfüllung der Unternehmens-Anforderungen in den Mittelpunkt.

Hinweis: Zum Thema ITIL finden Sie ausführliche Darstellungen in Kapitel 4 „IT-Service-management“.

2.2.12 Ausrichtung und Gestaltung der IT-Organisation

Die klassische Organisation der IT war die Einrichtung und der Betrieb eines Rechenzentrums. Im Laufe der Zeit sind spezielle Arbeitsbereiche dazugekommen; etwa die Anwendungsentwicklung oder das Managen von IT-Projekten. Mittlerweile findet im IT-Bereich ein weiteres Umdenken statt: Jahrelang haben sich IT-Abteilungen auf die Einführung und Unterstützung von Technologien und deren fachliche Beherrschung konzentriert. IT-Abteilungen müssen heute zahlreiche leistungsfähige Services erbringen, deren Ziel es in Zeiten von Kundenorientierung und Kostenbewusstsein ist, die bestmögliche Unterstützung der Geschäftsprozesse sicherzustellen. Die IT wird damit immer mehr Bestandteil des eigentlichen Geschäfts.

Abteilungen ergeben sich, indem mehrere Arbeitsaufgaben eines segmentierten, aber zusammengehörigen Aufgabenkomplexes in einen Organisationsbereich unter Leitung einer Instanz zusammengefasst werden. In einer Abteilung besteht ein Mindestmaß an direkten Arbeitsbeziehungen, so dass von einem quasi-geschlossenen Untersystem einer Institution gesprochen werden kann. Wird das Mindestmaß überschritten, werden Abteilungen i.d.R. zu „Hauptabteilungen“ gebündelt. Denkbar ist also die IT-Abteilung als Hauptabteilung (bei großen Organisationen) oder als „normale“ Abteilung.

Die **IT-(Aufbau)Organisation** beschreibt das organisatorische Konzept und den Ressourcenbedarf für die Nutzung der IT-Mittel im gesamten Unternehmen.

Wichtige **Fragen** dazu:

- Welche Bedeutung hat die IT für das Unternehmen?
- Wer sind die wichtigsten Stakeholder, und in welcher Form werden sie einbezogen?
- Was muss im eigenen Haus gemacht werden, und welche Ressourcen benötigt man (Entwicklung, Betrieb, Support)?
- Was wird besser fremd vergeben (Outsourcing)?
- Welchen Zentralisierungs-/Dezentralisierungsgrad soll die IT im Unternehmen haben?
- Wie viel Geld (absolut und/oder in Prozenten des Unternehmensaufwandes) darf für die IT aufgewendet werden, und wie wird es eingesetzt?

- Wie stellt man die richtige Qualifikation der Mitarbeitenden in der IT sicher?
- Wie wird für eine gute Projektkultur gesorgt?

u. a. m.

Erfolgreiche Aufbauorganisationen sind heute geprägt durch folgende Grundsätze:

- Die Struktur folgt den Prozessen.
- Kundenorientierung
- Bereichsdenken eingrenzen – für das Ganze denken können
- Flache Hierarchie
- Subsidiarität
- Job enlargement und Job enrichment
- Personen berücksichtigen, aber nicht um Personen herum organisieren
- Flexibel in Bezug auf zukünftige Entwicklungen



Beachten Sie:

Ein Hauptziel der IT-Abteilung lautet heute nicht mehr „Beherrschung und Unterstützung der Technik“, sondern „bestmögliche Unterstützung der Geschäftsprozesse (und Kunden) im Unternehmen“. Mit dieser Formulierung findet auch der Servicegedanke immer mehr Berücksichtigung bei der Gestaltung der IT-Organisation.

Die in vielen Unternehmen gewählte dezentrale Organisationsstruktur und der Trend zur unternehmensübergreifenden Vernetzung haben Auswirkungen auf die Führung und Organisation der Informatik im Unternehmen. Die unter dem Begriff **IT-Governance** zusammengefassten Fragestellungen rücken aus diesem Grund verstärkt in den Fokus des IT-Managements. Die Verantwortung für die IT wird in der Regel parallel zur Unternehmensorganisation gestaltet. Geschäftsbereiche und dezentrale Einheiten haben eigene IT-Abteilungen und sind für ihre Informationsversorgung selbst verantwortlich. Daneben existiert eine zentrale IT-Stelle oder -einheit, oft unter der Führung eines Chief Information Officer (CIO), die unternehmensübergreifende Aufgaben wahrnimmt.

Im Rahmen der IT-Governance sind vor allem Fragen zu adressieren, welche Aufgaben und Kompetenzen auf welcher Unternehmensebene anzusiedeln sind und wie die konkrete Organisation der Informationsverarbeitung auszusehen hat. Konflikte entstehen meist zwischen zentralen und dezentralen Unternehmenseinheiten, etwa bei der Festlegung der Kompetenzen eines zentralen CIO, der Verteilung von IT-Budgets oder der Umsetzung zentraler Planungsergebnisse, wie zum Beispiel Anwendungsarchitekturen und Standards, in den Geschäftsbereichen und dezentralen Einheiten.

Innerhalb eines Unternehmens liegen die Herausforderungen vor allem in der Beziehung zwischen dezentraler Einheit und Geschäftsbereich sowie zwischen Geschäftsbereich und Konzern. Daneben rücken verstärkt auch unternehmensübergreifende Herausforderungen in den Vordergrund. Vernetzte E-Business-Lösungen verlangen häufig nach unternehmensübergreifenden Organisationsstrukturen. Ein Beispiel hierfür sind die in großer Zahl entstandenen Konsortialmarktplätze, innerhalb derer jeweils mehrere Unternehmen zusammengeschlossen sind.

IT-Governance setzt durch die Definition von Marktregeln die Rahmenbedingungen für das Zusammenspiel von Leistungserbringern und -abnehmern. Hier sind besonders hervorzuheben:

Grundsätze zur Positionierung und Organisation:

- Strategische Positionierung und Rollen
- Anwendungsbereiche der IT
- Grundsätze für Liefer- und Leistungsbeziehungen
- Rechtliche Beziehungen
- Eskalations- und Schlichtungsprozesse (wenn nötig)

Wettbewerbssituation:

- Gestaltung der Bezugspflicht von IT-Leistungen
- Grad der Freigabe der Leistungserbringung
- Bezugsprinzip: Vorgehen, Prozess
- Rechtliche Voraussetzungen

Preisfindung und Leistungsverrechnung:

- Geltungsbereich, rechtlicher Rahmen
- Methoden, Preisfindungsprozess (für IT-Leistungen)
- Budgetierungsverfahren

Risiko- und Performance-Management:

- Verteilung des Risikos
- Verantwortung für Risiken und deren Kontrolle
- Risiko-Kontrollmechanismen (Risiko-Management-Prozess)
- Berichterstattungsprozesse
- Leistungsbeobachtung und -überprüfung [ZAR04]

Hinweis: Zum Thema IT-Governance finden Sie ausführliche Darstellungen in Kapitel 10 „IT-Governance“.

2.2.13 Vorhabensplanung aus IT-Strategien ableiten

Eine IT-Strategieentwicklung und – damit verbunden – eine IT-Masterplanung sollten ein unerlässlicher Bestandteil der Aktivitäten des IT-Managements sein. Die strategische Vorhabensplanung übersetzt Konzepte und Teilstrategien aus dem Business in Anforderungen, Zielvorgaben und kritische Erfolgsfaktoren für das strategische IT-Management.

Die IT-Strategie hilft, Chancen, die IT bietet, bewusst zu erkennen und deren Wert für das Unternehmen zu ermitteln. Sie liefert somit letztlich Impulse für neue IT-Produkte, verbesserte IT-Services und effizientere Geschäftsprozesse. Sie bestimmt technologische Standards und strategische Produkte, strukturiert und priorisiert die Aktivitäten zur Erschließung dieser Chancen und beschreibt Wege, um dabei Hindernisse zu überwinden und IT-Risiken zu minimieren. Außerdem legt sie Leitlinien für die Fragen der Auswahl und des effizienten Einsatzes interner und externer IT-Ressourcen fest.

In einem IT-Masterplan werden die aus der IT-Strategie resultierenden Maßnahmen in einem Gesamtplanungsdokument fixiert. Dabei legt man meist nach einer Standardvorlage langfristige Maßnahmen und Zielergebnisse im Kontext der Faktoren Zeit, Ressourcen und Budget fest. Eine **Maßnahmenkonkretisierung** ergibt sich im Wesentlichen aus den strategischen Zielen. Hierzu kann nach folgendem Muster vorgegangen werden:

Kunden-Ziel 1 (goal):

Hohe Kundenzufriedenheit halten

Aktivität/Maßnahme (activities)

Hauptaktivität/ Teilaktivitäten	2012	2013	2014

Zeitraum (time):

Grob geschätzte Kosten (costs):

Nutzen (benefit):

Verantwortliche Person/Team (Owner):

Daraus können sich letztlich mehr oder weniger viele IT-Projekte (unterschiedlicher Komplexität) ableiten. Ein IT-Projekt definiert einen erkannten IT-Veränderungsbedarf zwischen dem aktuellen Zustand und dem angestrebten Sollzustand. Ein Projekt verfügt über eine sachliche Zielsetzung, einen groben Terminplan, eine Abschätzung der benötigten Ressourcen (finanziell und personell) und die Definition der Abhängigkeit von den übrigen Projekten. Die Projektplanung soll erlauben, den Mittel- und Ressourcenbedarf für das Erreichen des Soll-Zustandes abzuschätzen.

Knappe IT-Budgets erfordern eine Auswahl von IT-Projekten aus dem gültigen IT-Projektportfolio. Es enthält die Wartungs- und Neuentwicklungsprojekte des Unternehmens, orientiert an der IT-Strategie. Auswahlkriterien orientieren sich am „Return on Investment“ und dem Beitrag der IT-Projekte zur Erreichung der Unternehmens-Strategie.

Der **Katalog der konzeptionellen Projekte** umfasst die nötigen Projekte, um die Soll-Architektur zu erreichen.

Mittels der **Projektbewertung** wird ein „planbares“ und „machbares“ Projekt Portfolio entwickelt. Es zeigt die konzeptionell relevanten Vorhaben bezüglich ihrer strategischen und wirtschaftlichen Bedeutung. Die Bewertung der Projekte erfolgt nach mehreren aus Zielsetzungen und Rahmenbedingungen abgeleiteten Faktoren. Die Übersicht über die kritischen Ressourcen zeigt über den Planungszeitraum hinweg die Belastung von Schlüsselressourcen. Dies erlaubt es, die Planung bezüglich ihrer Machbarkeit zu beurteilen. Auch ausbildungs-technische und beschaffungstechnische Maßnahmen lassen sich davon ableiten.

2.2.14 Projektportfolio ableiten und im IT-Masterplan dokumentieren

Es ist davon auszugehen, dass die für die Umsetzung notwendigen Ressourcen (wie z.B. Finanzen und Personal) knapp sind. Daher müssen Prioritäten gesetzt werden. Als Entscheidungsgrundlage hat sich das **Projekt-Portfolio** bewährt. Dieses Instrument vereinfacht die Festlegung der Prioritäten, Ressourcen und Synergien der ins Auge gefassten Projekte. Soll die strategische Ausrichtung der IT im Unternehmen gelingen, so sind die einzelnen Projekte des strategischen Projekt-Portfolios in der geplanten Abfolge rechtzeitig in Angriff zu nehmen und innerhalb der geplanten Zeit abzuwickeln.

Der Aufbau eines Projektportfolios erfolgt in drei Stufen, die den Entwicklungsstand widerspiegeln:

- Das „**Basis-Portfolio**“ liefert die Übersicht über alle Projekte/Vorhaben. Es gibt einen definierten Satz von Informationen zu allen Projekten (Eckdaten).
- In einem „**Profi-Portfolio**“ sind Prozesse und Methoden zur Ideen-Einreichung, Projektauswahl und Bewertung etabliert, und es gibt ein spezifisches Reporting.
- Ein „**exzellentes Portfolio**“ ist mit anderen Geschäftstätigkeiten – insbesondere mit der Strategieerarbeitung und dem Risikomanagement – verknüpft. Es erlaubt die gezielte Steuerung der finanziellen und personellen Ressourcen im Sinne einer optimalen Strategieumsetzung.

Als Grundlage dafür benötigt man geeignete **Projekt(kurz)beschreibungen**. Letztere können in der Folge auch zur Ausarbeitung der Projektaufträge verwendet werden. Diese bilden wiederum die Grundlage für die tatsächliche Realisierung der geplanten Vorhaben (Arbeitsaufträge).

Eine besondere Herausforderung auf dem Weg von der IT-Strategieerstellung zur IT-Strategieumsetzung stellt die **Priorisierung** und damit verbunden auch das Ausscheiden oder Zurückstellen von IT-Projekten dar. Um die in der Praxis damit verbundenen (persönlichen) Machtkämpfe so weit wie möglich hintanzustellen resp. zu versachlichen, ist ein transparenter Evaluationsprozess unter Verwendung geeigneter Evaluationskriterien erforderlich.

Bei der Festlegung der **Evaluationskriterien** sollten die Zukunftsträchtigkeit, die Wirksamkeit, die Wirtschaftlichkeit und die Dringlichkeit im Vordergrund stehen. Heinrich nennt in Anlehnung an Parker et al. fünf Evaluationskriterien der Business Domain:

- Strategischer Abgleich
- Wettbewerbsvorteil
- Führungsinformation
- Wettbewerbsschaden
- Projektrisiko

sowie vier Evaluationskriterien der Technology Domain:

- Strategische Architektur der Informationsstruktur
- Begriffliche Ungewissheit
- Technische Ungewissheit
- Informationsinfrastrukturrisiko [HEI03]

**Merke:**

In jeder Organisation sollte – unabhängig von der Größe und Branche – ein Konzept bzw. Vorgehensmodell existieren, das die Erarbeitung einer an den Unternehmenszielen ausgerichteten IT-Strategie ermöglicht, eine darauf aufbauende Enterprise-Architektur (bestehend aus der technischen IT-Architektur (IT-Infrastruktur), der Applikationsarchitektur sowie der fachlichen Architektur) beschreibt sowie die Darstellung und Vermarktung des daraus resultierenden Werts für die Kunden des IT-Bereichs realisiert und kommuniziert. Aus der IT-Strategie lassen sich gezielt Qualitätsziele für das jeweilige Jahr ableiten, Risikoabschätzungen vornehmen sowie sinnvolle IT-Projekte definieren.

■ 2.3 Eine IT-Strategie umsetzen

„Es gibt nichts Gutes – außer man tut es“ (Erich Kästner). Das gilt auch für IT-Strategien.

2.3.1 IT-Strategie kommunizieren

Organisationsprojekte wie das Umsetzen der IT-Strategie erfordern komplexe Kommunikationsprozesse zur Meinungsbildung, Ideenfindung und gemeinsamen Problemlösung. Am Beginn eines Projekts empfiehlt es sich, genau zu schauen, wer in welcher Weise zum Gelingen des Vorhabens beitragen kann und wer von den Auswirkungen in welcher Weise betroffen sein wird.

Als methodische Hilfsmittel eignen sich besonders:

- Projektabgrenzung und Projektkontextanalyse
- Betroffenheitsanalyse
- Kommunikationsplan
- Workshops

Da in der Regel nicht alle Betroffenen am Strategieprozess beteiligt werden können, ist durch geeignete Präsentationsveranstaltungen für entsprechende Information, Motivation und Interaktion zu sorgen.

Neben der Kommunikation gilt es, dass die strategischen IT-Ziele von der Unternehmensleitung und den Fachseiten getragen werden. Der Prozess der Abstimmung der strategischen IT-Ziele mit der Unternehmensleitung und den Fachseiten sowie die Ausrichtung der strategischen IT-Ziele auf die Unternehmensstrategie wird als IT-Business-Alignment bezeichnet.

Zur Erzielung des IT-Business-Alignment sollten die Fachabteilungen von Beginn an in die Entwicklung einer IT-Strategie eingebunden werden. Die Entwicklung einer IT-Strategie sollte darüber hinaus in enger Abstimmung mit dem CIO (Chief Information Officer) erfolgen. Man

sollte bewusst Zeit einplanen, um die strategischen IT-Ziele verständlich innerhalb ebenso wie außerhalb des IT-Bereiches zu kommunizieren.

**Merke:**

Die strategischen IT-Visionen, die IT-Ziele sowie die vorgesehenen Maßnahmen sollten gegenüber den Fachseiten und der Unternehmensleitung kommuniziert werden. Dieser Faktor wird von der IT-Seite oftmals unterschätzt, weil für diejenigen, die die IT-Ziele formuliert haben, keinerlei Erklärungsbedarf besteht, für die Unternehmensleitung und die Fachseiten hingegen die IT sich häufig als unverständliche Ansammlung von Abkürzungen, technischen Details und Erklärungsversuchen darstellt.

2.3.2 (IT-)Projekte realisieren

Mit den bisher erarbeiteten Unterlagen und einer zünftigen Portion Begeisterung im Gepäck gilt es nun die Projekte zu realisieren. Auslöser für diesen Schritt ist der Umstand, dass folgende Vorbereitungsarbeiten abgeschlossen sind:

- Alle strategischen Aktionsfelder wurden identifiziert.
- Alle Umsetzungsvarianten wurden bewertet bzw. überprüft.
- Alle Grobpläne wurden erstellt.
- Es wurde eine Entscheidung getroffen, welche Umsetzungsvariante die Grundlage für künftige Vorhaben darstellt.
- Die Entscheidung wurde allen betroffenen und an der Umsetzung beteiligten Personen kommuniziert.

2.3.3 Sonstige IT-Entwicklungsmaßnahmen umsetzen

Nicht alle geplanten IT-Entwicklungs-/Verbesserungsmaßnahmen sind so komplex, dass ihre Realisierung eine eigene Projektorganisation erfordert. Manche Aufgaben lassen sich mit anderen Vorhaben kombinieren oder werden in das routinemäßige Aufgaben- oder Problemmanagement eingebracht und abgearbeitet. Beispiele hierfür sind: Personalbeschaffung, Informationsgespräche mit Stakeholdern und Mitarbeitern.

2.3.4 Umsetzung der IT-Strategie prüfen

Um letztlich tatsächlich dort zu landen, wo wir hinwollen, müssen wir uns überlegen, wie sich die Zielerreichung ausreichend detaillieren sowie genau operationalisieren und messen lässt.

In diesem Zusammenhang sind folgende **Fragen** zu beantworten:

- Wozu machen wir das bzw. was wollen wir bewirken?

- Was messen und steuern wir?
(Betrachtungsobjekt – Produkt/Prozess/Ressource/Rahmenbedingung)
- Welche Aspekte gilt es zu berücksichtigen?
(Führungsgrößen/Eigenschaften/Merkmale)
- Mit welchem Maß erfolgt dies?
(Maßeinheit/Messgröße zur Messung der Ausprägung)
- Welche Zielwerte wählen wir?
(Angestrebte Zielwerte)
- Wie messen wir?
(Messmethode)
- Wann messen wir?
(Zeitpunkt/Zeitraum)
- Wo messen wir?
(Ort/Stelle)
- Wer misst?
(Person/Gerät)
- Wie werden die Messergebnisse dokumentiert?
(Qualitätsdaten)
- Wie werden Messergebnisse ausgewertet?
(Vergleich gegen Zielwerte)
- Welche Maßnahmen werden gegebenenfalls zur nachhaltigen Verringerung der Abweichungen respektive Streuungen ergriffen, und wer kontrolliert deren Wirkung?
- Welche Maßnahmen werden gegebenenfalls zur Vorbeugung ergriffen?

Ein bewährtes Instrument zur Steuerung der Umsetzung einer (IT-)Strategie sind die **Balanced Scorecards (BSC)**. Die Konzentration auf die strategischen Ziele erfordert eine Beschränkung auf ca. 20 Ziele. Um die Zielerreichung planen und verfolgen zu können, werden die Ziele mit monetären und nichtmonetären Messgrößen und deren Sollwerte beschrieben. Strategische Aktionen zu den einzelnen Zielen stellen die Zielerreichung sicher. Jede strategische Aktion erhält Termin- und Budgetvorgaben sowie einen Verantwortlichen. Aufgrund dieser Stringenz fügte Kaplan der BSC den Untertitel „Translating Strategy to Action“ bei.

Der BSC-Ansatz ist dadurch charakterisiert, dass die strategischen Ziele jeweils einer konkreten Betrachtungsweise – der sog. Perspektive – zugeordnet werden. Diese Zuordnung verhindert einseitiges Denken. Durch das Prinzip, alle – auch die nicht monetären – Sichtweisen zu berücksichtigen, die für die strategische Positionierung des Unternehmens wichtig sind, und alle Sichtweisen zu verknüpfen, macht die BSC komplexe Zusammenhänge transparent.

Die Verknüpfung erfolgt in Ursache-Wirkungsketten. Dabei wird in der Planung Top down und in der Umsetzung Bottom up gearbeitet. Im Rahmen der BSC werden vier Perspektiven unterschieden:

- Die *Finanzperspektive*:
Welche Zielsetzungen leiten wir aus den finanziellen Erwartungen unserer Kapitalgeber ab?
- Die *Kundenperspektive*:
Welche Ziele sind hinsichtlich Struktur und Anforderungen unserer Kunden zu setzen, um die finanziellen Ziele zu erreichen?

- Die *Prozessperspektive*:
Welche Ziele sind hinsichtlich unserer Prozessqualität zu setzen, um die Ziele der Finanz- und Kundenperspektive zu erreichen?
Die Prozessperspektive gibt an, bei welchen Prozessen was zu erreichen ist, um Kunden- oder Finanzziele zu erfüllen.
- Die *Potenzialperspektive*:
Welche Ziele müssen wir hinsichtlich unserer Potenziale setzen, um den aktuellen und zukünftigen Herausforderungen gewachsen zu sein?

Wie die verschiedenen Perspektiven bei der Entwicklung einer Balanced Scorecard auf den IT-Bereich übertragen werden können und so eine IT-Balanced Scorecard (IT-BSC) entsteht, verdeutlicht das Beispiel in Abbildung 2.12.

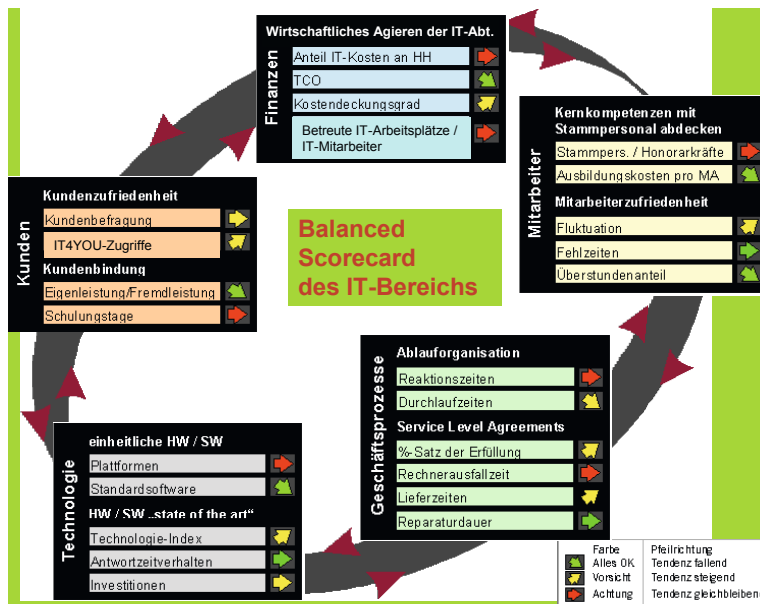


ABBILDUNG 2.12 Beispiel einer IT-BSC

Im Folgenden noch ein Beispiel für eine einzelne Zielsetzung: „Wirtschaftliches Agieren der IT-Abteilung“:

Mit einer einzigen Kennzahl ist das wohl kaum auszudrücken. Besser erscheint da etwa die ausgewählte Kombination einiger wesentlicher Kennzahlen wie „Total Cost of Ownership (TCO)-Wert absolut“, „TCO-Wert im Vergleich zu ähnlichen Organisationen“, „IT-Kosten relativ zum Gesamtumsatz“, „Produktpreise im Vergleich zum Markt bzw. zum Wettbewerb“, „Gemeinkostenanteil“ ... Anschließend legen wir die Zielwerte fest.

In Abbildung 2.13 sind in einer Tabelle bereits Statusindikatoren enthalten, die dem Leser auf einen Blick die „Einordnung“ der Kennzahl in verschiedene „Gefahrenklassen“ ermöglichen sollen bzw. den Trend einer Kennzahl anzeigen.

FINANZEN					
Ziel	Kennzahl	Status	Ist	Soll	Erfüllungs-grad %
Wirtschaftlich agierende IT-Abteilung	KZ-Berechnung	⇒		Maßnahmen	90%
	TCO-Wert	⇒	3.863	4.300	89,84%
	technische Innovation	✓	1,86%	2,00%	93,00%
	Kostendeckungsgrad	!	69,12%	100%	69,12%
	Betreuungsintensität	✓	51,10	50,00	97,85%
	VW-Gemeinkostenanteil	✓	13,88%	15,00%	92,53%
	Projekt-Leistung zu Pauschale	✓	38,29%	40,00%	95,73%

ABBILDUNG 2.13 Beispiel zu den Kennzahlen eines IT-Zieles

Wie kann man die strategische Planung der Informatik als unternehmensweiten Organisations-Entwicklungsprozess anpacken?

Im Folgenden ist eine Prozessbeschreibung: „IT Strategie entwickeln und umsetzen“ mit ihren wesentlichen Elementen skizziert. Dabei wird zwischen den Elementen Prozesscharakteristik und der eigentlichen Prozessbeschreibung unterschieden.

Prozesscharakteristik:

1. Prozess-Bezeichnung	IT-Strategie entwickeln und umsetzen
2. Prozesseigner	W
3. Zweck des Prozesses	Erstellen einer IT-Strategie und Vorbereiten der Realisierung
4. Geltungsbereich	ganzes Unternehmen
5. Vision	Das Unternehmen wird von der IT optimal unterstützt.
6. Wesentliche Erfolgskenngrößen	E1 Die Unternehmensleitung ist mit der IT-OE zufrieden. E2 Die Fachbereiche fühlen sich von der IT gut unterstützt in ihrer Arbeit.
7. Prozess-Führungsgrößen	F1 ... F2 ...
8. Prozess-Zielwerte	Z1 ... Z2 ...
9. Mitgeltende Unterlagen und Hilfsmittel	U1 Unternehmensstrategie

Input	Aktivität	Output
▪ Unternehmensleitbild ▪ Geschäftsprozesse ▪ IT-IST-Situation ▪ IT-Markt	Vorhandene Unterlagen/Informationen studieren und analysieren	▪ Strategische Grundsätze ▪ Situationsanalyse ▪ SWOT-Analyse ▪ IT-Landkarte

(Fortsetzung nächste Seite)

Input	Aktivität	Output
Anforderungen der IT-Anwender	Handlungsbedarfe identifizieren und konkretisieren	Liste/Beschreibung der Handlungsbedarfe
Handlungsbedarfsbeschreibung	Konzeptionelle Lösungsansätze entwickeln	Beschreibung der konzeptionellen Lösungsansätze
▪ Beschreibung der konzeptionellen Lösungsansätze ▪ IT-Strategie	Maßnahmen zur Umsetzung der konzeptionellen Lösungsansätze bestimmen	▪ Projekt(kurz)beschreibung ▪ Auftragsentwurf
▪ Beschreibungen der Lösungsansätze ▪ IT-Strategie	Präsentation vorbereiten	Präsentationsunterlagen
▪ Präsentationsunterlagen ▪ IT-Strategie	Mitarbeiter informieren	Informierte Mitarbeiter
Projekt(kurz)beschreibungen	Projekt(kurz)beschreibungen zur Bearbeitung weitergeben	Beauftragte
Aufträge	Aufträge zur Bearbeitung weitergeben	Beauftragte

ABBILDUNG 2.14 Beispiel einer Prozessbeschreibung

2.3.4.1 Ein Beispiel aus der Praxis

Im Folgenden wird ein konkretes Beispiel aus der Beratungspraxis des Autors beschrieben. Die Darstellung erfolgt in geraffter Form in Anlehnung an das entsprechende Projektlogbuch. Die Planung des Ablaufes erfolgte auf Basis des Aktionshandbuches „OE-Prozesse initiieren und gestalten“ des Management Center Vorarlberg in sieben Phasen:

1. Orientierung
2. Situationsklärung
3. Zielfindung (Auswahl und Entscheidung)
4. Offizielle Projektgründung
5. Information der Gesamtorganisation
6. Arbeiten in Teilprojekten
7. Absichern des in die Organisation integrierten Prozesses

Die Ausgangslage

In einem Unternehmen der Dienstleistungsbranche mit rund tausend Mitarbeitern bestand die Herausforderung darin, die strategische Planung des Unternehmens zu erarbeiten. Da man spürte, dass die Unternehmensstrategie nur realisiert werden kann, wenn die Informationsverarbeitung höchsten Ansprüchen genügt, wurde der Leiter IT mit der Ausarbeitung einer strategischen Planung der Informatik beauftragt.

Der IT-Leiter entschloss sich, einen externen Berater beizuziehen, der ursprünglich nur als Ideenlieferant für die zukünftige Informationsverarbeitungs-Landschaft gedacht war. Doch

bereits in den ersten Gesprächen zeigte sich, dass es zweckmäßig wäre, den Externen auch als „Change-Agent“ – als „Moderator“ – des unternehmungsweiten Veränderungsprozesses einzusetzen.

Nachdem frühere Strategieübungen nur Berichte erbrachten, die allzu früh in die Schubladen gewandert waren, stimmte man einem OE-orientierten Vorgehen zu, wohl wissend, dass dieser Weg erheblich mühsamer und langwieriger ist als eine Strategie am grünen Tisch.

Die Orientierungsphase

Zunächst ging es darum,

- die Betroffenen für notwendige Veränderungen und Entwicklungen in der Organisation zu sensibilisieren;
- dabei erste Entwicklungsmöglichkeiten und Ansatzpunkte zu erkennen;
- einen Grob Ablauf für einen Prozess zu erstellen;
- im Management zu einer Entscheidung über weitere Schritte zu kommen und
- den geplanten Prozess mit den betroffenen Menschen zu diskutieren.

Die Phase der Situationsklärung

Diese Phase hatte zum Ziel,

- die Erwartungen der Geschäftsleitung zu erheben;
- mit ausgewählten Mitarbeitern aus der Unternehmung ein gemeinsames Bild der IST-Situation in Form einer Selbstdiagnose zu erarbeiten;
- Zukunftsbilder (Visionen) zu erarbeiten;
- Veränderungsziele zu formulieren, die sich aus der Selbstdiagnose und den Zukunftsbildern ergaben („Wir wollen weg von ... hin zu ...“);
- Prioritätensvorschläge zu ausarbeiten;
- Anforderungen an zu treffende Maßnahmen zu definieren.

Große Bedeutung hatten gemeinsame Klausurtage, bei denen man sich mit Hilfe professioneller Moderation unter Einsatz aller erdenklichen Visualisierungs- und Kommunikationsmittel von vielen Einzelmeinungen über gemeinsame Sichten letztlich zu Konsenslösungen durchrang.

Phase der Zielfindung

Für Entscheidungen über das weitere Vorgehen war es an dieser Prozess-Stelle wieder erforderlich, die Geschäftsleitung in größerem Umfang einzubeziehen. Dies geschah in folgender Form:

- Impulsseminar für die erweiterte Geschäftsleitung zum Thema „IT für Führungskräfte“; anschließend
- Workshop über „Wandel im Markt, in der Unternehmung und deren Auswirkungen auf die Informatik“.

So vorbereitet, fiel die nachfolgende Präsentation der Ergebnisse aus der Situationsklärung auf äußerst fruchtbaren Boden, und die vorgeschlagenen Schwerpunkte für das weitere Vorgehen wurden zustimmend zur Kenntnis genommen, was grünes Licht für die offizielle Projektgründung inklusive der damit verbundenen Teilprojekte bedeutete.

Folgende Schwerpunktthemen wurden priorisiert:

- Verstärkung des Engagements der Geschäftsleitung in Sachen Informatik;
- Verbesserung und Intensivierung der Zusammenarbeit zwischen der IT- Abteilung und den Fachbereichen;
- Ausbau des Projektwesens und Einführung eines professionellen Projektmanagements in der gesamten Unternehmung;
- Reorganisation der IT-Abteilung unter besonderer Berücksichtigung möglicher Dezentralisierung;
- Einrichtung umfassender Aus- und Weiterbildungsmöglichkeiten bezüglich Informatik und Organisation.

Offizielle Projektgründung

Zur Steuerung der weiteren Arbeiten wurde eine dreiköpfige Projektleitung nominiert, die sich aus einem hochrangigen Vertreter der Fachbereiche, dem IT-Leiter und dem externen Berater zusammensetzte.

Gleichzeitig gründete man drei Teilprojekte, organisierte sie sowohl aufbau- als auch ablaufmäßig nach dem Muster des Gesamtprojektes und wies ihnen die ausgewählten Schwerpunktthemen zur weiteren Bearbeitung zu.

Information der Gesamtorganisation

Nun war es an der Zeit, alle involvierten Mitarbeiter von ihren Führungskräften informieren zu lassen über

- die bisherigen Schritte,
- die Steuerungsstruktur des Projektes und
- das weitere Vorgehen.

Arbeit in Teilprojekten

Nicht nur um die Arbeit, die mit jedem Innovationsprozess verbunden ist, aufzuteilen, sondern auch um von Anfang an alle möglichen Vorkehrungen in Richtung Umsetzung zu treffen, wurden zunächst drei Teilprojekte gegründet, in denen jeweils ca. sieben Leute mitarbeiteten:

- Teilprojekt 1: Management und IT
- Teilprojekt 2: Fachbereiche und IT
- Teilprojekt 3: Gestaltung der IT-Abteilung

In jedem Teilprojektteam wurde ein Leiter nominiert, der gleichzeitig der erweiterten Projektleitung angehörte und so für die Koordination mit dem Gesamtprojekt sorgte – inhaltlich, terminlich und budgetmäßig.

Auch in den Teilprojekten gab es jeweils passende Impulsseminare für die Mitarbeiter und moderierte Klausurtagungen. Die Dokumentation der Ergebnisse wurde meist in Form von Simultanprotokollen gemacht und allen Beteiligten ausgehändigt.

Die Abstimmung der Teilprojekte erfolgte in regelmäßigen Projektleitungs-Sitzungen.

Die in den Teilprojekten erarbeiteten Ergebnisse folgten einer Doppelstrategie, die darin bestand, die vorgeschlagenen Maßnahmen von Anfang an in kurzfristig zu erledigende und langfristige zu gliedern. (Für die Motivation der Beteiligten ist es ausgesprochen wichtig, möglichst bald erste greifbare Erfolge zu erzielen.)

Absichern des in die Unternehmung integrierten Prozesses

Um die spätere Umsetzung der konzeptmäßig erarbeiteten Strategie von Anfang an zu sichern, war während des gesamten Planungsprozesses auf allen Ebenen für ausreichende Kommunikation, Koordination und Kooperation zwischen der Projektorganisation und der Unternehmung zu sorgen.

An Möglichkeiten dazu wurden neben den bereits erwähnten Informationsveranstaltungen auch verschiedene Benutzerbefragungen und -diskussionen durchgeführt.

Dies war insbesondere deshalb von größter Bedeutung, weil man sehr bald erkennen konnte, dass im Zuge der Dezentralisierung der Informatik umfassende Aufgaben auf die einzelnen Fachbereiche der Unternehmung zukommen würden.

In Abständen wurde die Geschäftsleitung von der Projektleitung über den Fortgang der Arbeit informiert.

Nach Abschluss der Teilprojekte wurde ein als neues strategisches Rahmenkonzept konsolidierter Gesamtbericht erstellt. Ganz wesentlich dabei war die Vorgabe, dass die Planung nicht nur die anzustrebenden Ziele, sondern auch detaillierte Vorschläge umfassen sollte, und wie vorzugehen sei, um die Ziele innerhalb der gesteckten Fristen und des Budgets zu erreichen.

In einer sehr gut vorbereiteten formellen Präsentationsveranstaltung wurde dieses Konzept von der Projektleitung im Beisein der Teilprojektleiter der Geschäftsleitung vorgestellt, diskutiert und zur Genehmigung beantragt.

Nach der offiziellen Genehmigung der strategischen Planung der Informatik löste man die für diese Arbeit gebildete Projektorganisation auf – allerdings nicht ohne vorher das gute Gelingen der Planung mit einem schönen gemeinsamen Abendessen zu feiern.

Die anschließende Umsetzung der Planung im Unternehmen erfolgte wieder in der Linienorganisation, wobei man fallweise für besondere Aufgaben Arbeitsgruppen zusammenstellte, in denen wiederum meist IT-Leute und Vertreter der Anwender zusammenwirkten.



Das Wichtigste – zusammengefasst

- **Verzetteln Sie sich bei der Entwicklung und Dokumentation der IT-Strategie nicht in zu vielen Details.**

Bei einer IT-Strategie geht es primär um die Beschreibung der Grundsätze und die Festlegung von Standards zu den Architekturen sowie um die Entwicklung eines IT-Masterplans. Dies sollte allerdings wohl durchdacht und begründet sein.

- **Die Ausgestaltung der Details und die Umsetzung einer IT-Strategie erfolgt durch die einzelnen Organisationseinheiten der IT.**

Falls vorhanden, machen dies die IT-Architekten, die IT-Produkt- und Service-Verantwortlichen (ggf. zusammen mit anderen Fachabteilungen) sowie das Project-Office.

■ **Im Wesentlichen sollten Sie beim Aufstellen der IT-Strategie folgende Aktivitäten und Festlegungen beachten:**

- Grundsätze über die Rolle und die Intensität der Nutzung der IT
- Beurteilung der möglichen mittelfristigen internen und externen Veränderungen
- Festlegen der strategischen Schwerpunkte der IT-Nutzung
- Definieren der Grundsätze für die Zusammenarbeit mit externen Partnern
- Entscheidungen über die Priorisierung der Mittelfristplanung (welche IT-Projekte?)

■ **Die IT-Strategieentwicklung schafft die Voraussetzungen, um ...**

den IT-Einsatz im Unternehmen aktiv zu führen und die IT-Systeme effektiv und effizient einzusetzen, die optimale IT-Ausstattung und IT-Unterstützung (IT-Services) der Fachbereiche im Unternehmen zu planen sowie Interessengegensätze zwischen den Bedürfnissen der Fachbereiche und des IT-Bereichs zu identifizieren und zu lösen. So lassen sich die IT-Infrastrukturen und IT-Applikationen zukunftsorientiert planen sowie die Lösungsansätze der IT-Strategien in eine konsistente und realistische Mittelfristplanung überführen.

■ 2.4 Literatur

- [BRO96] *Brogli, Martin*: Steigerung der Performance von Informatikprozessen. Vieweg, 1996
- [BRE07] *Brenner, Walter; Witte, Christoph*: Erfolgsrezepte für CIOs. Hanser-Verlag. München 2007
- [BU05] *Buchta, Dirk; Eul, Marcus; Schulte-Croonenberg, Helmut*: Strategisches IT-Management Wert steigern, Leistung steuern, Kosten senken. Gabler-Verlag. Wiesbaden 2005
- [HA09] *Hanschke, Inge*: Strategisches Management der IT-Landschaft. Ein praktischer Leitfaden für das Enterprise Architecture Management. Hanser-Verlag. München 2009
- [HEI03] *Heinrich, Lutz J., und Burgholzer, Peter*: Informationsmanagement, 9. Auflage. Oldenbourg, 2003
- [ÖST95] *Österle, Hubert*: Business Engineering – Prozeß- und Systementwicklung. Springer, 1995
- [SCH03] *Schmid, Werner*: Seminarunterlagen, 2003
- [TIE07] *Tiemeyer, Ernst*: IT-Strategien entwickeln/IT-Architekturen planen. rauscher.Verlag. Haag i. Obb. 2007
- [WIN03] *Wintersteiger, Walter, et al.*: Informatikstrategie umsetzen. Compendio 2003
- [ZAR04] *Zarnekow, Rüdiger, et al. (Hrsg.)*: Informationsmanagement. dpunkt.verlag 2004

Enterprise Architecture Management (EAM) – IT-Architekturen erfolgreich planen und steuern

Ernst Tiemeyer



Fragen, die in diesem Kapitel beantwortet werden:

- Warum ist ein professionelles Management der IT-Architekturen in Unternehmen und Verwaltung unverzichtbar?
- Wie kann ein Ordnungsrahmen für die Realisierung von Enterprise-Architekturmanagement aussehen, und welche Domänen sind dabei zu unterscheiden?
- Was sind die wesentlichen Zielsetzungen für das Architekturmanagement, und welche Architekturprinzipien sind zu berücksichtigen?
- Wie lassen sich IT-Architekturen in den verschiedenen Domänen beschreiben und auch in vernetzter Form dokumentieren?
- Welche Planungsaktivitäten zu den Enterprise- bzw. IT-Architekturen sind in der Praxis hilfreich und notwendig?
- Welche Instrumente zur Bewertung von IT-Architekturen haben sich bewährt?
- Welche Organisationsstrukturen und Prozesse sind für die Einführung von Architekturmanagement in der Unternehmenspraxis zu etablieren?
- Welche Einsatzmöglichkeiten bietet das Framework TOGAF zur Unterstützung von Aufgaben im IT-Architekturmanagement?

Eine zentrale Herausforderung und Aufgabe im IT-Management besteht darin, eine strategische Planung der IT-Architekturen für die eigene Organisation vorzunehmen, die aktuell installierten IT-Systeme zu gegebener Zeit zu modernisieren und (mit einem ausgewogenen Migrationskonzept) auf den neuesten Stand zu bringen. Darüber hinaus gilt es, eine zunehmend komplexe IT-Infrastruktur zu verwalten.

Natürlich ist das gezielte Planen und Verwalten der IT-Architekturen kein Selbstzweck. Ziel ist letztlich die Bereitstellung von geeigneten Applikationen und einer anpassungsfähigen IT-Infrastruktur, die einen fortlaufenden und zuverlässigen IT-Betrieb gewährleisten und dabei gleichzeitig die Geschäftsprozesse optimal unterstützen. Gleichzeitig kommt es darauf an, die vorhandene IT-Infrastruktur mittels intelligenter und dynamischer Verwaltung optimal zu nutzen, um einerseits Kostenoptimierung und andererseits eine hohe Kundenzufriedenheit zu erreichen.

■ 3.1 Ausgangssituation und Herausforderungen

Eingesetzte IT-Infrastrukturen und IT-Applikationen sind insbesondere in mittleren und großen Unternehmen bzw. Verwaltungen oft organisch gewachsen. Über viele Jahre hinweg ist so eine umfangreiche IT-Anwendungslandschaft basierend auf sehr unterschiedlichen Infrastrukturen (Technologien, Entwicklungsparadigmen, Komponenten) und Werkzeugen entstanden.

Hinzu kommt, dass überall Redundanzen auftreten: in der Funktionsabdeckung der Anwendungen, in der Datenarchitektur, bei den Schnittstellen und bei der Ausstattung mit Technologieplattformen. Zu viele Softwaretools decken identische Funktionen ab. Vielfach wird außerdem festgestellt, dass die Anzahl und die Komplexität von Schnittstellen zwischen den installierten Anwendungen außer Kontrolle geraten sind.

Folgende **Herausforderungen** sind für die IT-Verantwortlichen zu beachten:

- Es muss ein Ausgleich gefunden werden zwischen der nachhaltigen Unterstützung von Geschäftsprozessen und der nach wie vor dynamischen Entwicklung der Informationstechnologie. Wesentlich wird dabei ein Beherrschen der Schnittstellen-Komplexität.
- Die „Architektur-Konformität“, bezogen auf die definierten Technologien und Migrationspläne, wird bei Architekturentscheidungen und bei der Durchführung von IT-Projekten oft nicht bedacht. Deshalb sollten IT-Architekten bei IT-Projekten auch in die Konzeptions- und Auswahlphase einbezogen werden.
- Ein zentraler Aspekt ist eine möglichst weitgehende Vereinfachung der integrierten Systemlandschaft, die auf prozess- und produktübergreifende IT-Architekturen zielt.

Den Zusammenhang zwischen IT-Architekturen und den sich daraus ergebenden IT-Services sowie der Unterstützung des Business zeigt Abbildung 3.1.

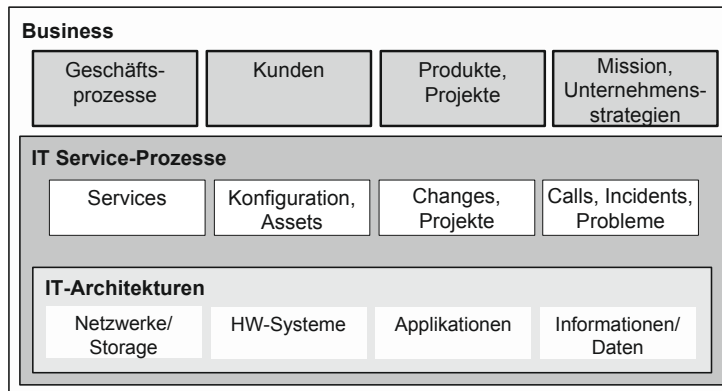


ABBILDUNG 3.1
IT-Architekturen und IT-Services bzw. Business-Anforderungen

Vielfach sind Unternehmensleitung und auch IT-Verantwortliche aufgrund der Anforderungen sowie der Fülle der Angebote und Lösungen für den IT-Bereich hoffnungslos überfordert. Entscheidungen über IT-Architekturen zu treffen, ist deshalb nicht immer ganz einfach. So wurden in der Vergangenheit oft unkoordiniert IT-Systeme aufgebaut und Applikationen entwickelt, die anschließend im Betrieb und Support Ummengen von Geld und Ressourcen verschlangen oder schlicht nicht mehr wartbar waren.

**Beachten Sie:**

Angebote und implementierte IT-Systeme weisen immer umfassendere Funktionalitäten auf und unterliegen raschen Entwicklungszyklen. Im Ergebnis ist bei Anwendern oft eine Vielzahl komplexer IT-Anwendungen auf unterschiedlichen Technologieplattformen vorhanden. Insgesamt kann außerdem festgestellt werden, dass die heute existierende IT-Anwendungslandschaft äußerst komplex ist und häufig überdimensionierte Lösungen und überflüssige Funktionalitäten enthält.

Aufgrund der Ist-Situation in der IT-Praxis ergeben sich für die IT-Verantwortlichen – dies zeigen auch Studien wie etwa die der Metagroup und von Gartner sowie von [De03] – zahlreiche **Problemfelder**:

- Fehlender Überblick für Anwender und Entscheidungsträger durch die hohe Komplexität der IT-Landschaft: Aufgrund der über viele Jahre gewachsenen IT-Systeme ist vielfach nicht mehr nachvollziehbar, wie das Zusammenspiel zwischen den Geschäftsprozessen bzw. Arbeitsabläufen und der eingesetzten Soft- und Hardware im Detail erfolgt. Analysen der IT-Landschaft in Bezug auf Redundanzen, Strukturprobleme oder Optimierungsmöglichkeiten sind nur schwer möglich. Hilfreich wäre als Minimum zumindest eine grafische Darstellung der IT-Landschaft als Kommunikationsmittel in einem Unternehmen.
- Erhöhte Risiken und fehlende Steuerbarkeit der IT: Softwareentwicklung und -beschaffung sind mangels eines umfassenden Überblicks über die IT-Architektur ebenfalls nicht mehr gezielt steuerbar (schlechte, kostenintensive Wartbarkeit der IT-Systeme). Infolgedessen ergeben sich erhöhte Risiken für die Bereitstellung, Integration und den Betrieb leistungsfähiger IT-Systeme und IT-Anwendungen.
- Fehlende Strategieorientierung bei Ad-hoc-Entscheidungen: Über fachliche Anforderungen werden aus dem Tagesgeschäft heraus Einzelfallentscheidungen getroffen – ohne übergreifende Gesamtsicht der IT. Entwicklungszusagen und vereinbarte Projektportfolios werden ständig geändert – mit einer Halbwertszeit von etwa 8 Wochen. Eine strategische Migration der existierenden IT-Architektur zu einer anderen Architektur wird vielfach erschwert oder ist oft kaum möglich. Unterschiedliche Entwicklungswege werden verfolgt – durch gegenläufige Technologie-Sets in der Infrastruktur entstehen eklatante Widersprüche.

Die **Folgen** liegen auf der Hand: Individualität und große Komplexität im IT-Bereich können Unternehmen und Verwaltungen teuer zu stehen kommen. Außerdem steigen durch die Standardisierung von Hard- und Software nicht nur die Administrationskosten, auch Änderungen in der IT-Infrastruktur lassen sich nicht so einfach und effizient durchführen. Letztlich führt dies zu einer erheblichen Verschlechterung im IT-Servicemanagement und zu einer nachlassenden Kundenzufriedenheit bezüglich der IT-Organisation.

Eine **Lösung** der genannten Probleme könnte ein gezieltes **IT-Architekturmanagement** und damit einhergehende Konsolidierungsbemühungen eröffnen. Notwendig ist dafür eine integrierte Sicht auf alle relevanten Aspekte der IT-Anwendungs- und Systemlandschaft, die auch eine Verbindung zu den unterstützten Geschäftsprozessen schafft. Architekturmanagement darf den Schwerpunkt nämlich nicht nur auf die Software- und Hardwarelandschaft einer Organisation legen, sondern muss vielmehr als integraler Bestandteil des Business und der organisatorischen Gegebenheiten behandelt werden. Damit erweitert sich das reine IT-Architekturmanagement zu einem **Enterprise Architecture Management** (kurz EAM).

Wie sehen die wesentlichen Rahmenbedingungen und Zielsetzungen für die **Einführung eines systematischen IT-Architekturmanagements** aus? Die folgenden Merkmale können herausgestellt werden und sollten bei der Implementierung Beachtung finden:

1. **Ganzheitliche IT-Strategieorientierung:** Geschäfts- und IT-Strategie müssen so in Übereinstimmung gebracht werden, dass die Gesamtstrategie der Organisation die Ausgestaltung der IT-Strategie ganzheitlich – und wechselseitig – ermöglicht („Strategic Alignment“) und IT-Architekturen darauf bezogen sinnvoll abgeleitet werden.
2. **Grad der Standardisierung:** Die Einführung von standardbasierten Hard- und Softwarelösungen führt zu erhöhter Datenverfügbarkeit und erleichtert die Flexibilität und Anpassungsfähigkeit der IT-Systeme.
3. **Modularität und Integration:** Durch eine modulare, integrierte Systemarchitektur lassen sich Skalierbarkeit, Effizienz und Ressourcenauslastung von IT-Anwendungen wesentlich verbessern.
4. **Wirtschaftlichkeit der IT:** Auf Grund der verschärften Wettbewerbssituation vieler Unternehmen und des damit verbundenen Kostendrucks müssen zunehmend betriebswirtschaftliche Betrachtungen (ROI, TCO) in den Vordergrund treten. Ziel ist es, durch eine Konsolidierung der IT auch die explodierenden Kosten für IT-Wartung bzw. Pflege in den Griff zu bekommen.
5. **Vorhandene Komplexität der IT-Landschaft:** Ist die Komplexität der IT-Landschaft zu hoch, gilt es, Hardware-Systeme (Server, Storage, Netze etc.), Daten (Datenbanken) und Applikationen zu konsolidieren. So kann eine Verbesserung der betrieblichen Effizienz erreicht sowie eine erhöhte Verfügbarkeit des Gesamtsystems sichergestellt werden. Der Verwaltungsaufwand wird reduziert, die Supportkosten werden gesenkt.
6. **Flexibilität in der Anwendungsrealisierung:** Die veränderten wirtschaftlichen Rahmenbedingungen erfordern eine höhere Flexibilität und schnellere Reaktionsfähigkeit (Time to Market) bei der Realisierung von IT-Anwendungen. Nur so lassen sich entscheidende Wettbewerbsvorteile realisieren.

Einen Überblick über mögliche Zielsetzungen in Verbindung mit der Einführung und Optimierung von IT-Architekturmanagement gibt Abbildung 3.2.



Praxistipp:

Eine wesentliche Aufgabe für das IT-Management besteht darin, ausgehend von strategischen Überlegungen und den vorliegenden Anforderungen die gewünschte **IT-Entwicklung als Orientierungsrahmen** vorzulegen: dies ist im Kern die **Zielarchitektur** für die IT-Infrastruktur und die Applikationslandschaft. Dazu sind Gestaltungsprinzipien und Systementscheidungen zu formulieren, ebenso wie „strategische“ Technologien und Produkte (als Standards) definiert und in geeigneter Form im Unternehmen kommuniziert werden sollten. Im Sinne eines erfolgreichen **Strategic Alignment** müssen daraus auch verbindliche „Roadmaps“ zur weiteren IT-Entwicklung abgeleitet werden (etwa die Erarbeitung konkreter Architektur-Vorgaben und -Standards).

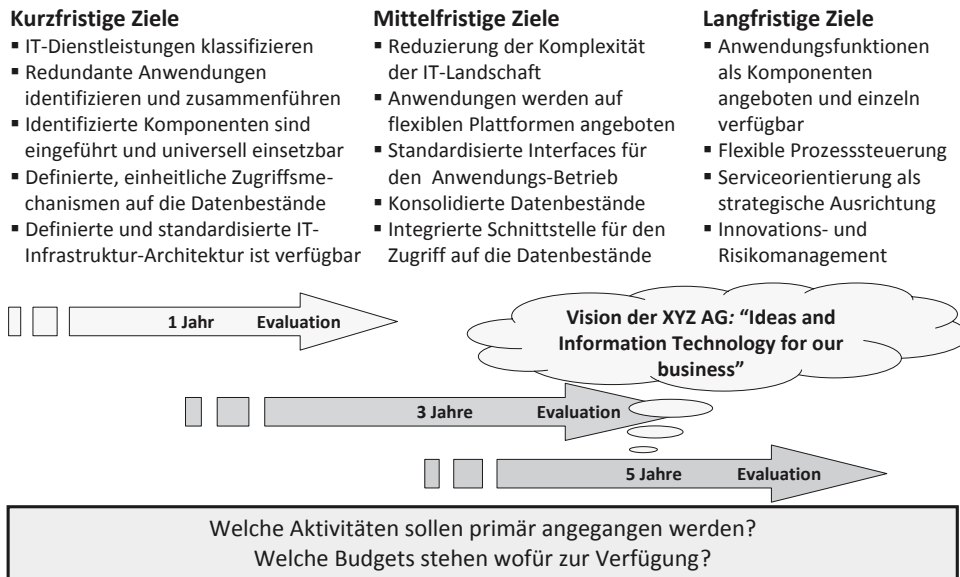


ABBILDUNG 3.2 Vision-Map zu Zielen im IT-Architekturmanagement

Nach Darlegung der Herausforderungen und Ziele stellt sich natürlich die Frage, wie der Begriff **IT-Architekturmanagement** genauer eingeordnet werden kann und welche Aspekte wie in der Praxis umzusetzen sind. Vielfach wird Architekturmanagement auch als die Lehre und Kunst der Strukturierung von IT-Systemen verstanden. Dabei geht es im IT-Architekturmanagement beispielsweise um Fragen,

- wie IT-Systeme strukturiert werden,
- wie verschiedene IT-Systeme zusammenwirken und
- wie die Komplexität von IT-Umgebungen mit Hilfe geeigneter Strukturierung beherrscht werden kann.

Abgegrenzt werden sollte der Begriff „IT-Architekturmanagement“ vom Begriff „**Enterprise Architecture Management**“ (kurz EAM). Ziel von EAM ist es, durch einen ganzheitlichen Blick die gesamte Unternehmensarchitektur in allen wesentlichen Teilbereichen (Domänen) transparenter zu machen und damit die Planbarkeit und Steuerbarkeit des Unternehmens sowie seiner Produkte und Services zu verbessern (in jedem Fall ist ein klares Top-down-Vorgehen gegeben).

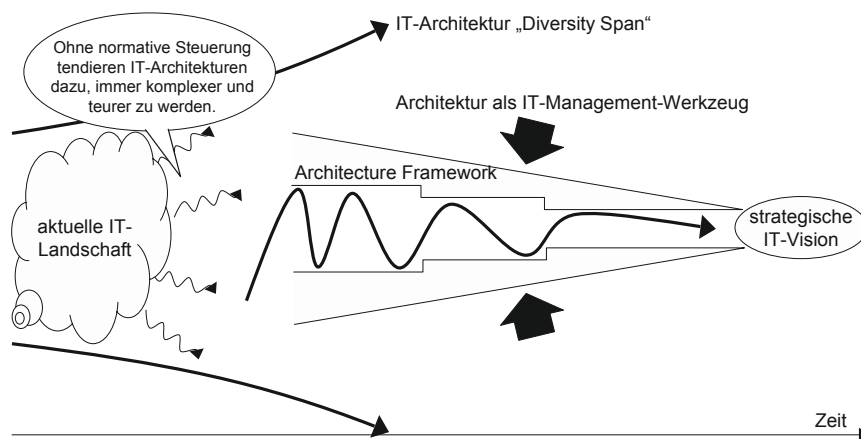
Mit der **Enterprise Architecture** werden die wesentlichen Elemente der Unternehmensarchitektur erfasst und dokumentiert; diese umfassen im Kern – ausgehend von der Unternehmensstrategie – die Geschäftsprozesse (Geschäftsprozessarchitektur oder fachliche Architektur), die Applikationen (Anwendungs- oder Applikationsarchitektur) sowie die zugrundeliegende IT-Infrastruktur mit ihren Komponenten (Technologiearchitektur). Ergänzend können die Geschäftsfelder (Geschäftsfeldarchitektur), die Datenarchitektur (Informationsarchitektur), die Softwarearchitektur und die IT-Produkte (IT-Servicearchitektur) aufgenommen und strukturiert dokumentiert werden

Aus den Ausführungen lassen sich wesentliche **Handlungsebenen für das Architekturmanagement** ableiten, die in der Checkliste in Tabelle 3.1 aufgezeigt werden.

TABELLE 3.1 Handlungsebenen für das IT-Architekturmanagement

Teilaktivitäten	Erläuterungen/Hinweise
Positionierung und Eckpunkte für die Umsetzung festlegen	▪ Institutionalisierung des Architekturmanagements (Planungs- und Steuerungsaufgaben, Prozesse) ▪ Kontinuierliche Entwicklung und Pflege der Architektur ▪ Situationsabhängige Durchsetzung der Architektur (etwa in IT-Projekten).
Ist-Architekturen erheben, beschreiben und analysieren	▪ Die vorhandenen Anwendungs- und Systemwelten sind systematisch zu strukturieren, der Ist-Zustand zu erheben und ganzheitlich in Bezug zu den Geschäftsarchitekturen zu dokumentieren. ▪ Dokumentation der Domänen (mit den jeweiligen Elementen und Beziehungen) sowie der Vernetzungen zwischen den Domänen ▪ Aus der Analyse und Bewertung der Ist-Architekturen lassen sich erste Stärken und Schwächen ableiten.
Soll-IT-Architekturen definieren und dokumentieren	▪ Durch die Definition von Soll-IT-Architekturen werden Rahmenbedingungen für eine flexible Anpassung der Informationstechnologien an veränderte Marktanforderungen geschaffen. ▪ Mit der Festlegung der Soll-IT-Architekturen lassen sich Unternehmensstrategien und Technologieentwicklungen sehr gut verbinden, um so den Aufbau von inkompatiblen IT-Systemen weitgehend zu verhindern.
Abstimmungen zwischen IT und Fachbereich vornehmen und Entscheidungsvorlagen erstellen	▪ IT-Architekturen stellen eine gemeinsame Entscheidungsbasis für den IT-Bereich, die Fachbereiche und das Management dar. ▪ Klare IT-Architekturen ermöglichen gezielte Analysen und fördern so Entscheidungsprozesse unter Berücksichtigung vielfältiger Sichtweisen.

Abbildung 3.3 zeigt, unter welchen Rahmenbedingungen moderne IT-Architekturen zu einem wesentlichen Managementinstrument werden.

**ABBILDUNG 3.3** IT-Architektur als Managementinstrument



Erfolgreiches Architekturmanagement erfordert abgestimmte und „gelebte“ Prozesse sowie verankerte organisatorische Strukturen (Rollenkonzepte, Gremien), um aus den strategischen Zielsetzungen des Unternehmens adäquate Fach-, Software- und Systemarchitekturen ableiten zu können, die optimal aufeinander abgestimmt sind.

■ 3.2 Ordnungsrahmen und Grundausrichtungen für das Architekturmanagement

Um die IT-Landschaft sicher steuern (lenken) und zukunftsorientiert weiterentwickeln (planen) zu können, ist für das IT-Management ein tragfähiges **Gesamtbild der IT-Architekturen als Orientierungsrahmen** unverzichtbar: die **Ist-Architektur** und **Ziel-Architektur** von Infrastruktur und Anwendungslandschaft. Dazu sind Gestaltungsprinzipien und Systementscheidungen zu formulieren, ebenso wie „strategische“ Technologien und Produkte (quasi als Standards) vereinbart und sodann kommuniziert werden sollten. Im Sinne des **Strategic Alignment** muss daraus auch die Konzeption von Zukunftsszenarien oder verbindlichen „Roadmaps“ für die weitere IT-Entwicklung ableitbar sein, ebenso wie jegliche Erarbeitung konkreter Vorgaben und Standards und die Möglichkeit einer sachgerechten Bewertung und Kontrolle.

Der Auftrag zur Entwicklung bzw. Steuerung eines komplexen Informationssystems in einem großen Unternehmen (also der IT- oder Enterprise-Architektur) lässt sich mit einem Auftrag zur Erschließung eines Wohngebietes in einer Stadt vergleichen. In beiden Fällen gibt es:

- gewachsene Strukturen (oft über lange Zeiträume)
- viele unterschiedliche Akteure mit unterschiedlichen Interessen
- lange Zeiträume für die Umsetzung struktureller Änderungen
- Steuerungs- und Kontrollstrukturen (Governance) auf verschiedensten Ebenen der Organisation

Im Rahmen des **Managements von IT-Architekturen** bedarf es in Analogie dazu

- der Festlegung eines **Ordnungsrahmens** mit der Beschreibung der grundlegenden Architektur-Elemente,
- der Formulierung einer **Vision** und daraus abgeleiteten strategischen **Architektur-Zielen** sowie
- der Entwicklung und der laufenden Verfolgung (der Einhaltung) von **Architekturprinzipien**.

3.2.1 Grundelemente einer Enterprise- bzw. IT-Architektur

Um zu einem geeigneten Ordnungsrahmen zu gelangen, wird eine IT-Architektur für Unternehmen häufig in Form folgender Grundbausteine beschrieben:

- Technologie-Architektur (IT-Infrastrukturen, die als sog. IT-Infrastructure-Layer aus der Abbildung 3.4 ersichtlich sind)
- Anwendungsarchitektur (Applikations-Architekturen, die typischerweise als Business-Layer bzw. Knowledge-Layer im Schichtenmodell abgebildet werden)
- Geschäftsarchitektur (fachliche Architekturen, Prozesse)
- Daten-/Informationsarchitektur

Eine Möglichkeit der **Systematisierung von IT-Architekturen** orientiert sich an Schichtenmodellen. Dies zeigt etwa das Beispiel in Abbildung 3.4.

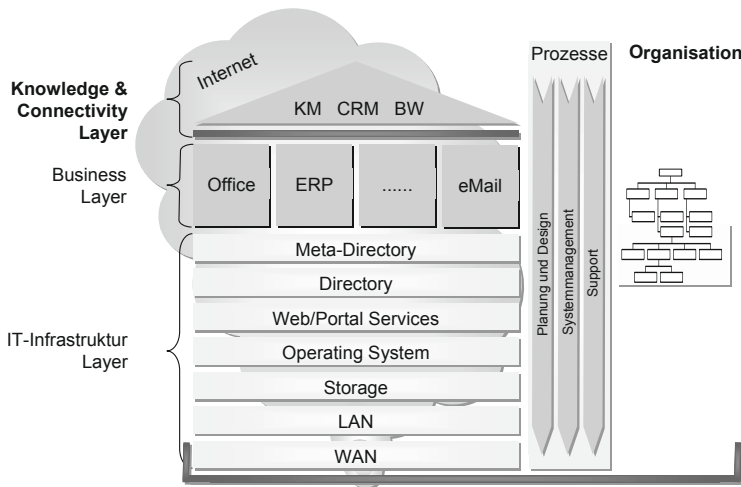


ABBILDUNG 3.4
IT-Architekturen als
Schichtenmodell

Diese Bereiche geben – technologieorientiert – den Rahmen für viele wesentliche Umsetzungsmöglichkeiten in der Praxis und auch für strategische Diskussionen vor. Von besonderer Relevanz ist aber auch die ganzheitliche Betrachtung auf Unternehmensebene und die Entwicklung von Architekturen im Großen sowie die Berücksichtigung der Wechselwirkungen zwischen den verschiedenen Architektur-Bausteinen. Sie zeigen, dass innerhalb der Anwendungslandschaft eines Unternehmens nicht von „der“ IT-Architektur, sondern von mehreren IT-Architekturen gesprochen werden muss.

Ein organisatorischer Rahmen (Rollen, Aufgaben, Prozesse) ist ebenso notwendig wie die Abgrenzung der Domänen. All dies bildet dann den Ordnungsrahmen für das Management der Architekturen. Ein entsprechendes Orientierungsgerüst zeigt (in Anlehnung an *Accenture*) die Abbildung 3.5.

Planungs-Bereiche:

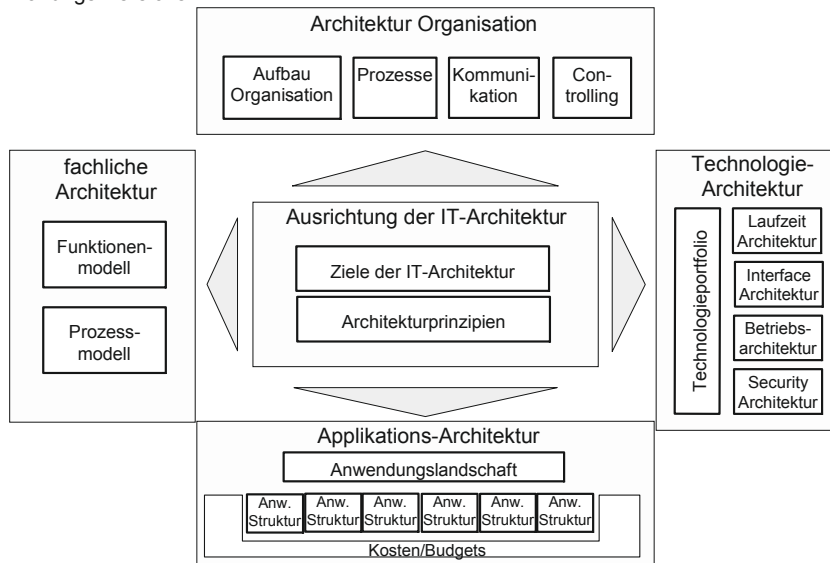


ABBILDUNG 3.5 Ordnungsrahmen für das IT-Architekturmanagement/Enterprise Architecture Management

Orientiert an dieser Festlegung kann die Konkretisierung eines Ordnungsrahmens für die jeweilige Organisation erfolgen. Zur Klarheit der begrifflichen Einordnung der Vielzahl praktischer Vorschläge finden Sie nachfolgend eine Zuordnung von meist synonym gebrauchten Bezeichnungen der Architekturelemente (Tabelle 3.2):

TABELLE 3.2 Einordnung der Architekturbegriffe

Begriff	Synonym verwendete Begriffe
Technologie-Architektur	▪ Infrastructure Architecture (IT-Infrastruktur-Architektur) ▪ System- und Sicherheitsarchitektur
Applikations-Architektur	▪ Application Architecture ▪ Anwendungsarchitektur ▪ Solution Architecture ▪ Software-Entwicklungsarchitektur ▪ Informationssystemarchitektur (umfasst mitunter die Kombination von Anwendungs- und Datenarchitektur)
Geschäftsarchitektur	▪ Fachliche Architektur ▪ Business Architecture ▪ Prozess-Architektur
Datenarchitektur	▪ Informationsarchitektur ▪ Information Architecture
Systementwicklungsprozess	▪ Softwareentwicklungsprozess-Architektur ▪ Anwendungsentwicklungsprozess ▪ Vorgehensmodell-Architektur
IT-Service-Architektur	▪ IT-Prozess-Architektur

3.2.2 Zielsetzungen und Handlungsprinzipien für das IT-Architekturmanagement

Grundvoraussetzung für die ebenso ganzheitliche wie nachhaltige Optimierung der IT-Landschaft ist die Festlegung von Architekturprinzipien, die eine wesentliche Leitlinie für das Handeln bei der Planung und Entwicklung von Architekturen bilden. Eine angestrebte eindeutige Neuausrichtung der gesamten Architektur bedarf darüber hinaus der Formulierung der strategischen Zielrichtung auf Basis der übergeordneten Unternehmensziele.

Wie sehen die wesentlichen Rahmenbedingungen und Zielsetzungen bei Einführung eines systematischen IT-Architekturmanagements aus? Detailziele, die sich – etwa orientiert an einer Balanced-Scorecard – daraus ableiten lassen, zeigt das Referenz-Anwendungsbeispiel in Tabelle 3.3.

TABELLE 3.3 IT-Architektur-Zielkatalog (Beispiel aus einer Referenzorganisation)

Zielbereiche	Zielsetzungen
Finanzielle Ziele	▪ Wirtschaftlich agierende IT gewährleisten ▪ TCO-Werte zu den Architekturen reduzieren ▪ Anteil an Neuinvestitionen erhöhen (Innovationsgrad der IT-Architekturen steigern) ▪ IT-Architektur-Wertbeitrag für das Business erhöhen
Kundenziele	▪ Kundenzufriedenheitsgrad mit den IT-Architekturen steigern ▪ Nutzungsgrad der eingesetzten IT-Architekturen erhöhen ▪ Architektur-Awareness beim Kunden erhöhen ▪ Lösungsentscheidungen zum Architektureinsatz in Kooperation mit dem Fachbereich erleichtern/versachlichen ▪ Beitrag der IT-Architektur zur Qualitätssicherung bewerten ▪ System- und Anwendungsarchitektur kommunizierbar machen (ggf. SLAs zu implementierten Architekturen verbessern) ▪ Zuverlässigkeit und Zukunftssicherheit gegenüber Kunden der IT durch Architekturentwicklung gewährleisten bzw. steigern ▪ Bedarfsorientierung der IT-Anwendungen erhöhen (durch angepasstes IT-Architektur-Anforderungsmanagement)
Architektur-Prozess-Ziele (IT-Service-Ziele)	▪ Architekturprozesse effektiv (Zeit, Qualität) gestalten ▪ Qualität der Ergebnisse der Architekturprozesse verbessern ▪ Einhaltung von Richtlinien/Vorgaben für Architekturen sicherstellen ▪ Software-Architekturentscheidungen verbessern ▪ Abstimmung zwischen den IT-Bereichen erleichtern ▪ Störungen/Ausfall der IT-Systeme zielsicher managen (Impact-Analysen ermöglichen und erleichtern)
Personalziele	▪ Hohe Mitarbeiterzufriedenheit sichern (insbesondere der IT-Architekten) ▪ IT-Architektur-Know-how des IT-Personals kontinuierlich entwickeln ▪ IT-Personal mit IT-Architektur-Know-how nachhaltig an das Unternehmen binden

Zielbereiche	Zielsetzungen
Ziele zu den IT-Systemen/ IT-Services	▪ Komplexität der IT-Systeme reduzieren ▪ Transparenz zur Hardware-Architektur erhöhen (Assets, Netzwerk, ...) ▪ Entscheidungssicherheit zu IT-Technologie-Auswahl- und Einsatzentscheidungen erhöhen ▪ Transparenz der Software-Eigenentwicklungen erhöhen ▪ Transparenz der Anwendungs-Architektur erhöhen (Layer) ▪ Daten-/Informationstransparenz erhöhen ▪ IT-Konsolidierung optimieren ▪ Dokumentation zu IT-Produkten/IT-Systemen verbessern ▪ Re-use-Faktor erhöhen (Stichwort SOA) ▪ Agilität der IT-Anwendungen steigern
Ziele zu den IT-Projekten	▪ Planungssicherheit für IT-Projekte erhöhen ▪ Migrationsplanung optimieren (ggf. Entscheidungssicherheit erhöhen, Portfoliomanagement)

In einem weiteren Schritt sind die IT-Architekturprinzipien zu formulieren und – falls vorhanden – ggf. fortzuschreiben. Als **Architekturprinzipien** werden alle Grundsätze und Leitlinien verstanden, die bei der Planung, der Umsetzung und beim Management der Unternehmens- bzw. IT-Architekturen (und den dabei festgelegten Informationssystemen bzw. IT-Lösungen) gelten sollen (vgl. [HA09], S. 27). Im Wesentlichen sind dabei die Anforderungen an die Gestaltung der IT-Landschaft zu fixieren, die

- standardisierend (Definition von Standards),
 - komplexitätssteuernd (Reduktion von Komplexität) und
 - richtungsgebend (Unterstützung von Auswahl- und Einsatzentscheidungen)
- wirken.

Architekturprinzipien haben also beispielsweise Einfluss auf die Planungsaktivitäten, darüber hinaus auf die Projekte (Auswahl und Steuerung des Projektportfolios) und auf die unternehmensübergreifende Steuerungsarbeit (Steuerung des Produkt-/Serviceportfolios, etc.). Die Prinzipien sind grundsätzlich anzuwenden. Abweichungen von den Grundsätzen sind nur mit entsprechender Begründung möglich. Prinzipien sind an sich beständig, werden also nicht durch den schnellen Technologie- oder Produktwechsel beeinflusst.

Beispiele für Architekturprinzipien und ihre Zuordnung zu Kategorien zeigt Tabelle 3.4.

TABELLE 3.4 Architekturprinzipien (Beispielkatalog)

Kategorie	Architekturprinzip
Value und Finanzen	▪ Wirtschaftlichkeit von eingesetzten Architekturen und der davon betroffenen Services, Prozesse und Projekte ▪ Nutzenmaximierung für die Auswahl und den Einsatz neuer Architekturen (Value-Management-Prinzip)
Kunden	▪ Kundenorientierte Kommunikation und Präsentation der IT-Architekturen

Kategorie	Architekturprinzip
Prozesse	- Compliance-Prinzip: Architekturentscheidungen erfordern die Beachtung der Konformität mit Recht und Normen - Sicherheit der IT-Architekturen gewährleisten - Standards festlegen und einhalten
Personal	- Klare Zuordnung von Verantwortlichen für die implementierten Unternehmensarchitekturen (und den damit verbundenen Prozessen und Services sowie den gespeicherten Daten) - Kommunikation auf der Basis eines einheitlichen Architekturverständnisses
Produkte/ Services	- Hohe Verfügbarkeit der implementierten IT-Architekturen - Sicherung einer weitgehenden Technologieunabhängigkeit - Reduktion und Begrenzung der Systemkomplexität
Projekte	- Beschlossene Architekturveränderungen sind über Projekte (Migrationsprojekte) zu realisieren - Verwendung von Vorgehensmodellen bei der Entwicklung von Anwendungen (bzw. bei der Vornahme von Veränderungen/Releases)
Anwendungen	- Mehrfachnutzung von Anwendungen und Services - Entscheidungsorientierung an Referenzarchitekturen - Opensource-Software als zulässige Einsatzoption - Hohe Benutzerfreundlichkeit der Anwendungen
Daten	Konsistente und redundanzfreie Datenhaltung

Den skizzierten Prinzipien ist in der Praxis absoluter Vorrang einzuräumen. Die Prinzipien geben den Gestaltungsrahmen vor, innerhalb dessen IT-Lösungen entwickelt und Architekturen eingesetzt werden. Die Bewertung der Qualität von Projekten oder bei Architekturentscheidungen erfolgt primär anhand der Einhaltung der Architekturprinzipien.

In einem nächsten Schritt bietet sich eine Detaillierung der jeweiligen Architekturprinzipien anhand eines Templates an. Ein Beispiel zeigt die Tabelle 3.5 für das Wirtschaftlichkeitsprinzip für IT-Architekturen.

TABELLE 3.5 Architekturprinzip „Wirtschaftlichkeit von IT-Architekturen“

Architekturprinzip	Wirtschaftlichkeit von IT-Architekturen (und der davon betroffenen Services, Prozesse und Projekte)
Beschreibung	Alle Architekturentscheidungen sind unter wirtschaftlichen Gesichtspunkten zu prüfen und werden so getroffen, dass nicht nur eine isolierte Wirtschaftlichkeit, sondern eine für die Gesamtorganisation hohe Wirtschaftlichkeit erzielt wird.
Begründung	Zunehmender Kostendruck bei den Kunden erfordert eine Neupositionierung bei der Erstellung von IT-Lösungen. Das Prinzip „Gut genug“ ist zu berücksichtigen.
Voraussetzungen zur Anwendung des Prinzips	Bereitstellung eines Portfolios an anwendbaren Methoden zur Wirtschaftlichkeitsberechnung Verfügbarkeit und Bereitstellung von Kosten- und Nutzendaten zur Anwendung der verfügbaren Verfahren

Anwendungskontext	Typische Anwendungskontexte (mögliche Prozesse und Projekte) sind: ▪ Ermittlung eines Business-Case für IT-Projekte ▪ Bewertungen zu Architekturen und Architekturbereichen unter Wirtschaftlichkeitsaspekten ▪ phasenweise Entscheidungshilfe über Architekturen im IT-Produkt-lebenszyklusmanagement
Anwendungshinweise	▪ Produkte und IT-Lösungen sind so zu dimensionieren, dass (nichtfunktionale) Anforderungen richtig erfüllt und nicht übererfüllt werden. ▪ Eine einfache und schnell durchführbare Redimensionierung/ Skalierbarkeit ist vorzusehen. ▪ Preise für neue, wirtschaftlichere IT-Lösungen sind so zu gestalten, dass ein maximaler Anreiz für eine schnelle Migration von alten, weniger wirtschaftlichen IT-Lösungen besteht.



Merke: Architekturprinzipien stellen eine wesentliche Leitlinie für Planungen und Entscheidungen im Architekturmanagement dar. Gleichzeitig unterstützen sie verschiedene andere strategische und operative Unternehmens- bzw. IT-Prozesse. Architekturprinzipien ermöglichen eine Orientierung für die Planung und Entwicklung von IT-Landschaften (Bebauungsplanung), dienen neben Architekturvorgaben zur Steuerung in Richtung einer Ziel-Architektur, unterstützen die Ziel-gerichtete Kommunikation bei der Gestaltung der IT-Landschaft und werden bei der Steuerung im Architekturmanagement in weiteren (mit dem Architekturmanagement verbundenen) Prozessen genutzt; etwa im IT-Projektportfoliomanagement, für das IT-Produkt-Lebenszyklusmanagement und in Projektmanagement-Prozessen.

■ 3.3 Dokumentation der Architekturen – Beschreibungsmodelle und Praxisbeispiele

Voraussetzung zur Entwicklung, Planung und Steuerung von IT-Architekturen ist es, die Ist-Situation der jeweiligen Unternehmensorganisation und ihre Architekturelemente in geeigneter Form zu dokumentieren. Dazu bieten sich mittlerweile zahlreiche **Beschreibungsmodelle** und **Dokumentationsformen** an, wobei natürlich vor allem in Abhängigkeit von dem jeweiligen Architekturbereich (der Domäne) Unterschiede gegeben sind.

Im Wesentlichen finden sich folgende Argumente, **warum IT-Architekturen einheitlich und aussagekräftig dokumentiert** werden müssen:

- Eine Dokumentation der IT-Landschaft ist unerlässlich, um Zusammenhänge zwischen Geschäftsprozessen, Anwendungen (IT-Applikationen) und IT-Komponenten zu verstehen.
- Ohne aktuelle IT-Architekturdokumentation befinden wir uns im Hinblick auf Planungen und Entscheidungen zu IT-Architekturen im „Blindflug“.

- Eine transparente IT-Architekturdokumentation ist ein hervorragendes Kommunikationsinstrument für das IT-Management (gegenüber Kunden und weiteren Stakeholdern).
- Eine Architekturdokumentation schafft auch Transparenz hinsichtlich der angewandten Methoden und Verfahren und der verwendeten technologischen Umsetzungen. Sie erhöht letztlich die Sicherheit im täglichen Handeln für verschiedene IT-Bereiche (IT-System- und IT-Servicemanagement u. a.).

Die Bereiche der Architektur (Geschäftsarchitektur (fachliche Architektur), Anwendungsarchitektur (Applikationsarchitektur), Technologiearchitektur (IT-Infrastrukturen, die als sog. IT-Infrastructure-Layer dargestellt werden) sowie Daten- und Informations-Architektur geben den Rahmen für Umsetzungsmöglichkeiten in der Praxis und auch für strategische Überlegungen verschiedenster Art vor.



Merke: Von besonderer Relevanz für die Dokumentation ist die ganzheitliche Betrachtung auf der Ebene der Gesamtorganisation. Die Erfassung und Beschreibung von Architekturen sollte „im Großen“ ansetzen (quasi als Big Picture) sowie die Wechselwirkungen zwischen den skizzierten Bausteinen der Architektur berücksichtigen.

Für jede Architektur-Variante sind nachfolgend die wichtigsten Merkmale angegeben, die zur Beschreibung und Dokumentation wesentlich sein können. Orientierung dazu bietet die Tabelle 3.6.

TABELLE 3.6 Architekturvarianten und Darstellungs-/Dokumentationsformen

Varianten	Darstellungen/Elemente
Geschäftsarchitektur (Fachliche Architekturen, Prozessarchitektur)	Die Geschäfte, Geschäftsfelder bzw. Geschäftsprozesse werden standardmäßig durch Wertschöpfungsketten und Fachlandkarten bzw. Prozesslandkarten abgebildet. In Detailabbildungen wird dann etwa die eEPK (= erweiterte ereignisgesteuerte Prozesskette) verwendet. Weitere Bereiche können die Darstellung der Geschäftsfelder und der Geschäftsfunktionen betreffen. Möglich sind auch die Fixierung der Steuerungsmechanismen.
Applikations-Architekturen	Eine Applikations-Architektur bestimmt die Ausrichtung der künftigen Anwendungslandschaft und macht konkrete Entwicklungsvorgaben. Für die wichtigsten Anwendungsgruppen sind die Applikationen zu clustern und in Diagrammen (Cluster-Darstellungen) abzubilden. Außerdem sind verbindliche Architekturleitlinien aufzustellen, wobei für jede Applikation plattformunabhängig grundsätzlich die gleichen Prinzipien und Leitlinien gelten.
Technologie-Architekturen	Eine Technologie-Architektur (Infrastruktur-Architektur) ▪ dokumentiert die technischen Komponenten der IT-Systeme und Standards für alle Infrastrukturebenen; ▪ skizziert „Roadmaps“ für die zukünftige Leistungsentwicklung; ▪ gibt konkrete Produktentscheidungen für eine Organisation vor (etwa die Standards für Server, PCs etc.).
Daten- und Informationsarchitekturen	Die Datenobjekte sind zum Beispiel in ERM-Modellen zu beschreiben. Darüber hinaus ist die gesamte Datenorganisation in Vernetzung zu dokumentieren und zu analysieren.

3.3.1 Dokumentationsformen für IT-Architekturen

Grundsätzlich ist festzustellen, dass durch eine strukturierte Dokumentation der IT-Architekturen sich ein wichtiger Nutzen für jede Organisation ergibt: Die inventarisierte IT-Architektur schafft Transparenz und macht so Auswirkungen geplanter Änderungen auf Anwendungen, Geschäftsprozesse und weitere Elemente der Architektur vorhersehbar. Damit verbundene Risiken lassen sich zielgerichteter erkennen und abschätzen. Prinzipiell unterscheidet man **drei Arten der Dokumentation**.

- **Textuelle Beschreibung** der IT-Architektur (Enterprise Architecture)
- **Tabellarische Darstellung** der IT-Bebauung
- **Grafische Darstellungen** zu den Architekturen (in der Regel als vernetzte Darstellungen zur Visualisierung von Zusammenhängen und Schnittstellen)

Bei der **textuellen Dokumentationsvariante** handelt es sich um eine reine bzw. primär verbale Darlegung zu den Architekturdomänen und ihren Elementen. Diese Dokumentationsart ist nur in sehr eingeschränkter Form und für kleinere Systeme sinnvoll. Sobald es sich um ein etwas umfangreicheres System handelt, geht schnell der Überblick verloren („Textwust“).

Die Dokumentationsform **Tabelle** ermöglicht es sehr gut, die Zusammenhänge zwischen zwei Größen (z. B. Applikationen und unterstützte Geschäftsprozesse) darzustellen und daraufhin verschiedene Analysen vorzunehmen (z. B. Gap-Analysen).

Die **grafische Form** der Dokumentation verwendet freie oder standardisierte Grafikelemente und eignet sich sowohl für ein Big Picture (als Überblick) als auch besonders gut zur Darstellung einzelner Architekturkomponenten und deren Zusammenhängen (Vernetzungen).



Zu beachten ist: Zentrale Einflussfaktoren für die Festlegung der Dokumentationsform für die IT-Architekturen (die IT-Bebauung) sind die Ziele und Fragestellungen bzw. Anforderungen der verschiedenen Stakeholder. Ein wichtiges Hilfsmittel zur Beantwortung der Fragestellungen sind verschiedene Visualisierungen und Auswertungen.

Im Einzelnen sind die folgenden **spezifischen Dokumentationstypen für IT-Architekturen** verbreitet:

1. **Clustergrafiken:** Applikationen und Geschäftsarchitekturen selbst lassen sich gut über eine so genannte Clustergrafik visualisieren. So können beispielsweise Prozesse oder Funktionen in fachlichen Blöcken gruppiert werden (als fachliche Domänen), um etwa einen fachlichen Rahmen für die Weiterentwicklung der IT-Bebauung bereitzustellen. In ähnlicher Form fasst man Anwendungen (Applikationen) in Applikationsblöcken zusammen, die etwa besondere Integrationszusammenhänge oder gleiche Adressatengruppen aufweisen.
2. **Anwendungslandkarte:** Diese Visualisierungsform gibt eine Übersicht über die wichtigsten Anwendungen (Applikationen) des Unternehmens, indem sie die Anwendungen und ihre Schnittstellen aufzeigt. Schnittstellen können in eigenen Diagrammen verfeinert dokumentiert werden.
3. **Zuordnungstabellen:** Mit Zuordnungstabellen besteht die Möglichkeit, die Art der Beziehung zwischen den wesentlichen Elementen der IT-Architektur zu visualisieren. So lässt

sich beispielsweise sehr übersichtlich darstellen, welche Applikationen welche Geschäftsprozesse unterstützen. Auf diese Weise erhält man einen guten Überblick über die Zusammenhänge von Geschäftsarchitekturen und Applikationsarchitekturen.

- 4. Bebauungsplan-Grafik:** Sie ermöglicht die Darstellung von Zusammenhängen zwischen den Elementen der Unternehmensarchitektur in Form einer Matrix. Durch eine flexible Zuordnung von Elementen zu Zeilen, Spalten und Inhalt der Grafik kann eine Vielzahl von Fragestellungen beantwortet werden. Zudem lassen sich Eigenschaften der Inhaltselemente über unterschiedliche Farben und Linientypen visualisieren, um so zusätzliche Informationen bereitzustellen (etwa hinsichtlich der Bewertung).



Hinweis: Umfang und Art der Informationen, die zu den IT-Architekturen dokumentiert werden, orientieren sich an den Zielsetzungen und den vorhandenen bzw. geplanten Architekturmanagementprozessen. Während bestimmte Informationen für alle Prozesse vorzuhalten sind, kann für weitere Elemente der Unternehmensarchitektur, z. B. Schnittstellen und Daten, eine spezifische Detaillierung erfolgen. Der Erhebungs- und Pflegeaufwand bleibt auf diese Weise kalkulierbar.

3.3.2 Technologie-Architektur

Die Technologie-Architektur nimmt eine ganzheitliche Sicht auf die Systeminfrastruktur einer Organisation (eines Unternehmens) vor. Dazu zählen sowohl das technische System mit ihren diversen Komponenten (Hardware, Plattformen, Standorte, Netzwerke) als auch die Konfiguration sowie (im weiteren Sinne) das Management des Systems. Im Kern zeigt die Technologie-Architektur die Elemente der technischen Basissysteme, die technischen Konzepte, Standards und Produktvorgaben. Wichtige Fragen in diesem Zusammenhang:

- Welche Grundsätze sollen hinsichtlich des Einstiegszeitpunktes bzgl. der Technologie-Architekturen gelten („Leader“, „Early follower“, „Cheapest“ ...)?
- Welcher Zentralisierungs-/Dezentralisierungsgrad der Systeme wird angestrebt?
- Welches Sourcing wird angestrebt und wie stellt sich die Finanzierung dar? (Lease or buy?)
- Wie soll mit Einheitlichkeit/Heterogenität umgegangen werden? (Standards?)

Aus **Infrastruktursicht** werden die verschiedenen IT-Komponenten in infrastrukturelevante Schichten gegliedert, beispielsweise um für ein IT-Arbeitsplatz-, Server- und Host-Umfeld einen Orientierungsrahmen zu finden. Dieses Vorgehen zielt gleichzeitig auf die Vorgabe verbindlicher Standards und Produkte zur Integration und Homogenisierung der Infrastruktur.

Zur Beschreibung der Ist-Architekturen ist es von Vorteil, wenn ein ordentliches **Asset-Management** im Einsatz ist. Um einen Überblick über eine komplexe IT-Infrastruktur zu bekommen, ist es notwendig, alle Komponenten zu erfassen. Solche Komponenten lassen sich wie folgt kategorisieren:

- Rechnertypen (technische Details, Betriebssysteme, Standorte, Anzahl)
- Backup-Systeme (Backup-Server, Datensicherungsanlagen, USV etc.)
- IT-Netze (Art der Netze, technische Details, Standorte der Netzanbindung)

- Peripheriegeräte (Drucker, Scanner, Datenspeicher etc.)
- Besondere Ein-/Ausgabegeräte (Mikrofon, Telefonschnittstelle, Touchscreen, Barcodeleser, Chipkartenleser, RFID-Tag-Lesegeräte, Plotter etc.)

In der **Beschreibung der Infrastruktur-Architektur mit Karten auf Typebene** werden primär die eingesetzten Systeme beschrieben. Ergänzend lassen sich Informationen zur physikalischen Ebene (Instanzen) angeben, denen dann Informationen wie eingesetzte Hardware, Netzwerksegmente, Systembetreuung, Ports oder IT-Adressen zugeordnet werden.

Diagrammtypen zur Dokumentation sind u. a. auch Netzwerkdiagramme. Bei einer Darstellung in Netzwerkdiagrammen besteht die Möglichkeit, den Zusammenhang zwischen Netzwerken, Routern, Switches und verwendeter Hardware (Server, Drucker, etc.) darzustellen. Es besteht dabei durchaus die Option, die verwendeten Symbole benutzerdefiniert anzupassen.

Im Rahmen der Arbeitsplatzarchitektur ist die Ausstattung der Clients festzulegen. In Abbildung 3.6 sehen Sie ein Beispiel zur Darstellung einer Serverarchitektur.

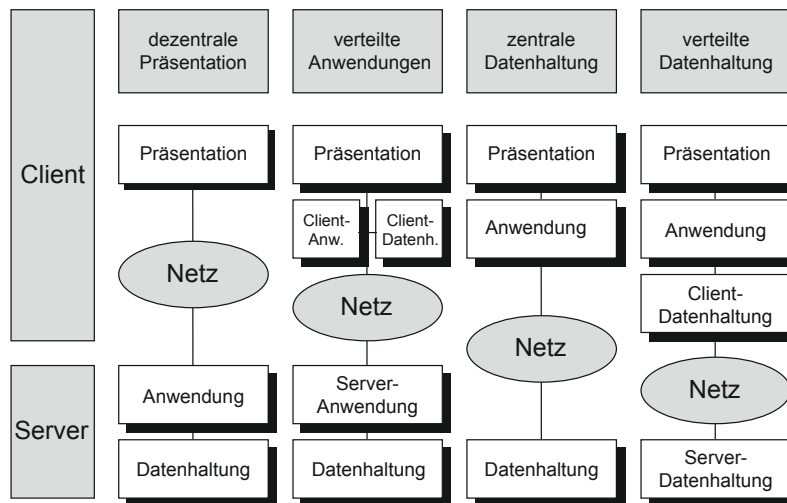


ABBILDUNG 3.6 Client-Server-Architektur-Varianten

Die zweischichtige Architektur (two tier architecture) ist eine Client-Server-Architektur, die softwareseitig als zweischichtiges System aufgebaut ist. Die Rechenkapazität wird dabei weitestgehend auf die Client-Rechner ausgelagert, um den Server zu entlasten. Traditionell kommen ein Fat-Client und ein Fat-Server zum Einsatz. Auf dem Server läuft eine Datenbankanwendung. Die Clients übernehmen dabei die Logik und die Darstellung der Benutzerschnittstelle.

Eine dreischichtige Architektur (three tier architecture) ist eine Client-Server-Architektur mit softwareseitig drei Schichten. Im Gegensatz zur zweischichtigen Architektur (two tier architecture) existiert bei der dreischichtigen Architektur eine zusätzliche Schicht, die Logikschicht, die die Datenverarbeitung vornimmt.

Man unterscheidet im Ergebnis:

- Präsentationsschicht (client tier, front end): Sie ist für die Repräsentation der Daten, Benutzereingaben und die Benutzerschnittstelle verantwortlich.

- Logikschicht (application-server tier, Businessschicht, Middle Tier oder Enterprise Tier): Sie beinhaltet alle Verarbeitungsmechanismen. Hier ist sozusagen die Anwendungslogik vereint.
- Datenhaltungsschicht (data-server tier, back end): Sie enthält die Datenbank und ist verantwortlich für das Speichern und Laden von Daten.



Hinweis: Das Infrastrukturkonzept hat den Vorteil, dass es die Anwendersicht auf die Systeme mit der IT-Sicht auf die Infrastruktur verbindet. Auf diese Weise lassen sich Beurteilungskriterien aus der Anwendersicht (Funktionalität, Flexibilität, Zuverlässigkeit und Schnelligkeit des Bereitstellens von neuen Funktionen) mit Beurteilungskriterien aus der IT-Sicht verbinden (Sicherstellen der Funktionsfähigkeit, Integrationsfähigkeit, Kostenreduktion durch Standardisierung).

3.3.3 Applikations-Architektur

Die Applikations-Architektur stellt einen Plan der eingesetzten Anwendungssysteme, deren Interaktionen und deren Beziehungen zu Kerngeschäftsprozessen der Organisation bereit. In der konkreten Beschreibung der Anwendungsarchitektur werden ergänzend dann die zwischen den Applikationen bestehenden Beziehungen und Schnittstellen analysiert und festgehalten.

Zur Beschreibung der IT-Anwendungen (ERP, E-Mail, CRM u. a.) empfiehlt sich eine Gliederung entlang der Hauptprozesse des Unternehmens (Kern- und Managementprozesse). Mit diesem Vorgehen können aus der Prozess-Sicht heraus Vorgaben für einheitliche Technologien zur Integration und Homogenisierung der Anwendungslandschaft entwickelt werden. Entsprechende Architekturkonzepte liefern für alle relevanten Planungsbereiche der IT konkrete, gegenseitig abgestimmte Konzepte bzw. „Bebauungspläne“ fachlicher und technischer Art, die zeigen, wie eine vorhandene IT-Strategie im Unternehmen umgesetzt werden soll und kann.

Aufbauend auf Standards, die vom Unternehmen für Geschäftsprozesse und Daten zu erarbeiten und vorzugeben sind, werden Architekturkomponenten zur Prozessunterstützung definiert. Die Architekturkomponenten decken durch unterschiedliche Applikationen verschiedene Funktionsbereiche des Unternehmens ab. Das lässt sich beispielsweise sehr anschaulich durch eine Funktionstabelle (Zuordnungstabelle) wiedergeben:

Bei der Planung und Entwicklung von IT-Applikations-Architekturen gilt es darüber hinaus zu beachten, dass mitunter neue geschäftliche Lösungen (etwa aufgrund neuer und veränderter Geschäftsfelder), welche den Kundennutzen erhöhen und/oder die Kosten senken, anstehen. Für die Detailbeschreibung der jeweiligen **Applikations-Architektur** kann eine Unterscheidung nach folgenden Bausteinen erfolgen:

- Die **Funktionalität** beschreibt die Soll-Applikationslandschaft aus zwei Sichten. Die Anwendersicht dient der Darstellung der Soll-Funktionalität der Anwendungen, bezogen auf die Unternehmensprozesse. Die technische Sicht zeigt die Systeme aus IT-Sicht mit ihren Bausteinen, ihrem Zusammenwirken sowie der datenmäßigen Integration.
- Der **System-Design** zeigt die Designprinzipien und genutzten Standards beim Aufbau der Applikationen, inklusive der Positionierung und Integration von eingekauften Komponenten.

**Beachten Sie:**

Die Dokumentation der Anwendungen (Applikationen) zielt unter anderem auf die Vorgabe von einheitlichen Technologien zur Integration und Homogenisierung der Anwendungslandschaft. Eine Anwendungsarchitektur bestimmt so die Ausrichtung der künftigen Anwendungslandschaft und macht konkrete Entwicklungsvorgaben. Für die wichtigsten Anwendungsgruppen sind verbindliche Architekturprinzipien und Leitlinien aufzustellen, wobei für jede Plattform grundsätzlich die gleichen Prinzipien und Leitlinien gelten.

3.3.4 Geschäftsarchitektur

Die Geschäftsarchitektur präzisiert die Business-Strategie, Steuerungsmechanismen, Organisation und Kerngeschäftsprozesse (Definition nach TOGAF). **Objekte**, die im Rahmen einer **Dokumentation der Geschäftsarchitektur** primär erfasst und dargestellt werden, sind:

- die **Grundstrukturen des Geschäfts** (incl. der Darstellung der Geschäftsziele),
- **Prozesse/Geschäftsprozesse**,
- **Organisationsstrukturen**
- und **Ressourcen** (Akteure, Sachmittel etc.).

Folgende Teilaktivitäten zur ganzheitlichen Dokumentation und Umsetzung der Geschäftsarchitektur können dabei vorkommen:

- Festlegung einer prozessorientierten Ausrichtung auf strategischer Ebene (Identifikation der Geschäftsfelder und Geschäftsprozesse);
- das Erstellen von Wertschöpfungsdiagrammen und Prozesslandkarten (in der alle wesentlichen Geschäftsprozesse identifiziert und definiert sind);
- das Benennen der Prozessverantwortlichen sowie der Festlegung der Aufgaben, Rechte und Pflichten (Organisation und Ressourcen);
- die Einführung und Umsetzung eines mit den Unternehmenszielen abgestimmten Prozesscontrollings (Planung, Kontrolle, Informationsbereitstellung).

Für eine Dokumentation der Geschäftsprozesse ist es unverzichtbar, die Geschäftsprozesse zu systematisieren. Dabei findet sich für eine Klassifizierung/Kategorisierung die Unterscheidung in Kern-, Unterstützungs- und Managementprozesse.

Um eine Dokumentation vornehmen zu können, ist oft vorab eine Erhebung der Ist-Situation notwendig. **Darstellungsformen für Geschäftsarchitekturen** (fachliche Architekturen, Prozess-Architekturen) gibt es sehr viele. Als Beispiele seien genannt:

- Wertschöpfungsdiagramme und Prozesslandkarten
- Bebauungspläne (Fachstrukturen)
- Ereignisgesteuerte Prozessketten
- Swim-Lane-Diagramme

**Beachten Sie:**

In der Geschäftsarchitektur werden die wesentlichen Geschäftsfelder, Dienstleistungen (Services) und die dafür benötigten Funktionen (Aufgaben), Prozesse, Lokationen, Rollen und Informationen sowie deren Beziehungen untereinander aufgenommen.

3.3.5 Datenarchitektur

Die Datenarchitektur beschreibt den statischen Zusammenhang zwischen Daten, die für das gesamte Unternehmen von Interesse sind, in Form von Datenmodellen. Darüber hinaus sollten die Struktur des logischen und physischen Datenbestandes einer Organisation sowie die Ressourcen zur Datenhaltung dokumentiert werden.

Aufgabe der Festlegung der Datenarchitektur und der Standardisierung ist es einmal, die unternehmensweit bedeutsamen Daten zu definieren, für einzelne Sichten (z.B. Vertriebs-sicht der Kundendaten, Buchhaltungssicht der Kundendaten) die jeweils verantwortlichen Organisationseinheiten zu identifizieren und ihnen die Kompetenz und Werkzeuge für die Verwaltung der Strukturen und Inhalte zu übertragen. Ohne ein unternehmensweites Master Data Management entstehen ungewollte Redundanzen, d.h. identische Daten werden mehrfach gespeichert oder aber inkonsistente, d.h. sich inhaltlich widersprechende Datenbestände.

Grundlage für die Abbildung der Datenarchitektur ist die Erhebung und Analyse der bestehenden Anwendungen und Informationsquellen. Daten müssen konsistent und redundanzfrei verwaltet werden. Dazu sind die Datenobjekte in der Organisation systematisch zu erfassen, zu strukturieren und Anwendungen zuzuordnen. Auf diese Weise lassen sich Abhängigkeiten erkennen, die bei der Planung und Weiterentwicklung der Anwendungen zu berücksichtigen sind. Durch ein adäquates Daten-Management wird außerdem die Konzeption der zukünftigen Datenarchitektur ermöglicht.

**Praxistipp:**

Die zur Realisierung von Geschäftsprozessen benötigten Daten müssen identifiziert und dokumentiert sowie mit ihren Beziehungen in einer Datenarchitektur beschrieben werden. Die Beschreibung sollte in einem Modell und einer Darstellungsform erfolgen, die die Gesamtheit der Daten vollständig für alle an Informationssystem-Entwicklungsprozessen beteiligte Akteure verständlich und konsistent wiedergibt.

Die Darstellung der Informations- bzw. Datenarchitekturen erfolgt in der Regel über ERM-Diagramme. Diese geben eine Datenübersicht sowie eine geeignete Beschreibung der Daten. Diese detaillierten Daten können dann in den Prozessbeschreibungen wieder verwendet werden; um Input-/Output-Daten von Aktivitäten, den Datenfluss und den Datenaustausch zwischen den Prozessbeteiligten zu beschreiben. Auch dienen die Datenobjekte als Grundlage, um den Datenaustausch zwischen den Applikationen zu beschreiben. Sie können darüber hinaus den Schnittstellen hinterlegt werden.

Folgende Fragen bedürfen in diesem Zusammenhang einer Klärung:

- Gibt es ein Verzeichnis aller Daten (Datenbanken/Datenbestände) des Unternehmens?
- Gibt es eine Klassifikation der Daten nach der Bedeutung für das Unternehmen?
- Ist sichergestellt, dass alle Daten Eigner haben?
- Ist geklärt, welche Pflichten/Rechte ein Daten-Eigner hat?
- Ist geklärt, wie für die Korrektheit und Vollständigkeit der Daten gesorgt wird?
- Gibt es Regelungen hinsichtlich der Datenverwendung?
- Gibt es Regelungen in Hinblick auf die Datenspeicherung (was, wo, wie, wie lange ...)?
- Datenzugriff via Internet?

Die Vermutung, dass in den riesigen Datenbanken wertvolle Informationen versteckt sind, hat zur Entwicklung leistungsfähiger Analysewerkzeuge geführt. Grundsätzlich gibt es zwei Möglichkeiten, die in Data Warehouses enthaltenen Informationen zu analysieren: OLAP-Analysen und Data-Mining. Auch hierüber gilt es strategische Festlegungen zu treffen.

**Beachten Sie:**

Die Architekturdokumentation (Beschreibung und Bewertung der IT-Architekturen) muss in regelmäßigen Abständen aktualisiert werden. So können Veränderungen in der IT-Architektur widerspiegelt und somit die Leistungsfähigkeit der IT-Systeme und IT-Prozesse verbessert werden. Die Architekturdokumentation wird unternehmensweit eingesetzt und zu jeder Architekturentscheidung herangezogen.

Die Architekturkomponenten sind so zu beschreiben, dass Entwicklungs- und Betriebsanforderungen abgedeckt werden. Die Architektur wird die strategischen Prozesse und Architekturmodelle unterstützen und agiert somit bereichsübergreifend. Es bietet Vorteile, gerade für die Dokumentation der Architekturen Tool-Unterstützung zu nutzen.

■ 3.4 IT-Architekturen planen und ausgestalten

Die Umsetzung der Konzepte des Architekturmanagements verändert in vielen Organisationen die Art und Weise, wie die Planung, Entwicklung und Einführung von Informationssystemen durchgeführt wird. Rollen und Abläufe müssen verändert werden, um die Architekturen erfolgreich planen und einführen zu können.

Nur in seltenen Fällen wird eine IT-Architektur wie vom Reißbrett nach vorgegebenen Standards und mit einheitlicher Methodik modelliert und implementiert – vielmehr beherrschen gewachsene Systeme mit unterschiedlichen Lebenszyklen die IT-Landschaft von Organisationen. Durch die immer weiter fortschreitende Vernetzung von Systemen und Applikationen entsteht – wie eingangs bereits ausführlich dargelegt – ein komplexes Geflecht von Beziehungen

und Abhängigkeiten. Dieses Geflecht muss handhabbar, steuerbar und stringent gestaltet sein und dem Architekten als Planer Mechanismen zur Verfügung stellen, um die Anforderungen aus der Unternehmensstrategie erfüllen zu können. Dazu ist auch eine Zuweisung der entstehenden Kosten an Geschäftsprozesse vonnöten, um die Erfolge der IT zur Unterstützung der Unternehmensstrategie messbar zu machen. Eine Gesamtorientierung gibt Abbildung 3.7.

Initialisierung durch Technologie-, Infrastruktur- und Anwendungsstrategie:

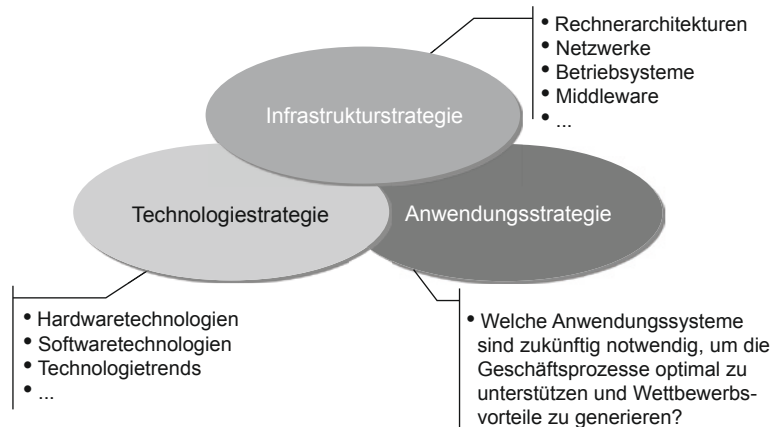


ABBILDUNG 3.7 Orientierungen für das IT-Architekturmanagement



Praxistipp:

IT-Architekturen müssen immer die Geschäftsprozesse unterstützen! Das Geschäft ist dynamisch und bringt jeden Tag neue Herausforderungen. Stellen Sie Ihre Architektur und Serviceorganisation darauf ein.

3.4.1 Generelle Vorgehensweise zur Architekturplanung

Im Rahmen des IT-Architekturmanagements sind Entscheidungen darüber zu treffen, wie eine standardisierte Entwicklung, Integration, Installation und Wartung (Modifikation) von IT-Systemen (IT-Architekturen) aufgrund von IT-Strategien erfolgen kann. Einen beispielhaften Überblick über einen möglichen Prozess in der Praxis und dabei einbezogene Akteure (Gruppen) gibt Abbildung 3.8.

Grundsätzlich gilt, dass die Erarbeitung einer IT-Strategie und der davon abgeleiteten IT-Architektur und Infrastruktur ein inkrementeller, iterativer Prozess ist. Dies soll auch die Abbildung 3.8 als Praxisbeispiel veranschaulichen. Jeder Durchlauf soll den Reifegrad des Ergebnisses erhöhen und nach Möglichkeit zusätzliche Bereiche abdecken. Die Initiierung eines Durchlaufs kann sowohl zeitgesteuert (reguläre Planung und Fortschreibung von Strategie und IT-Architekturen, mindestens einmal im Jahr) als auch ereignisgesteuert sein (gestartete bzw. laufende Projekte, Umweltänderungen).

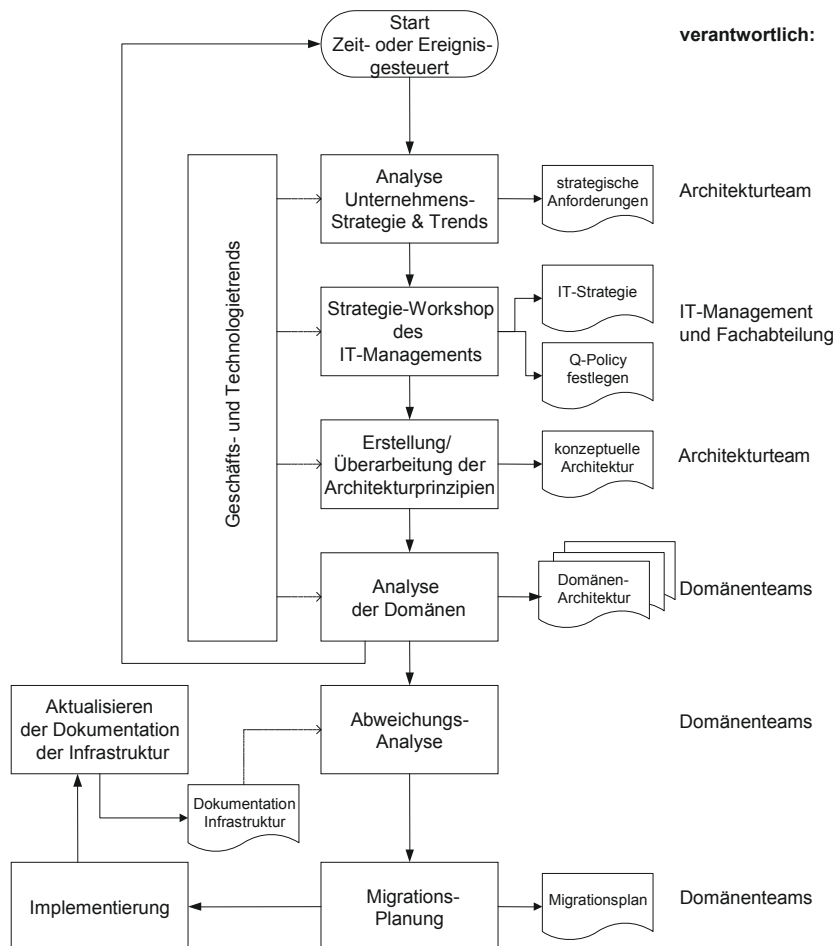


ABBILDUNG 3.8 Entscheidungen zu IT-Architekturen

In einem ersten Schritt sind vom Architekturteam die Anforderungen und die sich daraus ergebenden Auswirkungen auf die IT-Strategie zu analysieren. Die wesentlichen Treiber für die IT-Strategie werden festgehalten. Danach werden die daraus abgeleiteten Informationsbedürfnisse aufgezeigt. Im nächsten Schritt werden die aktuellen Markttrends analysiert und auf ihre Relevanz für das Unternehmen hin untersucht. Aus all diesen Grundlagen wird dann eine für Fachbereich und IT gemeinsame Vision der strategischen Anforderungen an den IT-Betrieb abgeleitet.

Ausgehend von den strategischen Anforderungen wird im Beispielfall vom Linienmanagement des IT-Bereichs im Rahmen eines Workshops die IT-Strategie der Organisation entwickelt bzw. angepasst. Diese beschreibt die Rolle der IT im sich ändernden Umfeld und liefert übergeordnete Zielsetzungen für alle Bereiche, von der technischen Architektur über anzustrebende Kooperationen bis hin zum Personaleinsatz und zur Personalentwicklung. Ein weiteres Ergebnis des Workshops sind eine eventuell erforderliche Aktualisierung der Q-Policy und die aktuellen Qualitätsziele für das laufende Jahr.

Aufbauend auf den strategischen Anforderungen und der IT-Strategie, wird unter Berücksichtigung der aus den Projekten des Unternehmens kommenden Anforderungen die **konzeptuelle Architektur** entwickelt bzw. in späteren Durchläufen adaptiert:

- Ein wesentliches Ergebnis sind die Architekturprinzipien. Diese stellen einen Satz logischer und konsistenter Grundsätze dar, die für alle technologischen Entscheidungen als Leitlinie dienen. Für jedes Prinzip werden die Begründung und die sich daraus ergebenden Auswirkungen dargestellt.
- Weiterer Inhalt der konzeptuellen Architektur ist die Definition und Abgrenzung der für das Unternehmen relevanten Domänen, – logisch zusammengehörende Teilbereiche der Infrastruktur, wie beispielsweise Betriebssysteme, Netzwerk oder Anwendungen.

Für jede Domäne sollte es ein von einem Domänenarchitekten geleitetes **Domänenteam** geben. Dieses

- legt Design-Prinzipien für die Domäne fest,
- identifiziert die für die Domäne relevanten Technologien und
- beschäftigt sich mit den dafür verfügbaren Standards.

Produkte und deren Lebenszyklus werden festgelegt und darauf aufbauend Konfigurationen erarbeitet. Für jede Domäne werden die Ergebnisse in der **Domänenarchitektur** festgehalten.

Diese Architektur wird anschließend mit dem Ist-Zustand abgeglichen und bei entsprechendem Bedarf ein Migrationsplan erstellt. Danach erfolgt die Implementierung der erforderlichen Änderungen. Nach erfolgter Implementierung wird die Beschreibung der aktuellen Infrastruktur entsprechend adaptiert, um beim nächsten Durchlauf für den erforderlichen Abgleich zur Verfügung zu stehen.

Es gibt Schnittstellen zu praktisch allen Prozessen, da die strategischen Vorgaben von allen zu berücksichtigen sind. Dies betrifft natürlich vor allem den Systementwicklungsprozess. Weil der Systementwicklungs-Prozess eine sehr breite Palette an Entwicklungs- und Integrations-tätigkeiten abdeckt (beispielsweise Entwicklung und Wartung von Anwendungssoftware, Installation von Systemsoftware und Hardware, Releasewechsel, Customizing von Standardsoftware, aber auch Rapid Application Development, Entwicklung von Internet/Intranet-Homepages etc.), steht im Normalverfahren auf oberster Ebene ein **allgemeines Prozessmodell**, das aus verschiedenen Phasen besteht:

- Zielanalyse
- Entwicklung/Integration
- Abnahme

Dieser Umsetzungsprozess aus dem Architekturmanagement wird über einen **Projektauftrag** oder über eine **IT-Anforderung** oder einen **internen Auftrag** angestoßen. Auslöser für den Prozess sind Anforderungen eines **Auftraggebers** zur Erstellung oder Modifikation eines IT-Systems.

Im Normalverfahren ist zu Beginn des Systementwicklungs-Prozesses vom beauftragten Systementwickler eine **Zielanalyse** durchzuführen. Dabei sind folgende Fragen zu klären:

- Welche Ziele will der Auftraggeber mit der Anforderung erreichen?
- Welche groben inhaltlichen bzw. funktionalen Vorgaben macht der Auftraggeber zur Realisierung seiner Anforderung?

- Welche technischen Rahmenbedingungen werden vom Auftraggeber bzw. IT-intern (z. B. durch vorhandene Architekturkonzepte, IT-Infrastruktur und IT-Systeme) vorgegeben?
- Welche organisatorischen Rahmenbedingungen sind vorgegeben?
- Welche Verfügbarkeit (Kritikalität) der IT-Lösung wird gefordert?
- Welche IT-Sicherheitsanforderungen werden vom Auftraggeber bzw. IT-intern vorgegeben?
- Welche weiteren Qualitätskriterien (z. B. hinsichtlich Bedienbarkeit, Performanz, Dokumentation, Produktionsfähigkeit etc.) werden vom Auftraggeber bzw. IT-intern vorgegeben?
- Was kann die Zielerreichung gefährden (kritische Erfolgsfaktoren, Risikoanalyse)?
- Welchen Endtermin für den Einsatz der entsprechenden Lösung fordert der Auftraggeber? Welche Meilensteine und zugehörige Zwischentermine sind erforderlich?
- Welcher Aufwand (IT-Personal und Nicht-IT-Personal) wird für das Vorhaben geschätzt?
- Welche Informationen benötigt der Auftraggeber während des Vorhabens?

Die oben genannten Punkte sind in einem **Pflichtenheft** zu dokumentieren. Insbesondere in IT-Projekten ist jedenfalls ein Pflichtenheft zu erstellen.

Die Phase „**Entwicklung/Integration**“ als Kernstück des allgemeinen Prozesses enthält grundsätzlich die Teilphasen:

- Analyse: Festlegung der detaillierten Anforderungen an das konkrete Vorhaben oder Teilvorhaben
- Design: Festlegung der technischen Umsetzung der Anforderungen
- Implementierung: Umsetzung der Anforderungen wie im Design vorgegeben
- Test: Test des resultierenden IT-Systems oder -Teilsystems

Die Phase „Entwicklung/Integration“ kann abhängig von der konkreten Aufgabenstellung sehr unterschiedlich gestaltet sein: die vier oben genannten Teilphasen können inkrementell, parallel oder iterativ durchlaufen werden; zusätzliche Teilphasen können definiert werden; Teilphasen können wegfallen etc. Der genaue Ablauf wird in verschiedenen Submodellen konkret beschrieben. Folgende konkrete Submodelle sind denkbar:

- Single-Tier-Entwicklung (für die prozedurale Entwicklung und Wartung von zentralisierten Single-Tier-IT-Systemen)
- Multi-Tier-Entwicklung (für die objektorientierte Entwicklung und Wartung von Multi-Tier-IT-Systemen)
- Systemintegration (für RZ-nahe Systementwicklung, -integration und -wartung; insbesondere von Systemsoftware und Hardware)

Die zweischichtige Architektur (two tier architecture) ist eine Client-Server-Architektur, die softwareseitig als zweischichtiges System aufgebaut ist. Die Rechenkapazität wird dabei weitestgehend auf die Client-Rechner ausgelagert, um den Server zu entlasten. Traditionell kommen ein Fat-Client und ein Fat-Server zum Einsatz. Auf dem Server läuft eine Datenbankanwendung. Die Clients übernehmen die Logik und die Darstellung der Benutzerschnittstelle.

Eine Weiterentwicklung stellt die Multi-Tier-Architektur dar. Bei dieser Art der Anwendungsarchitektur wird die Applikation in mehrere diskrete Komponenten aufgeteilt. Meist wird eine Dreischichtenarchitektur (Three-Tier) angewendet, in der Datenbank, Enterprise-Anwendungslogik und Präsentation (Web-Oberfläche oder Client) eingeteilt wird. Jede dieser Komponenten kann auf einem eigenen Computer laufen.

Beachten Sie:

Mit Hilfe einer stringenten und effektiven Vorgehensmethodik im Design von IT-Landschaften und einem integrierten, übergreifenden Management über sämtliche IT-Domänen kann die vorhandene Komplexität der IT-Architektur und der IT-Systeme auf ein optimales Maß reduziert und somit eine Balance aus Effektivität, Effizienz und Flexibilität gefunden und hergestellt werden.

3.4.2 Architekturlandschaften bewerten

Für Planungen und Entscheidungen ist es unverzichtbar, eine Bewertung der vorhandenen Architekturen vorzunehmen. Dazu stehen verschiedene Instrumente und Verfahren zur Wahl. Beispiele sind:

- SWOT-Analyse
- Maturitätsanalyse
- Nutzwertanalyse
- GAP-Analyse
- Impact-Analyse
- Risiko-Analyse

Abbildung 3.9 zeigt ein Beispiel für eine Maturitätsanalyse.

Maturitätsstufe	1	2	3	4	5
Hauptkriterium	Völlige Inkompatibilität zur System-Zielarchitektur	Erhebliche Inkompatibilität zur System-Zielarchitektur	Gewisse Inkompatibilität zur System-Zielarchitektur	Ausreichende Kompatibilität zur System-Zielarchitektur	Völlige Kompatibilität zur System-Zielarchitektur
Teilkriterien	▪ System erfüllt die Erwartungen und Anforderungen der Anwender/Nutzer ▪ System entspricht der angestrebten Zielarchitektur ▪ Kompatibilität der vorhandenen Architektur mit dem Marktstandard				
Indikatoren	Zu hohe Kosten für Weiterentwicklung	Anforderungen nur gering erfüllt	Durchschnittliche Akzeptanz	Nur geringe Abweichungen	Zielarchitektur erreicht, gute Bewertung
Handlungsbedarf (Maßnahme)	Ablösung	Größere Anpassungen	Anpassungen vornehmen	Schwachstellen ausbessern	Kein Handlungsbedarf

ABBILDUNG 3.9 Maturitätsanalyse „Beispielkonzept eines Anwenders“

Unter Anwendung ausgewählter Bewertungsattribute zu den Architekturen (Beispiele sind etwa Kriterien wie Vertraulichkeit, Integrität und Verfügbarkeit) ergeben sich (tabellarisch) gezielt Ergebnisse (sprich: Reifegrade). Die Einstufung der Reifegrade erfolgt in der Regel auf Basis des Capability-Maturity-Modells (CMM). Dieses Modell eignet sich grundsätzlich zur

Beurteilung und Verbesserung der Qualität von Objekten verschiedener Art (so zu Architekturen, Prozessen etc.). Es ermöglicht, Architekturen zu untersuchen und zu beurteilen, inwieweit sie in der Lage sind, die Erstellung von Produkten/Dienstleistungen bzw. die Erbringung von IT-Services in der gewünschten Qualität zu unterstützen. Im Ergebnis werden die Architekturen anhand ihrer Ausprägung einer bestimmten Reifegradstufe zugeordnet. Dieses Modell führt somit auf Basis einer strukturierten und zielorientierten Analyse der einzelnen Architekturen zu Aussagen über die Architekturreife u. a.

Die **GAP-Analyse** entspricht einem klassischen SOLL-IST-Vergleich und verfolgt das Ziel, so genannte „Lücken“ (auch im Sinne von Unterschiedlichkeiten) in den IT-Architekturen bei den zugeordneten Objekten und deren Attributen zu finden. Diese „Lücken“ sollen dann sinnvoll gefüllt werden oder bestätigen gewünschte Effekte (in einer neuen, besseren Architektur). Bei der Gap Analysis wird die zu überbrückende Lücke zwischen einem vorhandenen System und einem Geschäftsprozess, der mit diesem System abgewickelt werden soll, analysiert.

Ein besonderer Schwerpunkt der Architekturbewertung liegt vielfach auf der Anwendung von **Impact-Analysen**. Dieses mittlerweile sehr beliebte und verbreitete Analyseverfahren ermittelt und beschreibt, welche Folgen ein Ausfall eines Infrastrukturelementes auf die Applikationen und die zugeordneten Geschäftsprozesse (also die Geschäftsarchitektur) hat und inwieweit sie eingeschränkt lauffähig sind. Dadurch wird ermöglicht, dass ...

- alle Betroffenen zeitnah verständigt werden;
- Hilfestellungen bei der Fehlereingrenzung schnell vorgenommen werden können;
- das Wissensmanagement für Ausfallsituationen optimiert und
- ein sofortiges Erkennen von Handlungsnotwendigkeiten angezeigt wird;
- die erforderliche Kommunikation zielgerichtet formuliert werden kann.



Insgesamt ist festzuhalten: Für ein effektives IT-Architekturmanagement sind nicht nur einmalige, sondern auch fortlaufende Bewertungen notwendig. Durch die Offenlegung der Stärken und Schwächen der jeweiligen Architektur können Möglichkeiten und Gefahren für das Unternehmen identifiziert und Verbesserungsmaßnahmen untersucht werden. Hierzu bedarf es abgestimmter Bewertungskriterien und klar definierter Bewertungsverfahren.

3.4.3 Soll-IT-Architekturlandschaft entwickeln und darstellen

Auch das Ergebnis der IT-Architekturplanungen ist in geeigneter Weise zu dokumentieren. Ein Beispiel ist in vereinfachter Form in Abbildung 3.10 (nächste Seite) wiedergegeben.

Im Detail werden beispielsweise die Anwendungen (ERP, E-Mail, CRM u. a.) entlang der Hauptprozesse beschrieben. Dieses Vorgehen aus der Prozess-Sicht heraus zielt letztlich auf die Vorgabe von einheitlichen Technologien zur Integration und Homogenisierung der Anwendungslandschaft. Für die wichtigsten Anwendungsgruppen sind verbindliche Architekturleitlinien aufzustellen, wobei für jede Plattform grundsätzlich die gleichen Prinzipien und Leitlinien gelten. Eine Applikations-Strategie bestimmt die Ausrichtung der künftigen Anwendungslandschaft und macht konkrete Entwicklungsvorgaben.

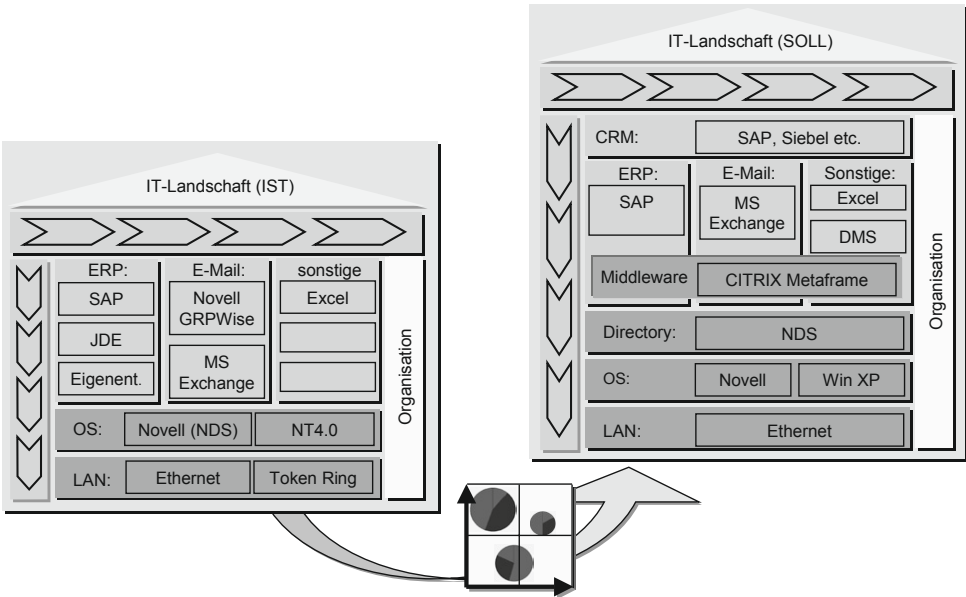


ABBILDUNG 3.10 Von der Ist-Landschaft zum Soll-Konzept für IT-Architekturen

Aus Infrastruktursicht werden die IT-Komponenten in Infrastruktur-relevante Schichten gegliedert, beispielsweise um für ein PC-, Server- und Host-Umfeld einen Orientierungsrahmen zu finden. Dieses Vorgehen zielt auf die Vorgabe von verbindlichen Standards und Produkten zur Integration und Homogenisierung der Infrastruktur. Eine Infrastruktur-Strategie definiert Gestaltungsprinzipien und Standards für alle Infrastrukturebenen, skizziert „Roadmaps“ für die zukünftige Leistungsentwicklung und gibt konkrete Produktentscheidungen vor.

Einen Überblick über die Aktivitäten und Ergebnisse zur Definition der Soll-IT-Architekturen gibt Tabelle 3.7.

TABELLE 3.7 Soll-IT-Architekturen definieren

Teilaufgaben	Mögliche Ergebnisse/Methoden
Bewertungen zu den Ist-IT-Architekturen analysieren	Auswertungen zu den Bewertungen und Analysen
Planungsaufgaben: Entwicklung und Bewertung von Szenarien	Ganzheitlich integrierte Bebauungsplanung/Soll-Architekturen im Kontext von IT-Management (Anforderungs- und Portfoliomanagement, Programm- und Servicemanagement) und durch Szenario-Methoden entwickeln
Formulierung von Standards und Richtlinien	Governance-Regeln zu IT-Architekturen und Standards vereinbaren, Richtlinien der Nutzung fixieren
Projekt-Portfolios erstellen	Umsetzungskonzepte bzw. Konsolidierungs-, Migrations- und Innovations-Projekte werden skizziert und zur Entscheidung „unterbreitet“.

■ 3.5 Organisation der Einführung und Optimierung von Enterprise Architecture Management (EAM)

Bei einer Neueinführung oder Neupositionierung von Architekturmanagement sollte ein gezieltes Vorgehen erfolgen. Tabelle 3.8 zeigt die besonderen organisatorischen Herausforderungen bei der Umsetzung von Enterprise Architecture Management.

TABELLE 3.8 Eckpunkte zur Umsetzung von Enterprise Architecture Management

Teilaufgaben	Mögliche Ergebnisse/Methoden
Organisatorische Institutionalisierung des IT-Architekturmanagements vorschlagen	Positionierung im Unternehmen, Rollenkonzepte, Stellenpläne, Stellenbeschreibungen, Aufgabenverteilungspläne, Organigramme
Prozessbeschreibungen zur kontinuierlichen Entwicklung und Pflege der Architektur erarbeiten	Prozessbeschreibungen zur Fixierung der Aufgaben im IT-Architekturmanagement (Erarbeitung in Workshops)
Projektportfolio-Modell zur Umsetzung von IT-Architekturlösungen entwickeln	Projektportfolios (mit Bewertungen durch verschiedene Akteure)/Meetings der Entscheidungsebene (Boards, etc.)

3.5.1 Aufgaben und Rollenkonzept im Architekturmanagement

Ohne strukturelle und personelle Voraussetzungen ist Architekturmanagement nicht erfolgreich zu verankern. Tabelle 3.9 gibt einen Überblick über typische Aufgabenfelder im Architekturmanagement.

TABELLE 3.9 Typische Aufgabenfelder von IT-Architekten

Aufgabenbereiche	Beispiele
Planungsaufgaben	▪ Zielplanung und Zielanalysen ▪ Soll-Architekturen planen (Bebauungsplanung) ▪ Szenarien zur Neuausrichtung von IT-Architekturen entwickeln (an der IT-Planung mitwirken)
Entscheidungsaufgaben (Analyse, Bewertung, Entscheidung)	▪ Ist-Architekturen analysieren und dokumentieren ▪ Architektur-Prinzipien formulieren und vereinbaren ▪ Architektur-Standards definieren ▪ Serviceportfolio festlegen ▪ Technologie-Management und Umfeldanalyse ▪ Architektur-Frameworks definieren und anwenden

Aufgabenbereiche	Beispiele
Kontrollaufgaben	▪ Abgleich der Architekturen (Prinzipien, Standards, Bebauungspläne entwickeln und pflegen) ▪ Einhaltung von Architektur-Richtlinien kontrollieren ▪ Architektur-Konformität von Change-Projekten prüfen ▪ Wirkungsanalysen und Konsolidierung von Projekten
Kommunikationsaufgaben	▪ Architekturinformationen an Stakeholder kommunizieren (Publikation, Schulung, Beratung) ▪ Kommunikation der architektonischen Auswirkungen an die betroffenen Linien- und Projektbereiche

Es ist aus Erfahrungen festzuhalten, dass Architekturarbeit eigentlich jeden Mitarbeiter der IT betrifft, insbesondere wenn sie als Kernkompetenz verankert ist. Jedoch sind eigenständige Teams zu installieren und Mitarbeiter zu entwickeln, die als qualifizierte „Prozess-Owner“ das Architekturmanagement ausüben. Die einzelnen, durchaus detaillierten Versatzstücke bedürfen der Zusammenführung in einer Gesamtarchitektur, was eben nur über einen querschnittlichen Steuerungsprozess zu leisten ist. Vergleiche hierzu ausführlich [De03] in Kapitel 6.3.

Der **Leiter einer Architekturgruppe** eines großen Unternehmens sieht sich vor die Herausforderung gestellt, verschiedene Architekturentwicklungen koordiniert durchzuführen. Im Kern muss er sicherstellen, dass sein IT-Architekturportfolio einen maximalen Wertbeitrag für das Business der Organisation liefert und gleichzeitig auf erweiterbaren und integrationsfähigen Architekturen beruht.

Der **IT-Architekt** – ob auf Unternehmens- oder auf Bereichs- und Projektebene – hat in der Regel den Auftrag, Architekturen für Informationssysteme termingerecht zu erstellen und Referenzarchitekturen abzuleiten, um so die längerfristige Tragfähigkeit der Anwendungslandschaft sicherzustellen.

Der **Business-Architekt** muss fachliche Architekturen entwickeln und dazu geeignete IT-Anforderungen (IT-Portfolios) berücksichtigen. Dabei ist sicherzustellen, dass das Alignment von Business und IT optimiert wird.

Tabelle 3.10 gibt einen Überblick darüber, welche Rollen im Architekturmanagement denkbar sind:

TABELLE 3.10 Rollenkonzept für das IT-Architekturmanagement

Rolle	Rollenverständnis	Business-Sicht
Business-Architekt	Gestaltung der Business-Architektur	▪ Analyse und Bewertung des IT-Portfolios im Hinblick auf die Elemente der Business-Architektur, ▪ Unterstützung von Software-Entwicklungsprojekten bei der fachlichen Analyse, ▪ Unterstützung bei der Entwicklung fachlicher Architekturen

Rolle	Rollenverständnis	Business-Sicht
IT-Architekt	Planung der IT-Architekturen auf Unternehmensebene	Gestaltung der Informationsarchitektur; Durchführung der übergreifenden Architekturplanung und Architektur-Releaseplanung
Software-Architekt	Design, Test und Realisierung von Softwarebausteinen von Informationssystemen auf der Basis der zugehörigen IT-Architektur	Unterstützung bei der Entwicklung der Softwarearchitektur und der Definition des Entwicklungsprozesses
System-Architekt	Unterstützung und Beratung der Entwicklung von Systemarchitekturen	auf der Grundlage der Plattformstrategie und bestehender bzw. geplanter Basisplattformen
Service-Manager	Abstimmung und Koordination von Anforderungen an die IT-Basis-Infrastruktur und deren Umsetzung	Einbringen von Anforderungen der IT-Basisinfrastruktur in Architektur-entwicklungen
Security-Ingenieur	Unterstützung und Beratung der Entwicklung von Sicherheitsarchitekturen	auf der Grundlage der Security-Strategie und bestehender bzw. geplanter Basisplattformen

**Beachten Sie:**

Allen diesen Rollen ist eines gemeinsam: sie sind an der Entwicklung von IT-Architekturen planend oder durchführend beteiligt. Planend dann, wenn es gilt, Architekturentwicklungen auf der Grundlage des IT-Portfolios übergreifend zu steuern. Durchführend dann, wenn es gilt, ein bestimmtes Informationssystem oder eine wichtige Komponente zu entwickeln und einzuführen.

Um zu einer technischen Gesamtlösung zu gelangen, muss **Architekturkompetenz** die Interessen der einzelnen Fachbereiche, Prozesse und Mitarbeiter effektiv zugunsten eines überlegenen Kundennutzens zusammenführen können. In diesem Verständnis ist Architekturmanagement ein wertschöpfender Mechanismus, der kontinuierlich einen nachhaltigen Wettbewerbsvorteil für das Unternehmen erzeugt, welcher auch langfristig verteidigbar erscheint.

Darüber hinaus sind Teambildungen sinnvoll. Typische **IT-Architekturteams** bestehen aus verschiedenen IT-Mitarbeitern (etwa Produktverantwortlichen) und werden von ein oder zwei Chefarchitekten geleitet. Die wichtigsten Aufgaben des Architekturteams:

- Das Architekturteam ist die treibende Kraft des gesamten Prozesses und soll die Wahrnehmung übergeordneter Interessen bei allen technologischen Entscheidungen sicherstellen.
- Das Architekturteam ist verantwortlich für die Koordinierung aller den Prozess betreffenden Aktivitäten und die Abstimmung mit dem Architektur-Review Board.
- Originäre Aufgaben des Architekturteams sind die Erarbeitung und Abstimmung der „Strategischen Anforderungen“ sowie der „Konzeptuellen Architektur“.

Für jede in der Konzeptionellen Architektur definierte Domäne könnte es (vor allem in größeren Organisationen) ein **Domänenteam** geben, das von einem Domänenarchitekten geleitet

wird. Im Rahmen der Domänenteams werden die für die jeweilige Domäne relevanten Technologien analysiert, die Produktauswahl getroffen und die Implementierung in die Wege geleitet. Das Domänenteam berichtet an das Architekturteam und erhält von diesem neben übergeordneten Prinzipien auch konkrete Aufträge zu speziellen Technologien.

Des Weiteren ist ein **Architektur Review Board** denkbar. Es besteht aus den Hauptabteilungsleitern der für den IT-Betrieb relevanten Bereiche und den Abteilungsleitern des IT-Bereichs. Es ist das Entscheidungsgremium für alle Technologiefragen und berichtet dem Lenkungsausschuss.

**Praxistipp:**

Intensive Kommunikation der Beteiligten ist notwendig. IT-Architekturen unterstützen die Kommunikation der an der Planung und Entwicklung von Informationssystemen Beteiligten durch die Bereitstellung strukturierender Abstraktionen. Diese Überlegungen führen zu folgender These: Management von IT-Architekturen erfordert vor allem Kommunikations- und Methodenkompetenz einer Rolle „IT-Architekt“, die auf angemessenes fachliches und technologisches Know-how gestützt ist.

Beachten Sie, dass sich eine IT-Architektur immer aus verschiedenen hierarchischen Stufen zusammensetzt (angefangen von einzelnen Komponenten über Systeme bis hin zu Domänen interagierender Systeme). Sie kann daher nur im Zusammenspiel dieser hierarchischen Stufen verstanden und effektiv gestaltet werden.

3.5.2 Prozesse im Architekturmanagement

Zur erfolgreichen Planung, Umsetzung und Weiterentwicklung der Enterprise-Architekturen können durchaus gezielte, vereinzelte Projekte (z. B. zur Konsolidierung/Virtualisierung der IT-Landschaften) hilfreich sein. Sie reichen aber überhaupt nicht aus, um nachhaltig die IT-Landschaft zu positionieren und die künftigen Herausforderungen der Geschäftsfelder und der sich daraus ergebenden Geschäftsprozesse des Unternehmens Rechnung zu tragen.

Wichtig sind vielmehr eingeführte und „gelebte“ kontinuierliche Architekturmanagement-Prozesse, die zur Aufnahme von aktuellen Architektur-Anforderungen und technologischen Entwicklungen bzw. zur laufenden Steuerung und Beratung im Architekturumfeld regelmäßig durchlaufen werden. Dadurch, dass im Unternehmen z. B. Änderungen wahrgenommen und umgesetzt werden oder die Entwicklung der Technologie voranschreitet, ist es erforderlich, dass die entworfene Geschäfts- und IT-Architektur kontinuierlich angepasst und ausgebaut wird.

Ein mögliches Einführungsmodell für die Architekturmanagement-Prozesse (Enterprise Architecture Management) ist nachfolgend in Abbildung 3.11 wiedergegeben:

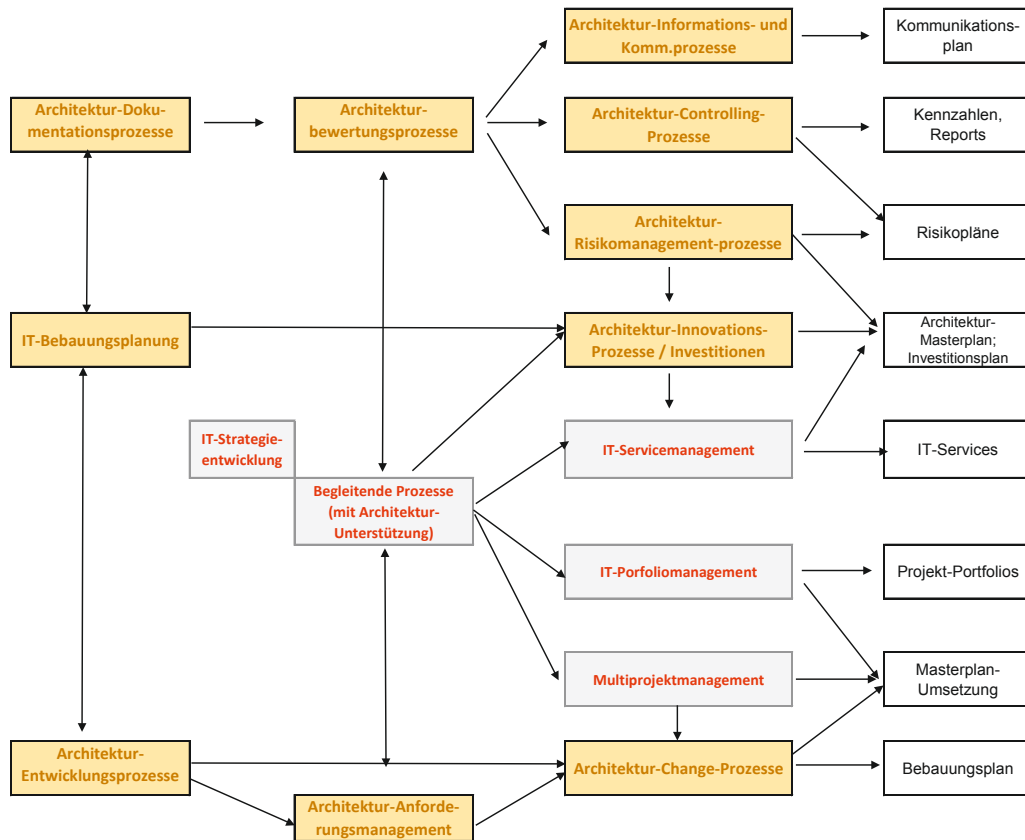


ABBILDUNG 3.11 Roadmap zur Einführung von Architekturmanagement

Die wesentlichen Elemente der hier vorgeschlagenen Architekturmanagementprozesse zeigt die Tabelle 3.11.

TABELLE 3.11 Wesentliche Architekturmanagementprozesse und ihre Teilprozesse

Architekturprozesse (Hauptprozesse)	typische Teilprozesse
IT-Bebauungsplanung	- IT-Strategie (bzw. strategische Ziele) analysieren - Anwendungs- und Systemlandschaft planen - Infrastruktur-Landschaft planen - Gesamtkonzept verabschieden - Architektur-Masterplan vereinbaren/kommunizieren
Architektur-Innovationsprozesse	- Architektur-Trends aufnehmen und dokumentieren - Innovationstrends analysieren - Konzeptentwicklungen für Architekturdomänen - Einführungen von innovativen Architekturen vorbereiten - Innovationen kommunizieren

Architekturprozesse (Hauptprozesse)	typische Teilprozesse
Architektur-Entwicklungsprozesse	▪ Prinzipien, Standards, Bebauungspläne entwickeln und pflegen (Abgleich der Architekturen) ▪ Einhaltung von Architektur-Richtlinien kontrollieren ▪ Architektur-Konformität von Change-Projekten prüfen ▪ Wirkungsanalysen von IT-Konsolidierungen und Projekten durchführen
Architektur-Change-Prozesse	▪ Architektur-Change-Auftrag prüfen ▪ Change planen ▪ Change durchführen ▪ Change-Ergebnis prüfen und abnehmen ▪ Architektur-Change dokumentieren/kommunizieren
Architektur-Dokumentationsprozesse	▪ Dokumentationsstandards festlegen/aktualisieren ▪ Ist-Zustand erheben/sichten; Änderungsmeldungen aufnehmen (etwa aus Change) ▪ Ist-Daten der Architekturen erfassen/dokumentieren (Geschäftsarchitekturen, Datenarchitekturen, Technologiearchitektur, Applikationsarchitektur) ▪ Teildokumentationen konsolidieren und vernetzen
Architektur-bewertungsprozesse	▪ Architekturbewertungsmethoden/-instrumenten festlegen ▪ Architekturbewertungen vornehmen (nach vorgegebenen Kriterien und Verfahren) ▪ Architekturbewertungen analysieren und interpretieren (Maturitätsanalyse, SWOT, Gap, Impact) ▪ Aktionsplan/Änderungsaktivitäten definieren
Architektur-Anforderungsmanagement	▪ Anforderungen zu den Architekturen (Enterprise-Architekturen) aufnehmen/sammeln ▪ Anforderungen harmonisieren und strukturieren ▪ Anforderungen priorisieren ▪ Architektur- und Projekt-Portfolios (Vorhaben) aus Architektur-Anforderungen ableiten
Architektur-Controlling-Prozesse	▪ Kennzahlen-System entwickeln und pflegen ▪ Reporting-Systeme entwickeln und pflegen ▪ Architekturdaten messen/Kennzahlenwerte bereitstellen ▪ Kennzahlenauswertung (Monitoring) ▪ Reporting (Reports bereitstellen und auswerten)
Architektur-Risiko-managementprozesse	▪ Risikoaufnahme/Risikoidentifikation ▪ Risikobewertung und Klassifikation ▪ Risikoanalyse/Auswirkungen ▪ Risikomaßnahmenplanungen/Risikobehandlung
Architektur-Informations- und Kommunikationsprozesse	▪ Stakeholderanalysen durchführen ▪ Kommunikationskonzepte entwickeln ▪ Informations- und Kommunikationsmaßnahmen durchführen ▪ Informations- und Kommunikationsaktivitäten evaluieren

Ausgehend von der tabellarischen Übersicht sollen die wesentlichen Prozesse im Architekturmanagement nachfolgend kurz eingeordnet werden.

Im Rahmen der **IT-Bebauungsplanung** sind Entscheidungen darüber zu treffen, wie eine standardisierte Entwicklung, Integration, Installation und Wartung (Modifikation) von IT-Systemen aufgrund von IT-Strategien erfolgen kann. Dazu gehören folgende **planerische Aufgabenbereiche**:

- Methodische Planung der Unternehmensarchitektur, eingebettet in den strategischen IT-Planungsprozess.
- Konzeption und Entwicklung der fachlichen Architektur begleiten
- Bebauungsplan für die Anwendungslandschaft des Unternehmens entwerfen (Applikations-Landscape)
- Effiziente und bedarfsgerechte Entwicklung der IT-Infrastruktur (Technologie-Architektur) konzipieren
- Risikomanagement für Technologie-intensive Projekte, präventive Planung und Review von Softwarearchitekturen

Um diesen Aufgaben gerecht zu werden, sind von dem IT-Architekten bzw. vom Architekturplanungsteam die Anforderungen und die sich daraus ergebenden Auswirkungen auf die IT-Strategie zu analysieren. Die wesentlichen Treiber für die IT-Strategie werden dabei festgehalten. Danach werden die daraus abgeleiteten Informationsbedürfnisse aufgezeigt. In einem gesonderten Schritt werden auch die aktuellen Markttrends analysiert und auf ihre Relevanz für das Unternehmen hin untersucht. Aus all diesen Grundlagen wird dann eine für Fachbereich (bzw. dem Kunden) und IT gemeinsame Vision der strategischen Anforderungen an die Bebauungslandschaft abgeleitet und überschaubar dokumentiert.

Eng verbunden mit der IT-Bebauungsplanung sind die zu implementierenden **Architektur-Innovationsprozesse**. In diesem Zusammenhang ist festzulegen,

- welche Innovationsinstrumente für das Architekturmanagement bedeutsam sind;
- wie ein optimales Innovationsmanagement eingeführt werden kann;
- welche Integrationen für ein umfassendes Produktdatenmanagement nötig sind (IT-Asset-Management, Configuration-Management, Lizenzmanagement, IT-Product-Life-Cycle-Management).

**Beachten Sie:**

Ein nachhaltiges Innovationsmanagement setzt sowohl eine Kenntnis der Anforderungen des Unternehmens bzw. der Kunden an die Architekturen sowie der Möglichkeiten auf dem Gebiet der Informations- und Kommunikations-Technologie (also ein Wissen um die aktuellen IT-Trends) voraus.

Ein Kernbereich der **Architekturentwicklung** ist die Erstellung, Abstimmung und Abnahme von Blueprints. Entsprechend gestalten sich hier Abstimmungsprozesse anhand von Blueprints, die Standards sowie best practices aufnehmen und im Ergebnis eine Referenzarchitektur anbieten (differenziert nach Sichten, adressiert für verschiedene Zielgruppen). Die Sichten können in Abhängigkeit zu den Zielgruppen von abstrakten, rein fachlichen Schwerpunkten

einer Architektur bis hin zu physischen Aspekten variieren (funktionale und nicht-funktionale Aspekte werden unterschieden). Es gehen sowohl Ist- als auch Soll-Aspekte ein. Die IT-Architekturentwicklung erfolgt in der Regel innerhalb von IT-Projekten und ist daher eng verzahnt mit dem Projektmanagement-Prozess. Kernbereiche sind:

- Blaupausen und Referenzarchitekturen ausgewählten IT-Projekten zur Verfügung stellen;
- Projektberatung zu den auszuwählenden bzw. eingesetzten Architekturen;
- Durchführung von speziellen Architekturprojekten (z. B. Konsolidierungsprojekte).

Die ständige Änderung und Weiterentwicklung der Enterprise-Architektur ist außerdem ebenfalls wichtig (Produktlebenszyklusmanagement) und bedarf der Unterstützung durch klar definierte **Architektur-Change-Prozesse**. Entscheidungen zu den Unternehmensarchitekturen sind ad hoc (etwa aus Anlass einer Neubeschaffung oder bei Eingehen eines Kundenauftrages) bzw. in regelmäßigen Abständen (etwa für das turnusmäßige Reporting) zu treffen. Die Festlegungen zu den betreffenden Architekturen haben häufig erhebliche Auswirkungen auf die zukünftige Fähigkeit des Unternehmens, seine Geschäfte mit IT-Unterstützung erfolgreich zu realisieren.

Die entwickelten Architekturen (vgl. Architekturentwicklungsprozesse) sowie die definierten Fachanforderungen seitens des Kunden (Fachabteilungen etc.) bilden in der Regel den Startschuss für Änderungen bzw. Anpassungen der IT-Architektur. In dem Architektur-Change-Prozess wird die Umsetzung der jeweils entwickelten Architektur im täglichen Arbeitsablauf sichergestellt. Reaktiv werden ggf. Reviews von neuen Geschäftsanforderungen durchgeführt und bestätigt bzw. abgelehnt und alle notwendigen Folgeaktivitäten initiiert. Proaktiv wird definiert, wie und wann neue Architekturkomponenten in den Einführungszyklus aufgenommen werden.

Voraussetzung zur Entwicklung, Planung und Steuerung von Enterprise-**Architekturen** ist es, die Ist-Situation der jeweiligen Unternehmensorganisation in geeigneter Form zu **dokumentieren** (also die Architekturlandschaft zu verwalten bzw. zu pflegen). Dazu bieten sich für die Architektur-Dokumentationsprozesse mittlerweile zahlreiche Beschreibungsmodelle und Dokumentationsformen an, wobei natürlich vor allem in Abhängigkeit von dem jeweiligen Architekturbereich Unterschiede gegeben sind (vgl. Kapitel 3.3 dieses Beitrags). Integriert ist in jedem Fall auch eine laufende Pflege der Architekturdokumentation sicherzustellen. Dies ist beispielsweise erforderlich, wenn neue Technologien bzw. Applikationen verfügbar sind bzw. neue technische Anforderungen (als Ergebnis eines Changes aufgrund geänderter Geschäftsanforderungen) in die Enterprise-Architektur zu integrieren sind.

Notwendig ist die **Orientierung an Dokumentationsstandards**, die vor allem die Inhalte und die Form/Formen der Dokumentation der einzelnen Architekturbereiche sowie deren Vernetzung untereinander festlegen. Abhängig von Architekturbereichen (Geschäftsarchitektur, Daten- und Informationsarchitektur, Applikationsarchitektur, Technologiearchitektur) sind also geeignete Dokumentationsformen zu vereinbaren. Außerdem ist darauf zu achten, dass auch alle notwendigen Architektur-Details erhoben und dokumentiert werden, die für die Erfüllung der Planungs- und Steuerungsaufgaben im Architekturmanagement sowie für die Unterstützung der ggf. initiierten Architekturprojekte sowie der durch Architekten begleiteten IT-Projekte benötigt werden.

**Beachten Sie:**

Bezüglich der Architekturdokumentation empfiehlt sich eine grafische Darstellung der aktuellen Unternehmensarchitektur (ein sog. Big Picture), die die Bereiche IT-Technologie, Anwendungen (IT-Applikationen), Datenarchitekturen sowie Geschäftsfunktionen/Geschäftsprozesse des jeweiligen Unternehmens in ihrem Zusammenhang abdeckt. Mit einer solchen Ist-Dokumentation werden das Management der gesamten IT-Landschaft wesentlich erleichtert, Potenziale für Kostensenkungen gezielt erkannt und die Effizienz der IT insgesamt signifikant erhöht.

Nachhaltig können Entscheidungen zu Architekturen nur dann getroffen werden, wenn zuvor eine gründliche **Bewertung der Architekturen bzw. der Architekturlandschaft** erfolgt ist und umfassende Analysen durchgeführt wurden, die die relevanten Aspekte zu den jeweiligen Entscheidungsobjekten umfassen. Die Art und Weise, wie Architekturen einer Bewertung unterzogen werden, ist in Organisationen mit ausgereifter Infrastruktur in der Regel im Detail vorzugeben. Dabei stellen geeignete Formulare (Dokumentvorlagen) und Checklisten sicher, dass wichtige Fragen, die zur Bewertung und Entscheidung notwendig sind, beantwortet werden.

Als Grundlage für die Bewertung von Architekturen dient einerseits das definierte Set von Kriterien, andererseits auch vereinbarte Bewertungsverfahren. Die Bewertungskriterien werden in einem auf die geschäftlichen Anforderungen zugeschnittenen Schema mit entsprechender Gewichtung abgebildet. Dabei berücksichtigt man sowohl die fachliche und die technische Bedeutung als auch die Dringlichkeit einer Entscheidung.

Um eine klare und akzeptierte Bewertung der Ist-Architekturen vorzunehmen, sollten spezifische Techniken und Verfahren verwendet werden. Die am häufigsten eingesetzten Verfahren zur Analyse und einer daran anschließenden Bewertung der IT-/Enterprise-Architekturen sind folgende: Maturitätsanalyse, Gap-Analyse, SWOT-Analyse, Impact-Analyse, Nutzwertanalyse, Portfoliotechnik, Risikoanalyse, Wirtschaftlichkeitsanalyse sowie Szenariotechnik.

Ein wichtiger Punkt bei der Architekturbewertung ist der Soll-Ist-Vergleich mit der Beurteilung von aktuellen Architekturen im Vergleich mit der Zielarchitektur. Kennzahlen dabei sind erreichte Ziele sowie erzielte Ergebnisse, um sicherzustellen, dass die getätigten Aktionen mit der Soll-Architektur konform gehen.

Im Rahmen der **Architektur-Controlling-Prozesse** geht es im Wesentlichen um das Steuern/Lenken bei der Entwicklung, Planung und dem Einsatz von Enterprise-Architekturen. Diese gezielte Steuerung durch die Unternehmensleitung, die IT-Leitung bzw. die IT-Architekten wird als dringend notwendig gesehen, weil

- die Enterprise-Architekturen – insbesondere die Geschäfts- und Applikationsarchitekturen neben der Technologiearchitektur – in vielen Unternehmen eine zunehmend wichtige Rolle (auch für das Business der Unternehmen) spielen und somit
- deren reibungsloser Einsatz und die konsequente Verbesserung der Geschäftsprozesse mittels geeigneter IT-Architekturen wesentliche Erfolgsfaktoren für die Unternehmen und Verwaltungen darstellen.

**Beachten Sie:**

Ein spezifisches Architektur-Controlling ist heute unverzichtbar, um die Architekturmanagement-Aktivitäten innerhalb einer Organisation transparent zu machen und erfolgreich zu steuern. Werden im Zuge der Umsetzung von Architekturvorgaben und Architekturplanungen Soll-Ist-Abweichungen festgestellt, sind Anpassungsmaßnahmen zu eruieren und ggf. zu ergreifen. Dies ist eine permanente Aufgabe im Architekturmanagement.

Die Identifikation, Analyse und Bewertung der in der Enterprise-Architektur vorhandenen Risiken ist ein wichtiges Element des Architekturmanagement (= **Architektur-Risikomanagementprozesse**). Notwendig für ein erfolgreiches Risikomanagement zu den Enterprise-Architekturen ist in jedem Fall die Differenzierung der Risiko-Arten für die jeweils unter Risikoaspekten analysierten Architekturen. Nur durch eine geeignete Kategorienbildung (etwa zu den Wahrscheinlichkeiten des Risikoeintritts sowie zur Schadenseinschätzung) ist eine differenzierte Risikoanalyse möglich und lassen sich geeignete Maßnahmenbündel ableiten. Insbesondere gilt es, herauszufinden, welche Risiken die größte Aufmerksamkeit brauchen, indem ihr Beitrag zum Gesamtrisiko zu den Enterprise-Architekturen erhoben wird. Die Risikoanalyse beginnt normalerweise bei den Business-Prozessen, die üblicherweise Risiken durch externe Ereignisse ausgesetzt sind. Dies sind beispielsweise Probleme

- im Zusammenhang mit der Einhaltung von Vorschriften,
- im Zusammenhang mit dem Markt und dem Wettbewerb oder
- Sicherheits- und Integritätsprobleme.

Die Analyse der Applikationen, die bestimmte Business-Prozesse unterstützen, liefert daraufhin wichtigen Input für die **Gesamtbewertung der Architekturrisiken**. Die relevanten Applikationen werden im Hinblick auf die Häufigkeit und die Höhe der mit der Gefahr eines Ausfalls verbundenen Verluste bewertet. Auf dieser Basis gilt es dann Maßnahmen zur Risikobehandlung zu formulieren und entsprechend umzusetzen.

Architektur-Informations- und Kommunikationsprozesse sollen sicherstellen, dass alle Architektur-Interessenträger und Betroffenen bzw. Nutzer über die Architektur informiert sind und dass der aktuelle Stand sowie zukünftige Änderungen frühzeitig kommuniziert werden. Informationsbereitstellungsprozesse (Infos zu den IT-Architekturen selektiv an den Kunden bzw. an Stakeholder weiterleiten) umfassen vor allem: Stakeholderanalysen, Informationsaustauschprozesse (Veranstaltungen, Portale) sowie Kunden-Marketing.

Mit einem sorgfältig dosierten Marketing-Mix lassen sich Anerkennung und Erfolg für ein IT-Architekturmanagement erheblich steigern. Die Wirkungen eines professionellen Architektur-Marketings sind weitreichend:

- Aktuelles aus der Arbeit wird zielgerichtet weitergegeben (abhängig von den Interessen der Stakeholder). Der verbesserte Informationsgrad zu den IT-Architekturen geht Hand in Hand mit einer vermehrten Anerkennung der IT-Architekten und der Ergebnisse ihrer Arbeit.
- Bei einem hohen Informationsgrad lassen sich Entscheidungen durch den Auftraggeber leichter durchsetzen. Der Hauptgrund liegt in einem verbesserten Informationsstand und dem sich daraus ergebenden Mehr an Vertrauen in die Qualität der Arbeit.

**Beachten Sie:**

Kernprozesse im Unternehmens- und IT-Management sind die Planung der Architekturlandschaften sowie die kontinuierliche Entwicklung und Beherrschung der installierten Architekturen. Von besonderer Relevanz sind die ganzheitliche Betrachtung auf Gesamtorganisationsebene sowie die Berücksichtigung der Wechselwirkungen zwischen den verschiedenen Bausteinen der IT- und Unternehmens-Architektur.

■ 3.6 Projektierungen von IT-Landschaften – IT-Konsolidierungsprojekte

Im Rahmen von IT-Konsolidierungsprojekten kann den Zielen reduzierter Gesamtkosten, gesteigerter Service Levels und erhöhter Flexibilität in besonderer Weise Rechnung getragen werden. Wesentliche Ansatzpunkte der IT-Konsolidierung sind Vereinfachung, Standardisierung, Modularisierung und Optimierung der IT-Landschaft.

Dazu sollte man schrittweise vorgehen, **erste Maßnahmen** sollten aber rasch eingeleitet werden:

- In einem ersten Schritt sollte die vorhandene Hardware-Vielfalt auf Arbeitsplatzebene auf ein vernünftiges Ausmaß zurückgeschraubt werden.
- Parallel zur Vereinheitlichung der PC-Frontends sollten Serverkonfigurationen entwickelt und standardisiert werden.
- Ein weiterer logischer Schritt zur Kosteneinsparung liegt in der Standardisierung der Software- und Netzwerkdienste.

Der eigentliche **Weg zur IT-Konsolidierung** kann auf verschiedenen Ebenen begonnen werden. Die Wahl des Einstiegspunktes ist dabei abhängig von dem aktuellen Organisationsstand der Infrastruktur und den individuellen Unternehmenszielen (siehe [Ti05]). Im Wesentlichen lassen sich folgende **Konsolidierungsebenen** unterscheiden:

- **Hardware-Konsolidierung:** Dienste, Applikationen und Datenbanken werden möglichst auf wenige, dafür hochverfügbare und dynamische Systeme zusammengeführt. Dies betrifft vor allem Server, Speichersysteme und Netzwerke.
- **Applikationskonsolidierung:** Hier geht es einmal um die Zentralisierung von Funktionalitäten der Anwendungssysteme und ihre Konzentration auf wenige Komponenten. Außerdem ist eine Geschäftsprozessorientierung unverzichtbar.
- **Datenkonsolidierung:** In Unternehmen gibt es Daten, redundante Daten, fehlerhafte Daten und fehlerhafte, redundante Daten. Oft sind sie in unterschiedlichen Datenbanken gespeichert. Über eine Konsolidierung in eine homogene Struktur lassen sich aus all diesen Daten pragmatisch und effizient konsistente Informationen gewinnen.

- **Prozesskonsolidierung:** Die IT-Leistungsprozesse sind zu definieren und zu beschreiben. So lassen sich Optimierungsansätze herausfiltern.

**Beachten Sie:**

Die Gartner-Group geht davon aus, dass sich mit einheitlichen Anwendungen die IT-Kosten um mehr als 25% senken lassen. Allerdings kann man mit unflexiblen Standards keinen Wettbewerbsvorteil erzielen. Hier gilt es einen Kompromiss zu finden.

3.6.1 Hardware-Konsolidierung

Eine typische **Ausgangslage** in vielen Unternehmen und Verwaltungen beschreiben die folgenden Merkmale:

- Der IT-Betrieb wird unter Einsatz einer großen Anzahl von Servern realisiert. Dies hat zur Folge, dass die Verwaltung der Server-Systeme mit einem unverhältnismäßig hohen Aufwand verbunden ist.
- Die mittlere Auslastung der Server ist sehr gering, was vielfach als unwirtschaftlich angesehen wird. Es gibt deshalb Überlegungen, nach Ansatzpunkten zu einer erhöhten Auslastung zu suchen.
- Es existiert eine komplexe Netzwerk-Infrastruktur. Genutzt werden unterschiedliche Netzwerkdienste bei Einsatz spezifischer Systemsoftware.
- Die existierenden Prozesse sind oftmals komplex, was zu unverhältnismäßig hohen Durchlaufzeiten und hohen Prozesskosten führt. Dies gilt sowohl für die Geschäftsprozesse als auch für die IT-Prozesse im Servicemanagement.
- Es finden sich oftmals multiple Kopien von Daten (etwa zu Kundendaten). Dadurch ergibt sich nicht nur ein erhöhter Aufwand, sondern eine überhöhte Fehlergefahr (inkonsistente Daten).

Es gilt deshalb in jedem Fall, die Komplexität zu reduzieren. Ziel ist letztlich eine Standardisierung und Konsolidierung der Hardware-Architektur. Entsprechend den Objekten werden *drei Varianten der Hardware-Konsolidierung* unterschieden:

- *Server-Konsolidierung*
Ziel ist die Konsolidierung von umfangreichen, oft heterogenen und verteilten Serverlandschaften. Dazu zählt:
 - eine Reduzierung der Anzahl der installierten Server,
 - eine Zusammenlegung von vielen (verteilten) Servern in einem einzigen großen System (Scale-Up) und
 - die Optimierung der Kapazitäten der Server.
- *Storage-Konsolidierung*
Eine Konsolidierung von verteilten Storage-Kapazitäten wird vor allem gesehen in
 - einer Optimierung der Speicherkapazitäten sowie
 - einer Effizienzsteigerung bzgl. der Speicherverwaltung.

- *Netzwerk-Konsolidierung*

Hier geht es um die Konsolidierung der vorhandenen Netzwerke. Diese betrifft:

- die Strukturen der Netzwerke,
- die Dienste im Netzbetrieb sowie
- die Systemsoftware.

3.6.1.1 Serverkonsolidierung

In der Vergangenheit erforderten bestimmte Applikationen spezielle Betriebssysteme, die ihrerseits spezielle Hardware benötigten. Das Ergebnis war und ist ein starker Technologie-Mix an Servern, der allein schon ein immenses Einsparpotenzial birgt sowie integriert zahlreiche Serviceverbesserungen ermöglicht (etwa durch eine Reduzierung der Anzahl der zu verwaltenden Server). Durch die starre Zuordnung der Applikationen zu den Servern ist nämlich eine Balance der unternehmensweiten IT nur schwer herzustellen, weil die Systeme bei Änderungen aufwändig umkonfiguriert werden müssen.

Im Detail sind folgende **Handlungsoptionen** zur Serverkonsolidierung gegeben:

- Die Anzahl der installierten Server wird reduziert.
- Viele (verteilte) Server werden in einem einzigen großen System bzw. wenigen großen Systemen zusammengefasst (Scale-Up).
- Es erfolgt eine Optimierung der Kapazitäten der Server.

Im Rahmen einer Serverkonsolidierung sollte insbesondere überprüft werden, ob bei vielen unterschiedlichen Servern keine **Harmonisierung** denkbar ist bzw. eine **Reduzierung der absoluten Anzahl der Server** sinnvoll ist. Eine Zusammenlegung von vielen (verteilten) Servern in einem einzigen großen System (**Scale-Up**) ergibt sich beispielsweise durch eine Konzentration aller Serverressourcen (Prozessoren, Hauptspeicher, Massenspeicher, Netzwerk). Insbesondere Anwendungen profitieren von einer Scale-Up-Architektur:

- Datenbanken
- ERP-Systeme
- Business-Intelligence-Lösungen
- CRM und SCM-Anwendungen

Eine weitere Handlungsoption ist die **Kapazitätsoptimierung der Server**. In früheren Zeiten, als Kostenüberlegungen nicht so stark im Vordergrund standen, wurden Server-Systeme bewusst so ausgelegt, dass evtl. auftretende Spitzenbelastungen möglichst gut abgefangen werden konnten. Auf diese Weise soll vermieden werden, dass die Server in Spitzenzeiten immer wieder überlastet sind. Weil die Spitzenlasten für das einzelne System jedoch vergleichsweise selten auftreten, resultieren aus diesem Ansatz aber auch beträchtliche Reservekapazitäten. Auslastungen von lediglich 20–30 Prozent waren bzw. sind an der Tagesordnung. Es gilt, die vorhandenen Kapazitäten der Server zu managen, aufzubauen, zu planen, zu integrieren und zu kontrollieren.

Als guter Kompromiss aus Performance- und Kostengründen gelten heute dauerhafte Auslastungen von 50–60 Prozent. Einerseits verfügen die Systeme dann noch über genügend Reserve, andererseits sind sie nicht überdimensioniert. Erfahrungsgemäß lassen sich hier im Sinne der „Economies of Scale“ großer Serversysteme etwa die Hälfte der IT-Kosten durch Prozessoptimierung einsparen.



Beispiel: Ausgehend davon, dass jeder Server eine halbe Stunde Wartung pro Woche benötigt, kann ein Administrator bei einer 35-Stunden-Woche etwa 70 Server administrieren. In den Rechenzentren stehen aber häufig mehrere tausend File- und Printserver. Die zuständigen Mitarbeiter sind nahezu ausschließlich damit beschäftigt, diese Systeme zu warten, zu verwalten, also in Betrieb zu halten, und nicht etwa damit, die Prozesse und den IT-Service zu optimieren.

Voraussetzung für eine derartige Konsolidierung ist die „Virtualisierung von Ressourcen“. Realisiert wird dies im Wesentlichen durch intelligente Managementsoftware als logische Zwischenschicht über der Hardware. Ziel ist es, durch eine einheitliche Schnittstelle eine deutliche Vereinfachung des IT-Managements zu bewirken.



Praxistipp:

Serverkonsolidierung verspricht leichtere Administration, mehr Flexibilität und Skalierbarkeit und dadurch die Chance, schneller auf veränderte Unternehmensanforderungen reagieren zu können. Mit heutigen Technologien lassen sich die einzelnen Kapazitäten hingegen als Gesamtkapazität betrachten, was ein wesentlich dynamischeres Agieren ermöglicht. Hinzu kommen Einsparungspotenziale beim Einkauf und Serviceverbesserungen durch eine einheitlichere Administration.

3.6.1.2 Storage-Konsolidierung

In der Praxis ergibt sich bei der Hardware-Infrastruktur aktuell der größte Konsolidierungsbedarf im Bereich **Speicherkonsolidierung** und **Speichermanagement**. Welche Einsparpotenziale im Storage-Bereich möglich sind, lässt sich allein daraus ableiten, dass bei einer TCO-Betrachtung über drei Jahre 80 Prozent der Kosten für Service, Support und Management anfallen.

Die Speicheranforderungen an die IT-Systeme sind in den letzten Jahren enorm (exponentiell) angestiegen. Die Datenexplosion mit den unvermeidlichen Engpässen und Staus verlangt geradezu nach einer Neuorientierung im Storage-Management.

Storage ist eine höchst heterogene Ressource und umfasst zahlreiche Technologien, die wiederum mit verschiedenen Rechnern unter diversen Betriebssystemen verknüpft werden müssen. Dennoch soll diese heterogene Landschaft miteinander laufen und im Fall der Storage-Konsolidierung auch beim Ausfall von Komponenten einen sicheren Weiterbetrieb gewährleisten. In einer geschäftskritischen Umgebung muss daher sofort klar sein, welcher Fehler einen etwaigen Ausfall verursacht hat, sodass möglichst unterbrechungsfrei auf andere Storage-Ressourcen umgeschaltet werden kann.

Die **Herausforderung** im Speicherumfeld besteht genau wie auf Serverseite darin, die Managementaufgaben, die Planung und die Ausfallzeiten so gering wie möglich zu halten. Die IT-Mitarbeiter sind terminlich so eingebunden, dass für mittel- und langfristige Planungen wenig Zeit bleibt. Limitierte Budgets bei erhöhten Verfügbarkeitsanforderungen tun ein Übriges.

Dabei gibt es viele ungenutzte Kapazitäten, die mit den entsprechenden Konzepten, Werkzeugen und der entsprechenden Software ausgereizt werden könnten.

Das Ziel muss folglich eine **Effizienzsteigerung** in der Speicherverwaltung sein. Geschäftskritische Applikationen müssen in die vorhandene Infrastruktur integrierbar sein, ohne sie komplett umbauen zu müssen. Die Speicher-Architektur sollte gewährleisten, dass die Speicherumgebung leicht steuerbar, einfach zu bedienen, hochverfügbar und leicht erweiterbar ist, sowohl von der Hardware- als auch von der Managementebene.



Beispiel zur Verfügbarkeit: Daten wie Applikationen müssen heute 24 x 7, also an 24 Stunden 7 Tage die Woche das ganze Jahr über rund um die Uhr verfügbar sein. Entsprechend muss das Storage Management so ausgelegt sein, dass die Backup-Infrastruktur die Verfügbarkeit und Performance der primären Speichereinheiten im operativen Betrieb nicht beeinträchtigt.



Praxistipp:

IT-Anwender benötigen eine Gesamtlösung, die einen Support einheitlich und komplett aus einer Hand bietet. In der Praxis bedeutet dies, dass der User Speicherkapazität je nach Bedarf in einem Netzwerk bereitgestellt bekommt – und nur die Ressourcen bezahlt, die tatsächlich notwendig waren. Und das an jedem Ort, zu jeder Zeit und bei überall gleich hoher Verfügbarkeit.

3.6.1.3 Netzwerkkonsolidierung

Das Netzwerk bildet vielfach den Kern und das „Nadelöhr“ der gesamten IT-Infrastruktur. In der Konzeption sind die meisten heute implementierten Netzwerke primär darauf ausgerichtet, Daten zu transportieren und Informationen auszutauschen. Die Handhabung von Netzwerken ist zwar einfach, Probleme ergeben sich aber oft für das zentrale Management. Außerdem ist bei „nicht intelligenten“ Netzwerken nicht in jedem Fall transparent,

- welche User oder Komponenten sich im Netz befinden,
- welche Funktion die Komponenten haben oder
- welche Applikationen sich im Einsatz befinden.

Werden gewünschte IT-Leistungen nicht erbracht, wird häufig das Netzwerk dafür verantwortlich gemacht, obwohl in vielen Fällen nicht die Netzwerk-Komponenten an sich, sondern an das Netzwerk angeschlossene Endgeräte diese Schwierigkeiten verursachen. Bei einem unintelligenten Netzwerk hat der Administrator Probleme nachzuweisen, dass das Netzwerk nicht die Ursache für Ausfälle ist. Außerdem birgt ein solches Netzwerk enorme Sicherheitsrisiken, da man nicht weiß, wer gerade versucht, sich am „Netzwerk-Edge“ einzuloggen, geschweige denn, wer sich überhaupt darin befindet.

Während Konsolidierung im Server- und Storagebereich grundsätzlich als Vereinfachung und bessere Nutzung brachliegender Ressourcen verstanden wird, ist Konsolidierung im Netzbereich eher unter dem Schlagwort „Konvergenz“ zu sehen. Dabei setzen Anbieterfirmen auf Architekturen, die Netzwerke mit mehr Intelligenz versieht.

Heute strukturieren die Unternehmen ihre Netzwerke in drei wesentliche Bereiche: einen **Core**-, einen **Distributions**- und einen **Access-Bereich**. Im teuren Core, dem „Hirn“ des Netzes, sitzt die gesamte Intelligenz. Je weiter man sich an den Rand des Netzwerks bewegt, desto

weniger Intelligenz weist das Netzwerk dort auf. Das Management dieser Randkomponenten wie Switches und Hubs ist in heutigen Netzwerken nur eingeschränkt möglich.

**Fazit:**

Wer also im Server- und Speichersegment virtuelle Ressourcenpools aufbauen will, benötigt intelligente Netzwerke. Denn auch neue Technologien wie Wireless LAN müssen sinnvoll und sicher ins Netzwerk integriert werden.

Im Rahmen des **Hardware-Architekturmanagements** findet sich die Vision der Auflösung starrer Systemkonfigurationen, in denen Server-, Speicher-, Netzwerk-Kapazitäten mit einzelnen Anwendungs-Sets zu festen und isolierten „Ressourcenpaketen“ zusammengebunden werden. Mit der Auflösung dieser festen Ressourcenpakete, vor allem der Entkopplung der Server-, Storage- und Applikationsebenen, wird die Voraussetzung geschaffen, vorhandene IT-Ressourcen zu bündeln. Darauf aufbauend, können dann Server- und Storagekapazitäten dynamisch wechselnden Bedarfsträgern zugeordnet werden.

3.6.2 Software-Konsolidierung (Applikationskonsolidierung)

Software-Konsolidierung stellt ebenfalls einen wesentlichen Beitrag zur IT-Service-Optimierung dar. Im Rahmen der Software-Konsolidierung (Anwendungs-Konsolidierung) stehen folgende **Handlungsoptionen** im Mittelpunkt:

- Zusammenlegung verschiedener Anwendungen auf ein oder wenige Server;
- Realisierung der Anwendungsintegration;
- Abbau von Komplexität bezüglich der Handhabung;
- Konsolidierung der Applikationszugriffe.

Bezüglich der **Zusammenlegung von Anwendungen** geht es darum, die in einer Unternehmung vorhandenen diversen Anwendungen so zusammenzulegen, dass nur ein einziges oder zumindest nur wenige große und partitionierte Serversysteme nötig sind. Außerdem erfolgt eine Zuordnung von Anwendungen mit unterschiedlichen Belastungsprofilen zu einzelnen Servern, sodass **ausgeglichene Gesamtbelastungsprofile** entstehen. Positive Folge: Reservekapazitäten lassen sich auf ein Minimum reduzieren.

Mit der **Integration der Anwendungen** ist der Weg zu einer geringeren Komplexität der IT geebnet. Erreicht wird dies unter anderem durch folgende Aktivitäten:

- Durch **eine verstärkte Geschäftsprozess-Orientierung** der Anwendungsentwicklung und -implementation kann die Anwendungslösung optimiert und gleichzeitig eine intelligente Integration in Angriff genommen werden.
- Durch den Übergang von Datensilos einzelner Abteilungen hin zu einer geschlossenen, **unternehmensweiten Informationssicht** lassen sich Datenredundanzen vermeiden und Mehrfacherfassungen reduzieren.

Im Verlauf des Konsolidierungsfortschritts wird es immer einfacher, von mehreren Anwendungen, die auf mehrere Datenbanken zugreifen, auf eine echte Integration von Datenbanken

und Anwendungen umzusteigen. Mit der Rationalisierung von Anwendungen lassen sich automatisch Kosten einsparen und mehr Flexibilität erreichen.

Ein weiterer Ansatzpunkt ist der **Abbau von Komplexität** hinsichtlich der Handhabung der Applikationen. Hauptziel ist es, nur jene Funktionen auf der Benutzeroberfläche anzubieten, die der Anwender tatsächlich und immer wieder benötigt. Insbesondere marktführende ERP-Anbieter arbeiten zudem daran, dass ihre Anwendungen künftig aus weitgehend standardisierten Bausteinen zusammengesetzt werden. Diese neue Architektur hat zum Ziel, die Systeme schnell und einfach aufzubauen und gleichzeitig die Bedienbarkeit zu erhöhen.

Konsolidierung des Applikationszugriffs: Bei der Vielzahl der in Unternehmen eingesetzten Applikationen ist die Forderung nach einem flexiblen, einfachen und integrierten Applikationszugriff leicht nachvollziehbar. Der Weg zu einem integrierten Multi-Channel-Zugriff auf alle Applikationen führt dabei über Stationen wie:

- die Rationalisierung von Webservern;
- Portalzugriff für alle Applikationen;
- Single Sign-On;
- Mobile/Wireless Zugriff etc.



Beachten Sie:

In diesem Umfeld muss Sicherheitsaspekten (wer darf worauf, wann, wie und wo zugreifen) natürlich große Aufmerksamkeit gezollt werden.

Die Übersicht in Tabelle 3.12 soll eine Orientierung für **die Festlegung von Standards** geben. Sie berücksichtigt auch die Tatsache, dass nicht freigegebene Produkte nur einen begrenzten oder überhaupt keinen Service durch die IT erhalten:

TABELLE 3.12 Festlegung von IT-Standards

	Standardisierungsbe- reich	Regelungen für den Einsatz, Unterstützungen durch IT
Unternehmensweite Standardprodukte	▪ Einsatz von HW/SW ▪ Betreuung ▪ Schnittstellen	▪ verbindlich ▪ volle Unterstützung zentral/dezentral ▪ werden unternehmensweit definiert
Fachbereichsspezifi- sche Standardprodukte	▪ Einsatz von HW/SW ▪ Betreuung ▪ Schnittstellen	▪ verbindlich für definierte Fachbereiche ▪ zentral/dezentral ▪ finden sich zu Standardprodukten
Nicht freigegebene Produkte	▪ Einsatz von HW/SW ▪ Betreuung ▪ Schnittstellen	▪ nicht offiziell, evtl. Einzelfall-Genehmigung ▪ keine ▪ keine Unterstützung

3.6.3 Datenkonsolidierung

In nahezu jeder Unternehmung und Verwaltung gibt es ein vergleichbares Grundproblem: Viele Daten sind verstreut gespeichert, werden auf unterschiedlichen Medien verwaltet, durch verschiedene Programmsysteme erzeugt und stehen somit für eine gezielte Verwendung nicht zur Verfügung. Die Folge: Zahlreiche Daten, die in den verschiedenen Systemen gespeichert sind, schlummern eigentlich nur so vor sich hin.

Nachfolgend einige Beispiele für aktuelle Mängel, die sich in der Firmenpraxis bemerkbar machen und für die alternative Lösungen gesucht werden müssen:

- **Verteilte Informationen auf verschiedenen Technologie-Plattformen:** Es gibt zwar Informationen im Unternehmen, und bis zu 25 Prozent der Daten werden systematisch in einer Datenbank abgelegt, doch die meisten Informationen liegen, beliebig verteilt über verschiedenste Systeme, im Unternehmen. Dabei stößt man auf unstrukturierte Dokumente, unterschiedliche Formate, Plattformen und Anwendungen. Kurz gefasst: die Daten stehen in keiner integrierten Form zur Verfügung.
- **Keine einheitliche Datenbasis:** Ohne klare Datenbasis ist es für die Verantwortlichen schwer, die existierenden Daten und Berichte miteinander zu vergleichen. Unterschiedliche Kontenpläne und Konzernsprachen gestalten das Konsolidieren sehr aufwändig.
- **Mehrfacherfassung derselben Daten:** Ein weiterer Aspekt des unnötig hohen administrativen Aufwandes ist das Doppelerfassen von Daten für Controlling- und Berichtszwecke. Dadurch entsteht zusätzlich eine gewisse Unsicherheit bezüglich der Datenqualität. Unterschiedlichste DV-Systeme verhindern außerdem oft die erforderliche Integrität der Daten im Unternehmen.
- **Unzureichendes Berichtswesen:** Berichte werden entweder nicht gelesen oder nicht verstanden. Es kommt immer wieder zu unnötigen Diskussionen und zeitraubenden Erklärungen.

Außerdem: Erst aus der gezielten Verdichtung der verstreut gespeicherten Daten entstehen neue, komprimierte Informationen, die wettbewerbsrelevant sind. Daraus ergibt sich eine klare **Anforderung an leistungsfähige Informationssysteme:** Aktuelle Informationen, die für Planungs- und Entscheidungsaufgaben benötigt werden, sind zu generieren und müssen den Entscheidungsträgern relativ einfach bereitgestellt werden.

3.6.4 Projektmäßige Umsetzung von IT-Konsolidierungen

In welchem Umfang in dem jeweiligen Anwendungsfall Konsolidierungsaktivitäten nötig sind, hängt natürlich von der spezifischen Ausgangssituation der Anwender ab. In der Regel wird eine umfassende IT-Konsolidierung nur durch ausdrückliche Inangriffnahme eines Projektes erfolgreich realisiert werden können.

Eine **typische Ausgangssituation** eines produzierenden mittelständischen Unternehmens:

- Wachstumsbedingt ist der Serverbestand des Unternehmens in den letzten Jahren erheblich angewachsen. Neben einer AS/400 für die Produktionsplanung und Produktionssteuerung müssen die Mitarbeiter der IT-Abteilung allein mehrere Intel-basierende Server betreuen.
- Weitere leistungsstarke Server gibt es jeweils für CAD-Anwendungen sowie für das HR-Modul des ERP-Anbieters sowie für die Firewall.

- Als Speicher-Lösung gibt es eine reine NAS-Lösung (NAS = Network Attached Storage) sowie verteilte Plattensysteme mit unterschiedlichen File-Strukturen (jeweils unter Windows und Linux).
- Die Netzwerk-Infrastruktur ist durch eine hohe Komplexität gekennzeichnet.

Handlungsbedarf: Aus der gewachsenen Architektursituation heraus liegt es nahe, dass sich unter anderem ein erheblicher Administrationsaufwand ergibt. Als weitere Probleme werden identifiziert:

- Komplizierte, kaum überschaubare Geschäftsprozesse;
- mittlere Auslastung der Server ist sehr gering;
- Personal im „Spezialisten-Modus“.

Diese erste Bestandsaufnahme lässt auf einen Handlungsbedarf schließen und den Wunsch nach einer optimierten – das heißt konsolidierten – Lösung aufkommen. Deshalb wird ein Projekt aufgesetzt, mit dem Ziel, alle Server- und Storagekapazitäten in raumoptimierten, Rack-basierenden Systemen unterzubringen und sie in einem zentralen Gesamtsystem zusammenzufassen.

Abbildung 3.12 zeigt die Phasen und Aktivitäten eines Konsolidierungsprojekts im Überblick.

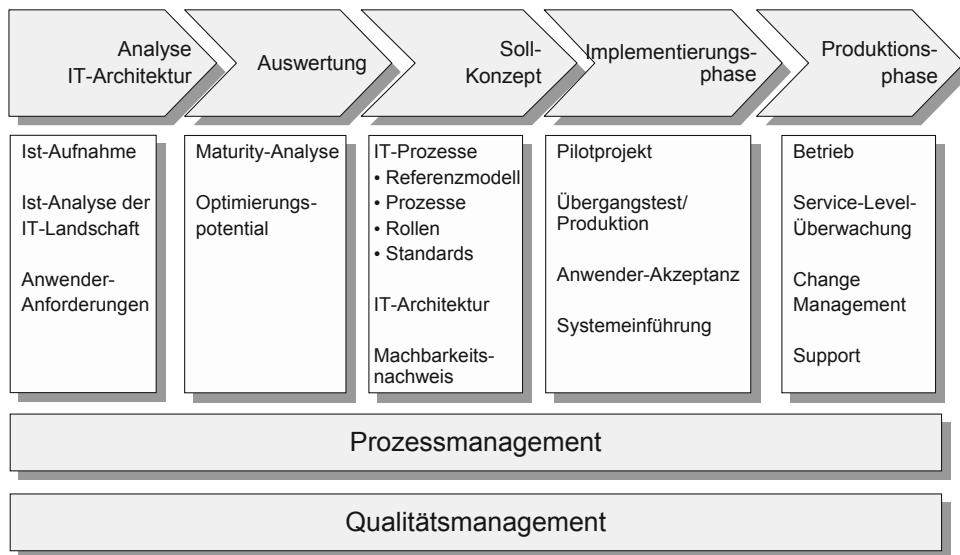


ABBILDUNG 3.12 Phasen und Arbeitspakete eines IT-Konsolidierungsprojektes



Fazit:

Im Rahmen von IT-Konsolidierungsprojekten kann den Zielen reduzierter Gesamtkosten, gesteigerter Service Levels und erhöhter Flexibilität Rechnung getragen werden. Wesentliche Stoßrichtungen der IT-Konsolidierung sind Vereinfachung, Standardisierung, Modularisierung und Optimierung der IT-Landschaft.

■ 3.7 Projektbeispiel „SOA-Einführung“

Die Einführung von Serviceorientierten Architekturen (kurz SOA) bedarf gezielter Planung und Steuerung durch das IT-Management. Das Kernstück einer SOA sind die Services, die jeweils zu implementieren sind. Ein solcher Service beschreibt eine wohl definierte, in sich abgeschlossene fachliche Funktion. Fachlich muss deshalb betont werden, weil der konventionelle Ansatz der Anwendungsarchitektur einen mehr technischen Schwerpunkt setzt, während SOA prozessorientiert die fachlichen Aspekte der Geschäftsprozesse in den Vordergrund stellt.

SOA ist letztlich eine IT-Architektur, die aus Services als atomaren Einheiten zusammengesetzt ist (anstatt aus Applikationen) und die Services auf Basis offener Standards lose koppelt. Sie bieten die Möglichkeit, Softwarekomponenten lose gekoppelt miteinander interagieren zu lassen. Der größte Nutzen dieser losen Kopplung ist die gewonnene Agilität, das heißt die Möglichkeit, durch Komposition der Services geänderte oder neue Geschäftsprozesse in kurzer Zeit abbilden zu können. Das setzt jedoch Erfahrung und Augenmaß bei der Konzeption der Granularität der Services voraus. Die Agilität stellt sich auch ein, wenn bereits vorhandene, starre Integrationen mit Hilfe einer Service-Architektur aufgebrochen werden können. Vor allem verhilft die gewonnene Flexibilität zu neuen Konzepten, mit denen man Kosten einsparen, aber auch das Geschäft verbessern kann.

Im Wesentlichen können Sie mittels SOA folgende **Vorteile** realisieren:

- SOA ist eine Technologie, die eine flexible, auf die tatsächlichen Geschäftsprozesse ausgerichtete Applikationsarchitektur ermöglicht.
- SOA kann heterogen gewachsene IT-Systeme verbinden.

Dabei ist zu beachten, dass diese Vorteile nur unter bestimmten Bedingungen zum Tragen kommen:

- SOA erfordert eine konsequente Abstimmung zwischen Business-Strategie und IT-Strategie (Business IT-Alignment).
- SOA erfordert die Ausrichtung der IT-Architektur auf die Geschäftsprozesse.
- SOA erfordert die Kommunikation und das gegenseitige Verständnis von Business und IT.
- SOA erfordert die Optimierung der Prozesse in der IT.

Die genannten Punkte machen deutlich, dass SOA kein Allheilmittel ist, sondern in Anwenderunternehmen strategisch geplant und gesteuert werden muss. Wesentliche **Planungselemente** einer solchen SOA-Governance betreffen

- Aspekte der Organisation,
- Konzepte des Architektur-Managements sowie
- Überlegungen zum Lifecycle-Management.

Wenn die **Einführung und Implementation einer serviceorientierten Architektur** erfolgreich realisiert werden soll, ist es unverzichtbar, dass die dazu notwendigen Schritte realistisch und systematisch für jede Organisation spezifisch geplant werden.

Eine wesentliche Aufgabe in der Startphase einer SOA-Einführung besteht darin, die Rahmenbedingungen für die Umsetzung „abzustecken“. Das ist z.B. im Rahmen von Assessments möglich.

Zu Beginn der Überlegungen über den Paradigmenwechsel hin zu SOA-Architekturen empfiehlt es sich für die Unternehmensführung und für das IT-Management, eine grundsätzliche Positionierung zum Thema SOA einzunehmen. Dabei kommt es vor allem darauf an, die mit der Einführung von SOA verbundenen Ziele möglichst präzise und operational zu bestimmen. Damit im Zusammenhang steht natürlich auch die Frage, eine gemeinsame Begriffsbestimmung vorzunehmen, um ein gemeinsames Verständnis von dem anstehenden Paradigmenwechsel in der Anwendungsentwicklung bzw. der Anwendungsintegration zu haben.

Typische **Auslöser von SOA-Projekten** sind:

- Der Bedarf an immer engerer Verzahnung von Business und IT steigt. Der Forderung nach flexibler Unterstützung von Geschäftsprozessen und mehr Effizienz steht in der Praxis jedoch eine historisch gewachsene IT-Landschaft entgegen.
- Ihre Analyse zeigte, dass mangelnde fachliche Integration vielfache Redundanzen zur Folge hatte. Die starre Verflechtung von Prozessen und IT-Systemen treibt die Komplexität der IT-Systeme weiter in die Höhe, obwohl paradoxerweise die einzelnen Anwendungen kaum übergreifend in Interaktion treten konnten.

Ein **stufenweiser Ansatz für eine Einführung** kann wie folgt aussehen:

- **Stufe 1 – Erste SOA-Initiativen (Positionierung und Pilotierung)**
 - Einzelne Web-Services werden quasi als Pilotversuche ausgewählt und implementiert.
 - Weniger kritische Geschäftsprozesse werden mittels SOA exemplarisch gelöst.
 - Eine strategische Bedeutung für das Unternehmen ist bei den ausgewählten Prozessen nicht gegeben.
- **Stufe 2 – Integrierte SOA-Anwendungen (integrierte Teil-Lösungen)**
 - Einzelne Applikationen werden unter Nutzung der SOA-Technologie grundlegend überarbeitet oder neu erstellt.
 - Es ergibt sich eine IT-Kostenreduktion in ausgewählten Bereichen.
 - Kritische Geschäftsprozesse werden in die strategischen Überlegungen der SOA-Einführung einbezogen.
- **Stufe 3 – SOA wird strategisches Ziel (flächendeckende Anwendungen)**
 - Alle Geschäftsprozesse und alle Applikationen sind von der SOA-Umstellung betroffen.
 - Es erfolgt eine Neupositionierung und Organisation der IT-Abteilung (insbesondere im Bereich der Softwareentwicklung und Softwareintegration). Das führt zu einer Veränderung der Unternehmenskultur durch eine intensivere Zusammenarbeit zwischen Fachabteilungen und IT.

■ 3.8 Framework TOGAF im Architekturmanagement nutzen

Mittlerweile gibt es verschiedene Frameworks, die in Verbindung mit dem Architekturmanagement orientierende Unterstützung geben. Beispiele sind:

- ISO-Standard 15704 (ISO 1999)
- GERAM – Generalised Enterprise Reference Architecture and Methodology (zum Vergleich und zur Bewertung verschiedener Frameworks)
- Zachmann Framework
- TOGAF –The Open Group Architecture Framework
- DoDAF – Department of Defense Architecture Framework
- Meta Group Enterprise Architecture Framework

Das bekannteste und derzeit am meisten genutzte Framework stellt TOGAF (Abkürzung für „The Open Group Architecture Framework“) dar, das bereits 1995 in der ersten Version veröffentlicht wurde (siehe auch <http://www.opengroup.org/overview/>). Es handelt sich bei TOGAF um ein Framework zum Architekturmanagement, das aus mehreren Teilen besteht; u. a.:

- **TOGAF Architecture Development Method (ADM)**
- **Enterprise Continuum („Virtuelles Repository“**, in dem Referenz-Modelle, Patterns, Architekturbeschreibungen und weitere Artefakte abgelegt werden, um diese wieder verwenden zu können): besteht aus dem Architecture Continuum (enthält wiederverwendbare Architekturbestandteile) und dem Solutions Continuum, das die Umsetzung des Architecture Continuum durch wiederverwendbare Bausteine beschreibt.
- **TOGAF Resource Base:** Die Resource Base stellt Werkzeuge, Richtlinien, Hintergrundinformationen und Techniken (Vorlagen, Checklisten) bereit, um TOGAF und ADM anzuwenden. Es wird primär als Nachschlagedokumentation während der Implementierung des ADM benutzt.
- **TOGAF Capability Framework:** „Capability Based Planning“ soll in allen Phasen der Architekturentwicklung eine Verbindung zu den strategischen und geschäftlichen Zielen des Unternehmens herstellen. Die Capabilities werden dabei direkt aus dem Strategieplan des Unternehmens abgeleitet. Ziel ist das „Alignment“ zwischen Capabilities und der „Enterprise Architecture“. Architekturdefinitionen und auch Projektziele sollen dadurch nicht nur in technischen Begriffen, sondern in Bezug auf Capabilities und den geschäftlichen Nutzen erfolgen.

Abbildung 3.13 skizziert den **Einsatz von ADM**.

Das **ADM** ist eine **Methode zur Architekturentwicklung**, die aus 8 zyklisch aneinander gereihten Phasen (A – H) besteht:

In der Phase A „Architecture Vision“ werden die Ziele der Beteiligten ermittelt.

In den Folgephasen B – D werden die drei Architekturbereiche von TOGAF deutlich. Hier erfolgt primär die Dokumentation der Ist- und Zielarchitekturen sowie das Aufzeigen von notwendigen Anpassungen:

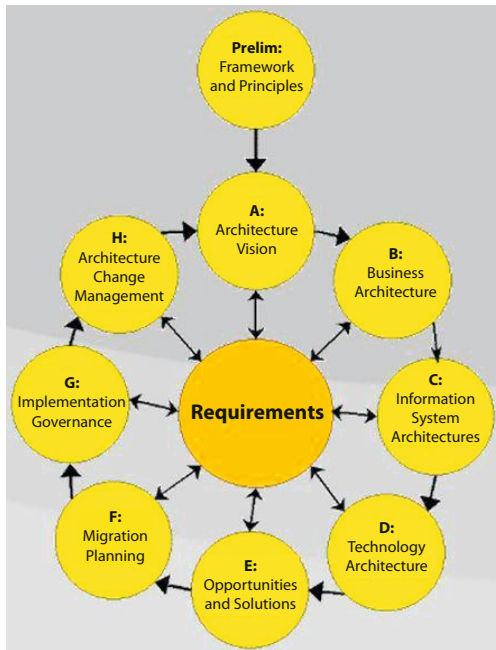


ABBILDUNG 3.13

TOGAF Architecture Development Method (ADM)

- **Business Architecture** (Geschäftsarchitektur): In diesem Bereich werden die Geschäftsprozesse modelliert, abgestimmt auf die strategische Zielsetzung des Unternehmens und dessen Organisationsstruktur.
- **IS-Architecture (Informationssystem-Architektur)**: Dies stellt eine Zusammenfassung aus Informations- und Datenarchitektur und Applikationsarchitektur dar. Die Datenarchitektur beschäftigt sich mit der Identifikation von Daten zu den jeweiligen Prozessen. Dabei müssen die Daten die Charaktereigenschaften stabil, vollständig und konsistent aufweisen. Das Ergebnis wird in einem Datenmodell zusammengefasst. Darüber hinaus wird in diesem Bereich ein Informationsmodell erstellt, welches die Informationsgruppen beinhaltet, also die Rollen im Unternehmen und deren Informationsbedürfnisse. Bezüglich der Anwendungsarchitektur werden die Applikationen (Anwendungen) erfasst, die Interaktion zwischen den Applikationen festgestellt und die dazugehörigen Schnittstellen dargestellt. Auch erfolgt eine Kategorisierung in die fachliche Funktionalität und die verarbeiteten Informationen. Die Applikationen innerhalb der Kategorie können im Laufe der Zeit verschwinden und ersetzt werden, weil sich neue Anforderungen stellen aufgrund von technischen Weiterentwicklungen.
- **Technologiearchitektur**: Dies ist jener Bereich, der die IT-Infrastruktur beschreibt. Im Kern erfolgt eine sehr konkrete Beschreibung der technischen Komponenten und deren Vernetzung, um eine hohe Qualität der Applikationen sicherzustellen.

In Phase E werden die Unterschiede zwischen den Phasen B-D und die Möglichkeiten bzw. Lösungsansätze herausgearbeitet, um von der Ist-Architektur zur Soll-Architektur zu kommen. Die Planung der Umsetzungen der getroffenen Entscheidungen wird in Phase F durchgeführt. Gemeinsam ist beiden Phasen, dass hier Optionen und Lösungsvarianten dargestellt sowie Bewertungsgrundlagen als Basis für die Implementierungsentscheidungen angeboten werden.

In Phase G kommt es zur konkreten Umsetzung und deren Überwachung. In Phase H wird das Re-Engineering „eingeläutet“, wobei Anforderungen von intern und außen erhoben und berücksichtigt werden. Die beiden Phasen G und H unterstützen letztlich die Steuerung der Implementierungsprojekte.



Mit dem Framework TOGAF wird ein Regelwerk bereitgestellt, um einzelne oder Gruppen von Informationssystemen architekturzentriert zu planen und zu entwickeln. Dem Anspruch eines übergreifenden Ziels, das der Komplexitätsbeherrschung der IT-Landschaft dient, wird TOGAF zwar nicht gerecht – für die Architektur-getriebene Planung und Entwicklung von Informationssystemen als Teildisziplin eines übergreifenden Architekturmanagement kann TOGAF jedoch Ideen und Anregungen liefern. Beispielsweise liefert TOGAF einen Beitrag zur Bildung eines gemeinsamen EAM-Verständnisses (Terminologie), Anregungen für einheitliche Ergebnisse (Architecture Descriptions/Views) und deren Beschreibung (Notation) sowie für ein einheitliches Vorgehen bei der Entwicklung der Unternehmensarchitektur (Phasenmodell).

■ 3.9 Nutzen eines IT-Architekturmanagements

Der Nutzen, den ein gezieltes und umfassendes IT-Architekturmanagement für die Praxis bietet, ist vielfältig. Im Wesentlichen seien folgende Vorteile herausgestellt:

- **Kosteneinsparung durch Vereinheitlichung der technischen IT-Infrastruktur:**
Die Vereinheitlichung bewirkt Effizienzsteigerungen und Kostenreduktionen; beispielsweise durch die Verringerung von Entwicklungs- und Betriebskosten, Lizenzkosteneinsparungen oder Verringerung des vorzuhaltenden Know-hows.
- **Ressourcen- und Kostensenkungen durch Standardisierung und Integration von Softwarelösungen:**
Aus der üblicherweise vorhandenen Unmenge verschiedener nicht aufeinander abgestimmter Softwareprodukte und Plattformen müssen die qualitativ und aus Kostengesichtspunkten geeignetsten Lösungen identifiziert und als Standard positioniert werden. Dabei werden neben der reinen Infrastrukturkonsolidierung auch Softwareplattformen und eigenentwickelte Architekturösungen in die Beurteilung mit einbezogen.
- **Wertvolle Entscheidungshilfen im Rahmen von IT-Projekten:**
Kosten und Nutzen von geplanten Vorhaben unter Berücksichtigung aller Auswirkungen auf die bestehende IT-Landschaft zählen zu den wichtigsten Kriterien bei Projektentscheidungen. Klare und direkt nutzbare Vorgaben helfen den Projekten, die aus Gesamt-IT-Sicht richtigen Architektur-Entscheidungen zu treffen, und verbessern die Wiederverwendung von im Unternehmen vorhandenen Lösungen und Know-how. Kosteneinsparungen von 5 bis 15 Prozent im Bereich Anwendungswartung und -betrieb sind durch geeignete Optimierungsmaßnahmen erzielbar.

▪ **Kosteninformationen als Entscheidungsgrundlage für das IT-Management:**

Aufschlüsselung der IT-Kosten auf die verschiedenen Anwendungen und Infrastrukturbereiche ist ein wichtiger Bestandteil des Architekturmanagements. Kosten müssen verursachungsgerecht zugerechnet werden, Budgetplanung und auch Controlling sind an den IT-Strukturen auszurichten. Durch die Transparenz der Anwendungsarchitektur und der verursachten Kosten lassen sich die Auswirkungen von Veränderungen bereits in der Planungsphase analysieren sowie besser und vollständiger beurteilen. Die nachvollziehbare Zusammensetzung der IT-Kosten sowie die Illustration der Auswirkungen von Vorhaben erleichtern signifikant die Kommunikation mit den Fachbereichen.



Das Wichtigste – zusammengefasst

- **Bei einer Neueinführung bzw. Weiterentwicklung des Architekturmanagements ist es wichtig, dieses Thema in geeigneter Weise im Unternehmen (sowohl in der Unternehmensführung als auch bei den IT-Experten) zu „verankern“. Ein ganzheitlicher Ansatz zur Planung, Entwicklung, Implementierung und Weiterentwicklung von Unternehmensarchitekturen hilft dabei.**

Im Architekturmanagement werden die wesentlichen Ebenen der Unternehmensarchitektur (Enterprise Architecture) in einem ganzheitlichen Zusammenhang betrachtet: Geschäftsebene (Geschäfts-(Prozess-)Architektur), Anwendungen (Applikationsarchitektur), Daten (Datenarchitektur) sowie Technologie (Technologiearchitektur).

- **Ein Managementkonzept ist für das Planen und Steuern der Unternehmens- und IT-Architektur unverzichtbar.**

Ein ausgewogenes Managementkonzept zu den Unternehmens- und IT-Architekturen umfasst neben der Dokumentation der Ist-Landschaft auch die Konzeption und Planung einer zukünftigen Soll-Landschaft des Unternehmens (Enterprise- bzw. IT-Bebauungsplanung) sowie Controlling-Instrumente zur kontinuierlichen erfolgreichen Steuerung und Weiterentwicklung der Enterprise Architecture.

- **Ermitteln Sie die Technologiearchitektur Ihrer Organisation!**

Die Technologiearchitektur beschreibt im Wesentlichen die Architekturelemente für den Aufbau und den Betrieb der IT-Infrastruktur. Dabei können Sie die IT-Komponenten in infrastrukturelevante Schichten gliedern, beispielsweise um für ein PC-, Server- und Host-Umfeld einen Orientierungsrahmen zu finden. Die Technologiearchitektur gibt dabei letztlich den Rahmen für eine Organisation vor, innerhalb dessen sich Anwendungen beschaffen, implementieren und betreiben lassen.

- Die **Applikationsarchitektur** dokumentiert systematisch die verschiedenen Anwendungen, die für die Ausführung der Geschäftsprozesse einer Organisation eingesetzt werden. Dabei werden die Anwendungen eines Unternehmens (ERP, E-Mail, CRM u. a.) sinnvollerweise in Orientierung an den Hauptprozessen beschrieben, wobei auch die Beziehungen/Schnittstellen zwischen den Anwendungen festzuhalten sind.

- **Beachten Sie, dass die Geschäftsarchitektur die Business-Strategie, Steuerungsmechanismen, Organisation und Kerngeschäftsprozesse für eine Anwenderorganisation präzisiert und versucht, diese bei der Entscheidungsfindung für die Umsetzung in Applikationen und Infrastrukturen zu berücksichtigen!**

Die Geschäftsarchitektur beschreibt im Wesentlichen die Grundstrukturen des Geschäfts (incl. der Ziele), die zugrundeliegenden Geschäftsprozesse sowie die hierfür erforderlichen Steuerungsmechanismen und strukturellen Anpassungen in der Organisation des Anwenders. Definition nach TOGAF: „A Business Architecture defines the business strategy, governance, organization, and key business processes.“

■ 3.10 Literatur

- [BiVa03] *Birkhölzer, Thomas; Vaupel, Jürgen*: IT-Architekturen. Vde-Verlag, Berlin, Offenbach 2003
- [BuDi05] *Buchta, Dirk; Eul, Marcus; Schulte-Croonenberg, Helmut*: Strategisches IT-Management Wert steigern, Leistung steuern, Kosten senken. Gabler, Wiesbaden 2005
- [Da93] *Davenport, T.H.*: Process Innovation. Harvard Business School Press, Boston, MA 1993
- [De03] *Dern, Gernot*: Management von IT-Architekturen. Informationssysteme im Fokus von Architekturplanung und -entwicklung. Aus der Reihe: Edition CIO, Vieweg, Wiesbaden 2003
- [HA09] *Hanschke, Inge*: Strategisches Management der IT-Landschaft. Ein praktischer Leitfaden für das Enterprise Architecture Management. Hanser-Verlag. München 2009
- [KrSe03] *Krüger, Sascha; Seelmann-Eggebert, Jörg*: IT-Architektur-Engineering – Systemkomplexität bewältigen und Kosten senken. Galileo Press, Bonn 2003
- [Nie035] *Niemann, Klaus D.*: Von der Unternehmensarchitektur zur IT-Governance. Bausteine für ein wirksames IT-Management. Vieweg, Wiesbaden 2005
- [Ti05] *Tiemeyer, Ernst*: IT-Servicemanagement kompakt. Elsevier, Spektrum Akademischer Verlag, Heidelberg 2005
- [Ti07] *Tiemeyer, Ernst*: IT-Strategien entwickeln. IT Architekturen planen. IT als Wertschöpfungsfaktor. Rauscher-Verlag für Wissenschaft und Technik GmbH 2007

4

IT-Servicemanagement

Dietmar Kopperger, Jörg Kunsmann, Anette Weisbecker



Fragen, die in diesem Kapitel beantwortet werden:

- Warum hat IT-Servicemanagement in der Praxis eine hohe Bedeutung erlangt?
- Was sind wichtige Erfolgsfaktoren für die Einführung von IT-Servicemanagement?
- Welche Rahmenbedingungen für eine erfolgreiche Einführung müssen unbedingt gegeben sein?
- Welche Herausforderungen bedürfen im Hinblick auf die Bereitstellung erfolgreicher IT-Services einer intensiven Beachtung?
- Welche Konzepte und Standards für das IT-Servicemanagement gibt es?
- Durch welche Merkmale und Prozesse zeichnet sich ITIL aus, und wie kann dieses Framework erfolgreich implementiert werden?
- Wie kann ein „Fahrplan“ zu einem optimalen IT-Servicemanagement aussehen?
- Wie können IT-Services wirtschaftlich verrechnet werden?
- Welche Faktoren, Kennzahlen und Methoden bieten sich für ein Monitoring der IT-Services an?

Die Informationstechnologie (IT) ist von entscheidender Bedeutung für die Erreichung der Unternehmensziele. Dabei steht nicht die Technikorientierung im Vordergrund, sondern ausschlaggebend sind die IT-Services für die konsequente Unterstützung der Geschäftsprozesse. Die Aufgabe der IT besteht somit immer mehr in der Erbringung von Dienstleistungen, durch die IT bedarfsgerecht, effizient, kundenorientiert und mit hoher Qualität bereitgestellt wird.

■ 4.1 Effizientes IT-Servicemanagement – eine permanente Herausforderung

*„Achte darauf, dass du die richtigen Mittel wählst,
dann wird das Ziel von selbst erreicht.“*

Mahatma Gandhi

Informations- und Kommunikationstechnologien sind die Grundlage für die Durchführung der Geschäftsprozesse in einem Unternehmen. Alle Geschäftsprozesse weisen heute einen

hohen Durchdringungsgrad mit Informations- und Kommunikationstechnologien auf. Dies gilt sowohl für die unternehmensinternen Prozesse vom Einkauf über die Produktion bis zum Verkauf und Service einschließlich aller Verwaltungsprozesse als auch für die zwischenbetrieblichen Geschäftsprozesse im Zuge des elektronischen Geschäftsverkehrs. Durch die rasante Entwicklung der Kommunikationstechnik und der mobilen Endgeräte verändert sich die Arbeitsweise für viele Beschäftigte. Jeder kann zu jeder Zeit, weltweit mit beliebigen Personen zusammenarbeiten, wobei auch immer mehr Personen mobil auf die unternehmensinterne IT zugreifen.

Die Produktivität und Flexibilität der Unternehmen sowie die Qualität ihrer Produkte und Dienstleistungen hängen somit heute bereits zum größten Teil von leistungsfähiger, zuverlässiger, flexibler und leicht benutzbarer Informationstechnologie ab [Wei02].

4.1.1 IT-Servicemanagement – begriffliche Orientierung

Die zunehmende Bedeutung der Informationstechnologie für die Durchführung der Geschäftsprozesse im Unternehmen erfordert eine prozessorientierte IT, die ihre Dienstleistungen kundenorientiert, effizient und effektiv erbringt. Die IT-Einheiten im Unternehmen haben sich somit zu Dienstleistern gewandelt, die sowohl für die qualitativ hochwertige Erbringung der Leistungen für den Betrieb der IT im Unternehmen als auch immer mehr für die Erschließung neuer Geschäftsfelder mittels IT zuständig sind. Dabei wird verstärkt auf den Beitrag zur Wertschöpfung geachtet.

Diese Herausforderungen steigern die Notwendigkeit, die Prozesse zur Erbringung der IT-Services zu standardisieren, die zu liefernden Ergebnisse zu kontrollieren und die Leistungen dem Kunden transparent darzustellen. Von entscheidender Bedeutung ist dabei auch die planvolle Entwicklung und Erbringung der Dienstleistungen. Um diesen Anforderungen gerecht zu werden, ist die Einführung eines IT-Servicemanagements unerlässlich. Das IT-Servicemanagement ist ein Instrument zur Planung, Steuerung und Kontrolle der IT-Services.

Das IT-Servicemanagement hat die Aufgabe, die Qualität und Quantität dieser vielfältigen IT-Services zielgerichtet, geschäftsprozessorientiert, benutzerfreundlich und kostenoptimiert zu überwachen und zu steuern. Dazu gehört auch die Anpassung und Weiterentwicklung der IT-Services an die aktuellen und zukünftigen Anforderungen der Kunden. Kundenorientierung und Kundenzufriedenheit stehen dabei immer im Vordergrund. Die unabdingbare Voraussetzung dafür ist eine Bereitschaft des Managements wie auch der Mitarbeiter zum Wandel in Richtung Kunden- und Serviceorientierung innerhalb der Organisationen.

Der Begriff Management steht dabei für Vorgehensweisen und Methoden zur Planung, Realisierung, Steuerung und Kontrolle der Prozesse zur Bereitstellung und Erbringung von Leistungen. Dabei sind strategische, taktische und operative Fragestellungen zu beantworten.

IT-Servicemanagement ist somit der Prozess, die Qualität und Quantität der gelieferten IT-Services zu planen, zu überwachen und zu steuern. Gleichzeitig müssen die Ziele der Geschäftsprozess- und der Kundenorientierung sowie der Kostenoptimierung gewahrt werden.

Zur Strukturierung können IT-Services in vier Gruppen unterteilt werden [ZaB03]:

- **IT-Ressourcen** stehen für die Bereitstellung von technischen Ressourcen und spiegeln die Sicht eines Rechenzentrums wider, das Hard- und Software bereitstellt und betreibt.
- **IT-Informationssysteme** beinhalten die Bereitstellung einer Anwendung, wobei diese für unternehmensinterne Kunden spezifisch entwickelt (bzw. eingekauft und konfiguriert) wird und alle Phasen von Entwicklung bis Betrieb und Support beinhaltet.
- **IT-Prozessunterstützung** für die explizite Unterstützung der Geschäftsprozesse.
- **IT-Services** sind ein Geschäftsprodukt, wenn sie als Bestandteil des Produkt- und Leistungsbündels eines Unternehmens am Markt angeboten werden.

Ein Service beschreibt eine nach außen sichtbare Wirkung, die in einem Geschäftsprozess des Kunden einen (direkten) Mehrwert erzeugt. Dabei besteht ein IT-Service (wie in Abbildung 4.1 verdeutlicht) aus einer Kombination von internen und/oder externen Dienstleistungen (Leistung) und Sachleistungen (Produkt).

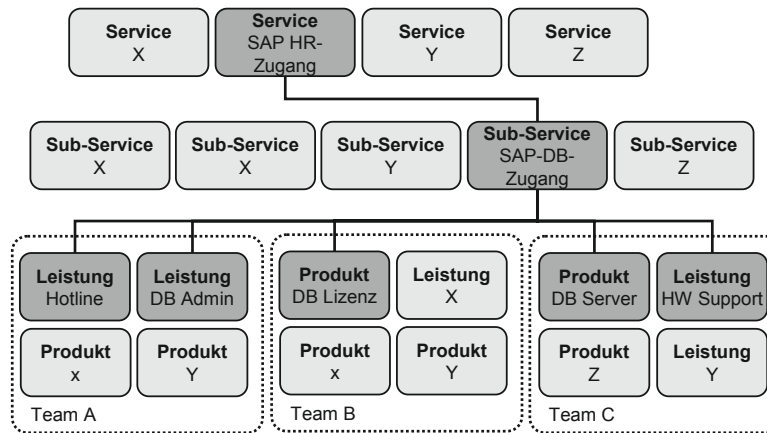


ABBILDUNG 4.1 Was ist ein IT-Service?

4.1.2 Grundlagen eines professionellen IT-Servicemanagements

Dem Leitgedanken des IT-Servicemanagements folgend, sind IT-Dienstleistungen allein dazu da, die Geschäftsprozesse und die Anwender bei ihren Aufgabenstellungen zu unterstützen. D. h. Zweck der IT ist die optimale Unterstützung der Geschäftsprozesse zur Erreichung der Unternehmensziele. Die Ziele des IT-Servicemanagements bestehen darin, die Entscheidungsfindung aus Prozesssicht zu gewährleisten sowie deren effiziente und erfolgreiche Umsetzung mit definierten Ansprechpartnern sicherzustellen.

Die Grundlage dafür bietet ITIL¹. ITIL hat sich zu einem De-facto-Standard entwickelt und bietet ein einheitliches Referenzmodell und „Best Practices“. Dieser Standard definiert generische Prozesse und deren Zusammenwirken und schafft eine einheitliche Datenbasis zur Steuerung der Prozesse. Es werden klare Zuordnungen von Verantwortlichkeiten getroffen

¹ <http://www.itil.co.uk/>

und Kriterien für die Bewertung der Servicequalität festgelegt. So wird ITIL der Forderung nach messbaren und bewertbaren Leistungen gerecht. Im Hinblick auf eine Standardisierung werden die Begriffe einheitlich festgelegt. Damit wird eine einheitliche Sprachregelung geschaffen, die die Grundlage für die Verständigung aller Beteiligten sowohl unter den Dienstleistungserbringern selbst als auch zwischen Dienstleistungserbringern und Kunden ist.

Das IT-Servicemanagement nach ITIL 3 [OSS07] unterteilt die zu unterstützenden Prozesse in vier Bereiche:

- *Strategische Ebene:*
Management von IT-Dienstleistungen; dazu zählen unter anderem „Qualitätsmanagement“ und „IT-Serviceorganisation“ (Service Strategy);
- *Taktische und operative Ebene:*
Planung und Steuerung von IT-Dienstleistungen (Service Delivery);
- *Operationelle Ebene:*
Unterstützung von IT-Dienstleistungen (Service Design, Service Transition und Service Operations);
- *Feedback und Lern-Ebene:*
Feedback und Lernmechanismen zu IT-Services (Continual Service Improvement).

ITIL verfolgt mit seiner Philosophie die drei Hauptziele des IT-Servicemanagements [MaR01]:

- die IT-Services auf die gegenwärtigen und zukünftigen Anforderungen des Unternehmens und seiner Kunden auszurichten;
- die Qualität der erbrachten IT-Services zu verbessern;
- die langfristigen Kosten der Service-Tätigkeit zu reduzieren.

Um diese Ziele zu erreichen, ist es für die Anbieter der IT-Services notwendig, Dienstleistungsorientierung, Prozessorientierung und Architekturorientierung für die Erstellung und Durchführung ihrer Leistungen zugrunde zu legen [BöhKrc04].

Dienstleistungsorientierung: Sie dient dazu, die Zufriedenheit der Kunden mit den erbrachten IT-Services sicherzustellen und umfasst sowohl die Kundenorientierung als auch die genaue Leistungsspezifikation und -messung. Die Dienstleistungsorientierung trägt damit zur systematischen Kommunikation mit den Kunden bei und zur Ableitung und Spezifikation des Leistungsangebots aus den Anforderungen der Kunden. Die Dienstleistungsorientierung führt auch in der IT zu neuen Modellen für die Erbringung und Nutzung von IT-Diensten. So entwickeln sich neue Modelle für die Bereitstellung von IT-Services gekoppelt mit neuen Geschäftsmodellen, wie z. B. Software-as-a-Service (SaaS). Bei Software-as-a-Service werden die IT-Anwendungen nicht mehr vom Unternehmen selbst betrieben, sondern als IT-Service unter Verwendung von Web-Technologien genutzt und in der Regel entsprechend der Nutzung gezahlt.

Prozessorientierung: Damit kann gewährleistet werden, dass die definierten IT-Services zuverlässig und optimiert den Erwartungen des Kunden entsprechend erbracht werden. Die Prozessorientierung erfordert ein Umdenken von der häufig noch funktionalen Ausrichtung hin zu einer prozessorientierten Ausrichtung von Organisation und Abläufen. Die in ITIL definierten Referenzprozesse (siehe Abschnitt 4.3) bieten die Grundlage für die Umsetzung der Prozessorientierung.

Ausschlaggebend für die Optimierung und Standardisierung von Prozessen ist allerdings die Kundenintegration, die ein Hauptbestandteil bei Dienstleistungen ist (siehe Abschnitt 4.1.1).

Um eine gute Kundenintegration zu erreichen, ist die Interaktion mit dem Kunden zu betrachten und bei den Prozessen zu berücksichtigen. Bei der Interaktion mit dem Kunden ist der Kunde zu identifizieren, d. h., es ist zu klären, wer in welcher Rolle mit welcher Intensität an dem Prozess beteiligt ist. Weitere zu beachtende Merkmale sind die Zeitdauer der Integration und der Integrationszweck. Mit der Kundenintegration geht bei den IT-Services auch die Integration von Geschäftsprozessen und IT einher.

Architekturorientierung: Um IT-Services an die Kundenanforderungen und an neue Geschäftsprozesse anzupassen bzw. sie weiterzuentwickeln, ist es notwendig, sie modular zu gestalten [BuM01]. Der Ansatz der serviceorientierten Architekturen (SOA) bietet hier die Grundlagen, Services zu strukturieren und deren Zusammenwirken zu beschreiben. Eine modular aufgebaute Servicearchitektur gewinnt angesichts der hohen Änderungshäufigkeit der IT-Services noch an Bedeutung. Wiederverwendung von Teillösungen trägt dazu bei, die Wirtschaftlichkeit bei der Erbringung von IT-Services zu verbessern.

Organisatorische Änderungen und die Automatisierung von Abläufen sind weitere Aktionen zur Verbesserung der Leistungsfähigkeit.

4.1.3 IT-Servicequalität definieren – ein wichtiger Produktivitätsfaktor

Nach [DIN92] ist Qualität definiert als „die Gesamtheit von Eigenschaften und Merkmalen eines Produktes oder einer Dienstleistung, die sich auf deren Eignung zur Erfüllung festgelegter oder vorausgesetzter Erfordernisse beziehen“. Im IT-Servicebereich ist eines der wichtigsten Ergebnisse der vom Kunden mit einer Leistung verbundene Nutzen sowie insbesondere die aus Kundensicht wahrgenommene Dienstleistungsqualität. Kundenorientierung und Dienstleistungsqualität stehen somit bei IT-Services in engem Zusammenhang.

Zur Bewertung der IT-Services und der Dienstleistungsqualität können Kennzahlen herangezogen werden (siehe Abschnitt 4.5).

Ein wichtiges Element bei der Messung der Ergebnisqualität sind die Service Level Agreements (SLA), die IT-Services prüf- und messbar machen. Sie legen gegenüber dem Kunden die Leistungen fest, die mit den IT-Services erbracht werden. Dazu gehören u. a. Verfügbarkeit, Unterstützungs- und Supportleistungen, Performance und Kapazität. Ein Service Level Agreement sollte mindestens Folgendes festlegen:

- Beschreibung des IT-Services und der Leistungsmerkmale
- Vereinbarte Service-Zeiten
- Reaktionszeiten
- Ziele für Verfügbarkeit, Sicherheit und Kontinuität des IT-Services
- Pflichten des Kunden und des Serviceanbieters.

Für die Definition, Einhaltung, Überwachung und Überprüfung der Service Level Agreements ist das Service Level Management zuständig (siehe Abschnitt 4.2.2). Das Service Level Management ist in ITIL 3 im Service Design und im Continual Service Improvement verankert.

Für die Bewertung der Prozessqualität wurde in Anlehnung an das Reifegradmodell der Carnegie Mellon University (Capability Maturity Model Integration – CMMI) ein Information Technology Service Capability Maturity Model (IT-Service CMM) entwickelt [NCV02].

4.1.4 Erfolge durch professionelles Management der IT und ihrer Services

Ein professionelles IT-Servicemanagement versetzt die Unternehmen in die Lage, die IT gewinnbringend bei der Durchführung ihrer Geschäftsprozesse und deren Weiterentwicklung einzusetzen. Unternehmen, die das IT-Servicemanagement konsequent umsetzen, gelingt es, mit der Informationstechnologie den Unternehmenserfolg zu beeinflussen und die Wettbewerbsfähigkeit zu erhöhen.

Die Kundenorientierung als Grundlage des IT-Servicemanagements ermöglicht es, die Hauptprobleme in der Beziehung zwischen Kunde und IT-Servicedienstleister zu beheben, indem

- klare, geschäftsbezogene Zielsetzungen definiert werden;
- Leistungen des Anbieters und die dazugehörigen Service Levels klar definiert sind;
- durch die transparente Darstellung der Leistungen der Kunde keine unrealistischen Erwartungen hat;
- optimierte Dienstleistungsprozesse die definierte Produkt- und Prozessqualität liefern;
- Prozesse durch Überwachung von Zeit, Kosten und Qualität kontinuierlich verbessert werden.

Der Anbieter der IT-Services kann schnell auf neue Anforderungen reagieren. Dies ist unabdingbar für den Erfolg, da sich Geschäft und Technologie in unvorhergesehener Weise ändern. Laufende Anpassungen sind notwendig, da sich aus unterschiedlichen Gründen Veränderungen ergeben können:

- personelle Veränderungen:
 - Veränderung der Anforderungen
 - Angst vor Arbeitsplatzverlust oder -änderung
- organisatorische Veränderungen:
 - Wechsel der Zuständigkeiten
 - Angst vor Kompetenzverlust
 - Veränderte Abläufe und Prozesse
 - Erfassbarkeit der zu erbringenden Leistung
 - Offenlegung und Beseitigung der Schwachstellen
- technische Veränderungen:
 - „Verbesserung“ bestehender IT-Ressourcen und Systeme
 - Einführung neuer IT-Technologien
 - Einführung neuer Systeme

Insgesamt können die Unternehmen aus einem erfolgreichen IT-Servicemanagement folgenden Nutzen ziehen:

- Verbesserung von Verlässlichkeit, Verfügbarkeit, Durchsatz, Kapazität, Wartungsfähigkeit und Widerstandsfähigkeit der eingesetzten IT-Ressourcen für die zu erbringenden Service Levels.
- Erhöhung von Flexibilität und Anpassbarkeit der IT-Prozesse.
- Beherrschbarkeit der Komplexität, die sich aus einer Vielzahl von Anwendungen zur Unterstützung der Geschäftsprozesse und neuen Technologien ergibt.

- Höhere Kundenzufriedenheit durch bessere und messbare Verfügbarkeit und Performance der IT-Servicequalität.
- Bessere Kommunikation zwischen der IT-Organisation und ihrer Kunden sowie innerhalb der IT-Organisation.
- Höhere Verlässlichkeit hinsichtlich der Erbringung vereinbarter Service Levels.
- Herstellen einer geschäftsmäßigen Beziehung zwischen der IT-Organisation und ihren Kunden, da die zu erbringenden Dienstleistungsgrade explizit ausgehandelt werden.

Um die Einführung des IT-Servicemanagements im Unternehmen zu erleichtern, ist die Nutzung von Standards wie ITIL zu empfehlen.

■ 4.2 IT-Servicemanagement – Konzepte und Standards

„Es ist ein Wunder, dass die Neugierde die schulische Ausbildung überlebt.“

Albert Einstein

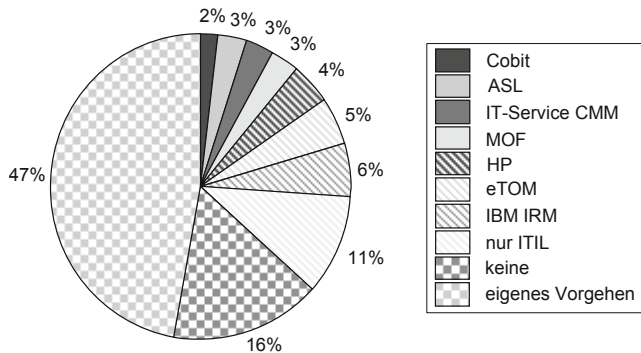
4.2.1 Die Vielfalt der Lösungen – Überblick über vorhandene Konzepte

Die Möglichkeiten, IT-Servicemanagement auf der Basis eines vorgegebenen Rahmenwerkes im eigenen Unternehmen aufzusetzen, sind im Laufe der vergangenen Jahre durch die zunehmende Publizität und Verbreitung des Themas deutlich gestiegen. Als ein Gradmesser der Variantenvielfalt kann hier auf das ITSM-Portal² verwiesen werden.

Es gibt die unterschiedlichsten Ansätze für das IT-Servicemanagement, die zum Teil von großen IT-Unternehmen angeboten werden, wie z.B. Microsoft Operation Framework (MOF), IT Service Management von HP oder Information Technology Process Model (ITPM) von IBM. Bei der Neuausrichtung der ISO 9000:2000 wurde die Prozessorientierung in den Vordergrund gestellt. ITIL unterstützt diesen Ansatz für den Bereich des IT-Servicemanagements und ist somit konform zur ISO-Norm.

Zum besseren Verständnis des Themenfeldes IT-Servicemanagement werden im Folgenden zunächst einige Konzepte exemplarisch vorgestellt. Im Anschluss daran wird das ITIL-Konzept als Grundlage der detaillierteren Betrachtung des Themas IT-Servicemanagement gewählt. Hierfür spricht u. a., dass ITIL sich in den letzten Jahren zu einem Quasi-Standard im Umfeld von IT-Services entwickelt hat. Nach einer Umfrage der DETECON 2003 (Abbildung 4.2, nächste Seite) stellt ITIL das meist verwendete, öffentlich zugängliche Rahmenwerk. Zudem schreiben immer mehr Unternehmen externe Leistungsvergaben nach ITIL aus.

² <http://www.itsmportal.com/frameworks>

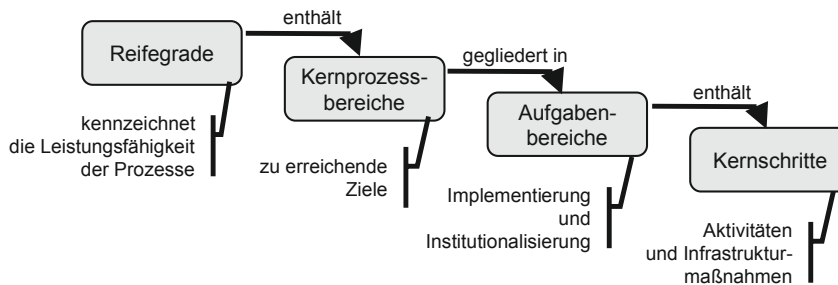
**ABBILDUNG 4.2**

Einsatz von Methoden im ITSM
(Quelle: [DET04])

4.2.1.1 IT-Service CMM

Das IT-Service CMM³ (Capability Maturity Model) ist ein Vertreter der IT-Servicemanagement-Modelle, die sich den Aufgaben und Prozessen über ein Reifegrad-Modell nähern.

Es handelt sich um ein frei verfügbares Referenzmodell, das beschreibt, welche Prozesse eine reife IT-Service-Organisation implementiert haben sollte (vgl. Abbildung 4.3). Ziel ist das Assessment der IT-Service-Fähigkeiten sowie Hinweise, wie diese zu verbessern sind.

**ABBILDUNG 4.3** Die Struktur der IT-Service CMM

IT-Service CMM zeigt den Reifegrad von IT-Organisationen in fünf Stufen [NCV02]:

1. *Initial*: Der Prozess der Erbringung der IT-Services ist chaotisch und erfolgt ad hoc. Nur wenige Prozesse sind definiert, und die erfolgreiche Durchführung eines IT-Service hängt vom individuell geleisteten Aufwand und Einsatz ab.
2. *Wiederholbar*: Grundlegende Servicemanagement-Prozesse sind etabliert. Ansätze zur Prozesssteuerung sind vorhanden, sodass frühere Erfolge auf ähnliche IT-Services mit ähnlichen Service Levels übertragen werden können.
3. *Definiert*: Die IT-Serviceprozesse sind dokumentiert, standardisiert und in einen standardisierten Dienstleistungsprozess integriert. Die Erbringung der Leistungen erfolgt nach definierten und geprüften Regeln.
4. *Gesteuert*: Detaillierte Messungen des Prozesses zur Erbringung der IT-Services und der Dienstleistungsqualität werden durchgeführt.

³ <http://www.itservicecmm.org>

5. *Optimiert*: Kontinuierliche Prozessverbesserung durch quantitative Messungen und Auswertung der IT-Serviceprozesse sowie durch neue Ideen und innovative Technologien.

Ziel des IT-Service CMM ist es, die Anbieter von IT-Services bei der Professionalisierung der IT-Servicemanagement-Prozesse zu unterstützen. Dies beinhaltet die Bewertung der bestehenden Prozesse und die Ableitung von Maßnahmen zur Verbesserung der IT-Servicemanagement-Prozesse.

4.2.1.2 COBIT

COBIT⁴ (Control Objectives for Information and Related Technology) ist ein Repräsentant der Referenzmodelle, die IT-Servicemanagement in Richtung IT-Governance erweitern.

COBIT ist ein Modell von Kontrollzielen speziell für IT-Prozesse, das seit 1993 von internationalen Gremien des Verbandes der EDV-Prüfer (Information Systems Audit and Control Association, ISACA) entwickelt wurde. Seit 2000 wird das Framework von der Schwesterorganisation IT Governance Institute weiterentwickelt.

COBIT beschreibt einen Kreislaufzusammenhang zwischen Unternehmensanforderungen, IT-Ressourcen und IT-Prozessen. Nach COBIT sind Enterprise Governance und IT-Governance direkt voneinander abhängig und dürfen nicht isoliert betrachtet werden [ISA00-3]. Der Steuerungsansatz von COBIT ist grundsätzlich Top-down. Ausgehend von Unternehmenszielen werden IT-Ziele festgelegt, die wiederum die Architektur der IT beeinflussen.

Mit der Version 4.1 wurde das Modell vollständig überarbeitet und weiter auf Governance-Aspekte fokussiert. In vier Dokumenten, die primär die organisatorischen Bereiche der IT abdecken, werden insgesamt 34 Prozesse definiert. Im Buch *Core Content* [ISA07-1] werden die Prozesse zunächst über die relevanten Aktivitäten und Messgrößen beschrieben. Für jeden Prozess werden auch Prozessziele (High Level Control Objectives) formuliert und verfeinert. Die Kontrollen werden auf die Erfüllung der Geschäftsanforderungen fokussiert. Zudem ordnet man den einzelnen Elementen „Management Guidelines“ zu. Diese bilden den eigentlichen Kern des IT-Governance-Ansatzes und enthalten neben dem High-Level-Kontrollziel die kritischen Erfolgsfaktoren, die Zielerreichungsindikatoren, die Leistungsindikatoren und eine Beschreibung der unterschiedlichen Reifegrade.

Das Buch *Control Objectives* [ISA07-2] enthält Kontrollpraktiken, die für jedes im Core Content vorhandene Kontrollziel Maßnahmen festlegen. Die Kontrollpraktiken sind aktionsorientiert und bieten „Warum durchführen?“-Argumente in Form des erzielten Werts und der zu vermeidenden Risiken. Das Buch *IT Governance Implementation Guide* [ISA07-3] bietet eine detaillierte Road Map zur Einführung einer effektiven IT-Governance in einer Organisation. Das Buch *IT Assurance Guide* [ISA07-4] bietet Anweisungen dazu, wie COBIT eine Vielzahl von Gewährleistungsaktivitäten unterstützt und wie man für die IT-Prozess Gewährleistungsüberprüfungen durchführt. Darüber hinaus enthält es Dokumente, die auf Spezial-Themen eingehen, wie z. B. Sabanes Oxley oder Basel II.

Die Hauptaufgaben der einzelnen Prozesse in den Domänen sind zusammengefasst:

- Planen und Organisieren: stellt die Einhaltung der Geschäftsziele sicher und formuliert strategische und taktische Vorgaben für die IT

⁴ <http://www.isaca.org/cobit>

- Beschaffen und Implementieren: fokussiert auf die Umsetzung der gewählten Strategie über Lösungen, die identifiziert, entwickelt oder gekauft und implementiert werden.
- Betreiben und Unterstützen: Fokus auf zeitgerechter Erbringung benötigter Leistungen.
- Überwachen und Evaluieren: zur regelmäßigen Bewertung der IT-Prozesse.

Gemäß dem COBIT-Prozessmodell ist jede Einzelleistung zu planen beziehungsweise mit den bestehenden Plänen und Strukturen abzustimmen, in der Folge zu beschaffen und einzuführen; darüber hinaus ist für laufende Unterstützung zu sorgen und entsprechende Überwachungsmaßnahmen sind zu implementieren, die bei Abweichungen in einen neuerlichen Durchlauf münden.

4.2.2 Servicemanagement nach ITIL

Die IT-Infrastructure Library (ITIL) ist ein Regelwerk, das sich aus einer Reihe von separierten Modulen zusammensetzt. Wichtig ist hier der Bezug auf die Kerngeschäfte des Unternehmens und die Konzentration des IT-Services auf die bestmögliche Unterstützung dieser Geschäftsprozesse. ITIL fußt auf der Annahme, dass IT-Servicemanagement in einem Unternehmen in direktem Bezug zu den verwendeten Informationstechnologien, für die die Servicedienstleistungen angeboten werden, steht.

Innerhalb von ITIL werden die einzelnen Module bzw. Disziplinen des IT-Services in einer Reihe von Büchern beschrieben. Dabei werden die Erfahrungen im Bereich des IT-Service-Managements kontinuierlich eingearbeitet, sodass dieses Regelwerk als praktische Erfahrungssammlung („Best Practice“-Richtlinie für die Realisierung von IT-Servicелеistungen) bezeichnet werden kann. ITIL beschreibt das „WAS“, aber nicht detailliert das „WIE“ im Sinne einer starren Vorgabe. Die Umsetzung ist auf die Größe, die interne Kultur und vor allem auf die Anforderungen des betroffenen Unternehmens abzustimmen und umzusetzen.

Seit Mitte der 90er Jahre des letzten Jahrhunderts hat sich ITIL als De-facto-Standard für das IT-Servicemanagement etabliert und wird vielfach synonym hierfür gebraucht. Die Bücher von ITIL sind bis heute die einzige umfassende, nicht-proprietäre und öffentlich zugängliche Verfahrensbibliothek in diesem Bereich. Darüber hinaus bietet ITIL eine Fülle von weiteren Produkten und Dienstleistungen, wie Schulungen, Zertifizierungen o. Ä.

Mitte 2007 wurde die neue Version 3 vorgestellt. Eine wesentliche Veränderung liegt in der Beziehung zwischen der IT und dem Kerngeschäft. Die bisherige Ausrichtung des Service-Managements auf die Geschäftsstrategie (IT/Business-Alignment) wird durch deren Integration in ein einheitliches System ersetzt (IT/Business-Integration) und zielt direkt auf einen Wertbeitrag zum Geschäftsnutzen. Wesentlichstes Merkmal ist der Schwenk von einer Sammlung integrierter Serviceprozesse hin zu einem ganzheitlich ausgerichteten Lebenszyklus von Services. Hier wird erstmals die strukturierte Planung, Entwicklung, Betrieb und Weiterentwicklung von IT-Services entlang ihrer Lebensphasen unterstützt.

Die Migration vom alten zum neuen Ansatz ist jedoch möglich, da ein Großteil der Prozesse grundsätzlich beibehalten wurden; diese wurden optimiert, sodass Anwender bei einer Umstellung auf Version 3 die Möglichkeit haben, auf ihre existierenden Prozesse nach Version 2 aufzubauen und ihr IT-Servicemanagement weiterzuentwickeln.

Da ITIL in der Version 2 eine sehr hohe praktische Verbreitung besitzt, werden im Folgenden sowohl Version 2 als auch 3 beschrieben und verglichen.

4.2.2.1 Überblick der Managementmodule der Version 2

Schwerpunkt der ITIL-Dokumente bilden die beiden Bereiche Service Support und Service Delivery. In diesen werden überschneidungsfrei alle anfallenden Leistungen und die interdisziplinären Prozessabläufe dargestellt (vgl. Abbildung 4.4).

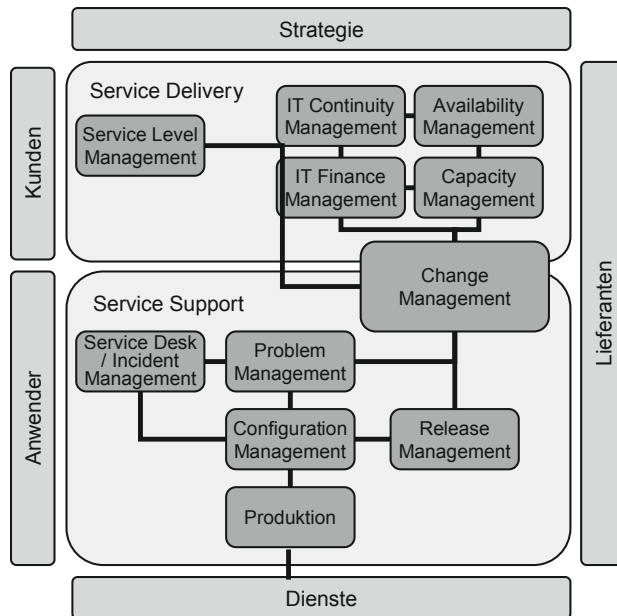


ABBILDUNG 4.4
Fokus ITIL-Servicemanagement

Service Support [OGC00] beschreibt die Prozesse und Disziplinen, die notwendig sind, um IT-Services auf eine effektive Weise anbieten zu können:

- *Funktion „Service Desk“:* Erfassung und Bearbeitung von Benutzeranfragen.
- *Problem Management:* Ursachenidentifikation und Problemlösung
- *Configuration Management:* Erfassung relevanter Informationen über IT-Anlagen.
- *Change Management:* standardisierter Umgang mit notwendigen Änderungen.
- *Release Management:* technische und nicht-technische Konsequenzen von Wechseln.

Service Delivery [OGC01] umfasst das Management der IT-Services selbst, damit IT-Services gemäß der Vereinbarung zwischen Anbietern und Nachfragenden erbracht werden:

- *Service Level Management:* Planung, Entwicklung, Vereinbarung und laufende Kontrolle von Service Level Agreements zwischen der IT-Abteilung und deren Kunden.
- *Availability Management:* Bereitstellung der erforderlichen Service-Verfügbarkeit.
- *Capacity Management:* Anforderungsgerechte Dimensionierung der Ressourcen.
- *Financial Management for IT Services:* Bepreisung und Transparenz über IT-Services auf Basis eines „IT-Warenkorbs“.
- *IT Service Continuity Management:* Sicherstellung der IT-Unterstützung für unternehmenskritische Prozesse als Teil des Risk-Managements.

ITIL liefert ein generisches und skalierbares Konzept, mit dem sich Qualität und Quantität von IT-Services zielgerichtet, geschäftsprozessorientiert und kostenbewusst steuern und kontinuierlich optimieren lassen. Die Bereiche werden im Folgenden beleuchtet.

Bei ITIL zeichnen sich aus der Praxis deutliche Präferenzen hinsichtlich der Einführungsaktivitäten für bestimmte Prozessgruppen ab. Im Vordergrund stehen hier jeweils die kunden nahen Prozesse wie Incident/Problem-Management und Service Level Management.

Überblick über die Managementmodule der Version 3

Die Version 3, die im Juni 2007 veröffentlicht wurde, baut auf der neuen Grundphilosophie der Orientierung am Lebenszyklus eines Services auf (vgl. Abbildung 4.5):

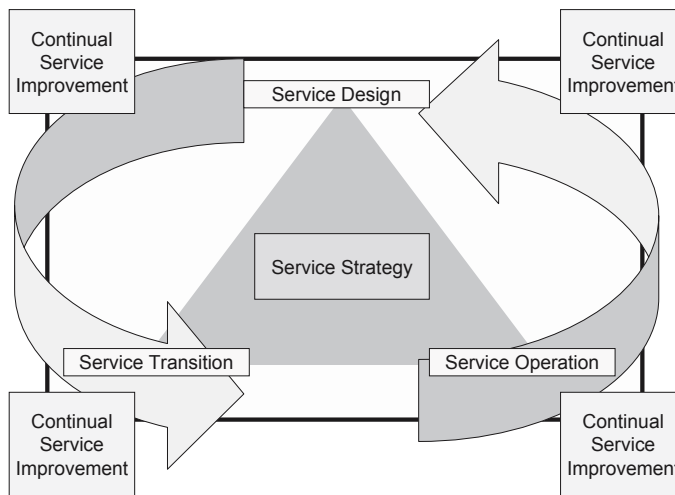


ABBILDUNG 4.5
Service-Lebenszyklus angelehnt an [OSS07 S.36]

In den Kern-Dokumenten der Version 3 sind – thematisch zusammengefasst – die unterschiedlichen Sichtweisen auf den Service-Lebenszyklus beschrieben.

Service Strategie [OSS07] umfasst alle Prozesse, um Servicemanagement strategisch im Unternehmen zu etablieren und Dienstleistungsnachfrage und -angebot zu strukturieren:

- *Financial Management*: analog zu ITIL Version 2.
- *Demand Management*: bildet den Rahmen, in dem potentielle zukünftige IT-Dienstleistungen und -Nachfragen analysiert und gewichtet werden.
- *Service Portfolio Management*: bildet eine Gesamtschau der IT-Services über den gesamten Lebenszyklus und steuert die Services durch die Phase.

Service Design [OSD07] beschreibt die Prozesse, die notwendig sind, um die strategischen Vorgaben in neue bzw. angepasste IT-Services umzusetzen:

- *Service Catalogue Management*: betreut alle angebotenen IT-Dienstleistungen.
- *Service Level Management*: analog zu ITIL Version 2.
- *Supplier Management*: betreut Lieferanten und deren nachgefragten Dienstleistungen und bindet diese nahtlos in die interne Prozesskette ein.
- *Service Capacity Management*: analog zu ITIL Version 2.

- *Service Availability Management*: analog zu ITIL Version 2.
- *IT Service Continuity Management*: analog zu ITIL Version 2.
- *Information Security Management*: analog zu ITIL Version 2.

Service Transition [OST07] umfasst die Prozesse, die der planvollen Inbetriebnahme von neuen bzw. angepassten IT-Services dienen:

- *Change Management*: analog zu ITIL Version 2.
- *Service Asset and Configuration Management*: analog zu ITIL Version 2.
- *Transition Planning and Support*: plant und koordiniert die Überführung eines neuen oder geänderten Service in den Betrieb gemäß den Zeit-, Qualität- und Kostenvorgaben.
- *Release and Deployment Management*: analog zu ITIL Version 2.
- *Service Testing and Validation*: stellt sicher, dass der neue oder geänderte Service sich wechselwirkungsfrei in die geplante Palette einpasst.
- *Evaluation*: ermittelt die tatsächlichen Performanzparameter bei der Operativsetzung eines Services und prüft diese gegen die erwarteten Kennzahlen.
- *Knowledge Management*: stellt die adäquate Versorgung mit servicebezogenen Informationen und den Wissensaufbau sicher.

Service Operation [OSO07] beschreibt die Prozesse, die im operativen Betrieb der Services für eine effiziente und störungsarme Erbringung notwendig sind:

- *Incident Management*: analog zu ITIL Version 2.
- *Problem Management*: analog zu ITIL Version 2.
- *Event Management*: analog zu ITIL Version 2.
- *Request Fulfilment*: Neben den Störungs- und Fehlermeldungen wird hier der Begriff der Anfrage weiter gefasst und deckt auch weitergehende Benutzeranfragen ab.
- *Access Management*: behandelt eigenständig das Rechte- und Rollenmanagement, also die Zuteilung von Berechtigungen für die Nutzung eines IT-Services.

Continual Service Improvement [OSC07] – direkt im Modell verankert sind hier die Prozesse zu einer langfristigen, kontinuierlichen Verbesserung des Service-Angebotes:

- *7-Step Improvement Process*: Hiermit wird ein eigenständiger Prozess zur kontinuierlichen Verbesserung als zentrales Element im Framework etabliert.
- *Service Measurement*: Messen von Service-Kennzahlen als generischer Prozess.
- *Service Reporting*: Analog zum Messen ist auch das Reporting hier jetzt als eigenständige Dienstleistung ausgegliedert.
- *Service Level Management*: analog zu ITIL Version 2.

Bei der Weiterentwicklung des Rahmenwerks wurde auf ein hohes Maß an Kontinuität gesetzt. Teilweise wurden Bezeichnungen angepasst und einzelne bestehende Prozesselemente (z.B. Measurement, Reporting) wurden als eigenständige Prozesse ausgegliedert.

4.2.2.2 Nutzen von ITIL

Neben den grundsätzlichen Nutzen von IT-Servicemanagement, wie sie in Abschnitt 4.1.4 dargestellt werden, lassen sich noch weitere Nutzenpotenziale aufzeigen, denn über die Prozesse der ITIL können Kunden-Lieferanten-Beziehungen definiert werden, in denen die Bereitstellung definierter IT-Services in bestimmter Qualität eingekauft werden kann. Aus dieser Konstellation ergeben sich sowohl für den Anwender als auch für den Anbieter Vorteile.

Vorteile für den *Anwender (Kunde)*:

- Die Kommunikation mit der IT-Organisation wird aufgrund von Vereinbarungen und definierten Ansprechpartnern verbessert.
- Qualität und Kosten der IT-Services lassen sich besser kontrollieren. Die IT-Services werden eher auf die Bedürfnisse der Kunden ausgerichtet.
- Absprachen und Vereinbarungen, auch über die Qualität der IT-Services, verbessern das Verhältnis zum Kunden.

Vorteile für den *Anbieter (IT-Organisation)*:

- Die IT-Abteilung profiliert sich als professioneller Anbieter von IT-Dienstleistungen.
- ITIL liefert einen klaren Referenzrahmen für die interne Kommunikation, Standardisierung und Erkennbarkeit von Vorgängen.
- Die IT-Service-Qualität wird messbar und lieferbar.
- Das Management kann die IT-Organisation besser steuern und bewerten. Änderungen lassen sich leichter kontrollieren.
- Eine sinnvolle Etablierung der ITIL-Prozesse bildet die Voraussetzung für ein fundiertes Outsourcing von Teilbereichen von IT-Services.

Auch ITIL hat seine Grenzen. ITIL ist keine Projektmanagementmethode: Sie soll nicht die Einführung einer IT-Infrastruktur organisieren, sondern vielmehr deren dauerhaften Betrieb. Die Bereiche der Einführung und der Weiterentwicklung werden zugunsten eines standardisierten Gesamtprozessmodells wesentlich zurückgestellt.⁵ Sie definiert klare Aufgabenstellungen, die beim Betrieb dieser Infrastruktur anfallen. In der Gleichartigkeit der Prozesse innerhalb der Betriebsphase liegt aber genau die Stärke der ITIL-Bibliothek.

ITIL ist keine fertige Gebrauchsanweisung, die ohne Adaption überall identisch anwendbar ist. ITIL ist ein generisches Modell, das allgemein gehalten und somit weitgehend global gültig ist. Daraus leitet sich die Notwendigkeit ab, dass die beschriebenen Prozesse jeweils an die Situation eines Unternehmens angepasst werden müssen. Die beschriebenen Module sind nicht unbedingt als eigenständige Organisationseinheiten abzubilden.

Die unterschiedlichen Aspekte bei der Einführung und dem kontrollierten Betrieb werden in Abschnitt 4.4 eingehender betrachtet.

⁵ Hier bietet sich beispielsweise das IT-Service Capability Maturity Model (IT-Service CMM) an, das sich auf das Schließen dieser Lücken konzentriert.

■ 4.3 ITIL unter der Lupe

*„Nichts auf der Welt ist so mächtig wie eine Idee,
deren Zeit gekommen ist.“*

Victor Hugo

Im Folgenden werden zunächst die Prozesse und Bereiche beschrieben, die sowohl in ITIL Version 2 als auch in der neu erschienenen Version 3 vorhanden sind. Die Gliederung orientiert sich an der Struktur von ITIL Version 2. Im Anschluss daran werden noch die in der Version 3 neu hinzugekommenen Prozesse vorgestellt.

4.3.1 Service-Support-Prozesse

Im Sinne von ITIL umfasst *Service Support* die unterstützenden Tätigkeiten für den Betrieb der IT-Services. Hierunter werden alle operativen Management-Prozesse im Bereich IT-Service-management verstanden. Darüber wird sichergestellt, dass der Benutzer Zugang zu den gewünschten IT-Services hat, um so seinen wertschöpfenden Arbeitsaufgaben nachgehen zu können.

4.3.1.1 Service Desk

Beim *Service Desk* handelt es sich nicht um einen Prozess, sondern um eine elementare Funktion des IT-Service-managements nach ITIL. Das Service Desk bildet den zentralen Anlauf- und Kontaktpunkt für alle Kundenfragen. Die kommunikativen Aufgaben beschränken sich nicht ausschließlich auf Support-Dienstleistungen und Fehleraufnahme. Das Service Desk bildet, als das „Gesicht der IT“, die universelle Schnittstelle zum Anwender und hält ihn auf dem Laufenden (Abbildung 4.6).

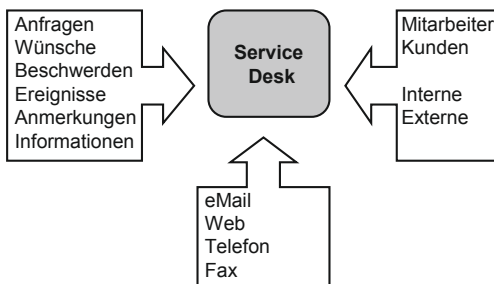


ABBILDUNG 4.6

Das Service Desk – One Face to the Customer

Hier werden Kundenkontakte über unterschiedliche Kanäle aufgenommen, strukturiert und einer Weiterbearbeitung zugeführt. Es dient als zentrale Informationsstelle zwischen Kunden, internen Service-Organisationen und externen Providern. Ihm obliegt auch die Koordination der nachfolgenden Supporteinheiten.

Zu den Aufgaben des Service Desks zählen in Verbindung mit dem Incident Management das Registrieren und Nachverfolgen von Störungsmeldungen und eine erste Prüfung eingegangener Meldungen. Je nach vereinbarten Service Levels wird die weitere Bearbeitung angestoßen;

während der Bearbeitung erfolgt am Service Desk auch die Information des Kunden bezüglich des Status und Fortschritts seiner Anfragen.

Weil das Service Desk in der Kommunikation mit dem Kunden eine zentrale Rolle einnimmt, ist es zudem prädestiniert zur Überwachung der Einhaltung von Service Level Agreements. Bei Nichteinhaltung (oder bereits bei der Gefahr) nimmt das Service Desk die Rolle des Initiators für geeignete Gegenmaßnahmen und Eskalationsschritte wahr.



Praxistipp:

Nutzen Sie die initiale Kommunikationsmöglichkeit mit einem Anwender schon bei der Kontaktaufnahme und informieren Sie z. B. bereits in der Telefonwarteschlange oder auf der Fehlermeldeseite des Intranets über aktuell vorliegende bekannte Störungen, die einen größeren Teil der Anwender betreffen.

Die Einführung eines Service Desk bringt neben einem verbesserten Kundenservice und dadurch erhöhter Kundenzufriedenheit vor allem eine schnellere und qualitativ hochwertigere Abwicklung von Kundenanfragen.

4.3.1.2 Incident Management

Nach ITIL [OGC00] wird unter einem Incident (Störung) ein Ereignis verstanden, das den standardmäßigen Betrieb der IT-Services unterbricht. Incidents umfassen dabei neben Störungen der Hardware (z. B. Druckerausfall) und Software (z. B. Verfügbarkeit eines Web-Services) auch benutzerbezogene Ereignisse (z. B. Passwort vergessen).

Durch ein Service-Request richtet ein Anwender seine Anfrage zur Unterstützung, Service-Erweiterung, Lieferung, Information, zur Beratung oder Dokumentation an das Incident Management. Primäre Aufgabe des Incident Managements ist, dass der Anwender wieder arbeiten kann, die Beseitigung der Störungsursache ist zunächst zweitrangig.

Ziel des Incident Managements ist die Wiederherstellung des definierten Betriebszustands eines IT-Services für den Anwender im Rahmen der vereinbarten Servicequalität, um die Minimierung der Beeinträchtigung der Geschäftsprozesse zu erreichen. Sobald das Incident Management die Einhaltung der Service Levels gefährdet sieht, erfolgt eine Eskalation. Innerhalb der IT-Organisation bildet das Incident Management die Schnittstelle zu anderen IT-Servicebereichen (z. B. Problem, Change, Configuration, Release ...). Meist werden neben Störungen auch andere Kundenanfragen (Service Requests) der Anwender über das Service Desk erfasst, erste Hilfestellung geleistet und gegebenenfalls die weitere Bearbeitung in den nachgelagerten Supporteinheiten koordiniert.

Das Incident Managements besteht zunächst darin, Anfragen und Störungsmeldungen zu dokumentieren. Dann erfolgt eine Priorisierung und Kategorisierung der Störungen sowie ggf. eine initiale Unterstützung des Anwenders. Eine erste Fehleranalyse überprüft, ob die Lösung bekannt ist und durch den First Level Support gelöst werden kann.

Kann sie nicht durch bekannte Lösungsmuster abgedeckt werden, wird der Fall an den Second Level Support weitergeleitet. Falls auch hier keine Behebung möglich scheint, erfolgt eine weitere Eskalation bis hin zu Entwickler im eigenen Haus oder Service des Herstellers. Mit einer Dokumentation der Störungslösung innerhalb der Störungsdatenbank endet der Prozess des Incident Managements.

**Praxistipp:**

Achten Sie auf die „leidige“ Dokumentation aller Aktivitäten/Work-Arounds zur Beseitigung einer Störung (inkl. der benötigten Zeit). Eine gute Fehlerlösungsdatenbank bildet eine wertvolle Grundlage für ein gezieltes Problem Management. Evtl. stehen für bestimmte Systeme bereits initiale Füllungen der Datenbank vom Hersteller oder Third-Party-Anbietern zur Verfügung.

Die Auswertung aller Incidents dient einerseits der Überführung von gleichartigen Vorkommnissen in den Prozess Problem Management, andererseits kann auch mittels Reporting für Kunden und Lieferantengespräche zur Service-Verbesserung beigetragen werden.

Durch den Einsatz des Incident-Management-Prozesses im IT-Service-Management sollen die Störungsbearbeitungen effektiver und effizienter durchgeführt werden. Dies soll zum einen zur Reduzierung der Support- und (verdeckten) IT-Kosten führen und zum anderen ermöglichen, die negativen Auswirkungen von Incidents auf die Geschäftsprozesse zu minimieren.

4.3.1.3 Problem Management

Die nachhaltige Beseitigung von gleichgelagerten Störungen steht im Fokus des Problem Managements. Es unterstützt das Incident Management bei schweren und umfangreichen Störungen, die seitens des Service Desks nicht behoben werden konnten. Hier werden dem Incident Management temporäre Lösungen zur Verfügung gestellt und endgültige Lösungen bekannter Fehler erarbeitet, die über das Change Management eingebracht werden.

Fehler in der IT-Infrastruktur führen zu einer oder mehreren Störungen (Incident) in den angebotenen IT-Services (Abbildung 4.7). Der bis dato unbekannte Grund wird als das Problem identifiziert. Lässt sich das Problem erfolgreich diagnostizieren und eine Behebung der Störung herbeiführen, so wird dieses als bekannter Fehler (Known Error) eingestuft. Mit der Identifikation kann eine Änderung des betroffenen Systems angestoßen werden (Request for Change), um so die zugrundeliegenden Ursachen strukturell zu beheben.

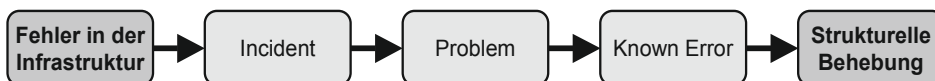


ABBILDUNG 4.7 Von der Störung über das Problem zum RFC

Aufgabe des Problem Managements ist somit die Bearbeitung aller Ausfälle von IT-Services unter dem speziellen Gesichtspunkt der Identifizierung der zugrundeliegenden Ursachen (siehe Abbildung 4.8, nächste Seite). Dazu gehören neben dem Second-Level- und Third-Level-Support für IT-Services auch die Wiederherstellung von IT-Services (Incident Support), das Ermitteln der Ursache von Störungen (Problem Control) sowie die Behebung von Problemen (Error Control) und ggf. eine Formulierung von Änderungsanforderungen (RFC).

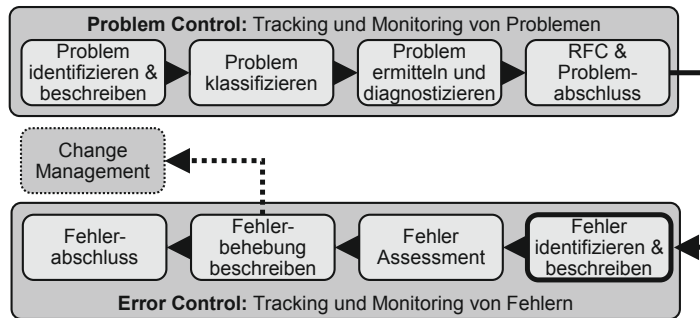


ABBILDUNG 4.8
Aktivitäten des
Problem-/Error Control

Zentrales Ziel ist die Unterstützung der Einhaltung der vereinbarten Service-Ziele. Dies soll einerseits durch die Minimierung der Auswirkungen von Incidents erreicht werden. Andererseits soll durch proaktive Ermittlung und Behebung der Ursachen von Ereignissen Problemen vorgebeugt oder Probleme ganz vermieden werden.



Praxistipp:

Ihr Ziel sollte es sein, 80 bis 90% der gemeldeten Vorfälle im Bereich des Incident Managements über Wissensdatenbanken u. Ä. lösen zu können. Nur max. 10 bis 20% der Fälle sollten an das Problem Management weitergeleitet werden.

Die Aktivitäten des *Problem Control* konzentrieren sich auf die Ermittlung der Ursache von Störungen und deren Auswirkungen auf die betroffenen Komponenten und Geschäftsprozesse. Mit der Verfügbarkeit von anwendbaren Problemlösungsanweisungen kann das Incident Management effektiv und frühzeitig eine gemeldete Störung beheben. Im Laufe eines IT-Betriebes werden eher selten neuartige Störungen über das Service Desk gemeldet. Typischerweise stellen sich schnell bekannte, wiederkehrende Störungsbilder ein. Eine Grundlage für die Effizienzsteigerung im Incident Management bildet die Analyse der Störungen und Bereitstellung von empfohlenen Vorgehensweisen.

Die Aktivitäten des *Error Control* umfassen die zielgerichtete Behandlung bekannter Fehler. Dies kann von einfachen Fehlerbehebungsroutrinen bis hin zum Anstoß eines Change-Management-Prozesses reichen.

Mit der *Bewertung des Fehlers* wird die Grundlage für die weitere Planung der Fehlerbehebung gelegt. Hier kann entschieden werden, ob aufgrund der Dringlichkeit eine kurzfristige Lösung vorab (Hotfix) herausgebracht wird, ob die Behebung des Fehlers in die weitere Release-Planung mit aufgenommen wird oder – auch das kann eine legitime Entscheidung sein – ob man den Fehler als solchen belässt und er mit seinem Work-Around bestehen bleibt.

4.3.1.4 Configuration Management

Ziel des Configuration Managements ist die Unterstützung anderer ITIL-Disziplinen durch die Bereitstellung eines möglichst detaillierten Modells der IT-Infrastruktur. Die für das IT-Servicemanagement notwendigen Informationen über die eingesetzten Elemente werden vom Configuration Management bereitgestellt. Alle Komponenten werden durch Configuration Items (CI) – mittels Kategorien, Attributen, Beziehungen zueinander, Status etc. – erfasst und

in einer Configuration-Management-Datenbank (CMDB) gesammelt. Dem Configuration Management fällt damit eine zentrale Rolle im kommunikativen und informativen Zusammenspiel der einzelnen Prozesse zu.

In der Configuration-Management-Datenbank sind ständig aktuelle und historische Informationen über die Configuration Items verfügbar. Sie bildet damit die Grundlage für wirtschaftliche IT-Dienstleistungen, Verbesserung der Servicequalität und der Kontrolle über die eingesetzten IT-Vermögenswerte. Gleichzeitig ist dies auch die Basis für die Kosten- und Leistungsverrechnung innerhalb des Service Level Managements.

Um die Anforderungen an das Configuration Management abzudecken, ist eine Reihe von Aufgaben zu bearbeiten. Diese gliedern sich in die Bereiche:

- Configuration-Management-Planung,
- Identifikation von Configuration Items,
- Kontrolle von Configuration Items,
- Konfigurationsstatus-Nachweise,
- Konfigurationsüberprüfung und -audit.

Der wesentliche Nutzen des Configuration Managements liegt in der Effektivitätssteigerung der anderen Prozesse. Neben der Grundlage für Bestands-/Planungsdaten und der effizienteren Verwaltung der eingesetzten IT-Ressourcen kann so eine verbesserte Überwachung und Kontrolle der eingesetzten Vermögenswerte erfolgen.

**Praxistipp:**

Der geeignete Ausgangspunkt für den sukzessiven Ausbau einer gut organisierten Configuration-Management-Datenbank kann eine Dokumentation aller IT-Assets (Hardware, Software, Lizenzen) sein.

Für den weiteren Verlauf und eine erfolgreiche Einführung ist es von wesentlicher Bedeutung, dass Sie hierbei den richtigen Detaillierungsgrad definieren.

Sie können ein Audit der Ausstattung von Arbeitsplatz-PCs durch Hardware-/Software-Inventarisierungs-Werkzeuge unterstützen. Das Ergebnis, das diese Werkzeuge ermitteln, sollten Sie mit dem erwarteten Bestand laut CMDB abgleichen.

4.3.1.5 Change Management

Dem Leitgedanken folgend, dass IT-Services der Unterstützung der Geschäftsprozesse dienen, erfordert die Veränderung der Geschäftsabläufe auch eine Spiegelung im IT-Service-Management. Somit sind Änderungen ein normaler Bestandteil des Betriebs und der IT-Services, bergen aber wiederum ein potenzielles Risiko für die stabile Serviceerbringung. Angesichts dessen ist eine restriktive Vorgehensweise in diesem Bereich notwendig, um eine kontinuierliche Stabilität der IT-Umgebung, aber auch deren Weiterentwicklung zu gewährleisten. Aufgabe und Ziel des Change Managements ist, die notwendigen Änderungen zu erfassen, zu planen und – mit dem Ziel einer wirtschaftlichen und termingerechten Durchführung von autorisierten Changes – umzusetzen. Hierbei sollen die Auswirkungen des Änderungsprozesses auf den produktiven Betrieb minimiert werden.

**Praxistipp:**

Change Management wird insbesondere dann interessant, wenn Sie sich für eine sehr starke Standardisierung Ihrer IT-Service-Erbringung entscheiden (z. B. durch Einführung einer zentralen Software-Verteilung oder bei Umstellung der Arbeitsplatz-Anwendungen auf Terminal Services).

Nach ITIL wird das Change Management als der Prozess definiert, um von einem definierten Zustand in einen neuen zu gelangen.⁶ Hieraus ergibt sich auch die Abgrenzung zum Störungsbehebungsprozess des Incident Managements und zu den Aktivitäten des Problem Managements. Das Change Management setzt weit vorne im Änderungsprozess eines Configuration Items (CI) an. Es gewährleistet die Abbildung eines Change Requests auf ein oder mehrere CIs und betreut den Änderungsprozess in Zusammenarbeit mit dem Release Management bis zum Rollout. Der Schwerpunkt der Tätigkeit liegt in den planerischen Aufgaben. Test und Durchführung sind eher dem Release Management zuzuordnen. Die Planung eines Release-Wechsels beinhaltet darüber hinaus auch Risikoanalyse und -vorsorge.

Die Aktivitäten des Change Managements erstrecken sich im Einzelnen über:

- Erfassen und Bewerten der Change Requests (Grund für die Änderung, von der Änderung betroffene CIs, Auswirkungen der Nicht-Durchführung, Verweise auf assoziierte Problem Records, Verantwortlichkeiten);
- Impact-Analyse der geplanten Changes (hinsichtlich Kosten, Nutzen und Risiken);
- Autorisierung und Planung von Changes (Begutachtung der Change Requests; ITIL empfiehlt die Schaffung einer Entscheidungsinstanz, den Change Advisory Board);
- Überwachung von Realisierung, Test und Implementierung von Changes;
- Abschluss und Review durchgeführter Changes.

Die Reihenfolge der einzelnen Schritte wird geplant und kommuniziert, um eventuelle Überschneidungen so früh wie möglich zu erkennen. Dabei spielt neben dem Change Manager das Change Advisory Board bei weitreichenden Veränderungen eine wichtige Rolle.

4.3.1.6 Release Management

Die stetig steigenden Abhängigkeiten zwischen verschiedenen Softwareversionen bewirken, dass Änderungen nicht mehr isoliert durchgeführt werden können. Um die Ausfallzeiten und Risiken bei anstehenden Änderungen zu minimieren, werden Änderungsmaßnahmen gebündelt. Nach ITIL bezeichnet der Begriff „Release“ hierbei einen oder mehrere autorisierte Änderungsmaßnahmen an bestehenden IT-Services und kann aus einer Kombination von Hardware, Software, Firmware bzw. Dokumentation bestehen.

Das Ziel des Release Managements ist die Verwaltung von autorisierter Hard- und Software, die Freigabe der jeweiligen Stände sowie deren Verteilung und Inbetriebnahme. Somit ist das Release Management verantwortlich für Planung, Entwurf, Erstellung, Konfiguration und Test von Release-Komponenten, das Zusammenstellen der Komponenten zu Releases sowie die Planung, Vorbereitung und Durchführung der Rollouts.

⁶ Vgl. [OGC00] S. 168

In engem Zusammenwirken mit den Aktivitäten des Change Managements und der Configuration-Management-Prozesse sorgt das Release Management einerseits für eine Dokumentation der erbrachten Änderungen in der CMDB sowie die Verwaltung der ausgebrachten Release-Stände in der Definitive Software Library (Abbildung 4.9).

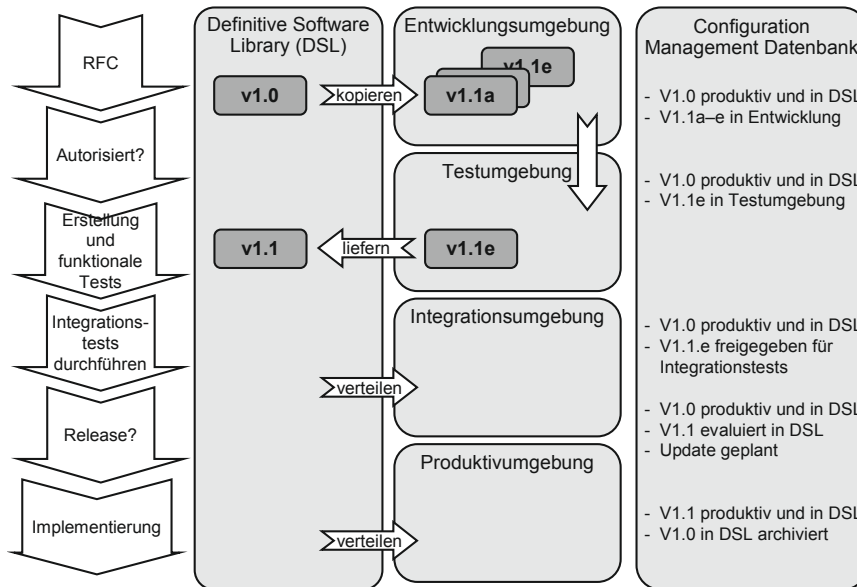


ABBILDUNG 4.9 Zusammenspiel von ITIL-Komponenten im Release Management

Aus der Kombination von Configuration Management, Change Management und Release Management ergeben sich so unterschiedlichste Nutzenpotenziale:

- Durch die gebündelte Änderung von Software- und Hardware-Komponenten über Releases kann die Anzahl der Serviceunterbrechungen minimiert werden.
- Es ist sichergestellt, dass die produktive Hard- und Software von bekannter Qualität ist.
- Bereitstellung konsistenter Software-Stände über alle Systeme hinweg.
- Erkennen falscher Versionen und nicht genehmigter Kopien.

4.3.2 Service-Delivery-Prozesse

Service Delivery nach ITIL [OGC01] ist das Management der für das Unternehmen wertschöpfenden Service-Prozesse. Diese Vorgänge bilden das Fundament für die planvolle Erbringung der IT-Services. Sie subsumieren die Prozesse eines Steuerungs-Regelungskreises der mittel- und langfristigen Service-Planung („Was könnte passieren und was müssten wir dagegen unternehmen?“). Gemeinsam haben alle Service-Delivery-Prozesse, dass sie periodisch anlaufen, das Ergebnis ihrer Arbeit in einem Plan zusammengefasst wird und ihnen die Überwachung des Planes obliegt.

4.3.2.1 Service Level Management

Während das Service Desk die zentrale Anlaufstelle für Kundenanfragen im laufenden Betrieb darstellt und somit die Nutzer eines IT-Services anspricht, richtet sich das Service Level Management als Dienstleister im Sinne einer Kundenbeziehung auf die Kommunikation über einen IT-Service auf Management-Ebene.

Ziel des Service Level Managements ist, die IT-Services auf die tatsächlichen Anforderungen der Geschäftsprozesse des Kunden auszurichten und die Übereinstimmung zwischen der erbrachten und der vereinbarten Leistung dauerhaft sicherzustellen.

Das Service Level Management stellt als Dreh- und Angelpunkt zu den Prozessen des Service Support die am häufigsten eingeführte Prozesskette aus dem Bereich Service Delivery dar. Grundlage einer serviceorientierten Kundenbeziehung bilden die so genannten Service Level Agreements (SLAs). In ihnen werden Art, Umfang, Verantwortlichkeiten und Konditionen der vereinbarten Dienstleistungspakete für beide Seiten bindend beschrieben.

Nach ITIL werden die Absprachen mit dem Kunden intern mit operativen Zusicherungen zur Erbringung der geforderten Kundenleistung hinterlegt. Diese so genannten Operational Level Agreements (OLAs) sorgen dafür, dass die vereinbarten Leistungsparameter auch von den internen Supporteinheiten erbracht werden können. Der Zukauf von externen Leistungen wird nach ITIL in Underpinning Contracts (UC) geregelt.

Aus dem Ziel der Definition, der vertraglichen Vereinbarung, der Steuerung und der Qualitätssicherung von Dienstleistungen zwischen Dienstleistungsanbietern und Kunden ergeben sich die in Abbildung 4.10 dargestellten Aufgaben.

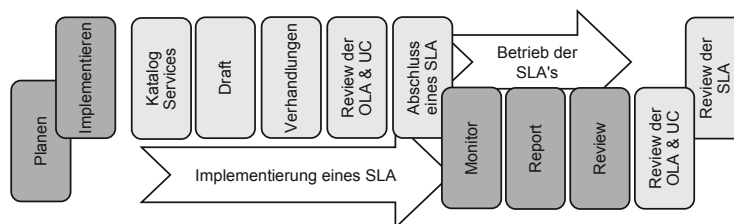


ABBILDUNG 4.10 Aktivitäten des Service Level Managements

Wesentlicher Nutzen des Service Level Managements stellt hier, neben der klareren Vorstellung der wechselseitigen Anforderungen und Verantwortlichkeiten, der zielgerichtete Einsatz von IT-Ressourcen zur Unterstützung der wertschöpfenden Prozesse der Fachabteilungen dar. Über klare Dienstleistungsvereinbarungen steht sowohl der IT-Organisation als auch dem nachfragenden Kunden eine bessere Planungsgrundlage zur Verfügung.



Praxistipp:

Beginnen Sie zunächst mit einer kleinen Anzahl von Service Level Agreements (SLA). Hier ist die Etablierung der neuen Art der Kundenkommunikation wichtiger als die vollständige Abdeckung des gesamten Leistungsspektrums.

Achten Sie zudem schon frühzeitig darauf, dass Sie die Leistungen des Service-Kataloges modular gestalten. So fällt es Ihnen später leichter, auf Varianten-Anforderungen einzugehen.

4.3.2.2 Availability Management

Mit der zunehmenden Abhängigkeit der wertschöpfenden Geschäftsprozesse von IT-Dienstleistungen einerseits, aber auch der größer werdenden Komplexität der IT-Systeme andererseits schlagen Service-Ausfälle immer deutlicher „spürbar“ auf die täglichen Arbeitsabläufe der Fachabteilungen durch. Der Ausfall des Produktionsfaktors „Information“ führt häufig bis zur Unterbrechung des eigentlichen Produktionsablaufes.

Das Ziel des Availability Managements ist deshalb, für die zugesicherte Verfügbarkeit der angebotenen IT-Services für den Kunden, entsprechend den vereinbarten Kriterien eines SLA, zu sorgen. Damit sollen die IT-Services des Kunden immer dann sicher zur Verfügung stehen, wenn sie im Rahmen der Geschäftstätigkeit benötigt werden, sodass aus der IT-Infrastruktur und den Dienstleistungen ein maximaler Nutzen gezogen werden kann.

Für den Benutzer ist lediglich die Verfügbarkeit eines IT-Services wahrnehmbar. Für die IT-Organisation drückt sich dies in Zuverlässigkeit und Wartbarkeit der Dienste bzw. in der Servicefähigkeit der externen Partner aus.

Dabei wird mit *Zuverlässigkeit* die Fähigkeit eines IT-Services definiert, eine erforderliche Funktion unter festgelegten Bedingungen über einen festgelegten Zeitraum fehlerfrei auszuführen. Mit *Wartbarkeit* wird hier die Fähigkeit eines IT-Services verstanden, in einem definierten Arbeitszustand gehalten oder in diesen Zustand zurückversetzt zu werden. Die *Servicefähigkeit* beschreibt die vertraglichen Bedingungen, zu denen externe Lieferanten Teile der IT-Infrastruktur oder auch IT-Services liefern.

Die Verfügbarkeit kann damit anhand von Zeiträumen zwischen zwei Ereignissen dargestellt werden. So ergibt sich:

- *Mean Time between System Incidents*, der mittlere Abstand zwischen zwei Störungen als Maß für die Zuverlässigkeit;
- *Mean Time to Repair*, die durchschnittliche Reparaturdauer als Maß der Wartbarkeit;
- *Mean Time between Failure*, die mittlere Zeit zwischen zwei Ausfällen als Maß für die Verfügbarkeit.

Availability Management bedeutet demnach die systematische Durchführung aller präventiven und korrigierenden Maßnahmen an den betreuten IT-Services.



Praxistipp:

Ziel des Availability Managements ist nicht die Erreichung von Hochverfügbarkeit in allen Segmenten; vielmehr geht es darum, ein sinnvolles Verhältnis von Aufwand und Kosten der vorgehaltenen Maßnahmen zu den Kosten der Nicht-Verfügbarkeit von IT-Services herzustellen. Wesentliche Kriterien sind hierbei u. a. ungenutzte Nutzer-Produktivität, entgangene Einnahmen, aber auch nicht genutzte Überkapazität bei Administrationspersonal, nicht ausgelastete Hardware oder Unzufriedenheit von Geschäftskunden.

Capacity Management

Sorgt das Availability Management für die Verfügbarkeit, so beschäftigt sich das Capacity Management (Kapazitätsmanagement) mit der Bereitstellung und Steuerung der angemessenen Menge an „informationsverarbeitenden“ Ressourcen und des bestmöglichen Einsatzes dieser Kapazität.

Das Capacity Management erfüllt hier zwei wesentliche Aufgaben. Einerseits muss es den Ausgleich zwischen angebotener und nachgefragter Kapazität herstellen und langfristig aufrechterhalten. Auf der anderen Seite müssen die Forderungen nach zusätzlichen Kapazitäten auch gegen den tatsächlichen Geschäftsnutzen und die entstehenden Kosten abgewogen werden. Die Nachfrage nach IT-Ressourcen basiert auf der Vereinbarung von IT-Service Levels mit den Kunden.

Die Bedürfnisse der Kunden werden anhand von Prognosen zum wahrscheinlichen Wachstum der Nachfrage nach aktuellen Serviceleistungen und anhand der Kalibrierung neuer Service-Elemente beurteilt. Die mit dem Capacity Management verbundenen Unterprozesse beziehen sich auf Prognosen zu den Arbeitsumfängen, zur Kalibrierung von Anwendungen und auf die Führung eines Kapazitätsplans, um bestehende und zukünftige Anforderungen erfüllen zu können.

Das Capacity Management wird bei ITIL generell in drei Bereiche untergliedert:

- Business Capacity Management (Bedarfsmanagement): Es hat die Aufgabe, die zukünftige Entwicklung der Geschäftsanforderungen an IT-Services zu analysieren, etwaige Trends zu erkennen und die vorausschauende Kapazitätsentwicklung zu skizzieren.
- Service Capacity Management (Auslastungsmanagement): Dimensionierung der Ressourcen, sodass, gemäß den vereinbarten Leistungsparametern für die aktuell aktiven IT-Services, die notwendige Ausführungskapazität zur Verfügung steht.
- Ressourcen Capacity Management

Die Feingliederung und gegenseitige Abhängigkeit dieser drei Bereiche sind in Abbildung 4.11 dargestellt.

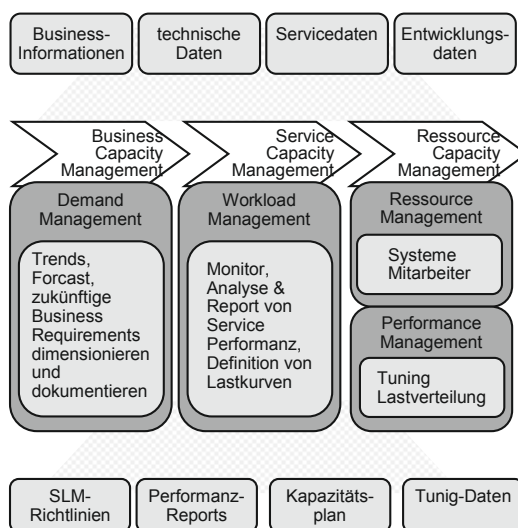


ABBILDUNG 4.11

Prozessfluss des Capacity Managements

Die Resultate der Aktivitäten münden in den Kapazitätsplan, der neben der jeweils für Services und Ressourcen gemessenen Ist-Auslastung und der geplanten Soll-Auslastung auch die Grundlage für einen weiteren Forecast und die Budgetplanung enthält.

Das Capacity Management ermöglicht die wirtschaftliche Ressourcennutzung. Darüber hinaus stehen neben der Sicherstellung von Performance und Durchsatz die Absicherung gegenüber „bösen Überraschungen“ durch Engpässe mittels einer vorausschauenden Planung (z. B. die Berücksichtigung der saisonal bedingten vermehrten Nutzung von Reporting-Services am Jahresende) im Vordergrund.



Praxistipp:

Auf allen Ebenen gilt, dass ein sauber geführtes, proaktives Kapazitätsmanagement hilft, „teure“ Reaktionen auf nicht erwartete Ereignisse zu reduzieren.

Financial Management

Der wachsende Kostendruck und die Suche nach Einsparpotenzialen richten sich auch auf die IT-Organisationen der Unternehmen. Hier finden sich häufig große Kostenblöcke und nicht weiter aufgeschlüsselte Leistungen, die von der IT erbracht werden (z. B. Hardware-Beschaffung und -Betreuung). Zudem verlangt die Unternehmensführung immer häufiger den Nachweis der Mehrwerte der IT für das Unternehmen (Kosten/Nutzen-Verhältnis).

Das Financial Management stellt Informationen zur betriebswirtschaftlichen Planung und Steuerung der IT-Organisation zur Verfügung.

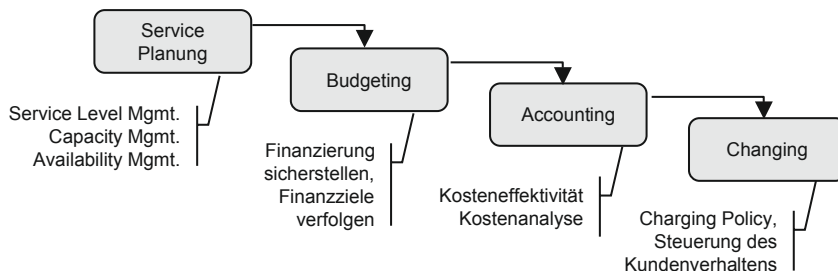


ABBILDUNG 4.12 Regelkreis des Financial Management

Entlang des in Abbildung 4.12 dargestellten Regelkreises nach ITIL gliedern sich die Aufgaben des Financial Managements in folgende Bereiche: die *Budgetierung* (IT-Budgetplanung), die gewährleistet, dass der IT für den Betrieb der geforderten IT-Services ein entsprechendes Äquivalent an Finanzen zur Verfügung steht. Mit dem *Accounting* (IT-Kostenrechnung) wird sichergestellt, dass die tatsächlichen Kosten für die angebotenen Dienstleistungen ermittelt werden. Um die Informationen über die tatsächlichen Kosten zu erlangen, ist eine enge Anbindung an das Capacity Management, das Configuration Management und das Service Level Management erforderlich. Das *Charging* (IT-Leistungsverrechnung) stellt das Einkommen der Organisationseinheit sicher, die den IT-Service leistet. Es ermöglicht die Erstellung einer Verrechnungsgrundlage für jede Leistung.

**Praxistipp:**

Über eine geeignete Preisgestaltung und durch die Schaffung eines Kostenbewusstseins können Sie auch im Financial Management das Benutzer- und Kundenverhalten beeinflussen.

Für eine eingehende Betrachtung der Aspekte der Kosten- und Leistungsverrechnung sei hier noch auf Abschnitt 4.5 verwiesen. Darüber hinaus bietet sich hier auch der Übergang zu Kapitel 7 dieses Buches an, das sich mit dem IT-Controlling beschäftigt.

4.3.3 Neue ITIL 3-Prozesse

Mit ITIL 3 sind neue Prozesse dazugekommen, die im Folgenden näher betrachtet werden.

4.3.3.1 Service Strategy

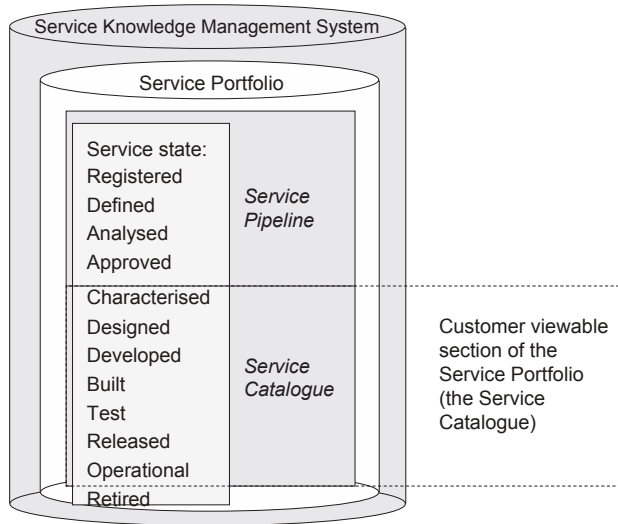
Service Strategy betrachtet das IT-Servicemanagement aus dem konzeptuellen und strategischen Blickwinkel und umfasst Definition, Spezifikation, Logistik und finanzielle Aspekte aus der Geschäftsperspektive. Die wesentlichen Aktivitäten zielen auf:

- *Die Definition und Abgrenzung des Marktes:* Hier wird das Verständnis über Bedürfnisse, Anforderungen und Opportunities des Kunden entwickelt.
- *Die Formulierung von Angeboten:* In ITIL 3 rückt immer mehr der Wertbeitrag für die wertschöpfenden Prozesse des Kunden in den Vordergrund der Betrachtungen. Dies umfasst den kompletten Lebenszyklus von zukünftigen (in der Service Pipeline) über aktuell angebotenen (im Servicekatalog) bis hin zu „außer Dienst gestellten“ Services.
- *Die Vorbereitung der Umsetzung und Ausführung:* Zur Absicherung der Weiterentwicklung gehört auch die Analyse der internen und externen Einflussfaktoren auf einen neuen Service (kritische Erfolgsfaktoren).

Innerhalb der Service Strategy ist der neue Prozess „Service Portfolio Management“ wesentlich sowie der schon aus Version 2 bekannten Prozess Finance Management, bei dem vor allem im Bereich Investitionsrechtfertigung Neuerungen zu finden sind.

Service Portfolio Management

Das Service Portfolio (vgl. Abbildung 4.13) stellt die vorhandenen Services unter wirtschaftlichen Aspekten dar. Dabei sind verschiedene Fragen von Bedeutung, z. B. warum ein Kunde die Services abnimmt, oder die Frage nach Stärken und Schwächen [OSS07 S.119]. Die Prozesse zur Erstellung und Verwaltung von IT-Services sind Bestandteil des IT-Servicemanagements. Die Verwaltung, Überwachung und das Berichtswesen von Business Services erfolgt im Rahmen des Business-Servicemanagements. Vervollständigt wird ITIL 3 noch durch das IT-Systemmanagement, das die Bereiche technische Ressourcen, Infrastruktur und Anwendungen im Einzelnen betrachtet und umfasst. Im Rahmen des Service Strategy Prozesses – Definieren, Analysieren, Genehmigen und Freigeben – wird für die Entscheidung, ob und wie eine Investition durchgeführt wird, das Option Space Tool eingesetzt. Es stellt ein Werkzeug zur Unterstützung der Entscheidungsfindung dar [OSS07 S.125ff.].

**ABBILDUNG 4.13**

Service Portfolio
(nach [OSS07 S72 ff])

Demand Management

Im Anforderungsmanagement gilt es, die Kundenanforderungen frühzeitig zu identifizieren und ein Kundenprofil zu ermitteln. Ziel ist die bestmögliche Abstimmung hinsichtlich Serviceart und Volumen mit den vorhandenen Kapazitäten. Der Prozess ist als kritisch anzusehen. Einerseits können fehlende Kapazitäten zu unzufriedenen Kunden führen. Andererseits verursachen ungenutzte Kapazitäten entsprechende Kosten. Für den Kundeneinsatz werden die Services in Bundle entsprechend zusammengestellt [OSS 07 S.134f.]. Jeder Service im Servicekatalog besteht aus einer Anzahl von Servicebeschreibungen, die zusammengefasst wurden und jeweils für eine spezifische Ergebnisausprägung stehen. Für den Service müssen nun für jede Beschreibung, bezogen auf den Kunden (z. B. Wie viel Flexibilität wird benötigt?), spezifische Service Level Packages ausgewählt werden, um das beste Ergebnis zu erzielen [OSS 07 S.135ff.].

Return on Investment

Im Bereich Financial Management wurden die ROI-Betrachtungen explizit als neuer Punkt aufgenommen [OSS07 S.112]. Dahinter verbirgt sich ein Konzept zur Quantifizierung von Investitionen. Servicemanagement bringt nicht von sich aus die taktischen Vorteile, für die das Management üblicherweise ein Budget bereitstellt. Eine der größten Herausforderungen ist, bei der Suche nach einem Budget für ITIL-Projekte eine spezifische Geschäftsnotwendigkeit zu identifizieren, die von IT-Servicemanagement abhängig ist. Eine weitere Betrachtung von ROI befindet sich im Bereich Continuous Service Improvement.

4.3.3.2 Service Design

Das Service Design (Abbildung 4.14) übersetzt die strategischen Vorgaben und Pläne in tatsächliche IT-Services und deren Strukturierung in Angebotsportfolios.

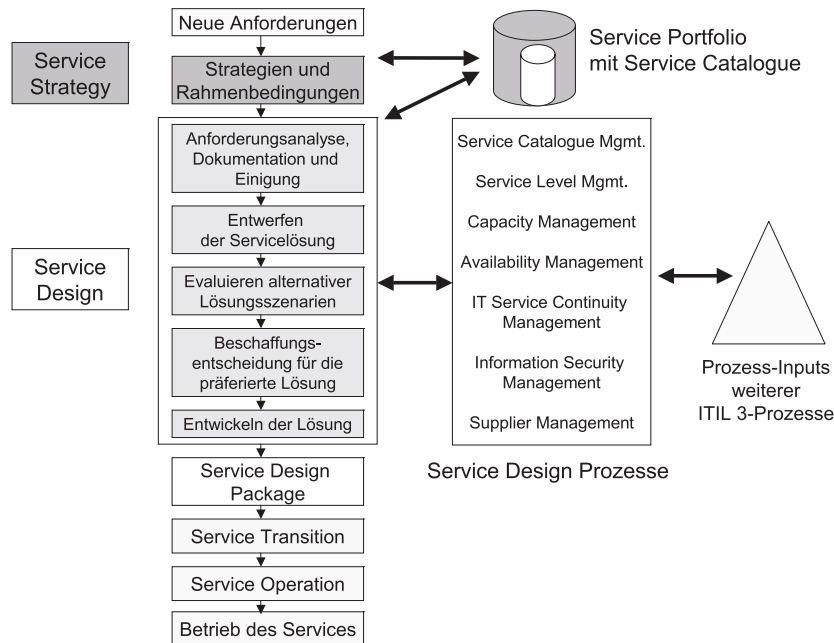


ABBILDUNG 4.14 Service Design angelehnt an [OSD07 S. 60]

Dieser ganzheitliche Ansatz entwickelt den IT-Service-Blueprint in fünf Dimensionen:

- *Design des neuen IT-Services:* Dies umfasst, neben der Abbildung der funktionalen Anforderungen, auch die Dimensionierung aller notwendigen Ressourcen.
- *Design des Service-Portfolios:* Positionierung und Dimensionierung des Services in der bestehenden Landschaft der angebotenen IT-Services.
- *Technisches Design des Services:* Hierunter fallen vor allem Fragen nach der problemadäquaten Technologie und dem Managementinstrumentarium zum Service-Betrieb.
- *Prozessdesign:* Dies beinhaltet den Entwurf aller Prozesse, die notwendig sind, um den geplanten IT-Service zu entwickeln, in Betrieb zu nehmen und operativ zu halten.
- *Design der Service-Überwachung:* Bereits beim Design eines neuen Services ist die Entwicklung von Messmethoden entlang der geforderten Messgrößen notwendig.

In Ergänzung zu den bekannten Prozessen aus Version 2 finden sich im Bereich Service Design vor allem die beiden Prozesse „Service Catalogue Management“ und „Supplier Management“.

Service Catalogue Management

Der Servicekatalog umfasst alle Informationen über die vorhandenen Services. Das Service Catalogue Management umfasst die Erstellung von Servicedefinitionen, die Erstellung und

Pflege des Katalogs und das Management von diversen Schnittstellen und Beziehungen zu anderen Prozessen [OSD 07 S. 60f.]. Der Katalog lässt sich von zwei Seiten betrachten, als Business-Service-Katalog und als Technical-Service-Katalog. Ersterer umfasst die Beziehungen der Services zu den Geschäftsprozessen (Kundensicht) [OGC, SD 07 S. 62]. Der zweite Bereich beinhaltet die detaillierten IT-Services und die Beziehungen zu den unterstützenden Services, der Infrastruktur und den Anwendungen [OGC, SD 07 S. 62].

Supplier Management

Das Lieferantenmanagement hat zum Ziel, die Lieferanten und ihre Services so zu verwalten, dass die angestrebte Qualität durchgängig erzielt und damit sichergestellt wird, dass ein entsprechender Gegenwert für die Bezahlung geleistet wird [OSD07 S. 149]. Es ist notwendig, dass dieser Prozess in alle Phasen des Service-Lebenszyklus eingebunden ist [OSD07 S. 149]. Der Prozess beinhaltet auch das Vertragsmanagement, und es wird eine Lieferanten- und Vertragsmanagement-Datenbank (SCD) geführt [OSD07 S. 150f.].

4.3.3.3 Service Transition

Mit Service Transition wird sichergestellt, dass die im Service Design umgesetzte Strategie auch mit der Überführung in den operativen Betrieb die Anforderungen erfüllt und zudem effizient zu betreiben und zu warten ist. Dieses Modul der neuen ITIL-Version erweitert den bekannten Bereich des Change und Release Management um weitere Aspekte:

- Überführung des geplanten Services entsprechend den Anforderungen und Maßgaben.
- Kunden und Geschäftsprozesse in die Lage versetzen, die Potentiale für eine Optimierung im Prozess durch die Einführung des neuen Service-Release auch auszunutzen.

Die maßgeblichen Erfolgsfaktoren liegen für den Bereich der Service Transition in diesen Bereichen:

- *Umsetzungsplanung*: Sie stellt sicher, dass neue Services zu den vorgegebenen Kosten, in der geplanten Qualität und zu den gesetzten Fristen produktiv gesetzt werden können.
- *Auswirkungsminimierung*: Die Überführung eines Services in den Betrieb sollte möglichst geringe Seiteneffekte erzeugen.
- *Zufriedenheitssteigerung*: Zielgruppen für eine verbesserte Zufriedenheit sollten – neben Benutzern als Hauptadressaten – auch Betreiber des Services und des Supports sein.

Transition Planning and Support

Transition Planning and Support soll sicherstellen, dass einerseits die Anforderungen, die in der Service Strategy definiert und in Service Design designiert wurden, in Service Operations effektiv umgesetzt werden, und andererseits eine Risiko- oder Problemidentifikation, eine Behandlung des Risikos oder Problems und dessen Kontrolle erfolgt [OST07 S. 35].

Service Validation and Testing

Das Ziel dieses Prozesses ist die Sicherstellung des Kundennutzens durch einen getesteten und validierten Prozess [OST07 S. 115]. Im Rahmen des Prozesses, der früher ebenfalls ein Teil des Release Managements war, werden die Teststrategie, die Testmodelle, die Testperspektiven und die zu verwendenden Techniken detailliert festgelegt.

Service Operation

Service Operation deckt alle Aspekte ab, die zur Verwaltung eines Services während der aktiven Phase seines Lebenszyklus notwendig sind. Vordringliche Ziele sind dabei:

- Der Betrieb der Services in einem stabilen und reaktiven Zustand
- Erfüllung der vereinbarten Service Levels (auch ggf. Vermeidung von Übererfüllung)
- Stabile Ende-zu-Ende Produktionsprozesse
- Reduktion der Incident- und Problem-Fälle für die Services

Hierzu setzt Service Operations auf Regelkreisen auf (Abbildung 4.15).

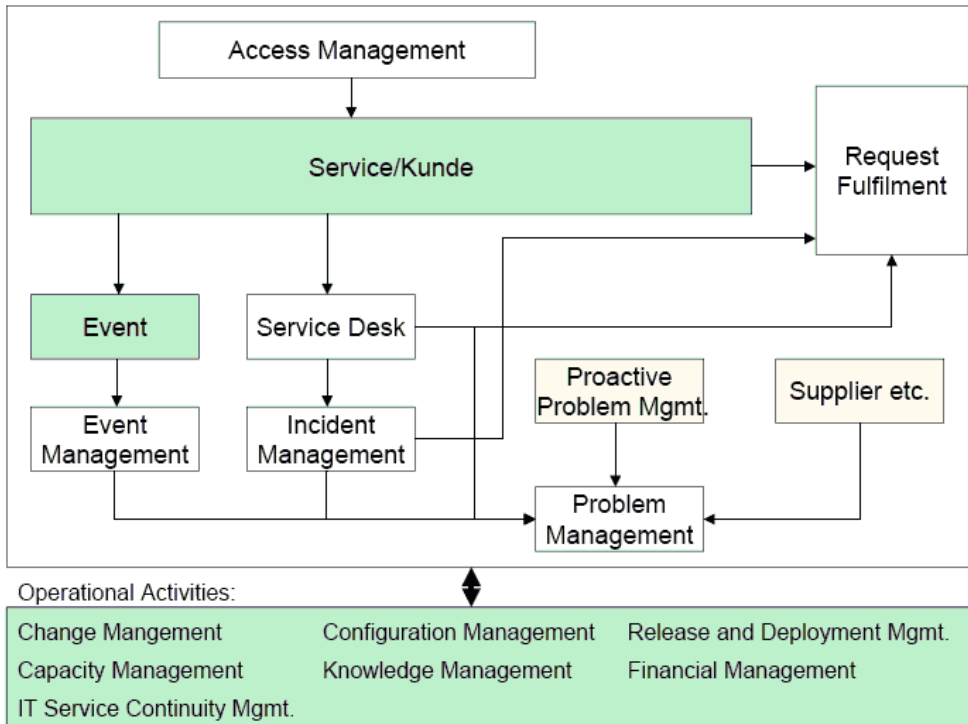


ABBILDUNG 4.15 Service Operation nach [OS007 S. 33ff.]

Im Zusammenspiel mit den anderen Bereichen ergibt sich somit ein komplexes Steuerungs- und Regelsystem, bei dem zur Aufrechterhaltung eines stabilen Betriebes Eskalationen und Reaktionen auf unterschiedlichen Ebenen möglich sind:

- Korrigierender Eingriff in die Aktivität als solche,
- Anpassung der Anforderungen über das Continual Service Improvement,
- Anpassung des Services über einen Änderungsauftrag an das Service Design,
- Anpassung der strategischen Anforderungen bis hin zur Außerbetriebnahme.

Event Management

Ein Event ist ein entdeckbares oder erkennbares Ereignis, das Bedeutung für die IT-Infrastruktur oder die Übergabe von IT-Services besitzt und das die Ursache für die Auslösung einer Evaluation auf Grund einer Abweichung eines Services ist [OSO07 S. 35f.]. Event Management bedeutet, Events und ihren Sinn zu erkennen sowie die geeigneten Prüfkationen zu veranlassen [OSO07 S. 36], und war früher im Incident Management angesiedelt.

Request Fulfilment

Der Prozess Request Fulfilment (RF) beschreibt die Abläufe, die sich auf den Umgang mit Servicenachfragen beziehen, also der Organisation des Nachfrageprozesses [OSO07 S. 56]. Service Request ist eine generische Beschreibung für viele verschiedene Nachfragetypen, die von Benutzern an die IT-Abteilung gestellt werden [OSO07 S. 55]. Der Prozess war bei ITIL 2 Teil des Incident Managements.

Access Management

Das Access Management stellt die Berechtigungen für die Nutzung von Services bereit [OSO07 S. 68]. Geregelt werden Nachfrage nach dem Zugang, Verifizierung, Bereitstellung der Berechtigungen, Überwachung der Identität, Aufzeichnen des Zutritts, Zutrittshistorie und die Entfernung oder Einschränkung der Benutzerrechte [OSO07 S. 68 ff.].

Continual Service Improvement

Mit der Version 3 von ITIL liegt ein kontinuierlicher Verbesserungsprozess vor, der direkt im ITIL-Standard verwurzelt ist und eine zentrale Stelle innerhalb des neuen Standards einnimmt. Begleitet wird er von zwei generischen Prozessen, die der Messung und dem Reporting für die unterschiedlichsten ITIL-Prozesse dienen sowie dem Service Level Management. Die wesentlichen Aufgaben sind demnach:

- die kontinuierliche Ausrichtung des IT-Service-Portfolios an den aktuellen und zukünftigen Bedürfnissen des Unternehmens.
- Reife der unterliegenden IT-Prozesse für Services im Rahmen eines Lebenszyklus.
- Planung der kontinuierlichen Verbesserung.
- Interpretation von Anpassungsanzeichen und Initiieren von Änderungsaktionen

7-Stufen-Verbesserungsprozess

Der Prozess beschreibt anhand von sieben Schritten, wie Verbesserungspotenziale identifiziert und konkrete Schritte zur Verbesserung vorgenommen werden können [OCS 07 S. 43 ff.]. Die ersten beiden Schritte, die Definition, was gemessen werden sollte, und die Definition, was gemessen werden kann, sind iterative Schritte und stellen die Grundlagen dar, während die restlichen fünf Schritte einen sich wiederholenden Zyklus bilden. Die Schritte im Einzelnen sind [OCS07 S. 31 ff.]:

1. *Messbedarf ermitteln:* Wünschenswerte Kenngrößen aus Nachfragersicht.
2. *Messoptionen feststellen:* Kenngrößen kritisch auf ihre Erhebbarkeit prüfen.
3. *Messdaten erheben:* Erhebung der Leistungsdaten, weitestgehend automatisiert.
4. *Messdaten verarbeiten:* Erhobene Daten in Zielformat konvertieren und aggregieren.

5. *Kennzahlen analysieren*: Abhängigkeitsanalysen, Trends und Zielerreichungen.
6. *Informationen darstellen und verwenden*: Aufdecken von Optimierungspotentialen.
7. *Umsetzung der korrigierenden Aktionen*: Maßnahmen ableiten und priorisieren.

Die ersten beiden Schritte des Prozesses werden häufig ignoriert. Es werden Daten erhoben, ohne sich zu überlegen, was sinnvoll erhoben werden sollte. Häufig werden auch Kundenwünsche nicht berücksichtigt, da man glaubt diese genau zu kennen [OGC, CSI 07 S. 43].

■ 4.4 Fahrplan zu einem optimalen IT-Servicemanagement

Planung und Kommunikation – zwei Pfeiler zum Erfolg

Nachdem in den vorhergehenden Abschnitten die Konzepte zum IT-Servicemanagement beschrieben wurden, geht es nun um die Einführung. Zwei Fragen stehen im Mittelpunkt: Welche Faktoren beeinflussen die Einführung, und wie sollte sie erfolgen? Abgerundet wird das Kapitel durch praktische Beispiele.

Die Anwendung von IT-Servicemanagement in einem Unternehmen führt einerseits in der Regel zu einer organisatorischen und zu einer Verhaltensänderung des IT-Bereichs und andererseits zu einer anderen Wahrnehmung und Verbindlichkeit bei den Fachabteilungen.

Im IT-Bereich müssen Zuordnungen entsprechend dem gewählten Konzept verändert und neu aufgebaut werden. D. h. die Struktur des Bereichs verändert sich, um auch die einzuführenden *Servicemanagementprozesse* entsprechend den aufgestellten *Service-Level-Agreements* bearbeiten zu können. Außerdem wird das Verständnis des IT-Bereichs, ein interner Dienstleister zu sein und auch als dieser aufzutreten, gestärkt. Dienstleistungen werden transparent, nachvollziehbar und besser planbar.

Auch bei den Fachabteilungen ergibt sich eine veränderte Sichtweise. Indem sich die Leistungen der IT-Abteilung einschätzen zu bestimmten Zeitpunkten einfordern lassen, können die Fachabteilungen leichter planen. Der Dienstleistungscharakter der IT-Abteilung wird spürbarer und die Einstellung zur IT verändert sich damit in der Regel.

Wie schnell sich Änderungen ergeben, das Neue angenommen wird und welche positiven oder negativen Auswirkungen IT-Servicemanagement hat, hängt von der Art der Einführung ab, die durch verschiedene Faktoren beeinflussbar ist.

4.4.1 Kritische Erfolgsfaktoren für die Einführung

Bevor wir die *kritischen Erfolgsfaktoren* (KEF) für die Einführung von IT-Services und IT-Servicemanagement darstellen, wollen wir den Begriff KEF folgendermaßen definieren: „Als kritische Erfolgsfaktoren bezeichnet man dabei im Allgemeinen solche Erfolgsfaktoren, die zwingend oder ganz dringend erfüllt sein müssen, um die gesetzten Unternehmensziele (die damit vor Bestimmung der Erfolgsfaktoren festgelegt sein müssen) erreichen zu können.“ [Roc82 S. 4]

Im Rahmen der Einführung von IT-Services und IT-Service-Management ergeben sich die in Abbildung 4.16 dargestellten kritischen Erfolgsfaktoren, die wir in den folgenden Abschnitten näher beschreiben.

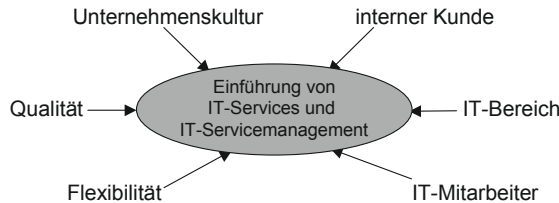


ABBILDUNG 4.16

Kritische Erfolgsfaktoren für die Einführung von IT-Service-Management und -Services

Jeder kritische Erfolgsfaktor muss bei der Einführung entsprechend berücksichtigt werden. Ob eine Einführung nun positiv oder negativ endet, hängt ganz wesentlich von der Beachtung der Randbedingungen und einer guten Planung ab. Eine wichtige Rolle spielt auch der Faktor Zeit. Eine Einführung unter Zeitdruck führt automatisch dazu, dass die Sorgfalt im Bereich der anderen Faktoren geringer wird und sich damit fast automatisch Probleme einstellen.

Im nächsten Abschnitt soll nun eine Vorgehensweise aufgezeigt werden, wie eine Einführung sinnvollerweise geplant, vorbereitet und durchgeführt werden sollte.

4.4.2 Einführung von IT-Service-Management – eine Vorgehensweise

Bei der Einführung von IT-Service-Management z.B. in Form von ITIL oder MOF sind eine Reihe von Aspekten zu beachten, sowohl was die Einführung als Ganzes als auch die der einzelnen Bereiche betrifft (siehe auch [Els05 S. 192]).

Um ein Service-Management in seiner Gesamtheit zu installieren, ist zuerst der *Leistungsumfang* des IT-Bereichs festzulegen. Danach sind die *Services* im Kundenumfeld zu verhandeln, anschließend die benötigten *Supportprozesse* einzuführen und abschließend die *Controlling-Mechanismen* einzurichten [ViG05 S. 91 ff.]. Die Controlling-Mechanismen und die Verrechnung der Services sind Thema von Abschnitt 4.5.

Eine Einführung einzelner IT-Services und die damit verbundenen Aktivitäten, wie das Aushandeln von *Service-Level-Agreements*, werden im Folgenden nicht näher beschrieben; hier geht es allein um die grundsätzliche Vorgehensweise bei der Einführung von IT-Service-Management.

Bei der Einführung eines IT-Service-Managements stehen neben den neu entstehenden Prozessen vor allem notwendige Änderungen bestehender Organisations- und Prozessstrukturen im Mittelpunkt.

Dies führt wie bei jedem Prozessmanagementprojekt (vgl. [SpW08]) zur Einführung von prozessspezifischen Rollen wie die des *Process Owners*, des *Process Managers* und die des *Service Managers*. Der Service Manager stellt dabei den Gesamtverantwortlichen für das IT-Service-Management dar. Der Process Owner trägt die Ergebnisverantwortung für den Prozess und damit für dessen Zweckmäßigkeit. Der Process Manager ist für das operative Management (Planung, Koordination, Monitoring und Berichterstattung) des entsprechenden Prozesses oder Teilprozesses zuständig (vgl. [BVG07, S. 26 und S. 230f.] und [BVG08, S. 155ff.]).

**Praxistipp:**

Die Besetzung der einzelnen Positionen ist für den stetigen Erfolg, vor allem im Sinne von ITIL 3, von großer Bedeutung. Als Service Manager ist ein erfahrener Manager auszuwählen, der Kunden- und Prozess-affin ist. Außerdem sollte er in der Lage sein, die strategische und taktische Ausrichtung des IT-Servicemanagements zu bestimmen. Bei ihm sind vor allem Weitsicht, Durchsetzungs- und Kommunikationsfähigkeit gefragt. Der Process Owner benötigt Prozess Erfahrung und sollte ein anerkannter Mitarbeiter ohne Konfliktpotenzial darstellen. Der Prozess Manager sollte seinen (Teil-)Prozess kennen und mit den Beteiligten umgehen können. Für die letzten beiden beschriebenen Positionen sollten keine Unternehmensneulinge eingesetzt werden. Mindestens zwei Jahre Betriebszugehörigkeit sind anzuraten.

Am besten sollte das Einführungsprojekt mit einem Change-Management-Projekt verbunden werden. Wie bei jedem Change-Management-Projekt im Bereich der Aufbau- und Ablauforganisation sind zunächst die Ziele genau zu definieren und andererseits die Ist-Situation aufzunehmen, um das Ergebnis mit der Ausgangssituation vergleichen zu können.

Um die Ziele definieren zu können, müssen die Fragen nach dem „Was“, dem „Wer“, dem „Wie“ und dem „Wann“ beantwortet werden.

4.4.2.1 Komplett- oder Teileinführung

Bei der Frage nach dem „Was“ geht es um die Überlegung, ob es eine Komplett-einführung oder Teileinführung (Einführung eines einzelnen Prozesses oder ausgewählter Prozesse) geben soll, bezogen auf das gesamte Unternehmen oder einzelne Organisationseinheiten. Bei jeder Art der Einführung sind Spezifika zu beachten [EgH04 S. 16].

Die Teileinführung bedingt die Auswahl einzelner Prozesse oder eines einzelnen Prozesses, sie kann nach den gleichen Kriterien, wie die Auswahl der Reihenfolge bei einer Komplett-einführung erfolgt, durchgeführt werden. Eine Komplett-einführung bedeutet, dass alle Prozesse zu einem bestimmten Zeitpunkt oder innerhalb eines definierten nicht zu langen Zeitraums eingeführt werden. Sie kann für das ganze Unternehmen oder nur bezogen auf eine Organisationseinheit erfolgen. In jedem Fall muss ein Gesamtkonzept geschaffen werden, das die kompletten Prozesse von z.B. ITIL 3 umfasst. Darin ist die Reihenfolge der Einführung der einzelnen Bereiche und Prozesse festzulegen [Som04 S. 42].

Für die Entscheidung über die Reihenfolge der Einführung sind die nachfolgenden Punkte zu beachten:

- **IT-Strategie aus Sicht des IT-Bereichs.** Sie beinhaltet die (organisatorische und technische) Ausrichtung der IT für die nächsten Jahre und die Bestimmung der Fachprozesse, die verstärkt unterstützt werden sollen. Stehen diese fest, lässt sich eine Reihenfolge aus IT-Strategie-Sicht festlegen.
- **Schwachpunkte.** Bestehende Schwachpunkte im Unternehmen, wie z.B. Kommunikationsprobleme mit Fachabteilungen oder Probleme beim Lizenzmanagement, können mit Hilfe von *IT-Servicemanagement-Prozessen* abgemildert oder ganz ausgemerzt werden. Das Ausmaß der Schwachpunkte lässt sich über ihre Auswirkungen sowie ihre politische Brisanz bestimmen und eine Rangliste erstellen, der dann die einzelnen Prozesse zugeordnet werden können.

- **Qualifikation der IT-Mitarbeiter.** Dieser Aspekt muss auf jeden Fall berücksichtigt werden. Dabei ist zu ermitteln, für welche Prozesse die Qualifikationen vorhanden sind und wofür sie noch fehlen. Für das Erlangen fehlender Qualifikationen stellen Sie einen Zeit- und Kostenplan auf und vergleichen ihn mit den allgemeinen Einführungsplanungen. Arbeiten Sie die GAPs (Lücken bei der Qualifizierung der IT-Mitarbeiter) heraus. Auf dieser Basis lässt sich dann wieder eine Rangliste zur Einführung erstellen.
- **Organisations- und Prozessstrategie der Fachabteilungen.** Dieser Punkt beinhaltet die Schwerpunktsetzung und somit auch die Unterstützungsnotwendigkeit durch die IT aus fachlicher Sicht. Aus ihr lässt sich ebenfalls eine Rangliste generieren.
- **Schnittstellen und Querbeziehungen der Prozesse.** Die Prozesse weisen eine Reihe von Querbeziehungen auf, die erhebliche Auswirkungen auf die Reihenfolge der Einführung haben. Aus diesen Abhängigkeiten ergeben sich auch Hinweise darauf, welche Einführungsreihenfolge positive Aspekte ergibt oder welche Prozesse im Rahmen einer Teileinführung gewählt werden sollten.

Weil die Einführung eines IT-Servicemanagements starke Auswirkungen auf die Prozesse der Fachabteilungen hat, sollten die einzelnen Prozesse nacheinander und auch zeitlich versetzt, bezogen auf die einzelnen Organisationseinheiten, eingeführt werden. Zwischen der Einführung der einzelnen Prozesse ist eine Auswirkungsanalyse durchzuführen, damit Fehlentwicklungen frühzeitig identifiziert und Gegenmaßnahmen rasch ergriffen werden können.

Fällt die Entscheidung für die Einführung eines einzelnen ITIL-Prozesses, so sind neben den grundsätzlichen Dingen, die bei einer Gesamteinführung bereits dargelegt wurden, besonders auch die Spezifika der einzelnen Prozesse zu beachten, die nach der Betrachtung des Einführungsablaufs detailliert dargestellt werden.

4.4.2.2 Projektorganisation und Projektteam

Nachdem die Frage nach Einführungsumfang und -art geklärt ist, ergibt sich die Frage, wer das IT-Servicemanagement einführt. Abbildung 4.17 zeigt, wie Projektorganisation und Projektteam aussehen sollen.

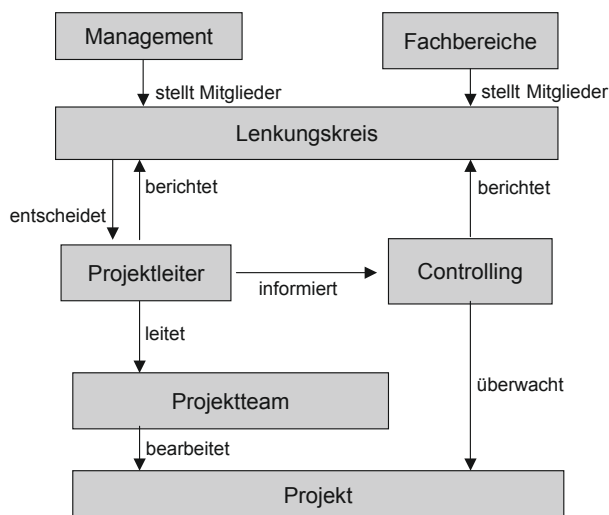


ABBILDUNG 4.17
Projektorganisation

Die Fortschritte des Projekts sollten den vorhandenen Gremien (z. B. Bereichsleitersitzungen) vorgestellt werden, um eine entsprechende Information und Kommunikation sicherzustellen. Bei der Bildung des **Projektteams** ergeben sich spezifische Anforderungen an den Projektleiter. Für diese Position sollten Sie einen Mitarbeiter wählen, der dem Unternehmen schon mehrere Jahre angehört, die internen Abläufe genauestens kennt, ein Standing hat und kein Konfliktpotenzial aufweist. Bei der Besetzung des Projektteams ist auf Ausgewogenheit bezüglich der beteiligten Bereiche zu achten, die alle vertreten sein sollten (vgl. auch [ZiS10 S. 136ff.]). Zur Unterstützung des Projektteams muss ein hochrangiger **Projektmentor** festgelegt werden, der das Projekt sichtbar und offiziell unterstützt und somit zeigt, dass es auf Wunsch der Unternehmensleitung durchgeführt wird.

4.4.2.3 Der Ablauf der Einführung

Der Einführungsablauf umfasst übergreifend betrachtet folgende Punkte:

- Services definieren und verhandeln,
- Planung,
- Sensibilisierung,
- Vorbereitung der Einführung (Analysen, Regelwerk, Umorganisation, Customizing und Projektmarketing),
- Schulung und Qualifikation,
- Testbetrieb,
- Produktivbetrieb.

Im ersten Schritt muss der Leistungsumfang der IT anhand der anzubietenden Services in Absprache mit den internen Kunden definiert werden. Danach müssen die Service Levels und die Verrechnung der Leistungen verhandelt werden. Diese Aktivitäten werden in Abschnitt 4.5 weitergehend betrachtet.

Im Rahmen der Planung werden Pläne bezüglich des Projektmarketings, des Projektablaufs, der organisatorischen Umsetzung, der Prozessanpassung, der Prozessumsetzung, der Qualifikation und Schulung sowie der Erstellung und Umsetzung des Regelwerks erstellt. Die einzelnen Pläne beinhalten die Dimensionen Kapazität, Zeit und Kosten.

In der Phase der Sensibilisierung wird zuerst das Projektteam mit der Vorgehensweise vertraut gemacht und auf sie eingeschworen. In einem zweiten Schritt werden dann die betroffenen Mitarbeiter umfassend informiert und auf ihre neue Aufgabe eingestellt.

Zur Vorbereitung der Einführung werden die bestehende Organisationsstruktur, die Personalstruktur, die bestehenden Prozesse mit der Aufgabenverteilung, die bestehenden Services und die Kultur analysiert. Auch findet eine Analyse der unterstützenden IT-Infrastruktur und der im Prozess anfallenden Daten statt. Die Analysen dienen dazu, die Schwachstellen und die Anforderungen zu identifizieren.

Im Anschluss erarbeitet das Projektteam die neuen Strukturen. Sie unterteilen sich in die Organisationsstruktur (Anpassung der Aufbau- und Ablauforganisation), die Identifikation der gewünschten Prozesse (inklusive der unternehmensspezifischen Anpassung, z. B. eines ITIL-Prozesses) und in die Erarbeitung der Arbeitsanweisungen für das Regelwerk. Bei der Aufstellung der neuen Struktur werden die ermittelten Schwachstellen und die Anforderun-

gen berücksichtigt und Maßnahmen zur Behebung der Schwachstellen und zur Umsetzung der Anforderungen geplant.

Sind die Vorarbeiten abgeschlossen, werden die Mitarbeiter entsprechend der benötigten Qualifikation geschult. Die Schulungen sollten auch die Themengebiete Kommunikation und Kundenbetreuung umfassen.

Im Testbetrieb werden die umgesetzten Prozesse erprobt. Dies bedeutet für die IT-Bereiche eine Umstellung auf die neue Art der Zusammenarbeit mit den Fachabteilungen, d.h. die Verinnerlichung des Dienstleistungsgedankens. Im Falle von Problemen, z. B. bei der Strukturierung des Prozesses, sind diese zu lösen und neu zu testen, bis ein positives Ergebnis erzielt wird. Scheint dies nicht möglich zu sein, sollten die gesetzten Ziele überprüft und evtl. angepasst werden.

An den erfolgreichen Testbetrieb schließt sich der Produktivbetrieb an und nachfolgend die Umsetzung eines neuen Gesamtprozesses als eigenständiges Projekt. Nach der ersten gelungenen Einführung eines Prozesses sinken der Überzeugungsaufwand und der Aufwand für das Projektmarketing.

Parallel zu allen Phasen betrachtet das Projektcontrolling die Abweichungen mittels Abweichungsanalysen und in den späten Phasen die Auswirkungen durch Wirkungsanalysen.

Insbesondere bei ITIL 3 ist es wichtig, dass die Mitarbeiter der Phase Service Operations bereits in die vorhergehenden Phasen Service Design und Service Transition involviert sind, um eine durchgängige, optimale Ausführung der Services sicherstellen zu können (vgl. [Bon+08, S. 141]).

4.4.2.4 Zeitliche Planung

Abschließend ist noch die Frage zu klären, in welchen Zeitabständen die Prozesse eingeführt werden sollten. Dabei ist zu bedenken, dass eine Einführung zu einer Änderung in der Kultur führt. Deshalb muss nach der Einführung der ersten Prozesstranche genügend Zeit vorhanden sein, um sich mit den neuen Gegebenheiten zurechtzufinden. In der Regel ist für die erste Prozesstranche von einem Zeitraum von ca. neun Monaten bis zu 18 Monaten auszugehen, in Abhängigkeit vom Ursprungszustand der IT und der geleisteten Vorarbeiten. Für die weiteren Einführungen können die Zeiträume in der Regel bis auf drei Monate verkürzt werden. Noch kürzere Zeiträume bergen im Hinblick auf die Wirkungsbetrachtung der Einführung größere Risiken und führen leicht zu erhöhter Unruhe im IT-Bereich.

4.4.3 Einführungsaspekte bei ITIL 3

Im Folgenden sind mögliche Vorgehensweisen und Einführungsaspekte dargestellt. Durch die Vielzahl der Prozesse und die hohe Detaillierung stellt ITIL 3 relativ hohe Anforderungen an die Einführung. Deshalb wird in der Literatur empfohlen mit ITIL 2 zu beginnen und im späteren Verlauf Stück für Stück gezielt auf ITIL 3 zu erweitern (vgl. auch [Wis09 S. 65]).

ITIL 2 und ITIL 3 unterscheiden sich in ihrem Aufbau und der wesentlich stärker ausgeprägten Prozessorientierung in ITIL 3. Jedoch sind alle Prozesse von ITIL 2 auch in ITIL 3 enthalten. Sie wurden nur statt auf zwei auf fünf Bereiche zugeordnet und um weitere Prozesse und Methoden ergänzt. Abbildung 4.18 (nächste Seite) zeigt die neue Zuordnung der Prozesse.

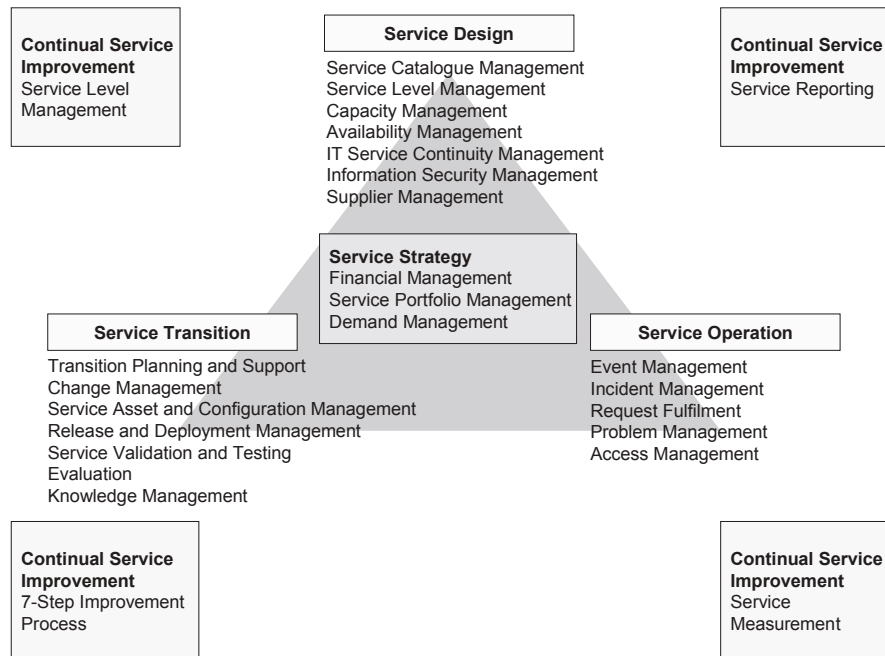


ABBILDUNG 4.18 Prozesse in ITIL 3 [OCS07] [OSD07] [OSO07] [OSS07] [OST07]

Für die Einführung von ITIL 3 gibt es prinzipiell drei unterschiedliche Ausgangslagen:

1. Das Unternehmen besitzt noch keine Services und kein IT-Servicemanagement
2. Services sind vorhanden und ein IT-Servicemanagement soll eingeführt werden
3. Ein IT-Servicemanagement ist vorhanden (dies soll hier am Beispiel von ITIL 2 betrachtet werden)

Erster und zweiter Fall: Im ersten Fall müssen zuerst die Services designt werden, dies wird in den Abschnitten 4.4.2 und 4.5.1 beschrieben. Wenn die Services dann vorhanden sind, ergibt sich eine Vorgehensweise wie beim zweiten Fall.

Der Ausgangspunkt für die Einführung eines komplexen Servicemanagements wie ITIL 3 liegt in der Strategiesicht, in deren Rahmen die Verwaltung und Weiterentwicklung des Kunden-, Service-, und Vertrags-Portfolios erfolgt. Die Planung der Services bezogen auf den Markt und den Kunden steht dabei im Mittelpunkt. Danach folgen die Bereiche Service Design, Service Transitions und Service Operations. Abgeschlossen wird die Einführung durch das Continual Service Improvement [OSD07 S. 161 ff.]. D.h., die Einführung richtet sich nach dem in ITIL Version 3 beschriebenen Lebenszyklus (vgl. [Bon+08, S. 59].

Bei der Ausgestaltung der Service Strategy sind auch die Auswirkungen auf Organisationsstruktur und -kultur zu beachten. Einflüsse ergeben sich durch die Prozesse des IT-Servicemanagements und auch durch Sourcing-Strategien. Dies kann zu Veränderungen beim Organisationsaufbau, bei den einzelnen Rollen und bei der Organisationskultur führen. Dies ist keine Besonderheit von ITIL 3, sollte aber im Rahmen der Konzeption explizit angesprochen werden. [OSS07 S. 139 ff.]

Die meisten Herausforderungen birgt die Einführung der Bereiche Service Design, Service Transitions und Service Operations hinsichtlich der richtigen Prozessreihenfolge.

Hier eine beispielhafte Reihenfolge für ein Einführungsszenario:

Zuerst ist die Strategie des IT-Servicemanagements festzulegen und zu implementieren. Dies geschieht mit dem Bereich Service Strategy und dort mit den Prozessen Service Portfolio Management, Demand Management und Financial Management. Danach folgt der Bereich Service Design mit den Prozessen Service Catalogue Management, Availability Management und vor allem Service Level Management (SLM), die weiteren Prozesse des Bereichs können anschließend sukzessive aufgebaut werden. Parallel dazu sollten im Bereich Service Transition die Prozesse Transition Planning and Support sowie Change Management aufgebaut werden, danach folgen die anderen Prozesse insbesondere Service Asset and Configuration Management sowie Release and Deployment Management.

Im Bereich Service Operations sollte mit dem Event Management begonnen werden, gefolgt von Incident Management, Problem Management, Request Fulfilment und Access Management.

Zum Schluss folgt das Continual Service Improvement, beginnend mit Service Measurement und Service Reporting. Das SLM existiert bereits und es muss nur eingebunden werden. Den Abschluss bilden der Prozess zur Serviceverbesserung und die Verknüpfung mit Financial Management (ROI). CSI kann dabei ebenfalls nach dem Lebenszyklusansatz implementiert werden, weitere Möglichkeiten sind ein auf spezifische Services abgestimmter Ansatz, der den Problemen mit spezifischen Services Rechnung trägt oder ein funktionaler Ansatz, der die Probleme von organisatorischen Funktionen, gekennzeichnet durch die Anhäufung von Incidents, besonders berücksichtigt (vgl. [Bon+08, S. 167]).

Bei der Einführung gilt es, jeden Prozess funktionsfähig zu implementieren. Es müssen jedoch nicht alle Details von Beginn an zur Verfügung stehen. Wichtig sind die Grundabläufe, Methoden und Strukturen. Wichtig ist es auch, die Grundfunktionalitäten über das gesamte Modell einzuführen und dies so zu tun, dass die Ausbauoptionen nicht behindert werden. Der reine Verbesserungsprozess kann auch noch nach der Kerneinführung implementiert werden. Am wichtigsten sind eine funktionierende Strategie und die Schnittstelle zum Kunden.

Mit dem Continual Service Improvement wird ein siebenstufiger Prozess zur Serviceverbesserung eingeführt, wie er Kapitel 4.3.3 dargestellt ist [OCS07 S. 43 ff.].

Das Continual Service Improvement rundet durch seine Ausrichtung auf eine stetige Prozessverbesserung das IT-Servicemanagement nach ITIL 3 ab.

Dritter Fall: Ist ein IT-Servicemanagement wie z. B. ITIL 2 vorhanden, so gilt es zuerst die neue Struktur von ITIL 3 zu verinnerlichen. Dazu werden zuerst die vorhandenen IT-Servicemanagementprozesse den ITIL-3-Bereichen zugeordnet, wie es in Abschnitt 4.3.3 dargestellt wurde.

Es zeigt sich, dass alle ITIL-2-Prozesse den Bereichen von ITIL 3 zugeordnet werden können. Bei ITIL 3 sind neue Prozesse hinzugekommen, die ebenfalls unter 4.3.3 beschrieben wurden.

Für ein bestehendes Servicemanagement auf Basis von ITIL 2 bedeutet dies, dass die vorhandenen Prozesse zugeordnet und um die Neuheiten von ITIL 3 ergänzt werden müssen. Das folgende Einführungsszenario bezieht sich auf ein komplett implementiertes ITIL 2. Bei vorhandenen Teilimplementierungen ändert sich das Einführungsschema individuell.

Das bestehende IT-Servicemanagement ist um die neuen Prozesse und Methoden zu ergänzen, wobei auch hier entsprechend des Lebenszyklus bei dem Bereich Service Strategy begonnen werden sollte. Hier ist sind das Service Portfolio Management und das Demand Manage-

ment zu implementieren, Das Financial Management ist als Prozess bereits vorhanden und muss nur dem Bereich Service Strategy zugeordnet werden.

Danach sind im Bereich Service Design das Service Catalogue Management und das Supplier Management explizit aufzubauen sowie die Prozesse Service Level Management, Capacity Management, Availability Management, IT Service Continuity Management und Information Security Management zuzuordnen.

Im Bereich Service Transition sind die Prozesse Change Management, Service Asset and Configuration Management sowie Release and Deployment Management neu zuzuordnen. Die Prozesse Transition Planning and Support sowie Knowledge Management müssen wie die Prozesse Service Validation and Testing sowie Evaluation, die früher dem Release Management zugeordnet waren, neu aufgebaut werden.

Das Service Operations erhält die Prozesse Incident Management und Problem Management zugeordnet. Die Prozesse Event Management, Request Fulfilment und Access Management müssen neu aufgebaut werden. Außerdem müssen die Verbindungen zu den Prozessen mit Betriebsaktivitäten in den anderen Lebenszyklusphasen hergestellt werden.

Den Abschluss macht das Continual Service Improvement mit seinem siebenstufigen Verbesserungsprozess, der wie das Service Reporting und das Service Measurement zu implementieren ist. Zum Prozess Service Level Management muss dann noch eine Verbindung geschaffen werden. Zusätzlich ergibt sich eine Verknüpfung zum Financial Management (ROI).

Wenn alle Bereiche von ITIL 3 implementiert sind und der Regelbetrieb läuft, d.h. der kontinuierliche Verbesserungsprozess angenommen wurde, dann ist ITIL 3 im Unternehmen angekommen. Der Reifegrad der ITIL-3-Prozesse kann im laufenden Betrieb mit Reifegradmodellen wie dem CMMI-Modell überprüft und verbessert werden (vgl. [Sol08, S. 3 ff.]).

4.4.4 Aufbau einer Servicekultur in der IT

Um nach der erfolgten Einführung zu einem langfristig erfolgreichen Regelbetrieb gelangen zu können, ist der Aufbau einer Servicekultur im Unternehmen notwendig.

Die Servicekultur wird dabei nachhaltig von der Unternehmenskultur geprägt und beeinflusst ihrerseits sehr stark die Aufbau- und Ablauforganisation in der IT sowie die Prozesse zu den Fachabteilungen, wie auch Abbildung 4.19 zeigt.

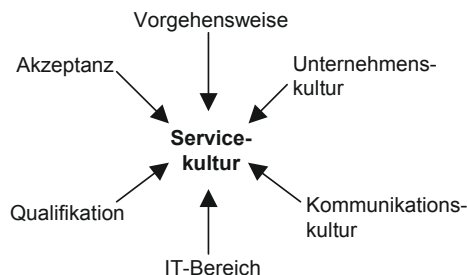


ABBILDUNG 4.19
Servicekultur und Einflussfaktoren

Der Begriff „Servicekultur“ umfasst das Verhalten der Beteiligten bei Prozessen aus den Bereichen Pre-Service, Anforderung, Erbringung, Verhandlungen und After-Service. Unter Pre-Service werden die Aktivitäten für die Fachabteilung verstanden, die die Informationsauf-

nahme, die Feststellung neuer Wünsche einer Fachabteilung und die Beratung im Vorfeld umfassen. Die Anforderungsphase definiert die Anforderungsaufnahme, die Erbringungsphase die Erbringung des Services und die Verhandlungsphase die Aktivitäten um Preis- und Leistungsverhandlungen. Die After-Services beinhalten alle Aufgaben nach der Erbringung, wie die Überprüfung der Zufriedenheit und die Betreuung nach der Dienstleistungserbringung.

Der Begriff „Verhalten“ umfasst sowohl den Umgang der IT-Mitarbeiter untereinander als auch den der IT-Abteilung mit den Fachabteilungen.

Der Aufbau einer Servicekultur umfasst die Analysen zur Ist-Situation, die Betrachtung der Unternehmenskultur, die Anpassung der Aufbau- und Ablauforganisation, die Qualifikation der Mitarbeiter und die Sensibilisierung für Verhaltensänderungen.

Diese Aktivitäten sind jedoch keine einmalige Angelegenheit, sondern Bestandteil eines fortlaufenden Prozesses, der dem Erhalt und der Optimierung der Servicekultur dient. D.h. die Qualität der Kultur ist laufend zu beobachten und auf einem hohen Standard zu halten. Hierfür ist ein Process Owner im Sinne eines intern-orientierten Servicemanagers notwendig.

Wird die Servicekultur entsprechend gelebt, führt das IT-Service-Management zu einer kunden- und serviceorientierten Arbeitsweise.

4.4.4.1 Kunden- und serviceorientierte IT-Organisation

Voraussetzungen für eine kunden- und serviceorientierte IT-Organisation sind eine gelebte Servicekultur und ein IT-Service-Management, das bezogen auf einen bestimmten Prozess durchgängig umgesetzt wurde, sodass es die Mitarbeiter bei ihrer Arbeit unterstützt.

Ein professionelles IT-Service-Management beeinflusst und prägt die *IT-Organisation*, wie Abbildung 4.20 zeigt.

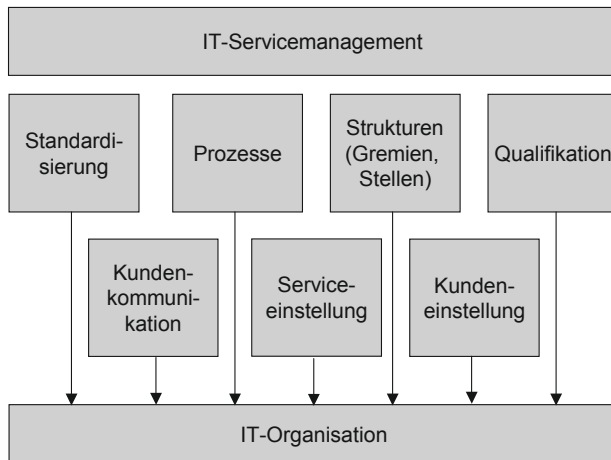


ABBILDUNG 4.20

IT-Organisation und IT-Service-Management

Das IT-Service-Management sorgt für eine Standardisierung der Prozesse innerhalb der IT-Organisation, indem sowohl interne als auch externe Leistungserbringung definiert und festgelegt werden. Die definierten Aufgaben bedingen, dass in der Aufbauorganisation entsprechende Rollen, wie z.B. Change-Manager oder Service-Level-Manager, und Gremien, wie z.B.

das CAB, geschaffen werden. Eine Übersicht der Rollen und Gremien zeigt Tabelle 4.1. Generelle Rollen sind die Rollen des Service Managers, Process Owners und Process Managers. Die Ausrichtung der Prozesse und der Struktur auf die Services führt zu einer eindeutigen Serviceorientierung der IT-Organisation.

TABELLE 4.1 Organisatorische Rollen in den ITIL-3-Prozessen [BJK08] [OCS07] [OSD07] [OSO07] [OSS07] [OST07]

Phasen von ITIL	Rollen/Gremien
Service Strategy	Director of Service Management (Service Manager), Vertragsmanager, Produktmanager, Process Owner, Vertreter des Business
Service Design	Process Owner, Service Design Manager, Service Catalogue Manager, Service Level Manager, Availability Manager, Security Manager, IT-Planer, IT-Designer/Architekt, IT-Service Continuity Manager, Capacity Manager, Supplier Manager
Service Transition	Service Manager, Process Owner, Service Transition Manager, Service Asset Manager, Configuration Manager, Change Manager, Change Advisory Board, Release-Paketierungs- und Build Manager, Deployment Manager, Configuration Analyst, CMS-Manager, Configuration Management Team, Change Authority, Risk Evaluation Manager, Service Knowledge Manager, Test Support, Early Life Support, Management der Entwicklungs- und Testumgebung
Service Operation	Service Desk Manager, Desk Supervisor, Service Desk Analyst, Super User, Technischer Manager, Technischer Analyst, Technischer Operator, Anwendungsmanager Application Management, Anwendungsanalyst/-architekt, Application Management, Incident Manager, Problem Manager, Access Manager (nur im Spezialfall eigenständige Rolle)
Continual Service Improvement	Service Manager, CSI Manager, Service Owner, Process Owner, Service Knowledge Manager, Berichts-Analyst, Kommunikations-Rolle

Die Einführung des IT-Servicemanagements bewirkt außerdem die Ausrichtung der IT-Organisation auf den Kunden. Da die Prozesse und die Strukturelemente der Ermittlung und Umsetzung von Kundenwünschen dienen, ist die Kundenorientierung Grundlage der Arbeit der gesamten IT-Organisation.

Die IT-Service-Organisation beinhaltet dabei auch das dreistufige Support-Konzept (first, second und third level support) mit einem single point of contact und deckt damit neben der Stufigkeit den Support für die drei Grundbereiche Geschäftsprozesse, Applikationen und Infrastruktur ab [BiI04].

Jeder ITIL-Prozess trägt zur Unterstützung eines kunden- und serviceorientierten Arbeitens bei.

Werden diese Potenziale konsequent genutzt und in die Prozesse zu den Kunden eingebracht, so werden Service- und Kundenorientierung gegenüber den internen Kunden deutlich sichtbar.

Beispiele in der Praxis, wie in Abschnitt 4.4.5 beschrieben, zeigen die Erfolge einer konsequenten Kunden- und Serviceorientierung. Verbunden ist dies mit einer unternehmensindividuellen Anpassung des IT-Servicemanagements.

4.4.5 IT-Servicemanagement in der Praxis

Für die Einführung eines IT-Servicemanagements nimmt ITIL eine bedeutende Rolle ein. Eine Untersuchung von Gartner attestiert ITIL, die einzige IT-Servicemanagement-Methode zu sein, die umfassend dokumentiert ist [LDL04 S. 68].

Bei einer Studie der IDC Central Europe⁷ von 2010, bei der 200 Unternehmen mit mehr als 500 Mitarbeiter/innen befragt wurden, zeigte sich, dass 60% der Befragten ITIL im Unternehmen einsetzen (2008: 56%), wobei immer häufiger die Version 3 von ITIL eingesetzt wird [IDC10].

Eine Übersicht über Erfahrungen der Bundesverwaltungen mit ITIL gibt eine Studie, die die KBSt in Zusammenarbeit mit der HiSolutions AG 2007 erstellt hat und die eine positive Bilanz zieht [KBS07].

Die folgenden Beispiele zeigen, dass je Unternehmen unterschiedliche Kombinationen aus ITIL-Prozessen zum Einsatz kamen und diese individuell an die Bedürfnisse der Unternehmen angepasst wurden:

Beispiel: Stadt Stuttgart [PfJ08]. Die Stadt Stuttgart als öffentlicher Dienstleister hatte im IT-Bereich im Jahr 2008 ca. 80 Mitarbeiter, die für die Betreuung von ca. 6800 Benutzern mit ca. 600 Fachanwendungen, verteilt auf über 44 Ämter und Eigenbetriebe, zuständig waren. Das ITIL 3-Projekt begann im Oktober 2006. Ziele des Projekts waren die Ausrichtung der Services an den Kundenanforderungen, eine „kontinuierliche Verbesserung von Services und internen Abläufen“ [PfJ08], die „Orientierung der eigenen Leistung am Wettbewerb der Wirtschaft“ [PfJ08] sowie der Nachweis und die „Optimierung der Wirtschaftlichkeit im Bereich IuK“ [PfJ08]. An Prozessen wurden z.B. das Incident Management, Problem-Management, Configuration Management, Change Management, Release Management und Service Level Management eingeführt

Beispiel: Schweizerisches Medizintechnikunternehmen [EgH04]. Bei dem schweizerischen Medizintechnikunternehmen handelt es sich um einen weltweit tätigen Konzern, der durch die Fusion entstand. Daher sind im Gesamtkonzern zwei IT-Abteilungen vorhanden. ITIL-Prozesse wurden von der IT-Abteilung eingeführt, die den europäischen und südamerikanischen Markt unterstützt. Die Projektvorgehensweise umfasste dabei die Schwachstellen-ermittlung, aus deren Ergebnis die Aufgaben und Teilprojekte abgeleitet wurden, und die Umsetzung. Auf der Basis der Schwachstellen wurden die umzusetzenden ITIL-Prozesse ausgewählt, auf einige wie das Financial-Management wurde bewusst in der ersten Phase verzichtet. Dafür wurde ein Projekt- und Portfoliomanagement eingeführt, das nicht direkter Bestandteil von ITIL 2 ist. Eingeführt wurden z.B. die Prozesse Incident Management, Problem-Management, Change Management, Configuration Management und Service Level Management (vgl. [EgH04 S. 18 ff.]).

⁷ http://www.idc.de/downloads/pdf/pm2010/09_ITSM_final.pdf

■ 4.5 IT Services verrechnen und überwachen

„Es kommt nicht darauf an, die Zukunft vorherzusagen,
sondern auf die Zukunft vorbereitet zu sein.“

Perikles

Wenn die IT-Services vereinbart sind, stellen sich als Nächstes die Fragen, wer welche Leistungen bezahlt und wie sichergestellt werden kann, dass die Leistungen das vereinbarte Niveau halten und Veränderungen sofort festgestellt werden. Dazu müssen Mechanismen für die Verrechnung der einzelnen Services und für die Überwachungsmöglichkeiten betrachtet werden. Im Rahmen des ITIL-Ansatzes werden die Fragen einer Verrechnung und des Berichtswesens im Modul Financial Management und dort in der *Leistungsverrechnung* (Charging) betrachtet (siehe Abschnitt 4.3). Einen weiteren Ansatz liefert z.B. CoBIT (siehe Abschnitt 4.2). Dieser Governance-Ansatz bietet ein großes Instrumentarium zum Controlling und zur Überwachung. Im Folgenden soll nun die Thematik allgemein dargestellt werden.

Dabei muss immer die Verhältnismäßigkeit der eingesetzten Mittel, im Sinne des zu erbringenden Aufwands, in alle Betrachtungen mit einbezogen werden.

4.5.1 IT-Services verrechnen

Bei der Verrechnung von IT-Services ist zunächst das Verrechnungsziel zu identifizieren. Ziele für die Verrechnung von IT-Services können z.B. die verursachungsgerechte Verrechnung, die Nachvollziehbarkeit oder die Vergleichbarkeit sein.

Je nach Zusammensetzung der Gründe gilt es, eine der verschiedenen Verrechnungsmethoden auszuwählen und anzuwenden. Jede Verrechnung von Services beinhaltet damit auch automatisch die Verrechnung der Kosten des Servicemanagements, die den einzelnen Services zugeordnet sind.

4.5.1.1 Möglichkeiten der Verrechnung

Im Rahmen der Verrechnung gibt es die beiden Ansätze *Umlageverfahren* und *direkte Kostenverrechnung*.

Umlageverfahren. Im Rahmen des Umlageverfahrens werden die durch innerbetriebliche Leistungen entstandenen Kosten auf der Basis von Umlageschlüsseln verrechnet. Dabei kommen verschiedene Verfahren wie z.B. Einzelkosten-, Kostenumlage-, Kostenausgleichs- oder Kostenträgerverfahren zum Einsatz. Auf die Betrachtung von Verfahren mit simultanen Gleichungssystemen, die bei multilateralen Leistungsströmen zur Anwendung gelangen, wird hier verzichtet, da in diesem spezifischen Fall keine anderen Ergebnisse zu erwarten sind [Sch98 S. 70 ff.].

Alle Verfahren sind lediglich Näherungsverfahren, die nur geringe Aufwände verursachen, vereinfachend wirken und nur ungenaue Ergebnisse erzielen. Genaue Ergebnisse lassen sich nur mit der direkten Leistungsverrechnung erzielen.

Direkte Kostenverrechnung. Verrechnungspreise (VP) sind ein Instrument zum effizienten Betrieb und zur effizienten Steuerung von Unternehmen. Mit ihnen können die erbrachten Leistungen auch von der Kostenseite her, intern wie extern, transparent dargestellt werden.

Unter Verrechnungspreisen versteht man die monetäre Bewertung von Lieferungen und Leistungen zwischen verschiedenen Bereichen eines Unternehmens. Diese Form der Verrechnung innerbetrieblicher Leistungen ist fester Bestandteil einer modernen Organisationsstruktur und hat die klassische Form der Umlage aufgrund von spezifischen Funktionen und Vorteilen in den letzten Jahren zunehmend abgelöst. Die Verrechnungspreise werden auch als Transfer-, Lenk-, Knappheits-, oder Bereichsabgabepreise bezeichnet [Kre97 S. 14].

Verrechnungspreise werden unterschieden in:

- marktorientierte Verrechnungspreise,
- kostenorientierte Verrechnungspreise,
- Verrechnungspreise als Verhandlungsergebnis und
- duale Verrechnungspreise [Kre97 S. 27 ff.].

Die ersten beiden Verrechnungspreisarten sollen im Folgenden detaillierter betrachtet werden.

Die *marktorientierten Verrechnungspreise* [Sch98 S. 134 ff., Kre97 S. 33 ff.] orientieren sich an den Marktpreisen von Dienstleistern. Das Problem hierbei stellt die Vergleichbarkeit der Leistungen dar. Voraussetzungen für diese Art von Verrechnungspreisen sind, dass

- die Einheiten über Marktinformationen verfügen;
- die Leistungen externe Marktfähigkeit aufweisen oder
- die Leistungen mit marktfähigen Leistungen vergleichbar sind.

Dabei können folgende Preise angesetzt werden:

- aktueller Marktpreis,
- durchschnittlicher Marktpreis,
- Marktpreis minus Abschläge,
- Marktpreis mit Sonderkonditionen,
- Marktpreis ähnlicher Leistungen.

Um Preise objektiv beurteilen zu können, ist es wichtig, dass die Service-Beschreibung sehr detailliert ist und alle relevanten Punkte beinhaltet.



Praxistipp:

Prüfen Sie, ob Ihre Service-Beschreibung alle wichtigen Punkte beinhaltet, d. h. ob alle vorhandenen Anwendungsszenarien damit abgedeckt sind. Prüfen Sie vor allem auch auf Reaktionsverhalten, Ausführungsart und Vollständigkeit anhand einer Szenarien-bezogenen Betrachtung. Erstellen Sie dann aus den identifizierten Punkten eine Liste, und spiegeln Sie an ihr die Angebote des Marktes.

Die Preisfindung bei *marktorientierten Verrechnungspreisen* ist nicht einfach, da häufig entsprechende Substitutionsleistungen oder ähnliche, vergleichbare Leistungen mit betrachtet werden müssen und zu einem hohen Aufwand bei der Datenbeschaffung führen. Auch erfolgt

eine Lenkung der Abnahme von Services über einen gesteuerten Preis durch eine Unternehmensstelle bei einem reinen Marktpreis (ohne Ab- oder Zuschläge) nicht. Der Vorteil dieses Verrechnungspreises ist seine Akzeptanz.

Bei *kostenorientierten Verrechnungspreisen* [Sch98 S. 128 ff., Kre97 S. 30 ff.] bilden interne Größen aus dem Werteverzehr die Basis für die Preisfindung. Dabei ist der Umfang der Verteilung der Kosten auf die Kostenträger die bestimmende Variable zur Preisfindung. Es sind dabei folgende Untergruppen zu unterscheiden:

- Vollkosten,
- Vollkosten plus Zuschlag,
- Prozesskosten,
- Grenzkosten,
- Grenzkosten plus Zuschlag,
- Knappheitswerte.

Zusammenfassend lässt sich sagen, dass die kostenorientierten Verrechnungspreise hauptsächlich der Abrechnung der Services dienen. Gleichzeitig helfen sie bei der Lenkung, Motivation und Erfolgsermittlung. Da sie nicht am Markt orientiert sind, besteht aber die Gefahr, dass sie nicht akzeptiert werden. Um dieses Problem abzumildern, sind bestimmte Vorkehrungen zu treffen.



Praxistipp:

Wenn Sie kostenorientierte Verrechnungspreise wählen, ist es unbedingt notwendig, bei der Kommunikation mit den Leistungsabnehmern auf Transparenz zu achten. Machen Sie daher bei der Vorstellung des Preises die eingeflossenen Kostenbestandteile und die entsprechenden Leistungen deutlich (z. B. in Tabellenform), um den Kosten gleich den Nutzen gegenüberzustellen. Schon vor der Veröffentlichung der Preise sollten Sie klärende Gespräche mit den Meinungsführern der Leistungsabnehmer führen, in denen Sie die Angemessenheit der Preise nachweisen.

In der Praxis gibt es auch Mischformen, bei denen man für einen Service eine Grundleistung festlegt und um eine variable Komponente entweder in Form eines Muss- oder Kann-Services ergänzt.

Aus den Vorteilen lässt sich jedoch nur dann ein Nutzen ziehen, wenn die Verrechnungspreise entsprechend eingeführt werden.

4.5.1.2 Verrechnungspreise – Grundlagen und Einführung

Einführungsprojekt. Die Einführung von Verrechnungspreisen ist als normales Einführungsprojekt anzusehen, das vorbereitet werden muss. Dabei ist jedoch zu bedenken, dass die neu geschaffene Transparenz nicht in allen Bereichen willkommen ist und unkritisch gesehen wird. Deshalb ist es sehr wichtig, durch aktives *Projektmarketing* ein positives Umfeld mit entsprechender Akzeptanz zu schaffen.

Projektmarketing. Eine Aufgabe ist es, eine gute Kommunikation und Transparenz aufzubauen und alle Bereiche (Unternehmensführung, Management der Leistungsabnehmer, Betriebsrat und Unternehmensöffentlichkeit) frühzeitig einzubinden, zu informieren und

Transparenz zu schaffen. Zusätzlich ist laufend die Stimmung gegenüber dem Projekt zu beachten, um Ad-hoc-Maßnahmen einleiten zu können. Bei der Einführung von Verrechnungspreisen ist das sehr wichtig, weil die Services fast immer auch die bestehenden Kernprozesse des Unternehmens tangieren.

Die allgemeinen Aktivitäten des Projektmarketings reichen von Veröffentlichungen in der Hauszeitschrift und Intranet bis zu Projektwerbeartikeln (z. B. Mousepad mit Projektlogo).

Als spezifische Maßnahmen werden Einzelgespräche und kleine Workshops eingesetzt, um das Vertrauen in die Verrechnungspreise erzeugen zu können.

Ablauf der Einführung. Die Einführung der Verrechnungspreise erfolgt anhand der in der nachfolgenden Auflistung dargestellten Vorgehensweise:

- Festlegung der Bestimmungsinstanz,
- Festlegung der Beteiligten,
- Identifikation der Art des Verrechnungspreises,
- Bestimmung der Geltungsperiode,
- Identifikation der Services und der SLAs,
- Unterscheidung in direkte und indirekte interne Leistungen,
- Bepreisung der direkten Leistungen,
- Zuschlagung der indirekten Leistungen auf die direkten Leistungen,
- Berechnung des Verrechnungspreises,
- Erstellung eines Preiskataloges,
- Preisverhandlungen,
- Jährliche Überprüfung der Verrechnungspreise durch Preiskommission.

Vorarbeiten. Die Einführung von Verrechnungspreisen beginnt mit diesen Vorarbeiten:

- Identifikation der momentanen Verrechnung,
- Gremium bestimmen,
- Gültigkeitsdauer der Preise bestimmen und
- Identifikation der Nachfrage- und Abnahmemengen für die Leistungen, die in einzelnen Services zusammengefasst sind.

Identifikation. Im Rahmen der Identifikation der bisherigen Verrechnung werden die Verrechnungsart (keine oder Umlageverfahren) ermittelt. Dabei werden Umlageschlüssel und Umlagehöhen dokumentiert.

Preisgremium. Parallel dazu wird ein Gremium aufgestellt, dessen Aufgabe die Überwachung der Preisgestaltung und der Preisverhandlungen ist. Das Gremium dient im Streitfall gleichzeitig als Schiedsgericht und ist deshalb mit einer ungeraden Personenzahl besetzt.



Praxistipp:

Für die Besetzung des Preisgremiums kommen Mitglieder der Unternehmensleitung und angesehene, integrierende Mitarbeiter in Betracht. Das Gremium sollte je nach Unternehmensgröße aus drei, fünf oder sieben Mitgliedern bestehen, darunter mindestens ein Mitglied der Unternehmensleitung.

Gültigkeitsdauer. Ein weiterer wichtiger Punkt, der nach der Bildung des Preisgremiums betrachtet werden sollte, ist die Gültigkeitsdauer der zu vereinbarenden Preise. Davon abhängig ist die Frequenz der *Preisverhandlungen* und damit auch der Verwaltungsaufwand.

In der Praxis hat sich eine Gültigkeitsdauer von einem Jahr bewährt. Von der gewählten Gültigkeitsdauer sollte nur bei außergewöhnlichen Änderungen von Randbedingungen (wie z. B. Veränderung der Servicebeschreibungen, *Outsourcing* der IT) abgewichen werden. Eine weitere Abweichung ergibt sich in der Einführungsphase der Verrechnungspreise. Hier sollte innerhalb kürzerer Zeit eine Überprüfung der Auswirkungen und gegebenenfalls Nachjustierung der Preise erfolgen.



Bei einer einjährigen Gültigkeitsdauer von Verrechnungspreisen sollte bei der Einführung eine Überprüfung der Verrechnungspreise nach ca. einem halben Jahr erfolgen, um frühzeitig Abweichungen feststellen und ändern zu können.

Identifizieren der Services. Ein weiterer Schritt besteht in der Identifizierung der Mengen sowie der Verteilung der bisherigen Nachfragen und Abnahmen der Leistungen, die die Services repräsentieren.



Die Identifizierung bezogen auf einen Service für ein Anwendungssystem beinhaltet dabei neben den Mengen- und Kostenverteilungen für die Bereitstellung des Systems auch die Inanspruchnahme von spezifischen Administrationsaufgaben, wie die Neuvergabe oder Änderung von Berechtigungen und die Nutzung des Supports (z. B. über die Zahl der Trouble-Tickets).

Planung der Services. Als nächster großer Schritt erfolgt die Planung der Verrechnungspreis-Services, die sich aus folgenden Teilschritten zusammensetzt:

- Beschreibung der Services (Leistungskatalog),
- Vorplanung,
- Identifikation der Verrechnungspreis-Services,
- Vorfestlegung von Muss- und Kann-Services.



Praxistipp:

Beachten Sie bei der Identifikation der Services, dass die Aufteilung und Verrechnung etwas Neues darstellt und am Anfang nicht zu komplex sein darf. Gehen Sie daher zunächst von Dienstleistungsbündeln aus. Beschränken Sie die Anzahl der Services auf die notwendigsten. Verwenden Sie ein bis zwei Grundservices und weisen Sie nur ausgewählten Leistungen einen Verrechnungspreis zu. Sie können später die einzelnen Dienstleistungsbündel immer noch aufteilen und daraus eigenständige Verrechnungspreise gestalten.

Art des Verrechnungspreises. Der nächste große Schritt umfasst die Bestimmung der Art des Verrechnungspreises und die Bepreisung der ausgewählten Services.

Bei der Bestimmung der Verrechnungspreisart stellt sich die Frage nach einem markt- oder kostenbasierten Preis. Für den marktbasieren Preis sprechen die Akzeptanz und die bessere Vergleichbarkeit, für den kostenorientierten die geringeren Aufwände für die Datensammlung.

Doch zunächst muss für jeden Verrechnungspreis ein vergleichbarer Wert auf dem Markt ermittelt werden. Dazu muss für jeden Service ein Anbieter oder ein Vergleichsunternehmen identifiziert werden.

Ist der Preis für einen gleichartigen oder substituierbaren Service ermittelbar, kann ein Marktpreis zugrunde gelegt werden. Bei ähnlichen Leistungen stellt sich die Frage der Vergleichbarkeit und damit der Anwendbarkeit des Preises, die zu klären ist.

Ist kein Marktpreis ermittelbar, so ist ein kostenorientierter Verrechnungspreis festzulegen.

Bepreisung. Wenn die Preise ihrer Art nach festgelegt sind, beginnt die Bepreisung. Im Falle eines Marktpreises ist sie mehr oder weniger vorgegeben. Bei einem kostenorientierten Preis erfolgt die Berechnung. Wenn bestimmte Services verteuert oder verbilligt werden sollen, sind die ermittelten Preise um die Zu- oder Abschläge zu korrigieren.

Verhandlungsphase. Nun folgt die Verhandlungsphase. Sie umfasst

- die Prüfung der Preise,
- die Vorbereitungen zur Preiserfassung und Verrechnungsumsetzung (Schaffung der Infrastruktur),
- die Verhandlungen mit den Leistungsabnehmern,
- eventuell die Anpassung der Leistungen und Preise,
- die Absegnung der Preise
- die Verkündung der Preise und
- die Überprüfung der Preise nach einer vereinbarten Zeit



Praxistipp:

Es ist sinnvoll, diese erste Überprüfung nach der Einführung nach ca. sechs Monaten vorzunehmen, um einerseits verwertbare Daten zu erhalten und andererseits den Leistungsabnehmern, dem Controlling und der IT-Abteilung ausreichend Zeit zu lassen, um sich an die neue Situation zu gewöhnen sowie erste Erfahrungen sammeln zu können.

Regelmäßige Preisverhandlungen. Wenn sich die gewählte Verrechnungsperiode dem Ende zuneigt, werden im Rahmen neuer Preisverhandlungen (wie oben beschrieben) die Verrechnungspreise bestätigt oder neu festgelegt sowie die Mengen festgelegt. Dazu sind im Vorfeld im Bereich der IT-Abteilungen die Verrechnungspreise, wie oben beschrieben, zu prüfen. Ausnahmen ergeben sich in Einführungsphase, bei der Einführung von großen Anwendungen oder bei umfangreicheren Infrastrukturänderungen.

Des Weiteren besteht im Laufe der Zeit die Möglichkeit, bestehende Verrechnungspreis-Services, die aus einem Leistungsbündel bestehen, aufzuspalten und die Servicelandschaft zu verfeinern, womit sich die Zahl der Verrechnungspreise erhöht.

Probleme und Gefahren. Bei der Einführung von Verrechnungspreisen ergeben sich auch Probleme und Gefahren, u. a.:

- Verfehlen der richtigen Gliederungsebene des VP, abhängig von Unternehmensgröße und Dienstleistungsangebot
- Zusätzlicher Verwaltungsaufwand
- Unstimmigkeiten hinsichtlich SLA, Qualität, klare Definition, Umfang und dem Ablauf der Preisbildung
- Marktpreis vs. IT-Service-Angebot („Kaufhaus-Syndrom“)
- Sparen am falschen Platz (Hotline vs. Schulung)

4.5.1.3 Einsatz von Verrechnungspreisen

Die Erfahrung zeigt, dass der Einsatz von Verrechnungspreisen so umfassend wie möglich erfolgen sollte. Ausnahmen stellen dabei Führungsleistungen und andere nicht direkt zuordenbare Leistungen der IT-Abteilung dar, die als Umlage verrechnet werden können.

Nicht zu diesen Leistungen zählen große Projekte, für die noch keine Services vorhanden sind, wie z. B. Vorbereitung einer SAP-Einführung. Für die Verrechnung solcher Leistungen gibt es die Möglichkeit einer Umlage oder einen Infrastruktur-Verrechnungspreis den Leistungsabnehmern belastet werden.

Bei einer Integration von Umlagen werden für eine Leistung zwei Verrechnungspreis-Services vergeben. Ein Verrechnungspreis-Service wird dabei von jedem Mitarbeiter nur einmal in Anspruch genommen und entspricht von seiner Art her einer Umlage mit dem Schlüssel Mitarbeiteranzahl. Der zweite Verrechnungspreis-Service ist abhängig von der wirklichen Inanspruchnahme. Mit diesen zusätzlichen Konstrukten ist es möglich, Verrechnungspreise unternehmensweit für die Verrechnung von IT-Services im Rahmen des *Service-Katalogs* einzuführen und anzuwenden.

Für die Beobachtung von Änderungen und Abweichungen in einem laufenden System gilt es jedoch, die in Abschnitt 4.5.2 beschriebenen Mechanismen bereitzuhalten, um in der Lage zu sein, Abweichungen frühzeitig zu erkennen.

4.5.2 IT-Services überwachen

Das Überwachen von IT-Services bezieht sich nicht nur auf die Überwachung von Preisen und Kosten, sondern vor allem auf die Einhaltung der Service Levels hinsichtlich Umfang, Zeit und Qualität.

Um dies koordiniert durchführen zu können, ist ein System mit verschiedenen Mechanismen aufzubauen, die im Folgenden beschrieben werden.

4.5.2.1 Schlüsselfaktoren und Methoden

Schlüsselfaktoren werden auch als *kritische Erfolgsfaktoren* bezeichnet; sie wurden grundsätzlich bereits in Abschnitt 4.4 erläutert. Im Zusammenhang mit der Überwachung von IT-Services spielen vor allem die exakte Serviceabwicklung und die schnelle Reaktionsfähigkeit bei Problemen mit definierten Eskalationsstufen eine Rolle.

Die *Serviceabwicklung* wird dabei an den Kriterien Menge (Einhaltung des vereinbarten Umfangs), Zeit, Qualität, Kosten und Preis gemessen. Jegliche Abweichung oder Veränderung ist zu ermitteln und zu dokumentieren.

Treten Probleme auf, so gilt es, schnell und strukturiert zu reagieren. Dies ist nur mit einer entsprechenden Vorbereitung möglich, die in Form eines Risikomanagements erfolgen kann. Bei Problemen sind Eskalationsstufen festzulegen, wie das folgende Beispiel zeigt.



Eine mehrstufige *Eskalationsstrategie* könnte so aussehen: Zunächst wird der Bearbeiter kurz vor Überschreiten des Service Levels informiert und dann einen Tag nach Überschreitung erneut. Zwei Tage nach Überschreitung des Service Levels wird der Vorgesetzte informiert. Einen Tag später der Process Owner. Wurden bei einem Bearbeiter in mehr als 25% der bearbeiteten Fälle die Service Levels überschritten, erfolgt eine Meldung an den Vorgesetzten und den Process Owner.

Zur Messung, Identifikation und Dokumentation von Abweichungen benötigt man erprobte Methoden. Mit ihrer Hilfe werden die Art, der Prozess und die Struktur der Überwachung geplant und unterstützt.

Eine Auswahl an Methoden zeigt die folgende Auflistung:

- Risikomanagement (vgl. auch [Hub09 S. 128ff.])
- Kennzahlen
- Berichtswesen (Reports und Möglichkeiten des Feedbacks (evtl. Befragungen))
- Darstellung mittels Balanced-Scorecard (vgl. auch [GaM10, S. 135ff.] und [KaN97])

Diese Methoden können in einem System zusammengefasst werden vgl. Abbildung 4.21.

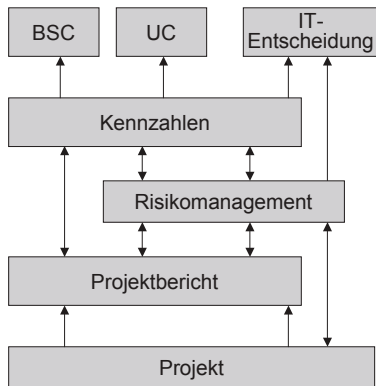


ABBILDUNG 4.21

System zur Überwachung der IT-Services

Die Messgrößen der Balanced Scorecard und die in den folgenden Abschnitten beschriebenen Kennzahlen sind das Herzstück des hier dargestellten Systems.

4.5.2.2 Kennzahlen und ihre Funktionen im IT-Servicemanagement-Umfeld

„Kennzahlen bezeichnen jene Zahlen, die quantitativ erfassbare Sachverhalte in konzentrierter Form wiedergeben.“ [Rei93 S. 343].

Im Folgenden werden unter *Kennzahlen* sowohl Verhältniszahlen (Beziehungs-, Gliederungs- und Indexzahlen) als auch – auf Grund der hohen Informationswerte (z. B. Umsätze) – absolute Zahlen⁸ (Einzelkennzahlen, Summen und Differenzen) subsummiert [Gro91 S. 11]. Bezogen auf das IT-Servicemanagement gewinnen Kennzahlen vor allem bei ITIL immer mehr an Bedeutung. In der Literatur werden Ansätze beschrieben, bei denen den einzelnen ITIL-Prozessen Kennzahlen zugeordnet werden, wie Tabelle 4.2 zeigt [Küt03 S. 75 ff.] [OCS07] [OSD07] [OSO07] [OSS07] [OST07].

TABELLE 4.2 Beispielhafte Zusammenstellung von Kennzahlen, zugeordnet zu ausgewählten ITIL 3-Prozessen [Küt03 S. 92 f.] [OCS07] [OSD07] [OSO07] [OSS07] [OST07]

ITIL-Prozess	Kennzahl	Messgröße
Financial Management	- Rechnungsvolumen; - VP für Service 1	- Gesamtsumme der Rechnungen; - Summe aller Kostenblöcke von Service 1
Service Portfolio Management	Budget/Risiko	Budget je Investitionskategorie
Demand Management	Nachfrageentwicklung nach einem Service Package	Service Package x Nachfrage (Vorjahr) zu Service Package x Nachfrage (laufendes Jahr)
Service Catalogue Management	- Serviceanzahl - Servicewachstum Business	- Anzahl Business Service + Anzahl Technical Service; - Anzahl Business Services letztes Jahr zu Anzahl Business Services momentaner Stand;
Service Level Management	- Offene Aufträge; - Abweichungsquote Service Levels	- Anzahl offener Kundenaufträge; - Anzahl der Prozesse mit Abweichungen im Verhältnis zur Gesamtzahl
Capacity Management	- Auslastungsgrad der Ressourcen; - Antwortzeiten	- Belegte Ressourcen im Verhältnis zu den gesamten Ressourcen; - Zeit von der Anfrage bis zur Reaktion
IT-Service-Continuity Management	- Risikoanzahl pro Kategorie - Erfolgreiche Testquote zum Wiederanlauf	- Anzahl erkannter Risiken pro Kategorie im Verhältnis zur Gesamtzahl; - Erfolgreiche Tests im Verhältnis zur Gesamtzahl

Die Kennzahlen, im Einzelnen betrachtet, geben nur für ihren spezifischen Betrachtungsgegenstand einen Status ab, können aber keinen Gesamtüberblick über das komplette zu betrachtende Szenario liefern. Dafür wird eine Zusammenstellung verschiedenster Kennzahlen benötigt, die in einem Kennzahlensystem zusammengefasst sind.

⁸ In der betriebswirtschaftlichen Literatur herrscht Uneinigkeit über die Abgrenzung des Begriffs Kennzahl bezüglich der Zurechenbarkeit absoluter Zahlen zum Kennzahlenbegriff [MöK04].

4.5.2.3 Kennzahlensysteme im IT-Servicemanagement-Umfeld

Unter *Kennzahlensystemen* wird „die Gesamtheit von geordneten Kennzahlen, die die Zusammenhänge zwischen verschiedenen Größen aufzeigen und so betriebswirtschaftlich sinnvolle Aussagen über Unternehmungen und ihre Teile vermitteln“ [Gla03 S. 91], verstanden.

Bei Kennzahlensystemen gibt es verschiedene Einteilungsvarianten, z. B. [Küt03 S. 44, Gla03 S. 91]:

- Rechensysteme versus Ordnungssysteme,
- Kennzahlensysteme versus Kennzahlensystematiken,
- Analyse- versus Steuerungskennzahlensysteme,
- mathematische versus sachlogisch strukturierte Kennzahlensysteme versus Mischformen,
- traditionelle versus moderne Kennzahlensysteme.

Im Bereich des *IT-Controllings* gibt es eine Reihe von Kennzahlensystemen, die prinzipiell auch für das IT-Servicemanagement von Interesse sind. Einen Überblick gibt Tabelle 4.3.

TABELLE 4.3 Auflistung von Kennzahlensystemen [Küt03 S. 153 ff.]

Kennzahlensystem	Entstehungsjahr/ Publikation	Art
SVD-Kennzahlensystem	1980	Ordnungssystem
Kennzahlensystem von Diebold	1984	Rechensystem
Kennzahlensystem von Lippold	1985	Ordnungssystem
Kennzahlensystem von Zilahi-Szabó	1988	Ordnungssystem
Kennzahlensystem von Kargl	1996	Ordnungssystem
Kennzahlensystem von Brogli	1996	Ordnungssystem
Kennzahlensystem von van der Zee	1996	Ordnungssystem
Kennzahlensystem von Baumöl/Reichmann	1996	Ordnungssystem
Kennzahlensystem von Wies/Lohmann/Picot	1997	Ordnungssystem
Kennzahlensystem CobiT	2000	Ordnungssystem

Die hier aufgelisteten Systeme, vor allem die von Brogli, van der Zee und das CobiT-Kennzahlensystem beinhalten direkte Verbindungen und Zuordnungen von Kennzahlen zu IT-Service-Prozessen, wie sie z. B. in ITIL dargestellt sind. Über diese Abbildungsmöglichkeiten ist das Überwachungsrepertoire vollständig dargestellt.

Nachdem damit gezeigt wurde, wie Verrechnungspreise gestaltet, eingesetzt und überwacht werden können, stellt sich nun die Frage, die am Anfang eines jeden Projektes steht: Wie wirtschaftlich sind die IT-Services, ihre Verrechnung und IT-Servicemanagementprozesse? Welche Kosteneffekte ergeben sich?

4.5.3 IT-Servicemanagement und Wirtschaftlichkeit

Die bewusste Bildung von IT-Services führt wie ihre Verrechnung zu einem zusätzlichen administrativen Aufwand und damit zu Kosten, denen Nutzeneffekte gegenüberstehen, die in Abschnitt 4.5.1 beschrieben wurden. Diese Kosten- und Nutzeneffekte gilt es zu erfassen und zu verrechnen, um die Wirtschaftlichkeit ermitteln zu können.

Bei ITIL wird die Investitionsplanung durch die Kostenrechnung unterstützt, im Microsoft Operations Framework wird eine Investition mittels einer Kosten-Nutzen-Analyse abgeschätzt.

Die normalerweise verwendeten Ansätze beruhen dabei auf budgetierten Kosten. Hier sollen nun weitergehende Ansätze im Sinne von *Total-Cost-of-Ownership* und *Total-Value-of-IT* für IT-Services und IT-Servicemanagement-Investitionen aufgezeigt werden, die schon bei verschiedensten Unternehmen in der Praxis zum Einsatz kamen.

4.5.3.1 Total-Cost-of-Ownership – Entstehung und Grundlagen [KoG00, KoW02]

Der Begriff *Total-Cost-of-Ownership* (TCO) wurde Mitte der 80er Jahre vom Unternehmen Gartner kreiert. Neben dem Modell von Gartner wurden weitere TCO-Modelle geschaffen. Tabelle 4.4 zeigt eine Übersicht über verschiedene Ansätze.

TABELLE 4.4 Übersicht über verschiedene TCO-Ansätze

Name	Besonderheit
Gartner	Erstes Modell, Mitte der 80er Jahre
Forrester	Variation bei den indirekten Kosten
Meta Group	Real Cost of Ownership – keine indirekten Kosten
Fraunhofer IAO	Ergänzung der Kosten- um eine Nutzensicht

Unter TCO werden die Gesamtkosten bezogen auf den Lebenszyklus eines Betrachtungselements verstanden. Die Gesamtkosten spalten sich in so genannte *Hard Factors* und *Soft Factors* auf. Die Hard Factors sind dabei die budgetierbaren Kosten. Die Soft Factors sind die so genannten Endbenutzerkosten. Dies sind z.B. die Bereiche *Endbenutzer* (Supporttätigkeit, Qualifizierungstätigkeiten, ...) und *Downtime* (geplante Dienstunterbrechung, ungeplante Systemstörungen, ...).

Im Sinne von Lebenszykluskosten werden alle Kosten in einem Kostenmodell erfasst. Die Kostengliederung in Bezug auf IT-Services kann sich dabei z.B. an den ITIL-Prozessen ausrichten, ergänzt um weitere Kostenkategorien wie die der *Soft Factors*.

Die Betrachtung von IT-Servicemanagement-Investitionen, z.B. die Investition in ein Change-Management, erfolgt in ähnlicher Weise, nur werden dann die Kostenkategorien aus den hier anfallenden Lebenszykluskosten gebildet.

Bei zurechenbaren Kosten werden auch *Opportunitätskosten* (entgangener Grenznutzen durch Auswahl einer spezifischen Alternative) berücksichtigt.

Wichtige Punkte stellen noch die Periodizität und die Rahmenbedingungen dar. Bei der Periodizität wird die geplante Lebenszeit respektive Betrachtungszeit festgelegt. Dies hat auch Auswirkungen auf die Rahmenbedingungen, hier z.B. auf die Berücksichtigung der Abschreibungen.

4.5.3.2 Total-Value-of-Information-Technology

Die Methode *Total-Value-of-Information-Technology* (TVIT) stellt eine Möglichkeit dar, den Wert von IT-Servicemanagement umfassend zu ermitteln, zu bewerten und bestehende Potenziale anhand historischer Daten vorherzusagen (vgl. [Han08] und [Hei07]).

Dazu werden die Prozesse, die anfallenden Kosten und der Reifegrad der Prozesse betrachtet. Bei zunehmendem Reifegrad ergeben sich immer mehr Kosteneinsparungen, z. B. durch Rationalisierungen, denen aber ebenfalls mit zunehmendem Reifegrad die Kosten für die Prozessverwaltung (Standardisierung und Management der Prozesse inklusive der Prozesspflege) gegenüberstehen. Wenn die beiden Kostenentwicklungen als Kurven betrachtet werden (vgl. Abbildung 4.22), dann ergibt sich bei einem bestimmten Prozessreifegrad ein Punkt mit den niedrigsten Kosten (vgl. [Hei07]).

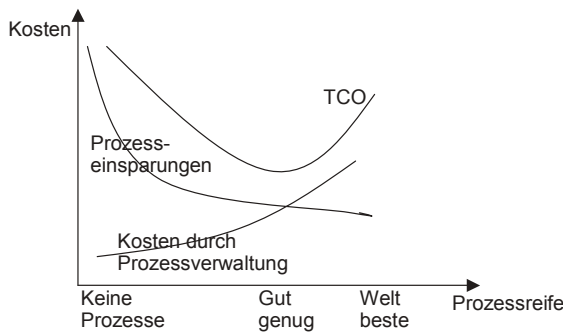


ABBILDUNG 4.22
Kosten und Prozessreife (vgl. [Hei07])

TVIT basiert auf der Kostenseite auf dem TCO-Ansatz von Gartner und verwendet das Reifegradmodell von Gartner und der itSMF, das auf CMMI und ISO 15504 aufsetzt (vgl. [Hei07]).

Der TVIT-Prozess umfasst die Projektfestlegung (Umfang etc.), die Darstellung der unternehmensindividuellen Chancen mit IT-Servicemanagement und detaillierte Umsetzungspläne für eine zielorientierte Optimierung der bestehenden IT-Organisation.

Unternehmen, die diese Methode anbieten, müssen von itSMF und Gartner zertifiziert sein (vgl. [Han08]).

4.5.3.3 Fazit

Die gezeigten und erwähnten Verfahren sind in der Lage, die Wirtschaftlichkeit der IT-Services oder der IT-Servicemanagement-Prozesse aufzuzeigen. Eine Verrechnung der Services und damit der IT-Servicemanagement-Prozesse mit ihrer verursachungsgerechten Zuordnung hilft, das Kostenbewusstsein und die Kostentransparenz zu steigern und damit letztendlich auch einen Beitrag zu einer Verbesserung der Wirtschaftlichkeit zu leisten.

Einen weiteren positiven Beitrag können Tools zur Unterstützung des IT-Servicemanagements leisten.

■ 4.6 Toolauswahl für das IT-Servicemanagement

Die Planung hängt von der Leistungsfähigkeit ab – und vice versa.

Das IT-Servicemanagement ist durch eine Vielzahl von Faktoren gekennzeichnet, die es beeinflussen. Dies sind z. B. die *IT-Organisation*, die Prozesse, die IT-Mitarbeiter und ihr Qualifikationsstand ebenso wie die *IT-Technik*.

Software-Tools zur Unterstützung von IT-Servicemanagement-Prozessen wie z. B. bei ITIL müssen die in den Prozessen benötigten Funktionalitäten abdecken. Die am Markt verfügbaren Tools variieren dabei von der Unterstützung eines spezifischen Prozesses bis zur Unterstützung mehrerer Prozesse.

In diesem Kapitel wird gezeigt, wie eine Auswahl erfolgen sollte, was zu beachten ist und welche Rahmenbedingen zu erfüllen sind. Anschließend werden die Tools klassifiziert und einzelne ausgewählte näher betrachtet.

4.6.1 Die richtigen Werkzeuge wählen – eine Vorgehensweise

Auf dem Software-Markt existieren sehr viele unterschiedliche Tools, die sich nach ihrem Funktionsumfang, ihrer Ausrichtung und nach den Anforderungen, die sie stellen, unterscheiden. Deshalb erfordert die Auswahl des richtigen Werkzeugs einen professionellen Auswahlprozess. Der im Folgenden beschriebene Auswahlprozess umfasst folgende Schritte:

- Phase 0: Sensibilisierung
 - Durchführung von Workshops zur Erläuterung
- Phase 1: Analyse
 - Skills
 - Datenbestand
 - Datenfluss
 - Geschäftsprozesse
 - IT-Prozesse
 - Kommunikation
 - Technische Infrastruktur
- Phase 2: Sollkonzept
 - Kriterienkatalog
 - Lastenheft
- Phase 3: Systemauswahl
 - Marktrecherche
 - Erstellung und Versand der Ausschreibungsunterlagen
 - Ausschreibung

- Präsentation
- Referenzkundenbesuche
- Testinstallation
- Auswahlentscheidung
- Vertragsverhandlungen

Phase 0: Sensibilisierung. Der Auswahlprozess beginnt mit der Vorbereitungsphase, in der zuerst das Ziel schriftlich zu fixieren ist. Nur ein dokumentiertes Ziel lässt sich später eindeutig mit einem Ergebnis vergleichen. Anschließend wird ein entsprechendes *Projektteam* gebildet. Für den Projektleiter gelten die gleichen Anforderungen, wie sie in Abschnitt 4.4 im Rahmen des Einführungsprojekts beschrieben wurden. Die anderen Projektmitglieder sollten überwiegend mindestens drei Jahre im Unternehmen sein und mit der Thematik vertraut sein. Das Projektteam sollte aus drei bis fünf Personen bestehen.

Phase 1: Analyse. Die erste Aufgabe des Projektteams ist eine Ist-Aufnahme der aktuellen Situation in dem Bereich (z.B. Problem-Management), in dem das Tool zum Einsatz kommen soll, gepaart mit einer Anforderungs- und Schwachstellenaufnahme. Sollte die Auswahl für eine kommende Einführung eines IT-Servicemanagement-Prozesses erfolgen, so ist die Soll-Situation mit ihren Anforderungen zugrunde zu legen.

Die Aufnahme bezieht sich auf die Prozesse, Daten, Schnittstellen, Infrastruktur und eventuell Dokumente. Sie erfolgt mittels Interviews und schriftlichen Befragungen sowie Auswertungen von Zusammenstellungen, die vorhanden sind. Dabei werden auch die Schwachstellen und Anforderungen ermittelt, analysiert und im Rahmen der Sollkonzeption in Anforderungen und Maßnahmen hinsichtlich eines Tools konkretisiert.

Phase 2: Sollkonzept. Das Ergebnis der Aufnahme fließt in zwei Dokumente ein, den *Kriterienkatalog* und das *Lastenheft*. Der Kriterienkatalog (Abbildung 4.23 zeigt ein Beispiel) beinhaltet die Anforderungen an das Tool in Kriterienform und soll zu einem späteren Zeitpunkt von den Anbietern befüllt werden.

7	Kaufmännische Kriterien	Antwort	
7.1	Hersteller System 1		
7.1.1	Die Firma existiert seit:		
7.1.2	Ist die Firma ISO zertifiziert?		
7.1.3	Sind Insolvenzverfahren anhängig?		
7.1.4	Ist ein gerichtliches Vergleichsverfahren anhängig?		
7.1.5	Ist eine Liquiditation anhängig?		
7.1.6	Geschäftsbericht/Bilanz ihres Unternehmens (bitte beilegen)		
7.1.7	Organigramm ihres Unternehmens (bitte beilegen)		
7.1.8	Geplante Fusionsvorhaben ihres Unternehmens?		
7.1.9	Mitarbeiter		
7.1.9.1	im Gesamtunternehmen:		
7.1.9.2	im Themenbereich:		
7.1.9.3	Wie hoch ist die Fluktuationsrate im Unternehmen?		
7.1.9.3.1	Wie hoch im Entwicklungsbereich?		
7.1.9.3.2	Wie hoch im Beratungsbereich?		

ABBILDUNG 4.23 Beispiel-Kriterienkatalog

Ein Kriterienkatalog besteht aus vier Teilen:

- allgemeine Anbieterdaten (Produktname etc.),
- technische Anforderungen (Betriebssystem etc.),
- fachliche Anforderungen (z. B. Workflowkomponente) und
- kaufmännische Daten (Umsatz, Lizenzzahlen etc.).

Er ist so ausgestaltet, dass die Anbieter die gestellten Fragen entweder frei oder mit vorgelegten Antworten beantworten können. Je mehr vorgelegte Fragen beinhaltet sind, desto vergleichbarer und einfacher auswertbar sind die Antworten.

Je Fragenart sollten allgemein für die einzelnen Antwortmöglichkeiten Punkte vergeben werden (z. B. Antwort erfüllt: 10 Punkte, Antwort teilweise erfüllt: 5 Punkte). Da die Antworten nicht alle gleichwertig sind, sollten vor dem Einsatz des Kriterienkatalogs die einzelnen Fragen hinsichtlich ihrer Wichtigkeit gewertet werden, und es sollten so genannte K.o.-Fragen, wenn es geeignete gibt, bestimmt werden, bei deren Nichterfüllung ein Anbieter sofort ausscheidet.

Die Umsetzung erfolgt über ein Tabellenkalkulationsprogramm, damit die Auswertung schnell und automatisch durchgeführt werden kann.

Das zweite Dokument, das Lastenheft, beschreibt die Ist- und Soll-Situation und dient dem Anbieter als weitergehende Information. Ein Beispiel ist in Abbildung 4.24 dargestellt.

Inhalt	
1	Einleitung 3
2	Angebotserstellung..... 3
3	Analyse 4
3.1	Prozessanalyse 4
3.1.1	Begriffsbestimmung..... 4
3.1.2	Ablaufmodell Projekte und Prozesse..... 5
3.1.3	Leistungserstellungsprozess 6
3.1.4	Serviceprozesse..... 6
3.1.5	Funktionale Gliederung..... 6
3.1.6	Geschäftsprozesse 7
3.2	Funktionsübersicht 18
3.3	Informationsanalyse 19
3.3.1	Daten..... 19
3.3.2	Dokumente..... 19
3.4	IT-Analyse 19
4	Konzeption..... 21
4.1	Grundlagen 21
4.2	Systemübersicht 23
4.3	Nutzeranforderungen an die neuen Systemkomponenten 23
4.3.1	Incident-Management und Service Desk..... 23
4.3.2	Problem-Management..... 23
4.3.3	Configuration-Management..... 24
4.3.4	Capacity-Management 24
4.3.5	Service-Level-Management..... 24
4.4	Schnittstellenanforderungen an vorhandene Systemkomponenten 27
4.4.1	ERP 27
4.4.2	Personal-Management..... 32
4.4.3	Projekt-Management..... 34
4.4.4	Dokumenten-Management..... 36
4.4.5	Mail-Management..... 36

ABBILDUNG 4.24 Beispiel-Lastenheft

Das Lastenheft beinhaltet die folgenden Teile:

- Ist-Situation
- Soll-Szenario
- Allgemeine Punkte (Qualitätssicherung, Projektdurchführung etc.)
- Glossar

Das Soll-Szenario unterteilt sich meistens in die Punkte Soll-Prozesse, technische Infrastruktur, spezifische fachliche Anforderungen, Datenstrukturen, Schnittstellen, Migration, Betrieb und Wartung.

Ein weiterer wichtiger Punkt stellt das Glossar dar. In ihm werden unternehmensspezifische und allgemeine Punkte erläutert, um ein gemeinsames Verständnis von Begriffen zu schaffen.

Das Lastenheft besitzt je Gliederungspunkt eine Tabelle, die in der Ausschreibung vom entsprechenden Anbieter ausgefüllt werden kann. Rein physikalisch ist es als ein Hauptdokument mit Anhangsdokumenten (z. B. Prozessbeschreibungen) zu sehen.

Diese Dokumente werden dem Projektleitungsausschuss und der IT-/Geschäftsleitung vorgestellt und mit ihnen abgestimmt.

Phase 3: Systemauswahl. Sind diese Dokumente abgenommen, beginnt die Ermittlung geeigneter Anbieter. Dies kann erfolgen durch

- das Studium von Marktübersichten,
- das Studium von Zeitschriften und anderen Publikationen,
- eine Internetrecherche,
- den Besuch einer Messe,
- den Besuch einer themenbezogenen Veranstaltung,
- die Befragung eines Experten oder
- das Sammeln und Auswerten von Werbung.

Es sollten nicht mehr als 10–15 Anbieter vorausgewählt werden. Stehen mehr Anbieter zur Auswahl, so ist eine Vorauswahl mittels eines kleinen Kriterienkatalogs durchzuführen. Dieser sollte maximal zehn wichtige Fragen umfassen und den Anbietern mit der Bitte zur Beantwortung zugesandt werden.



Praxistipp:

Rufen Sie den Anbieter unbedingt vorher an und ermitteln Sie den richtigen Ansprechpartner. Reden Sie mit ihm, und stellen Sie die Situation dar. Ein Versand der Unterlagen ohne vorherige Kontaktaufnahme führt in der Regel dazu, dass entweder nicht geantwortet wird oder die Antwort erst nach mehreren Wochen kommt. Teilen Sie später dem Anbieter einen Stand (Absage oder nächste Ausschreibungsrunde) mit.

Für eine derartige Aktion müssen Sie dem Anbieter ein bis zwei Wochen (je nach Jahres-situation (Messen, Urlaub etc.)) zur Beantwortung einräumen.

Ausschreibung. Wenn die gewünschte Anzahl der Anbieter feststeht und mit den hausinternen Gremien abgestimmt ist, wird wieder mit den Ansprechpartnern Kontakt aufgenommen, und die Ausschreibungsunterlagen werden angekündigt.

Die *Ausschreibungsunterlagen* bestehen in der Regel aus dem Lastenheft, dem Kriterienkatalog (Version ohne Gewichtung und Auswertungsteil), Extrablatt zum preislichen Angebot und einem Rückantwortfax zur Teilnahme. Ob vorab eine Non-disclosure-Erklärung versandt wird, hängt von der Geschäftssituation und den versandten Informationen ab. Wenn eine Vorbefragung, wie beschrieben, stattfindet, kann sie zusammen mit der Non-disclosure-Erklärung versandt werden. Wird die Erklärung einzeln versandt, ist für den Rücklauf eine Woche einzukalkulieren. Für die Befüllung der Unterlagen sollte von einer Frist von ca. sechs Wochen ausgegangen werden. Fordern Sie die Ausschreibungsunterlagen in Papier- und elektronischer Form. Teilen Sie dem Anbieter mit, dass die mitgesandten Formulare verwendet werden müssen, dass der Kriterienkatalog nicht verändert werden darf (durch z.B. Einfügen neuer Zeilen), und weisen Sie im Anschreiben noch einmal auf wichtige Punkte (z.B. Ausschlusskriterien) hin. Die Frist für die Rücksendung des Rückantwortfaxes zur Teilnahme sollte ca. drei Wochen betragen.



Praxistipp:

Wenn Sie sichergehen wollen, dass die Unterlagen von möglichst vielen Anbietern bearbeitet werden und Sie die Unterlagen rechtzeitig zurückerhalten, rufen Sie nach ca. zwei Wochen die Anbieter an und fragen nach dem Stand und ob Fragen bestehen. Bei begründeten Problemen, die dazu führen, dass ein Anbieter die Unterlagen nicht befüllen kann, können Sie sich dann frühzeitig überlegen, wie Sie verfahren, ob Sie die Ausschreibungsfrist verlängern oder ihn aus der Ausschreibung nehmen.

Nach Ablauf der Ausschreibungsfrist kommen die befüllten Ausschreibungsunterlagen. Nun beginnt die Auswertung. Hierbei werden die Antwortspalten aus dem Anbieterkriterienkatalog in den kompletten Kriterienkatalog mit den Gewichtungsfaktoren kopiert, und dieser berechnet dann eine Punktezahl pro Anbieter. Jeder Antwortkatalog muss natürlich noch darauf hin überprüft werden, ob der Anbieter Änderungen am *Kriterienkatalog* selbst vorgenommen hat und sich somit Spalten verschoben haben. Außerdem sind die Antworten hinsichtlich Sinnhaftigkeit und Belegbarkeit (z.B. durch Auszüge aus einem Handbuch) zu prüfen. Die freien Fragen müssen ebenfalls noch von Hand bewertet werden. Im *Lastenheft* haben die Anbieter Stellung zur Realisierung genommen; diese Kommentare sind ebenfalls auf Vollständigkeit und Sinnhaftigkeit zu prüfen. Mit den so ermittelten Informationen in Verbindung mit den allgemeinen und den Preisdaten, die im Rahmen einer Wirtschaftlichkeitsbetrachtung einander gegenübergestellt werden, wählt man die vier bis sechs besten Anbieter aus, die nach Meinung des Projektteams präsentieren dürfen.

Dieses Ergebnis wird dem Projektlenkungsausschuss und der IT-/Geschäftsleitung vorgestellt und abgestimmt.

Präsentation. Zur Präsentation erhalten die Anbieter eine Agenda, die den genauen Ablauf aufzeigt. Die Agenda (ein Beispiel zeigt Abbildung 4.25) beinhaltet eine allgemeine Anbieterdarstellung, die Vorstellung eines bestimmten Szenarios, die Beantwortung ausgewählter Fragen und die Vorstellung des voraussichtlichen Projektteams.

Agenda	
Anbieterpräsentation	
	Zeitraumen: 3,5 Stunden
1.	Vorstellung des Anbieters
2.	Produktvorstellung
	– Demonstration des Clients und des Systems
	– Zusatzthema: »Service Desk Prozess«
3.	Projektablauf, Teamzusammensetzung
4.	Beantwortung der Fragen*
5.	Diskussion des Kriterienkatalogs
6.	Aufwandsbestimmung (auf Basis einer Datenzusammenstellung)

ABBILDUNG 4.25
Beispiel-Agenda einer
Anbieterpräsentation

Für das Szenario ist ein häufig vorkommender Fall vorzusehen, den der Anbieter mit seinem Tool abbildet. Dies ist mit ihm abzustimmen, sodass sich der Aufwand auch für den Anbieter in Grenzen hält. Bei den Fragen sollten maximal acht spezifische ausgewählt werden, vor allem Fragen, die in den Ausschreibungsunterlagen offen geblieben sind. Auf die Vorstellung eines Projektteams ist zu bestehen. Der Anbieter wird nicht das komplette Team mitbringen können, aber wenigstens den potenziellen Projektleiter.



Praxistipp:

Wenn ein interessanter Anbieter zum Präsentationstermin keinen Projektleiter vorstellen kann, dann schlagen Sie ihm einen anderen Termin vor, wo Sie das Projektteam in den Räumen des Anbieters kennen lernen können. Damit erhalten Sie zusätzliche Informationen über den Anbieter durch den Einblick in seine Geschäftsräume.

Die Dauer der Präsentation sollte 4,5 Stunden nicht überschreiten. Dies bedeutet, dass ca. eine viertel Stunde für Begrüßung und Vorstellungsrunde, eine halbe Stunde für die allgemeine Anbieterpräsentation, eine Stunde für die Vorstellung des Szenarios, eine Stunde für die vorgegebenen Fragen, eine Stunde für die Vorstellung und Befragung des Projektteams, eine viertel Stunde für die abschließenden Worte und eine halbe Stunde an Pausenzeit vorzusehen sind. Diese Zeiten sind Näherungswerte und können je nach Situation anders verteilt werden. Für die Präsentation sind für die Beteiligten des Unternehmens zwei weitere Dokumente vorzubereiten. Eine Frageliste, die drei bis vier Fragen zum Szenario und drei bis vier Fragen an das potenzielle Projektteam umfassen sollte, und einen kleinen Fragebogen, der mehrere Fragen zum Eindruck der Präsentation auf die Zuhörer beinhalten sollte.

Der Fragebogen wird ausgewertet und hilft bei der Einschätzung der einzelnen Präsentationen. Die kompletten Präsentationsunterlagen der Anbieter sind in elektronischer Form einzufordern.

Pro Tag sind maximal zwei Präsentationen zu planen. Sie sollten an aufeinanderfolgenden Tagen stattfinden. Am Ende eines jeden Präsentationstages sollten sich die internen Präsentationsteilnehmer noch eine halbe bis eine Stunde zusammensetzen und über die Präsentationen des Tages reden.

Im Anschluss an die Präsentationstermine wird in einem internen Meeting die Rangfolge der Anbieter festgelegt. Hierfür werden noch einmal die Ergebnisse des Fragebogens und der Wirtschaftlichkeitsbetrachtung, die Dokumentation der Präsentationen und die dokumentierten Eindrücke herangezogen. Nach einer Entscheidung wird in einer *internen* Präsentation vor den entsprechenden Gremien die Rangliste vorgestellt und besprochen.

Referenzkundenbesuche. Als Nächstes werden mit den beiden Bestplatzierten der Rangliste Termine für Besuche von jeweils zwei Referenzkunden vereinbart. Die Anbieter sollen eine Liste möglicher Referenzkunden mit den Besonderheiten der Installationen zur Verfügung stellen. Aus dieser Liste erfolgt dann die Auswahl, mit weiteren Vertretern der Liste können bei Bedarf Telefonate geführt werden.

Für die Referenzbesuche ist eine Frageliste zusammenzustellen, die Fragen zu den mit dem Anbieter und seinem Tool gemachten Erfahrungen über den Ablauf des Projekts, die Betreuung durch den Anbieter und über das Projektteam umfassen sollte.

Testinstallation. Parallel zu den Referenzbesuchen sollte die Möglichkeit einer Testinstallation mit Testdaten diskutiert werden. Wichtig ist dies vor allem, wenn die beiden Anbieter in der Bewertung sehr eng zusammenliegen. Eine Testinstallation sollte vier Wochen nicht überschreiten. Je nach Produktart verlangt der Anbieter hierfür Geld.

Auswahl. Mit diesen Informationen ist dann die Auswahl des geeigneten Anbieters möglich. Auch diese Entscheidung ist den internen Gremien mitzuteilen und mit ihnen abzustimmen. Dem Zweitplatzierten sollte noch nicht definitiv abgesagt werden, da zuerst die Verträge abzuschließen sind.

Im Rahmen des Projekts muss dann noch die detailliertere Dokumentation der technischen Lösung in einem Pflichtenheft, auf Basis des Lastenhefts und der Anmerkungen des Anbieters erfolgen. Dies ist jedoch in der Regel nur eine kleinere Aufgabe, da der Lösungsweg beim Anbieter bekannt ist.

Je nach Tool gibt es bei den fachlichen Punkten Unterschiede, auch solche bezüglich des Umfangs der Ausschreibungsunterlagen. Die Klassifikation der Tools beschreiben wir im nächsten Abschnitt.

4.6.2 Funktionsvielfalt und Produktkategorisierung

Um die verschiedenen Software-Tools hinsichtlich Qualität und Effizienz bewerten zu können, stellte das britische *Office of Government Commerce* (OGC) in den 90er Jahren im Rahmen von ITIL Bewertungskriterien auf. Einige davon werden in den folgenden Absätzen näher betrachtet [LDL04 S. 77]. Weitere Checklisten finden Sie in der Literatur (z. B. [Els05]).

Anforderungen an das Tool beziehen sich nicht nur auf die Funktionalitäten, sondern auch auf die Benutzungsoberfläche und damit verbunden die Bedienbarkeit, die Systemvoraussetzungen und die Architektur des Tools.

Die Benutzungsoberfläche des Tools muss klar geordnet sein. Dem Suchenden müssen die relevanten Informationen einfach erkennbar dargestellt werden. Die Farbgebung muss die Übersichtlichkeit und Lesbarkeit unterstützen. Die Bedienung muss intuitiv und verständlich sein, d. h. sie sollte durchgängig dem gleichen Prinzip verpflichtet sein; Hilfetexte und Warnungen sollten zur Verfügung stehen.

Hinsichtlich der Systemvoraussetzungen sind Betriebssystem, Hardware-Voraussetzungen und Datenbank zu beachten.

Ein weiterer Punkt ist die Architektur des Systems. Zu klärende Fragen wären etwa:

- Handelt es sich um eine 3-Tier-Architektur?
- Wie sind die Clients angebunden?
- Welche Schnittstellen sind vorhanden?
- Ist eine Auswertekomponente Bestandteil der Software oder besteht eine Schnittstelle zu einem Auswertetool?

Alle genannten Anforderungen müssen von einem Tool pro Prozess komplett erfüllt werden, um die benötigte Unterstützung zu bieten.

Die Werkzeuge lassen sich nach [LDL04 S. 68] in die folgenden drei Gruppen eingeteilt werden:

- Monitoring- und Infrastruktur-Analysetools,
- Software Delivery-Tools und
- Service Desk-Tools.



Das Wichtigste – zusammengefasst

- **Beachten Sie, dass IT-Servicemanagement immer mehr an Bedeutung gewinnt und es für jede IT-Organisation unverzichtbar ist, sich den Herausforderungen an eine gute Serviceorganisation zu stellen!**

Erforderlich ist eine prozessorientierte IT, die ihre Dienstleistungen kundenorientiert, effizient und effektiv erbringt.

- **Stellen Sie sicher, dass durch ein professionalisiertes IT-Servicemanagement für die IT-Organisation enorme Nutzensvorteile realisiert werden.**

Als wesentliche Nutzengrößen können herausgestellt werden, dass die IT-Services auf die gegenwärtigen und zukünftigen Anforderungen des Unternehmens und seiner Kunden ausgerichtet, die Qualität der erbrachten IT-Services enorm verbessert sowie die langfristigen Kosten der Service-Tätigkeit reduziert werden können.

- **Beachten Sie, dass eine hohe Servicequalität durch das Abschließen von SLAs sichergestellt werden kann!**

Service Level Agreements (SLA) stellen eine wichtige Option bei der Messung der Ergebnisqualität dar, da auf diese Weise die IT-Services sehr gut prüf- und messbar gemacht werden können. Sie legen gegenüber dem Kunden letztlich die Leistungen fest, die mit den IT-Services erbracht werden.

- **Favorisieren Sie eine schrittweise Einführung.**
Wichtig ist, dass Sie für die Einführung des IT-Servicemanagements zuerst den Leistungsumfang des IT-Bereichs festlegen und die kritischen Erfolgsfaktoren definieren, anhand derer das IT-Servicemanagement gemessen werden soll.
- **Beachten Sie, dass nach dem Leitgedanken des IT-Servicemanagements die IT-Dienstleistungen allein dazu dienen, die Geschäftsprozesse und die Anwender bei ihren Aufgaben zu unterstützen.** Klären Sie deshalb welche Geschäftsprozesse wie zu unterstützen sind und welche IT-Dienstleistungen die Anwender benötigen und erwarten.
- **Prüfen Sie, ob ein Arbeiten auf der Grundlage von ITIL möglich ist!**
Orientieren Sie sich an empfohlenen Einführungsvorgehensweisen und an Best Practice Beispielen. Dabei erfolgt in der Regel ein Einstieg über die Optimierung der Prozesse im Incident- und Problemmanagement. Aber auch Prozesse wie Release-Management und Changemanagement weisen in der Praxis bereits vielfach einen hohen Reifegrad auf.
- **Machen Sie auch von den Optionen der Version ITIL 3 Gebrauch!**
Ein wesentlicher Vorteil der Version 3 liegt darin, dass stärker auch die strategischen Fragestellungen im IT-Servicemanagement Berücksichtigung finden.
- **Organisieren Sie das Änderungsmanagement.**
Wichtig ist, dass durch die Einführung eines IT-Servicemanagements neue Prozesse entstehen und bestehende Organisations- und Prozessstrukturen sich verändern. Deshalb sollte der Änderungsprozess frühzeitig organisiert und kommuniziert werden.
- **Sichern Sie die gewonnenen Erfahrungen.**
Aus Erfahrungen kann man lernen, wie man Organisation und Prozesse verbessern kann und wie ein kontinuierlicher Verbesserungsprozess aufgesetzt werden kann.

■ 4.7 Literatur

- [BöK04] *Böhmman, T.; Krcmar, H.: Grundlagen und Entwicklungstrends im IT-Servicemanagement. In: HMD – Praxis der Wirtschaftsinformatik, Heft Nr. 237, 2004, S. 7–21*
- [BJK08] *van Bon, J.; de Jong, A.; Kolthof, A.; Pieper, M.; Tjassing, R.; van der Veen, A.; Verheijen, T.: Foundations in IT Service Management basierend auf ITIL V3. 3. Auflage, Van Haren Publishing, Zaltbommel, ITSM Library, 2008*
- [BuM01] *Bullinger, H.-J.; Meiren, T.: Service Engineering – Entwicklung und Gestaltung von Dienstleistungen. In: Bruhn, M.; Meffert, H. (Hrsg.): Handbuch Dienstleistungsmanagement. 2. Auflage, Springer, 2001, S. 149–175*
- [BVG08] *Buchsein, R.; Victor, F.; Günther, H.; Machmeier, V.: IT-Management mit ITIL V3. 2. Auflage. Vieweg & Sohn, Wiesbaden, 2008*

- [BVG07] *Buchsein, R.; Victor, F.; Günther, H.; Machmeier, V.*: IT-Management mit ITIL V3. Vieweg & Sohn, Wiesbaden, 2007
- [DET04] *Detecon*: IT Service Management – Trends und Perspektiven der IT Infrastructure Library (ITIL) in Deutschland; 2004
- [DIN92] *Deutsches Institut für Normung e.V.*: DIN ISO 9004-2 Norm (1992-06-00): Qualitätsmanagement und Elemente eines Qualitätssicherungssystems; Leitfaden für Dienstleistungen. Beuth, 1992
- [DIN98]: *Deutsches Institut für Normung e.V.*: Service Engineering – Entwicklungsbegleitende Normung für Dienstleistungen. DIN-Fachbericht 75. Beuth, 1998
- [Don80] *Donabedian, A.*: Explorations in Quality Assessment and Monitoring. Volume I: The Definition of Quality and Approaches to its Assessment. AnnArbor, 1980
- [EgH04] *Eggenberger, S.; Helbig, R.*: Implementierung von ITIL im Unternehmen – Vorgehen, Hilfsmittel, Konsequenzen und Grenzen. In: Information Management & Consulting 19 (2004) 1, S. 14 – 20
- [Els05] *Elsässer, W.*: ITIL einführen und umsetzen. Hanser, München, Wien, 2005
- [Fäm99] *Fährnrich, K.-P.; Meiren, T., et al.*: Service Engineering. Ergebnisse einer empirischen Studie zum Stand der Dienstleistungsentwicklung in Deutschland. Fraunhofer IRB, 1999
- [GaM10] *Gadatsch, A.; Mayer, E.*: Masterkurs IT-Controlling. 4., erweiterte. Auflage Vieweg + Teubner/Springer Fachmedien, Wiesbaden 2010
- [Gla03] *Gladen, W.*: Kennzahlen- und Berichtssysteme. 2. überarb. Auflage Gabler, Wiesbaden 2003
- [Gro91] *Groll, K.-H.*: Erfolgssicherung durch Kennzahlensysteme. 4. erw. Aufl. Haufe, Freiburg im Breisgau, 1991
- [Han08] *Handgraetinger S.*: Die Begriffswelt des IT Service Management (ITSM). Vortrag auf dem „IT-Workshop der EKD“ am 28./29. Mai 2008 in Berlin
- [Hei07] *Heiss D.*: Der ITSM Business Case. Vortrag auf dem Forum „ITSM in der Öffentlichen Verwaltung“ am 24.09.2007 in Stuttgart, unter <http://www.fit-oev.de/vortraege-20070924.html> am 22.12.2008.
- [Hub09] *Huber, B. M.*: Managementsysteme für IT-Serviceorganisationen, dpunkt.verlag, 2009
- [HWB04] *Hochstein, A.; Wetzel, Y.; Brenner, W.*: Fallstudie: ITIL-konformer Service Desk bei T-Mobile Deutschland. In: *Meier, A.; Myrach T.* (Hrsg.): IT-Servicemanagement, dpunkt.verlag, Heidelberg, HMD 237, Juni 2004, S. 32–42
- [ISA00-1] *Information Systems Audit and Control Foundation* (Hrsg.): COBIT – 3rd Edition: Framework. Rolling Meadows 2000
- [ISA00-2] *Information Systems Audit and Control Foundation* (Hrsg.): COBIT – 3rd Edition: Management Guidelines. Rolling Meadows 2000
- [ISA00-3] *Information Systems Audit and Control Foundation* (Hrsg.): COBIT – 3rd Edition: Control Objectives. Rolling Meadows 2000
- [ISA00-4] *Information Systems Audit and Control Foundation* (Hrsg.): COBIT – 3rd Edition: Implementation Tool Set. Rolling Meadows 2000
- [ISA00-5] *Information Systems Audit and Control Foundation* (Hrsg.): COBIT – 3rd Edition: Framework. Rolling Meadows 2000
- [ISA00-6] *Information Systems Audit and Control Foundation* (Hrsg.): COBIT – 3rd Edition: Audit Guidelines. Rolling Meadows 2000
- [ISA07-1] *Information Systems Audit and Control Foundation* (Hrsg.): COBIT – 4.1 Edition: Core Content. Rolling Meadows 2007
- [ISA07-2] *Information Systems Audit and Control Foundation* (Hrsg.): COBIT – 4.1 Edition: Control Practices. Rolling Meadows 2007

- [ISA07-3] *Information Systems Audit and Control Foundation* (Hrsg.): COBIT – 4.1 Edition: IT Governance Implementation Guide. Rolling Meadows 2007
- [ISA07-4] *Information Systems Audit and Control Foundation* (Hrsg.): COBIT – 4.1 Edition: IT Assurance Guide. Rolling Meadows 2007
- [IDC10] *IDC Central Europe* (Hrsg.): IDC-Studie: IT Service Management – Aligning IT with Business, Deutschland 2010
- [ITS01] *itsMF* (Hrsg.): IT Service Management, Early, 2001
- [KaN97] *Kaplan, R. S.; Norton, D. P.*: Balanced Scorecard – Strategien erfolgreich umsetzen. Poeschel, Stuttgart, 1997, S. 7ff.
- [KBS07] *Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung.*: ITIL Erfahrungsberichte. Erstellt in Zusammenarbeit mit der HiSolutions AG. Schriftenreihe der KBSt Band 94, April 2007
- [KHP04] *Kemper, H.-G.; Hadjicharalambous, E.; Paschke, J.*: IT-Servicemanagement in deutschen Unternehmen – Ergebnisse einer empirischen Studie zu ITIL. In: *Meier, A.; Myrach T.* (Hrsg.): IT-Servicemanagement, dpunkt., Heidelberg, HMD 237, Juni 2004, S. 25f.
- [KoG00] *Kopperger, D.; Graß, G.-M.*: Kostenermittlung – Pi-mal-Daumen? In: IT – Industrielle Informationstechnik, 8/2000, Hanser, München, 2000, S. 59 – 61
- [KoW02] *Kopperger, D.; Weisbecker, A.*: Sparpotenziale im Visier. In: Microsoft Magazin, 1/2002, Microsoft Press, 2002, S. 24–25
- [Kre97] *Kreuter, A.*: Verrechnungspreise in Profit-Center-Organisationen. Rainer Hampp, München, Mering, 1997
- [Küt03] *Kütz, M.* (Hrsg.): Kennzahlen in der IT. dpunkt.verlag, Heidelberg, 2003, S. 75ff.
- [LDL04] *Lehner, F.; Dirmeyer, J.; Lindner O.*: Softwarewerkzeuge zum IT-Servicemanagement. In: *Meier, A.; Myrach T.* (Hrsg.): IT-Servicemanagement. dpunkt., Heidelberg, HMD 237, Juni 2004
- [MaR01] *Macfarlane, I.; Rudd, C.*: IT Service Management. ItsMF, 2001
- [MeM87] *Meyer, A.; Mattmüller, R.*: Qualität von Dienstleistungen – Entwurf eines praxisorientierten Qualitätsmodells. In: Marketing – Zeitschrift für Forschung und Praxis (ZFP), Nr. 3, 1987, S. 187 – 195
- [MöK04] *Mörschel, I. C.; Kopperger, D.*: Integriertes Kennzahlensystem für die Bewertung von Dienstleistungen. In: *Scheer, A.-W.; Spath, D.*: Computer Aided Service Engineering. Springer, 2004, S. 121 – 143
- [NCV02] *Niessink, F; Clerc, V.; van Vliet, H.*: The IT Service Capability Maturity Model. IT Service CMM, 2002
- [OCS07] *Office of Government Commerce (OGC)* (Hrsg.): Continual Service Improvement, London: TSO, Crown Copyright, 2007
- [OGC00] *Office of Government Commerce (OGC)* (Hrsg.): Service Support, Norwich, 2000
- [OGC01] *Office of Government Commerce (OGC)* (Hrsg.): Service Delivery, Norwich, 2001
- [OGC03] *Office of Government Commerce (OGC)* (Hrsg.): Planning to Implement Service Management, Norwich, 2003
- [OSD07] *Office of Government Commerce (OGC)* (Hrsg.): Service Design, London: TSO, Crown Copyright, 2007
- [OSO07] *Office of Government Commerce (OGC)* (Hrsg.): Service Operation, London: TSO, Crown Copyright, 2007
- [OSS07] *Office of Government Commerce (OGC)* (Hrsg.): Service Strategy, London: TSO, Crown Copyright, 2007
- [OST07] *Office of Government Commerce (OGC)* (Hrsg.): Service Transition, London: TSO, Crown Copyright, 2007

- [Pff08] *Pfeifer, W.; Job, G.*: Das ITIL-Referenzmodell. Bei der Landeshauptstadt Stuttgart. Vortrag auf der 3. FIT-öV-Veranstaltung, Gunzenhausen, 15. Juli 2008
- [Pin09] *Pink Elephant*: Leading The Way In IT Management Best Practices: Pink-Verify TM – Certified Toolsets 2009, <https://www.pinkelephant.com/en-GB/ResourceCenter/PinkVerify/PinkVERIFYTools.htm/consulting/toolsets> am 18.01.2009
- [Pop04] *Popp, H.-J.*: Incident Management – Prozessimplementation in der betrieblichen Praxis. In: Information Management & Consulting 19 (2004) 1, S. 21ff.
- [Rei93] *Reichmann, T.*: Kennzahlen. In: *Horváth, P.; Reichmann, T.* (Hrsg.): Vahlens Großes Controllinglexikon. Vahlen, München, 1993, S. 343–344
- [Roc82] *Rockart, J.F.*: The Changing Role of the Information Systems Executive: A Critical Success Factors Perspective. In: Sloan Management Review 23 (1982), S. 3 – 13
- [Sch03] *Schreiner, P.*: Der Kunde im Zentrum einer qualitätsorientierten Dienstleistungsentwicklung. In: *Spath, D.; Zahn, E.* (Hrsg.): Kundenorientierte Dienstleistungsentwicklung in deutschen Unternehmen. Springer, 2003, S. 137 – 256
- [Sch98] *Scherz, E.*: Verrechnungspreise für unternehmensinterne Dienstleistungen. Gabler Verlag, Deutscher Universitäts-Verlag, Wiesbaden, 1998
- [Sol08] *Solbach, M.*: Erfolgreiches Veränderungsmanagement im IT-Betrieb mit CITIL = CMMI+ITIL. In: IT Service Management, Heft 6, 2008, S. 3 – 7
- [Som04] *Sommer, J.*: IT-Servicemanagement mit ITIL® und MOF. mitp, Bonn, 2004
- [SpW08] *Spath, D.; Weisbecker, A.* (Hrsg.): Business Process Management Tools 2008. Eine evaluierende Marktstudie zu aktuellen Werkzeugen. Fraunhofer IAO, Stuttgart, 2008
- [Ver03] *Versteegen, G.* (Hrsg.): Risikomanagement in IT-Projekten. Springer, Berlin, Heidelberg, New York, 2003
- [ViG05] *Victor, F.; Günther, H.*: Optimierte IT-Management mit ITIL. 2. durchgesehene Auflage, Vieweg, Wiesbaden, 2005
- [Wei02] *Weisbecker, A.*: Software-Management für komponentenbasierte Software-Entwicklung. Jost-Jetter, 2002
- [Wis09] *Wischki, C.*: ITIL ® V2, ITIL ® V3. 3. A und ISO/IEC 20000, Hanser, München, Wien, 2009
- [ZaB03] *Zarnekow, R.; Brenner, W.*: Auf dem Weg zu einem produkt- und dienstleistungsorientierten IT-Management. In: HMD – Praxis der Wirtschaftsinformatik, Heft Nr. 232, 2003, S. 7 – 16
- [ZiS10] *Zielke, F.; Schinkel, A.-W.*: ITIL überzeugend einführen. Symposium Publishing, Düsseldorf, 2010

Ernst Tiemeyer**Fragen, die in diesem Kapitel beantwortet werden:**

- Was sind die Erfolgsfaktoren für die Durchführung von IT-Projekten, und wie können bewährte Konzepte für ein Management von IT-Projekten erfolgreich umgesetzt werden?
- Zu welchen Inhalten sollten im Projektantrag für IT-Projekte typischerweise Aussagen gemacht werden?
- Welche Bedeutung kommt der Projektplanung für ein erfolgreiches Projektmanagement zu, und welche Teilbereiche der Projektplanung sind wie erfolgreich umzusetzen?
- Was zeichnet Phasenmodelle bei IT-Projekten aus, welche Varianten werden unterschieden, und inwiefern sind diese für die Projektplanung nützlich?
- Welche Aktivitäten müssen Sie zum Projektende unbedingt in Angriff nehmen, um ein IT-Projekt erfolgreich abzuschließen?
- Mit welchen Werkzeugen kann das Controlling von IT-Projekten wirksam und nachhaltig unterstützt werden?
- Welche Handlungsfelder lassen sich für die professionelle Umsetzung von Multiprojektmanagement in IT-Organisationen unterscheiden?
- Welche Zielsetzungen werden mit der Einführung von besonderen Verfahren, Organisationsformen und Instrumenten eines Multiprojektmanagements in der IT verfolgt?
- Können Computertools für das IT-Projektmanagement eine Hilfe sein?

Das Arbeiten in Projekten ist im IT-Bereich weit verbreitet. Sei es die Entwicklung einer Software, die Aktualisierung eines Internet-Auftritts, der Aufbau eines Mitarbeiterportals, die Integration und Weiterentwicklung von Standardsoftware (etwa die Integration einer ERP-Lösung), die Umstellung von Anwendungen auf Software-as-a-Service (SaaS), die Einführung einer Dokumentenmanagement-Lösung (DMS) oder die Implementierung einer komplexen Netzwerk- oder Speichertechnologie – all diesen Aktivitäten liegt in der Regel ein IT-Projekt zugrunde.

In der IT-Praxis hat Projektarbeit in der letzten Zeit eine immer größere Bedeutung erlangt. Umfangreiche, funktionsübergreifende Aufgaben werden heute fast nur noch in Projektform abgewickelt. Ein wesentlicher Grund dafür liegt darin, dass viele der anstehenden Aufgaben

so komplex sind, dass sie nur in Zusammenarbeit verschiedener Experten gelöst werden können.

Mit den richtigen Methoden, Techniken und Prozessen sowie einem guten Projektmanagement werden die Erfolgchancen erheblich verbessert. Erfahrungen aus zahlreichen IT-Projekten haben gezeigt: **Gutes IT-Projektmanagement lohnt sich**, auch und gerade finanziell. Dazu kommt, dass heutige Projektausschreibungen die Anwendung etablierter Techniken der Projektsteuerung vertraglich fordern. Und auch angesichts einer sich verschärfenden Produkthaftung ist professionelles IT-Projektmanagement für IT-Organisationen aller Art (IT-Abteilungen, Software- und Systemhäuser etc.) geradezu überlebensnotwendig.

■ 5.1 Von der Projektinitiative zum Projektantrag

5.1.1 IT-Projekttypen und ihre Besonderheiten

Bei einem Projekt handelt es sich grundsätzlich um eine sachlich und zeitlich begrenzte Aufgabe, die durch eine Zusammenarbeit mehrerer Personen gelöst werden muss. Hinzu kommen Kennzeichen wie Zielorientierung und Neuartigkeit der Aufgabe für die Organisation. **Wesentliche Merkmale eines Projekts** sind:

Aufgabenstellung mit zeitlicher Befristung (vorgegebener Abschlusstermin): Ein Projekt besitzt einen definierten Umfang (es muss eine lösbare Aufgabenstellung vorliegen), wobei zwischen definiertem Anfangs- und Endzeitpunkt ein relativ großer Abstand besteht. Dies können mehrere Monate, aber auch mehrere Jahre sein.

Zielvorgabe: Unabhängig von dem zu erreichenden Gesamtergebnis (dem realisierten Softwareprodukt) existiert eine Gruppe von Projektzielen. Dies können Qualitätsziele, Terminziele oder Kostenziele (ggf. auch Einnahmeziele) sein. Hilfreich sind möglichst klare, ergebnisorientierte und messbare Zielvorgaben.

Aufgabenstellung mit Einmaligkeitscharakter, hoher Komplexität und Risiko: Bei einem Projekt handelt es sich um eine Aufgabe von relativer Neuartigkeit (gewisser Einmaligkeitscharakter, keine Routineaufgabe). Diese Neuartigkeit kann sich sowohl auf das Vorgehen bei der Problemlösung als auch auf das angestrebte Ergebnis beziehen. Damit verbunden ist ein gewisses Risiko hinsichtlich der Zielerreichung.

Begrenzte Ressourcen und begrenzter finanzieller Rahmen (Budgetierung): Für das Projekt stehen begrenzte Ressourcen (Personen, Sachmittel) mit einer definierten Kapazität zur Verfügung. Für die im Zusammenhang mit der Projektbearbeitung anfallenden Kosten und Investitionen wird ein Projektbudget als Kostenrahmen aufgestellt.

Teamarbeit und interdisziplinäre Teambildung: Aufgabenstellungen im Projekt können im Regelfall nur fach- und bereichsübergreifend gelöst werden. Die Projektdurchführung erfordert deshalb eine besondere, über die Sichtweise eines speziellen Tätigkeitsbereichs hinausgreifende Koordination. Projektarbeit ist typischerweise Teamarbeit mit allen Vor- und Nachteilen.

**Beachten Sie:**

Eine genaue Prüfung der Projektmerkmale ist deshalb sinnvoll, weil jedes Projekt eine spezifische Organisationsform benötigt, die zur Aufgabenstellung des Projektes passt.

Ein **Anwendungsbeispiel**: Nehmen wir als Beispiel ein Projekt, das ausgehend von einem vorhandenen Intranet den Aufbau eines Mitarbeiterportals zum Gegenstand hat. Folgende Aspekte zeigen, dass ein Projekt vorliegt:

- Die Aufgabenstellung besitzt einen definierten zeitlichen Umfang. Ausgehend von dem vorhandenen firmeninternen Webangebot sollen konkrete Angebote und Produkte entwickelt (Weblösungen mit umfassender Informationsbereitstellung für die Mitarbeiter eines Unternehmens) und eingeführt werden.
- Im Mittelpunkt des Projektes steht die Online-Bereitstellung neuer Informationen und Möglichkeiten für die Mitarbeiterinnen und Mitarbeiter eines Unternehmens. Dazu müssen die zugrunde liegenden Informations- und Kommunikationsprozesse systematisch geplant und unter Einsatz moderner Webtechnologien realisiert werden.
- Das Beispielprojekt weist eine hohe Komplexität auf, wobei organisatorische, medientechnische, personal- und betriebswirtschaftliche sowie informationstechnische Fragestellungen in einer Gesamtheit zu bearbeiten sind.
- Hauptziel eines Projektes „Mitarbeiterportal“ ist letztlich die Realisierung eines umfassenden Webangebotes für die definierte Zielgruppe der Beschäftigten eines Unternehmens.

Vielfach werden in der Praxis alle Vorhaben, die mehrere Teilaufgaben umfassen, als Projekt bezeichnet. Hier gilt es genau zu beachten: Alle eingeführten, permanent durchzuführenden Vorgänge und Prozesse in einer Organisation (einem Unternehmen oder einer Institution) sind **nicht als Projekt** anzusehen. Dies betrifft im IT-Bereich etwa

- Regelprozesse (laufende Aufgaben und Tätigkeiten, wie etwa bestimmte IT-Services),
- Linienmaßnahmen, die eindeutig einem bestimmten Ressort zugeordnet werden können (hier dem IT-Ressort) sowie
- einfache Vorhaben.

All diese Aktivitäten benötigen dann auch nicht die besonderen organisatorischen Rahmenbedingungen, Methoden und Techniken, wie diese sich im Projektmanagement bewährt haben.

Die in der Praxis durchzuführenden **IT-Projekte** unterscheiden sich im Wesentlichen durch die folgenden **Merkmale**:

- Art der Aufgabenstellung (Projekthinhalte)
- Größe/Umfang (Budget, Dauer)
- Innovationsgrad und Komplexität
- Auftraggeber-/Auftragnehmerverhältnis

Für die IT-Praxis können **bezüglich der Projektaufgabe (der Projekthinhalte)** folgende **Projekttypen** unterschieden werden:

- Softwareentwicklungsprojekte
- Integrations- und Implementierungsprojekte für Business-Software (ERP, SCM, CRM, etc.)

- Informationssystem-Projekte (CMS-Projekte, Datenbankprojekte, DMS-Projekte etc.)
- IT-Infrastrukturprojekte (z. B. Storage-Einführungsprojekte, LAN-Implementierungen etc.)
- Strategische IT-Projekte (z. B. EAM-Einführung, Outsourcing-Projekte etc.)

Bezüglich der **Projektgröße** (Teamgröße, Dauer, Budget) kann folgende Differenzierung (Tabelle 5.1) vorgenommen werden:

TABELLE 5.1 Projekteinordnung nach der Projektgröße

Projektgröße	Anzahl Teammitglieder	Personenjahre	Budget (Mio. Euro)
sehr klein	< 3	< 0,4	< 0,05
klein	3 – 10	0,4 – 5	0,05 – 0,5
mittel	10 – 50	5 – 50	0,5 – 5
groß	50 – 150	50 – 500	5 – 50
sehr groß	> 150	> 500	> 50

Ein Projekt sollte in der Regel nicht kürzer als zwei Monate und nicht länger als fünf Jahre dauern. Die **Projektdauer** ist steuerbar; beispielsweise über die Anzahl der eingesetzten Projektmitarbeiter. Insbesondere hängen Projektdauer und Projektgröße voneinander ab. Bezogen auf die Projektdauer bzw. den Projektaufwand gibt es eine optimale Anzahl von Projektmitarbeitern.

Eine besondere Rolle für eine Projektklassifizierung spielt natürlich der Grad der **Einzigartigkeit der Aufgabenstellung**, die es erfordert, das vorhandene Know-how stets neu zu organisieren und zusammenzuführen. Dies wird insbesondere bei IT-Projekten zum Problem, deren Aufgabenstellung zu Projektbeginn noch weitgehend offen ist.

Hinsichtlich der **Auslösung von Projekten** und der sich daraus ergebenden Auftraggeber-/Auftragnehmer-Verhältnisse kann zwischen internen und externen Projekten unterschieden werden:

- Bei **internen IT-Projekten** ist der Auftraggeber in der Regel die Unternehmensführung oder eine Fachabteilung, die dann auch grob die Zielsetzungen und die erwarteten Ergebnisse vorgibt.
- Bei **externen IT-Projekten** werden Projekte für einen (unternehmens-)fremden Auftraggeber durchgeführt. Dies gilt etwa für spezielle IT-Softwarehäuser oder Systemhäuser, die für ein Anwenderunternehmen ein IT-Projekt realisieren. Diese Projekte führen dann meist zu einer definierten Leistung, wobei ein klar definierter Projektauftrag vereinbart wird.

5.1.2 Auslöser für IT-Projekte

Wie beginnen IT-Projekte in der Praxis? Im Wesentlichen können drei typische **Ausgangsfälle für die Inangriffnahme von IT-Projekten** unterschieden werden:

- IT-Projekte ergeben sich als Ergebnis einer IT-Langfristplanung und werden aus IT-Strategien abgeleitet. Dabei werden die Ergebnisse des Strategieentwicklungsprozesses im IT-Masterplan dokumentiert.

- Konkrete Anforderungen von Fachabteilungen oder der Unternehmensleitung sowie Praxis-Probleme sind die Auslöser für IT-Projekte bzw. Projektanträge.
- Veränderungen des Umfeldes (etwa technologische Entwicklungssprünge, Marktveränderungen, organisatorische Veränderungen oder gesetzliche Auflagen) machen das Auflegen eines IT-Projektes notwendig.

Die **Projekt-Auslöser** im Zusammenhang zeigt Abbildung 5.1.

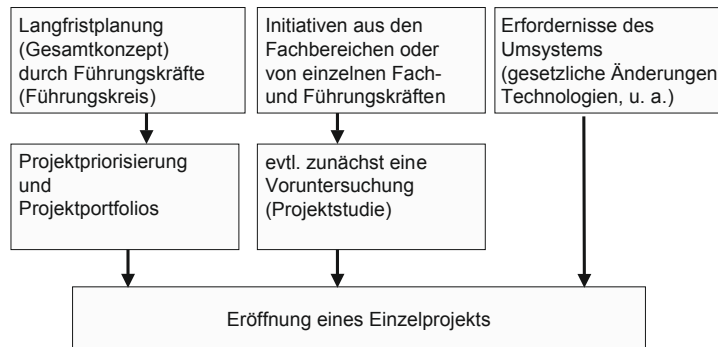


ABBILDUNG 5.1 Projekt-Auslöser im Zusammenhang

Leider zeigt die Praxis: In zahlreichen Firmen und Behörden ist die langfristige Planung von IT-Projekten unterentwickelt. Eine Gesamtkonzeption ist oft nicht einmal vorhanden oder weitgehend überholt.

Konkreter Auslöser für Projekte in der Wirtschaftspraxis sind meist Ideen aus den Fachbereichen oder Anregungen seitens der Geschäftsführung; etwa der Wunsch von Geschäftsführung und Fachabteilung nach schneller oder sicherer Abwicklung von Geschäftsprozessen. Verschiedene Gründe führen dazu, dass bei den Verantwortlichen entsprechende Anträge gestellt werden, um zu neueren, leistungsfähigeren Lösungen zu kommen. Varianten zeigt Tabelle 5.2.

TABELLE 5.2 Auslöser und Initiatoren von Projekten

Projekt-Auftraggeber (Wer erteilt den Auftrag?)	Projektideen (Wofür?)	Projektanlässe (Warum?)	Projekt-Initiatoren (angeregt durch?)
▪ Unternehmensführung ▪ Personalabteilung/ Human Resources (HR) ▪ Finanz- und Rechnungswesen ▪ Einkauf/Material- wirtschaft ▪ Marketing/Vertrieb ▪ Produktion ▪ IT-Abteilung	▪ Aufbau eines Mitarbeiterportals ▪ Neue Software ein- führen (etwa Open Source Software) ▪ E-Business-Projekt (E-Procurement, CRM u. a.) ▪ Neue Technologien einführen (etwa Mobiles Computing) ▪ Internet-Auftritt optimieren	▪ Erweiterter Informations- bedarf ▪ Arbeitserleichte- rung ▪ Gesetzliche Anforderung ▪ Umsatzförderung ▪ Prestige-Bedürfnis ▪ Personalförderung	▪ Vorgesetzte ▪ Kollegen ▪ Seminare ▪ Verbände ▪ Organisation ▪ Hersteller ▪ Medien

Um aufgrund von aktuellen Anlässen und Anforderungen zu einem konkreten Auftrag für ein IT-Projekt zu gelangen, sind besondere **Voraussetzungen und Vorgehensweisen** denkbar:

- **Antragsverfahren:** Der Eröffnung eines IT-Projektes geht in diesem Fall ein stufenweiser Entscheidungsprozess voraus, ehe die Projektinitialisierung mit der Freigabe eines Projekts endet. So muss insbesondere in größeren Organisationen zunächst mittels eines „Kanalisierungsverfahrens“ eine Beurteilung über Projektanträge erfolgen.
- **Durchführung einer Vorstudie:** Bevor das Hauptprojekt durchgeführt wird, ist eventuell vorab eine Vorstudie sinnvoll. Ziel einer solchen Voruntersuchung ist eine genauere Prüfung, ob das Projekt in dieser Form gestartet (Machbarkeitsstudie) und welche spezifische Projektausrichtung eingeschlagen werden soll (Festlegung eines Ziel- und Handlungsrahmens für das IT-Projekt).



Beachten Sie:

Die Projektinitialisierung zählt zu den schwierigsten Projektabschnitten, wie einige Negativbeispiele zeigen. So erfolgt oft ein voreiliger Projektstart, ohne dass die Rahmenbedingungen für die Projektdurchführung geklärt und die notwendigen Voraussetzungen geschaffen worden sind. Probleme sind darüber hinaus vorprogrammiert, wenn die Entscheidung für ein IT-Projekt aufgrund eines „einsamen“ Managemententschlusses gegen den erklärten Willen der Fachbereiche bzw. der Betroffenen erfolgt.

5.1.3 Wichtige Voraussetzungen für erfolgreiche Projektarbeit

Erfahrungen aus der Praxis und zahlreiche Studien zeigen, dass IT-Projekte zu einem nicht unerheblichen Teil scheitern. Nehmen Sie als Beispiel das Ergebnis einer Forsa-Studie (vgl. [Sch04], S. 14):

- 59% aller Softwareprojekte überziehen das geplante Budget.
- 46% aller Softwareprojekte überschreiten die geplanten Termine, um durchschnittlich 7 Monate.
- Die Fluktuationsrate der Projektleiter beträgt 68%.

Das ist ein untragbarer Zustand, der – das dokumentieren ebenfalls vielfältige Erfahrungen – nicht sein muss. Die Lösung liegt in der Festlegung eines ausgewogenen IT-Projektportfolios („die richtigen IT-Projekte machen“) sowie in der Verankerung eines konsequenten, ganzheitlichen Projektmanagements („die IT-Projekte richtig machen“).

Die Zahl der IT-Projekte, die beendet werden, ohne dass der festgesetzte Zeitpunkt oder der Kostenrahmen überschritten wird, ist also immer noch gering. IT-Projekte sind mit Risiken und Problemen verbunden. Der Projektleiter, die Projektmitglieder und der Auftraggeber des Projektes sollten in jedem Fall die typischen **Projektrisiken** kennen, um ein Scheitern eines Projektes zu vermeiden. Diese Risiken können in folgende Gruppen eingeteilt werden:

- Unzureichende Projektdefinition (ungenau Zielsetzungen, Abgrenzungsprobleme mit anderen Projekten, mangelhafte Abstimmung mit Stakeholdern, etc.);

- fehlender Einsatz geeigneter Methoden (Planungs- und Steuerungsinstrumente) und unzureichende Nutzung bewährter Arbeitstechniken;
- Risiken personeller Art;
- fehlende oder unzureichende Projektplanung;
- Mängel in der Projektdurchführung bzw. bei der Projektsteuerung.

Was sind die Konsequenzen? **Wie lassen sich Projektfehlschläge vermeiden?** Eine These vorweg: **Erfolgreiche IT-Projekte sind ohne effizientes Projektmanagement undenkbar.** Nur so sind die für die Projektabwicklung anfallenden Teilaufgaben überschaubar und lassen sich Problemsituationen rechtzeitig erkennen. Außerdem wird es den Mitarbeitern im Projekt dann weniger schwer fallen, zielorientiert zu handeln.

**Beachten Sie:**

Nehmen die Projekte einen gewissen Umfang an, empfiehlt sich fast immer ein durchdachtes Projektmanagement, also eine vorherige Projektdefinition (eventuell auch eine Vorstudie), nach der Genehmigung eine differenzierte und gründliche Planung sowie in der Phase der eigentlichen Durchführung eine fortlaufende Überwachung und Steuerung des Projektes. Bloßes „Draufloswerkeln“ birgt nämlich erhebliche Gefahren und Nachteile in sich, die vielen Projektleitern und Mitarbeitern in Projekten sicherlich bekannt sind: Zeitverzögerungen, unnötige Kostensteigerungen, Leerlauf durch fehlende Verfügbarkeit der notwendigen Ressourcen (Sachmittel und Personal) sowie eine unzureichende Qualität der Ergebnisse.

5.1.4 Die Projektskizze

Aus den Projektideen ist in einer ersten Phase eine grobe **Projektskizze** (= Projektdefinition) zu erarbeiten. Hier geht es darum, die für eine Grundsatzentscheidung bzw. die Erarbeitung eines detaillierten Projektantrages wesentlichen Punkte abzuklären und zu fixieren. Dazu gehören insbesondere:

- die **Skizzierung der Aufgabenstellung** (Herausforderungen und Zielsetzungen),
- die **Analyse der Rahmenbedingungen** (sachliches und soziales Umfeld, andere Projekte und Produkte) sowie
- die erwarteten **Ergebnisse**.

Mit einer groben Projektskizze wird die Initiative für die Durchführung eines Projektes fixiert. Daraus kann dann ein konkreter Projektantrag/Projektvorschlag erarbeitet werden. Hierüber muss der Auftraggeber befinden (bzw. ein evtl. existenter Projekt-Entscheidungsausschuss des Unternehmens). Wird das Projekt genehmigt, mündet der Antrag in einen konkreten Projektauftrag.

**Beachten Sie:**

Mit einer klaren Projektdefinition wird die erste Voraussetzung geschaffen, um einen Projektantrag erarbeiten zu können. In dem Projektantrag sollten alle zum aktuellen Zeitpunkt absehbaren Daten, die für eine Entscheidung über die Projektdurchführung wichtig sind, schriftlich fixiert werden. So können hier etwa auch die entstehenden Chancen und Risiken sowie die erwarteten Kosten und Nutzengrößen quantifiziert werden.

5.1.5 Der Projektantrag

Um alle an einem IT-Projekt Beteiligten dazu zu zwingen, die aus der Projektinitiative resultierenden Informationen und Probleme sachgerecht zu durchdenken, hat es sich in der Praxis als sinnvoll erwiesen, einen Projektantrag zu formalisieren und typische Inhalte vorzugeben. Eine **mögliche Inhaltsgliederung eines Projektvorschlages** wird nachfolgend skizziert.



- Beschreibung des Projektgegenstandes
- Strategierelevanz des Projekts
- Skizzierung der Projektziele und ggf. Wirtschaftlichkeitsbeurteilung (WBU) bzw. Nutzenbetrachtung zum Projekt
- Erste Aktivitätenplanung
- Vorgehensmodell (Projektphasen) mit grobem Terminplan (Projektstart & -ende) und Projekt-Meilensteinen
- Erste Ressourcenplanung
- Grober Kostenplan: Aufwands- & Kostenschätzung
- Projektrollen (Kunde, Projektleitung, Projektteam)
- Zu erwartende Ergebnisse des Projektes
- Rahmenbedingungen für die Projekt-Umsetzung (Risikobetrachtung, Qualitätsmanagement etc.)
- Berichtsplan

Ausgangspunkt des Projektantrages ist eine kurze Beschreibung des geplanten Projektes (bzw. des **Projektgegenstandes**). Dabei ist die Ausgangslage zu skizzieren, mit der dargelegt wird, warum das Projekt durchgeführt werden soll.

Gewünscht ist oft auch eine kurze Einschätzung der Bedeutung des Projektes in Bezug auf die strategischen Zielsetzungen der Organisation (**Strategierelevanz des Projektes**). Neben einer quantitativen Beurteilung (hoch, mittel, niedrig) kann auch eine qualitative Begründung für die Festlegung angegeben werden.

Zumindest grob sollten im Projektantrag die **Projektziele**, der **Projektnutzen** und die **erwarteten Ergebnisse** umrissen werden. Eine Hilfe ist dabei das Arbeiten mit Zielhierarchien. Dies bedeutet, dass ausgehend von einem Oberziel verschiedene Teilziele abgeleitet werden. Zunehmend setzt sich auch die Orientierung anhand einer Balanced Scorecard durch.

TABELLE 5.3 Zielsetzungen in IT-Projekten

Zielbereiche	Zielsetzungen
Finanzielle Ziele	▪ Projektbudget einhalten (Abweichung unter 10%) ▪ Flexibilität bei der Budgetverwendung erhöhen ▪ Projektkosten minimieren ▪ Nutzwert des IT-Projektes transparent darstellen und kommunizieren
Kundenziele	▪ hohen Kundenzufriedenheitsgrad erreichen (Zufriedenheitsindex von mindestens 98% sichern) ▪ hohen Nutzungsgrad (Verbreitungsgrad) der Projektergebnisse gewährleisten (mindestens 95%) ▪ Wirkung von Projekt-Marketingmaßnahmen erhöhen (Bekanntheitsgrad der IT-Projekte im Unternehmen auf 80% steigern)
Prozess-Ziele	▪ Projekterfolgsquote verbessern (etwa auf 95% steigern) ▪ Auslastungsrate im Projekt erhöhen ▪ Vereinbarte Termine/Zeiten zu 99% einhalten (Arbeiten in time)
Personalziele	▪ Hohe Zufriedenheit der Projektmitarbeiter sichern ▪ Projekt-Personal kontinuierlich entwickeln ▪ Personalbindung für das IT-Projekt herstellen (Mitarbeiter halten und damit eine niedrige Fluktuationsrate gewährleisten)
Produktorientierte Ziele	▪ Projektergebnisse in hoher Qualität bereitstellen ▪ Projektergebnisse zeitnah/zeitgerecht ausliefern ▪ Abnahme der Projektergebnisse durch den Auftraggeber sichern (Erst-Abnahmequote von 95%)

Interessant in Verbindung mit den Zielen und den erwarteten Ergebnissen sind unter Umständen auch spezifische **Wirtschaftlichkeitsüberlegungen**. Ohne eine Skizzierung der Kosten-/Nutzenaspekte ist heute ein IT-Projekt kaum noch realisierbar. Der **Kostenaspekt** lässt sich dabei leichter ermitteln. Mitunter können Erfahrungen aus vorherigen Projekten herangezogen werden.

Problematischer (weil nicht unbedingt quantifizierbar) sind die **Nutzenaspekte**. Wichtige Nutzenaspekte, die in Projekten herausgestellt werden können, sind:

- verbesserte Kundenorientierung
- Kostensenkung
- Amortisationsdauer (ROI-Beitrag)
- Innovations-, Qualitäts- und Flexibilitätsförderung
- Beitrag zu Green-IT-Zielen



Beachten Sie:

Wenn am Ende eines Projektes die Frage gestellt wird, ob die Projektziele erreicht wurden, hört man in der Regel ausweichende Antworten. Die Hoffnung, dass die zu Projektbeginn oft noch nicht eindeutig geklärten Ziele sich im Verlauf schon klären werden, erfüllt sich erfahrungsgemäß nicht. Die Projektziele, der Projektnutzen und die erwarteten Ergebnisse sollten zu Beginn fest umrissen werden, damit es hinterher kein böses Erwachen gibt.

Bei IT-Projekten ist es üblich, zwischen der Entwicklung des **Fachkonzeptes** sowie des **Architektur-Konzeptes** zu unterscheiden.

Bezüglich der fachlichen Anforderungen kann dargelegt werden:

- unterstützte Prozesse (prozessuale Anforderungen)
- gewünschte Funktionen (funktionelle Anforderungen)
- Informationsbedarf (informationelle Anforderungen)

Als Teilbereiche des IT-Architektur-Entwurfs kommen in Betracht:

- Architekturentwicklung (z. B. Blueprint-Entwurf, etc.)
- Datenbankentwurf = Planung der Funktions- und Datenstrukturen (allerdings Flexibilität beachten)
- Design der Benutzeroberfläche (Beachtung ergonomischer Kriterien)
- Realisierungsinstrumente: Plattformen, Komponenten der IT-Infrastruktur, Applikationslandschaft

Um eine Übersicht über die wesentlichen Aktivitäten zur Durchführung zu erhalten, bietet sich im Projektantrag die Skizzierung der gewählten Projektphasen an. Je nach Projektgegenstand sind entsprechende **Vorgehensmodelle** zu adaptieren (zum Beispiel ein Phasenmodell oder ein agiles Vorgehen nach Scrum). Wichtig ist, dass in einem Projektantrag ein Projektplan als Richtschnur existiert und hierin die Meilensteine und auch Termine festgehalten werden.

Tabelle 5.4 zeigt einen möglichen groben Projekt-Zeitplan, wie er für ein Beispielprojekt „Aufbau eines Mitarbeiterportals“ aus definierten Projektphasen abgeleitet werden kann.

TABELLE 5.4 Ausschnitt eines Projekt-Zeitplans

Projekt-Zeitplan – Aufbau eines Mitarbeiterportals				
Phase	Inhalt	Verantwortlich	Termin (Beginn)	Termin (Ende)
Definition	Systemerhebung und Systembeschreibung	Herr Meyer	01. Okt. ..	01. Feb. ..
Design, Plan	Entwicklung des Fach- und Architektur-Konzeptes (Inhalte etc.)	Frau Riedel	01. Feb. ..	31. März ..
	Entwicklung Web-Design			
Build	Systemrealisierung	Herr Meyer	01. April ..	30. Mai ..
Roll-out	stufenweise Umstellung	Frau Ziegler	01. Juni ..	01. August ..
Produktivstart	Customizing und Test	Fachabteilung Marketing	01. August	

Schließlich sind im Projektantrag erste Angaben zum benötigten **Budget** zu machen. Aus dem Bedarf an Einsatz- und Finanzmitteln, der durch die Aufwandsschätzung für Arbeitspakete, Vorgänge und Projekte bestimmt wurde, können die gesamten Projektkosten hochgerechnet werden. Dies ist Aufgabe der **Kostenplanung**, die den einzelnen Elementen die voraussichtlichen Kosten zuordnet. Ziel der Kostenplanung ist letztlich das Ermitteln der für das Projekt erforderlichen Geldmittel und das Vorbereiten der Entscheidung über die Zuteilung eines Budgets.

Bezüglich des Vorgehens empfiehlt es sich, eine Gliederung der **Haupt-Kostenarten eines Projektes** nach betriebswirtschaftlichen Gesichtspunkten vorzunehmen:

- interne Personalkosten (Löhne, Gehälter, Sozialkosten, Erfolgsbeteiligungen)
- Fremd-Personalkosten (beispielsweise Kosten für externe Beratung und Unterstützung)
- Sach- und Dienstleistungskosten (beispielsweise Instandhaltung, Energie, Hilfsmaterial, Reisekosten, Nachrichtenkosten, Werbekosten, Büromaterial)
- Kapitaleinsatzkosten (Investitionskosten): kalkulatorische Abschreibungen, Zinsen, Wagnisse, Steuern, Versicherungen

Hinsichtlich der Vorgehensweise beginnt man in der Regel mit den Personalkosten. Dazu sind meist die anfallenden Aufgaben (Arbeitspakete des Projektes) eine gute Basis. Daraufhin werden auch die externen Kosten (als gesonderte Größe) geschätzt. Anschließend werden die Sach- und Kapitalkosten kalkuliert.

Die **Auflistung der gewünschten Ergebnisse** (Funktionen, Deliverables), die nach Umsetzung des Projektes vorliegen sollen, sind ein weiterer Hauptpunkt innerhalb eines Projektantrages. Sie bildet eine gute Grundlage für die konkrete Formulierung der Anforderungen an die künftige Lösung.

Darüber hinaus sind Fragen im Hinblick auf die **Projektumsetzung** anzusprechen und daraufhin im Projektantrag zu fixieren:

- **Qualitätsmanagement:** Anzugeben sind spezifische Qualitätssicherungs-Maßnahmen, die gewährleisten, dass die angestrebten Projektergebnisse tatsächlich erreicht werden.
- **Änderungsmanagement (Change-Management):** Hier sind die Aktivitäten aufzulisten, die sicherstellen, dass die Betroffenen den Projektergebnissen positiv gegenüberstehen und eine Umsetzung in die Realität gewährleisten.
- **Risikomanagement:** Hilfreich sind die Aufzählung der Risikoarten (beispielsweise Risiken hinsichtlich Terminen, Kosten, Realisierung), denkbare Risikoursachen sowie die möglichen Handlungsfelder für den Fall des Risikoeintritts. Außerdem können hier alle jene Maßnahmen angeführt werden, die bereits im Vorfeld getroffen wurden, um das Projektrisiko zu minimieren.
- **Projekt-Berichtswesen:** Nützlich sind Überlegungen zur Art der abzuliefernden Dokumente/Berichte. Dabei können Termine vorgegeben bzw. die Periodizität der abzuliefernden Berichte festgelegt werden.



Wichtige Merkmale, die erfolgreiche Projekte aufweisen, sind:

- die „richtigen“ Projekte
- ausreichende Berücksichtigung des Projektumfeldes
- leistungsfähige und hochmotivierte Mitarbeiter
- sinnvolle organisatorische Einbettung der Projekte
- systematische Projektplanung
- sorgfältige Projektsteuerung
- integriertes Projekt-Qualitätsmanagement

■ 5.2 Vereinbarung eines Projektauftrages

Der Projektantrag ist gestellt. Meist wird nach einem genau vereinbarten Verfahren entschieden, ob das IT-Projekt durchgeführt werden soll. Dazu wird insbesondere der vorliegende Projektantrag einer genaueren Prüfung und Bewertung unterzogen. Die Gesamtbewertung sollte möglichst durch ein neutrales Gremium erfolgen. Nach der Genehmigung des Projektes ist dann der (in aller Regel) schriftlich fixierte Projektauftrag die Grundlage für alle weiteren Projektaktivitäten.

5.2.1 Bewertungskriterien für IT-Projekte und Priorisierungsverfahren

Für die Behandlung von Projektanträgen empfiehlt sich ein formalisiertes Verfahren, meist unter Einschaltung eines Koordinierungsausschusses. Dieser Ausschuss (besetzt etwa aus der Geschäftsleitung und weiteren Vertretern der Managementebene) entscheidet dann – möglichst unter Hinzuziehung der IT-Leitung – letztlich darüber, ob das IT-Projekt durchgeführt werden soll oder nicht. Den Zusammenhang zeigt Abbildung 5.2.

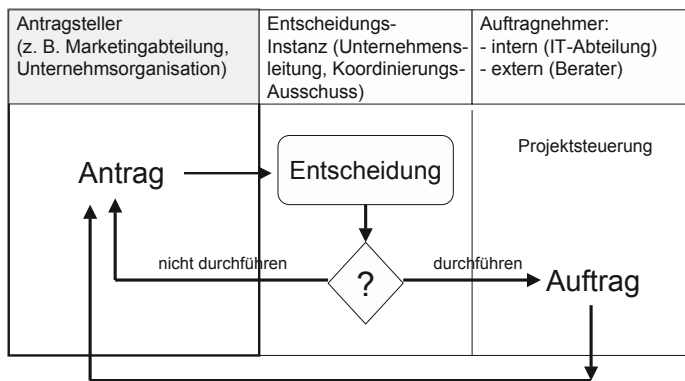


ABBILDUNG 5.2
Projekt-Genehmigungsverfahren (Beispiel)

Die Art und Weise, wie erste Projektideen offiziell vorgestellt werden, ist in Organisationen mit ausgereifter Projekt-Infrastruktur in der Regel im Detail vorgegeben. Dabei stellen geeignete Formulare und Checklisten sicher, dass wichtige Fragen, die zur Bewertung und Entscheidung über die Umsetzung der Idee notwendig sind, beantwortet werden.



Fragen, die bei der Projektselektion zu bearbeiten bzw. zu prüfen sind:

- Ist das IT-Projekt hinsichtlich der technischen Komplexität überhaupt beherrschbar?
- Besteht tatsächlich ein echter Bedarf an den Projektergebnissen? (Analyse der Kundenwünsche, Prüfung der Konkurrenzsituation, etc.)
- Können durch dieses Projekt die operativen Kosten merklich gesenkt werden? Ist der erwartete Nutzen hoch genug? Mitunter kann hier der Return on Investment (das Ergebnis der Wirtschaftlichkeitsbeurteilung) herangezogen werden.

- Stehen überhaupt genügend Ressourcen zur Verfügung, um das beantragte IT-Projekt durchführen zu können (ausreichende Anzahl qualifizierter Personen, genügend Finanzmittel)?
- Steht das IT-Projekt im Zusammenhang mit anderen (wichtigen) Projekten? Welche Vor- bzw. Folgeprojekte sind zu dem vorgeschlagenen Projekt notwendig? Ein Projekt „Mitarbeiterportal“ steht beispielsweise in Abhängigkeit zu verschiedenen weiteren IT-Projekten (Datenbanklösungen, Dokumentenmanagement, Web-Auftritt etc.).
- Was geschieht nach dem eigentlichen Projekt?
- Welche Auswirkungen sind zu erwarten, wenn das Projekt nicht durchgeführt wird? Zu prüfen sind etwa die Auswirkungen auf die Kosten-/Nutzensituation sowie die Auswirkungen in personeller Hinsicht.

Um eine klare und akzeptierte **Priorisierung der möglichen IT-Projekte** vorzunehmen, sollten spezifische Techniken verwendet werden. Die am häufigsten eingesetzten Varianten zeigt Tabelle 5.5:

TABELLE 5.5 Verfahren für die Priorisierung von IT-Projekten

Verfahren	Kennzeichnendes Merkmal
Rangfolgeverfahren im Entscheidungsteam (Koordinierungsausschuss)	Teammitglieder bewerten die zur Wahl stehenden Projekte und stellen eine Rangfolge der Notwendigkeit/Wünschbarkeit auf.
ABC-Technik	Eingereichte Projekte werden entweder als A-, B- oder C-Projekt eingestuft. A-Projekte sind von besonders hoher Bedeutung und sollten in jedem Fall durchgeführt werden.
Portfoliotechnik	Es wird ein Handlungsportfolio erstellt, wobei eine gründliche Einschätzung nach zwei Hauptmerkmalen – etwa strategische Projektrelevanz und Wirtschaftlichkeit – erfolgt.

Bei Anwendung des **Rangfolgeverfahrens** erfolgt eine Priorisierung, indem aus den zur Wahl stehenden Alternativen eine Rangfolge durch die Mitglieder des Projektteams gebildet wird. Diese Rangfolgebildung sollte möglichst von jedem Mitglied des Entscheidungsgremiums selbstständig vorgenommen werden. Die Rangordnung der Projekte ergibt sich dann aus der Summierung der Daten der verschiedenen Teammitglieder.

Die **ABC-Technik** versucht eine Verfeinerung vorzunehmen, indem IT-Projekte von der IT-Leitung oder dem Auswahlgremium einer der drei Klassen zugeordnet werden:

- A = Projekt von hoher Bedeutung und besonderer Dringlichkeit,
- B = Projekt von mittlerer Bedeutung,
- C = Projekt von minderer Bedeutung und Dringlichkeit.

Nützlich ist dabei eine möglichst klare Spezifizierung von Kriterien zur Festlegung der Bedeutung und Dringlichkeit.

In der Praxis hat sich darüber hinaus die Fixierung der Überlegungen in Form von **Handlungsportfolios** als hilfreich erwiesen. Hier werden die strategischen Alternativen fixiert und

visualisiert. Dazu können die alternativen Projekte zunächst nach einzelnen Kategorien (z. B. monetären Kriterien, effizienzbezogenen Kriterien, effektivitätsbezogenen Kriterien) in verschiedenen Teilportfolios positioniert werden. Dabei werden beispielsweise die Wirtschaftlichkeits- und Nutzenbeurteilungen anhand einer Bewertungsskala zur strategischen Relevanz des Projektes in Beziehung gesetzt. Um daraufhin zu einer endgültigen Positionierung der Alternativen zu gelangen, müssen die unterschiedlichen Portfolios zusammengefasst werden. Hierfür ist es sinnvoll, die unterschiedliche Bedeutung der Beurteilungsklassen durch Gewichtungsfaktoren darzustellen und durch Aufrechnung eine generelle Positionierung zu erreichen.

Zwei wesentliche Kategorien von Priorisierungskriterien werden unterschieden (siehe auch Abbildung 5.3):

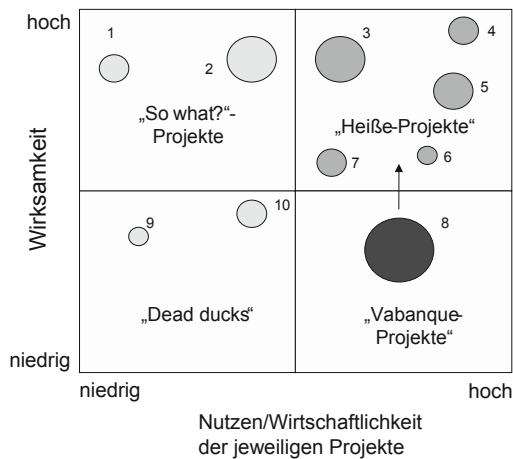


ABBILDUNG 5.3

Portfolio-Analyse für die Projektpriorisierung

- an **Wirtschaftlichkeit** orientierte Kriterien: Aus der Nutzung von Projektergebnissen ist über die investierten Entwicklungskosten und die laufenden Betriebskosten hinaus ein angemessenes Ergebnis zu erwirtschaften.
- an **Wirksamkeit/Risikograd** orientierte Kriterien. Hierunter können vor allem betriebswirtschaftliche Nutzenkomponenten verstanden werden; wie Serviceverbesserungen, aktuelle Informationen, bessere Entscheidungsbasis, höhere Mitarbeitermotivation, Erlangung von Wettbewerbsvorteilen, Imageverbesserung, Sicherheitserhöhung in der Geschäftsabwicklung.

Ziel der Bewertungsüberlegungen sollte ein Projektportfolio sein, in dem strategische und wirtschaftliche Projekte in einem ausgewogenen Verhältnis stehen.



Beachten Sie:

Neben den Kriterienkategorien müssen in das Priorisierungsverfahren auch die Erfolgsposition des Geschäftssegments und die diesbezüglichen Unternehmensziele einfließen. Hier wird dann eine Einordnung nach der geschäftlichen (strategischen) Relevanz vorgenommen.

5.2.2 Wirtschaftlichkeitsbeurteilung von IT-Projekten

Ohne eine **Skizzierung der Kosten-/Nutzenaspekte** ist heute ein IT-Projekt kaum noch realisierbar. In besonderer Weise ist ein Projektantrag daraufhin zu prüfen, ob das beantragte Projekt wirtschaftlich ist und wie es finanziert werden kann. Ein Projekt kann demnach auch immer als Investitionsvorhaben betrachtet werden (Business-Case-Analyse). Der **Kostenaspekt** lässt sich dabei leichter ermitteln. Mitunter können Erfahrungen aus vorherigen Projekten herangezogen werden. Problematischer (weil nicht unbedingt quantifizierbar) sind die **Nutzenaspekte**.

Für die Wirtschaftlichkeitsbeurteilung eines Projektes ist es zunächst notwendig, die kalkulatorische Nutzungsdauer der Projektergebnisse abzuschätzen. Dies ist die erwartete oder beabsichtigte Nutzungsdauer der durch die Projektarbeit hervorgebrachten neuen IT-Lösungen bis zur Gesamtablöse bzw. Generalüberholung (z. B. Ablöse der bisherigen Lösung).

Die durch das geplante Projekt angestrebte Lösung wird **zunächst immer isoliert** für sich betrachtet und die Daten separat erhoben (kalkulatorische Nutzungsdauer, Anschaffungsausgaben, laufende Einnahmen und laufende Ausgaben). Daraus werden die entscheidungsrelevanten Ergebnisse errechnet (Gesamtergebnis am Ende der Nutzungsdauer, Amortisationsdauer im Verhältnis zur Nutzungsdauer und Rentabilität).

Zusätzlich wird das absolute Ergebnis jeder untersuchten Projektlösung mit dem Ergebnis der Ist-Variante verglichen und dargestellt (relatives Ergebnis). Damit kann festgestellt werden, um wie viel günstiger bzw. ungünstiger die untersuchte Projektlösung finanziell im Vergleich mit einer Fortschreibung des Ist-Zustandes abschneidet.

Einen Überblick der verschiedenen **Verfahren zur Wirtschaftlichkeitsbeurteilung** von IT-Projekten gibt Abbildung 5.4.

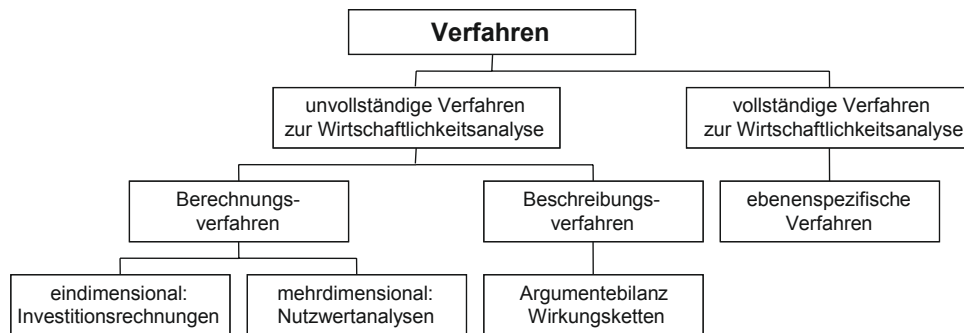


ABBILDUNG 5.4 Verfahren zur Wirtschaftlichkeitsanalyse

- Dies sind einmal die Verfahren der betriebswirtschaftlichen Investitionsrechnung (etwa die Kostenvergleichsrechnung sowie die Amortisationsrechnung).
- Eine andere Option ist die Anwendung der Nutzwertanalyse, die versucht, neben finanziellen Kriterien auch besondere (etwa qualitative) Nutzengrößen zu quantifizieren.
- Eine weitere Variante ist der Verzicht auf reine Berechnungen und die Konzentration auf die Beschreibung der Wirkungen der neuen Lösungen (Argumentebilanz mit der Darstellung von Wirkungsketten).

Abbildung 5.5 zeigt ein Beispiel für ein Formular zur Wirtschaftlichkeitsberechnung.

Wirtschaftlichkeits-Rechnung		Projekt: Ersteller:	
Berechnungsgrundlage			
1. Totalausgaben des Projekts			
2. Mit dem Projekt verbundene Wiederverkaufserlöse			
3. Durch das Projekt abzuschreibende Restbuchwerte			
4. Saldo			3.-2.
5. Berechnungsgrundlage			1.+4.
6. Abschreibungsdauer			Jahre
7. Abschreibungen pro Jahr			5./6.
8. Ertragssteuersatz			%
Voraussichtliche Einsparung/Jahr		Personal	Sachkosten
9. Aktuelle Kosten/Jahr			
10. Zukünftige Kosten/Jahr			
11. Durchschn. Einsparung p.a.	9.-10.		
Wirtschaftlichkeit		12./vor Steuern	13./nach Steuern
12./13. Kalkulation des Ertrages	11.-7.	12.-(12*8.)	
14. Durchschn. Einsparung p.a. nach Steuern		11.-(12*8.)	
15./16. Rückflussdauer (Jahre)	15.=5./11.	16.=5./14.	
17./18. Rentabilität (%)	17.= 12./0.5*5.	18.= 13./0.5*5.	

ABBILDUNG 5.5
Formular zur Wirtschaftlichkeitsberechnung

Hinsichtlich der **Finanzierungsfrage** ist zu unterscheiden, ob es sich um externe Kunden oder interne Auftraggeber handelt:

- Bei **externen Kunden** erfolgt die Finanzierung dadurch, dass diese eine Zahlung an den Auftragnehmer leisten (sei es als Teilzahlungen bei Projekten mit längerer Laufzeit oder als Gesamtzahlung).
- Handelt es sich um einen **internen Auftraggeber** für das Projekt (Fachabteilung, Geschäftsführung), muss geprüft werden, aus welchem Budget die IT-Projekte finanziert werden können. Die Beantwortung der Frage hängt natürlich auch von der Positionierung der IT-Abteilung im Unternehmen ab, also davon, ob sie als Cost-Center oder als Profit-Center geführt wird.



Beachten Sie:

Im späteren Projektverlauf muss dann durch ein konsequentes Projektcontrolling die Liquidität des Projektes sichergestellt werden. Dazu sind die Ein- und Ausgänge der Zahlungen ständig zu überwachen, sodass bei Liquiditätsengpässen rechtzeitig eingegriffen und entsprechende Maßnahmen durchgeführt werden können.

5.2.3 Der Projektauftrag als Grundlage für die Projektarbeit

Ist die Entscheidung für die Durchführung eines IT-Projektes positiv gefallen (das Projekt wurde also genehmigt), muss noch ein entsprechender **Projektauftrag** ausformuliert werden.



Inhalte eines Projektauftrags:

- die Aufgabenstellung des Projektes sowie die damit verbundenen Zielsetzungen und erwarteten Ergebnisse;
- die verschiedenen Rollen und verantwortlichen Entscheidungsgremien;
- das bei der Projektgenehmigung vereinbarte Projektbudget sowie
- alle Rahmenbedingungen, unter denen das Projekt durchzuführen ist.

Dabei können weitgehend die im Projektantrag festgehaltenen Informationen als Basis genommen werden. Außerdem sind die Anregungen und Vorgaben aus den Gutachten und dem Entscheidungsgremium einzuarbeiten.

Es empfiehlt sich, die hier getroffenen Festlegungen genau zu lesen und im Projektteam ausführlich zu besprechen. Dabei ist zu berücksichtigen, dass insbesondere die Festschreibungen zu dem angestrebten Endzustand Größen darstellen, die in der laufenden Projektarbeit immer wieder Gegenstand von Auseinandersetzungen sein können.

Außerdem ist zu beachten, dass zum Zeitpunkt der Fixierung des Projektauftrages noch nicht alle Details übersehen werden können. So stellt sich mitunter erst im Verlauf der Projektarbeit heraus, dass die Projektarbeit sehr stark mit anderen Fragestellungen verwoben ist, die eigentlich zuvor hätten geklärt werden müssen und ohne deren Beantwortung das laufende Projekt nicht vorankommt.

5.2.4 Projektaufträge erfolgreich umsetzen

Projektmanagement ist das Management von komplexen Problemlösungsprozessen. Unabhängig von Projektart und Projektgröße hat es sich bewährt, das **Durchführungsmanagement von Projekten** in vier Hauptabschnitte einzuteilen.



Die vier Hauptabschnitte der Projektdurchführung:

- Startphase (Projektvorbereitung),
- Analyse und Entwurfsphase (Think, Design),
- Realisierung (Enable) sowie
- die Einführung (Run).

Diesen Abschnitten können nun bestimmte Projektmanagementaufgaben zugeordnet werden. Eine mögliche Zuordnung zeigt Abbildung 5.6 (nächste Seite).

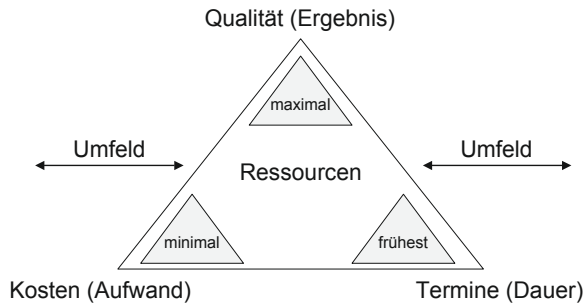
Projektphasen/ Betrachtungs- objekte	Startphase (Vorbereitung)	Analyse und Entwurfsphase (Think, Design)	Realisierung (Enable)	Einführung (Run)
Methoden und Instrumente	Projektdefinition (Zielklärung, Grobplanung, Wirtschaftlichkeit, Projektauftrag)	Projektplanung (Feinplanung der Arbeits- pakete, Termine, Kosten, Ressourcen)	Projektkontrolle und Projektsteuerung	Projektabschluss und -auswertung (Evaluation)
Projekt- Teamarbeit (soziale Aspekte)	Auswahl des Projektteams	Teament- wicklung (Teamkultur)	Meeting- Management, Konflikt- management	Auflösung des Projektteams, Reintegration der Mitarbeiter
Projekt- organisation	Rollendefinition (Teams, Ausschüsse)	Aufgaben- verteilung	Einbettung von - Controlling - QS - externe	Abschlussbericht und Abschluss-Sitzung
Projektumfeld	Stakeholder- analyse	Projekt- marketing	Claim- Management, Change- Management	Produktübergabe, Abnahme beim Kunden, Präsentation

ABBILDUNG 5.6 Übersicht über Phasen und Projektmanagementaufgaben

Welchen **Nutzen** bringt die konsequente **Anwendung des Projektmanagements**?

- Die bei der Projektrealisierung anfallenden Aufgaben werden transparenter und überschaubarer.
- Problemsituationen können rechtzeitig erkannt werden. So kann rasch auf sich ergebende Chancen und Bedrohungen reagiert werden.
- Es fällt den Beteiligten nicht so schwer, zielorientiert zu handeln, da klare Vorgaben fixiert und den Betroffenen bekannt sind.
- Durch die Benennung eines Projektleiters sowie von Verantwortlichen für Teilaufgaben (Arbeitspaketen) ergibt sich eine personifizierte Verantwortung.
- Durch Übertragung anspruchsvoller Projektaufgaben kann die Personalentwicklung und die Motivation der Projektmitarbeiter gefördert werden.
- Insgesamt ergeben sich durch ein gezieltes Management der Projektarbeit qualitativ bessere Arbeitsergebnisse.

Das Projektmanagement muss bei der Durchführung von Projekten immer drei zentrale Zielgrößen im Auge behalten: Qualität, Termine, Kosten (sog. magisches Dreieck des Projektmanagements). Diese gelten durchgängig für die Planung, die Steuerung und die Kontrolle. Wird eines dieser Ziele gefährdet, wirkt sich das auch auf die anderen Ziele aus. Wird beispielsweise an der „Kostenschraube“ gedreht, kann sich dies gegebenenfalls unmittelbar auf die Qualität der Projektergebnisse auswirken. Den Zusammenhang verdeutlicht Abbildung 5.7.

**ABBILDUNG 5.7**

„Magisches Dreieck“ des Projektmanagements

■ 5.3 IT-Projekte starten

Mit der Genehmigung eines IT-Projektes kann die eigentliche Arbeit beginnen. „So wie Sie starten, liegen Sie im Rennen“, dieser Satz gilt insbesondere auch für erfolgreiche Projekte. Um einen gelungenen Projektstart „hinzulegen“, sind zum Projektbeginn folgende **Handlungen und Entscheidungen** unerlässlich:

- **Durchführung von Startveranstaltungen**, etwa eines **Start-up-Workshops** mit dem Projektteam und eines **Kick-off-Meetings** als Informationsveranstaltung für alle vom Projekt betroffenen Personengruppen.
- **Entwicklung von Projektvisionen**, um dem IT-Projekt eine klare Orientierung zu geben.
- **Präzisierung und Fixierung der Projektziele**. Im Projektauftrag sind die groben Projektziele vorgegeben. Diese müssen nun vom Projektteam weiter konkretisiert werden. Dazu ist unter Umständen eine unmittelbare Abstimmung mit dem Projekt-Auftraggeber sinnvoll.
- **Durchführung einer Projektumfeldanalyse**. Durch die Identifikation und Analyse der Einflussnehmer auf das Projekt bzw. eine systematische Analyse der von den Projektergebnissen Betroffenen lassen sich geeignete Maßnahmen für die Information und Schulung, für das Projektmarketing sowie für die Vereinbarung von Rahmenbedingungen (etwa rechtlicher Art) ableiten.
- **Festlegung der Projektphasen und der wichtigsten Meilensteine**. Im Ergebnis ergibt sich eine erste grobe Projektterminplanung. Hierzu gehören auch die Konkretisierung der Aufgabenstellung sowie eine Präzisierung der gewünschten Projektergebnisse.

5.3.1 Start-up-Workshop/Kick-off-Meeting

Gerade zu Beginn eines Projektes kommt der Motivation und der Vereinbarung von Kooperationsformen für die Mitglieder des Projektteams eine besondere Bedeutung zu. Außerdem sind alle von den Projektergebnissen künftig Betroffenen sowie die in die Projektarbeit einzu-

beziehenden Personen vorab in ausreichender Weise zu informieren. Es hat sich bewährt, **zwei Arten von Startveranstaltungen** durchzuführen:

- einen **Start-up-Workshop** mit dem Projektteam sowie
- eine Informationsveranstaltung für alle Betroffenen (= **Kick-off-Meeting**).

Gut vorbereitet und professionell durchgeführt, werden mit einem **Projekt-Start-up-Workshop** die ersten Grundlagen für ein erfolgreiches Projekt gelegt. Insbesondere kann ein Start-up-Workshop dazu beitragen, dass

- sich die Mitglieder des Projektteams näher kennen lernen (auch persönliche Erfahrungen und Ziele können angesprochen werden);
- sich ein „Wir-Gefühl“ im Projektteam entwickelt;
- eine erste Rollenverteilung im Projekt vorgenommen wird;
- mögliche Risiken und Konflikte für die Projektarbeit schon in der Startphase erkannt werden;

Das **Kick-off-Meeting** wird in der Regel von der Projektleitung bzw. in Kooperation mit dem Projektteam vorbereitet und unterscheidet sich vom Start-up-Workshop einmal durch die Teilnehmergruppe. Teilnehmen sollten daran neben der Projektleitung und dem Projektteam

- Vertreter des Auftraggebers (bei externen Projekten Vertreter des Kunden),
- die Leitung der durchführenden Institution (etwa ein Sponsor aus der Unternehmensführung) sowie
- die wesentlichen Projektinteressenten und Personen, die von den Projektergebnissen betroffen sind (Stakeholder).

Ziel der Kick-off-Veranstaltung ist es, dass Auftraggeber und Projektleitung gemeinsam den Betroffenen einen Überblick über das anstehende Projekt geben sowie die Gelegenheit eröffnen, alle relevanten Fragen zu dem neuen Projekt zu klären. So sollen insbesondere im Vorhinein schon eine gewisse Abklärung geschaffen und eine Aufbruchstimmung für die Projektarbeit erzeugt werden, um über die gesamte Projektlaufzeit möglichst erhalten zu bleiben.

5.3.2 Projekt-Visionen entwickeln

Eine Orientierung der Projektarbeit an Visionen und Zielen stellt eine wesentliche Basis für den Projekterfolg dar:

- Eine Vision vermittelt allen Projekt-Beteiligten und Projekt-Betroffenen eine Vorstellung, wo die Reise im Projekt hingeht. Sie haben als Folge davon das Gefühl, an einer wertvollen Sache mitzuwirken.
- Für die Projektmitarbeiter wird darüber hinaus eine positive Grundstimmung erzeugt. Die strategische Stoßrichtung des Projektes wird deutlich, und damit werden die im Projekt anfallenden und übertragenen Aufgaben gerne übernommen, und es wird als lohnend angesehen, sich entsprechend zu bemühen.
- Es entwickelt sich ein „Wir-Gefühl“ unter den Personen im Projektteam. Die Vision wird so zur Grundlage eines gleichgerichteten Verhaltens aller im Sinne des Gesamtprojektes.

- Für die Erreichung der Projektergebnisse ergeben sich neue Impulse. Letztlich kann so ein erfolgreiches Projektmanagement betrieben werden.

Ergebnis des Visionen-Entwicklungsprozesses sollten dokumentierte Überlegungen sein, die Formulierungen einer umsetzbaren Vision unter Berücksichtigung späterer Ausbaustufen enthalten. Dazu gehören:

- die Darlegung der Rahmenbedingungen;
- das Formulieren einprägsamer Visionsgrundsätze für die Projektarbeit;
- die Erarbeitung einer Vision-Map (etwa unter Berücksichtigung einer Zeitachse oder in Form eines Mindmaps).

Eine Vision-Map für das jeweilige IT-Projekt macht die Richtung der Projektarbeit für die Beteiligten und Betroffenen deutlich. Ein Beispiel mit einer Differenzierung nach kurz-, mittel- und langfristigen Orientierungen sowie der Formulierung der Vision gibt für das Beispielprojekt „Mitarbeiterportal“ Abbildung 5.8.

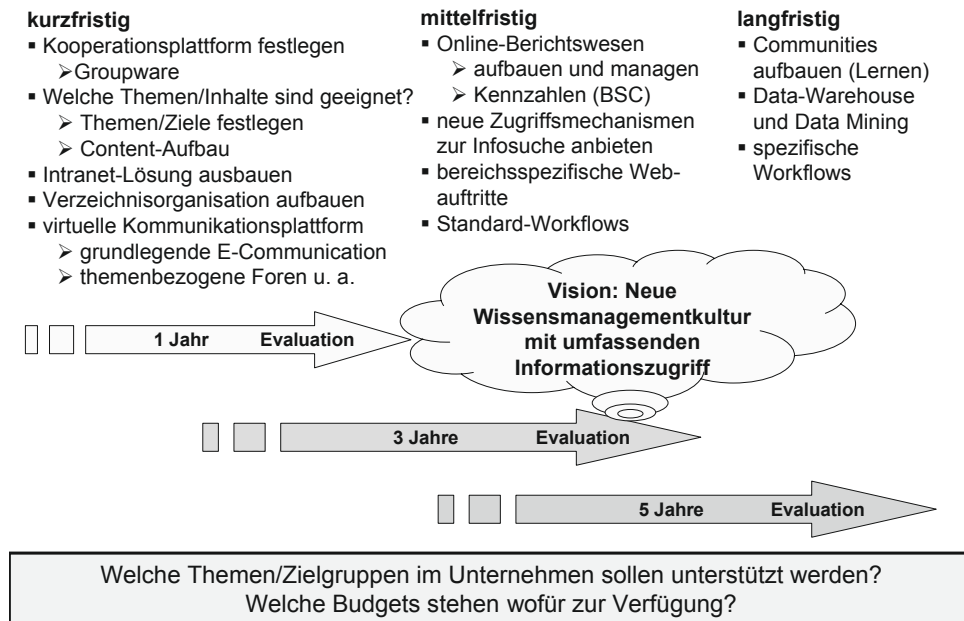


ABBILDUNG 5.8 Vision-Map „Portalprojekt“



Beachten Sie:

Prüfen Sie, ob Sie selbst und Ihr Projektteam über ausreichende Visionen verfügen. Kommen Sie zu einem negativen Ergebnis, sollten Sie aktiv werden und überlegen, welche Veränderungen möglich sind. Beachten Sie außerdem, dass eine Vision nicht nur gedacht werden darf. Sie muss vielmehr auch kommuniziert und durchgesetzt werden. Tun Sie dazu das Ihnen Mögliche!

5.3.3 Stakeholderanalyse und Stakeholdermanagement

Viele gute Projektideen scheitern schon in der Frühphase an einem kleinen Detail: Die Betroffenen – das können beispielsweise Kunden oder Mitarbeiter aus anderen Abteilungen sein – werden zu spät oder unzureichend über das Projekt und mögliche Veränderungen informiert. Die Folge: sie fühlen sich übergangen, „mauern“, und das Projekt „geht baden“. Daher ist es unabdingbar, wenn die Projektleitung schon frühzeitig das Projektumfeld (sog. Stakeholder) analysiert und wichtige Personen/Personengruppen „mit ins Boot holt“.

Vielfältige Erfahrungen zeigen, dass IT-Projekte dann leichter zum Erfolg geführt werden, wenn die Projektleitung und das Projektteam das so genannte Projektumfeld bereits zu Beginn des Projektes in die Planungs- und Gestaltungsüberlegungen einbezieht. Erwartungen und Hindernisse können so frühzeitig erkannt werden.

Im Einzelnen sind bei der Umfeldanalyse folgende **Aktivitäten** notwendig:

- Ganzheitliche und frühzeitige Erfassung aller Einflussfaktoren auf ein IT-Projekt
- Identifikation von Potenzialen und Problemfeldern eines IT-Projekts
- Beurteilung der Konsequenzen für die Projektdurchführung
- Feststellung der Abhängigkeiten von anderen Aufgaben und Projekten im Unternehmen
- Verbesserung der Kommunikation im IT-Projekt durch grafische Darstellung von Umfeldbeziehungen
- Ableitung von Maßnahmen zur Optimierung von Umfeldbeziehungen (Projektmarketing)



Beachten Sie:

Grundsätzlich ist beim Projekt-Design darauf zu achten, dass alle wichtigen Stakeholder eingebunden werden, um die Projektziele zu kommunizieren und die Ansprüche der Zielgruppen frühzeitig berücksichtigen zu können. Die Ermittlung dieser Ansprüche ist ein wichtiges, ja sogar unerlässliches Instrument, um einen Projekterfolg sicherzustellen. Dennoch sollte man nicht zu sehr ins Detail gehen, sondern versuchen, sich auf die wesentlichen Gruppen und ihre Hauptansprüche zu konzentrieren.

Bewährt hat sich im Rahmen einer Projektumfeldanalyse das Instrument der **Stakeholderanalyse**. Als Stakeholder werden die Anspruchsgruppen und -personen bezeichnet, die unmittelbaren Einfluss auf den Projektfortschritt haben und/oder von den Projektzielen direkt oder indirekt betroffen sind. Folgende **Schritte** sind zur Durchführung einer Stakeholderanalyse in Angriff zu nehmen:

1. **Identifikation der Stakeholder und ihre Gliederung.** Ausgehend vom Projektauftrag sind zunächst alle Personen und Gruppen zu ermitteln, die Interesse an dem Projekt bzw. den Projektergebnissen haben oder davon in irgendeiner Weise betroffen sind. Dabei sollte auch eine erste Gliederung vorgenommen werden. Eine Orientierung zur Identifikation der Stakeholder und ihre Gliederung in einem Projekt gibt Abbildung 5.9.

Aus der Klärung der Anspruchsgruppen und ihren jeweils zentralen Ansprüchen können die speziellen Ansprüche für das in Angriff zu nehmende Projekt abgeleitet werden.



ABBILDUNG 5.9 Stakeholder-Identifikation und ihre Ansprüche

2. **Bewertung der Stakeholder** (evtl. unter Nutzung vorliegender Erhebungen im Projektteam). In einem Ranking kann die Bewertung des Einflusses der Anspruchsgruppen in einer Zahl (beispielsweise Skala von 1 (nicht sehr wichtig) bis 5 (äußerst wichtig)) vorgenommen werden. Ziel einer solchen zu einem bestimmten Zeitpunkt durchgeführten Bewertung ist es, die wesentlichen von weniger bedeutenden Einflussgruppen zu unterscheiden und in der Folge das Hauptaugenmerk auf die Stakeholder mit einem hohen Ranking zu legen.
3. **Auftrag/Zielsetzungen:** Um anschließend die zentralen Ansprüche genauer zu ermitteln, kommen verschiedene Methoden und Instrumente in Betracht. Vor Beginn eines Projektes können die Ansprüche der verschiedenen Gruppen durch quantitative Analysen, Prozessanalysen und Interviews mit Betroffenen ermittelt werden. Die meisten Ansprüche entstehen aber erst im Laufe der Projektarbeit.
4. **Analyse der Chancen und Risiken**, die die jeweiligen Stakeholdergruppen in dem Projekt sehen. Die entscheidende Frage ist natürlich die Analyse, inwieweit die Stakeholder das Projekt unterstützen oder – im anderen Extremfall – auch dagegen opponieren.
5. **Maßnahmenfestlegung:** Abhängig von der Bewertung sowie den Analyseinformationen sind daraufhin verschiedene Maßnahmen und Strategien für die weitere Projektarbeit zu entwickeln. Die möglichen Maßnahmen, die aus der Analyse der Stakeholder abgeleitet werden können, lassen sich folgenden Bereichen zuordnen:
 - Veröffentlichungen in der Mitarbeiterzeitung oder über einen Newsletter;
 - Informationen im Intranet bzw. Internet;
 - Besondere Informationsveranstaltungen (etwa Kick-Off im Corporate TV, Online-Chat mit Vorstand);
 - Einbindung der Führungskräfte und dezentraler Multiplikatoren durch Präsentation des Projektes in Sitzungen der Führungsgremien;
 - Absicherung durch rechtliche Vereinbarungen (etwa mit dem Betriebsrat).
6. **Dokumentation der Stakeholderanalyse:** Für die Dokumentation sind die folgenden Informationen in einer Tabelle zusammenzustellen:
 - Identifikation nach Rolle, Name, Funktion
 - Analyse und Klärung von Auftrag und wesentliche Zielsetzungen der jeweiligen Stakeholder

- Betroffenheit der Stakeholder durch das Projekt (High-Middle-Low = ABC im Hinblick auf Interesse und Einfluss bezüglich des Projektes)
- Analyse der Stakeholder nach Chancen/Interessen durch das Projekt
- Analyse der Stakeholder nach persönlichen Risiken und möglichen Konfliktpotenzialen
- Maßnahmen/Konsequenzen für die weitere Projektarbeit

Ergebnis kann eine Stakeholderliste (Tabelle) sein, wie sie Abbildung 5.10 zeigt.

Name, Funktion	Auftrag, Ziele	Bewertung (Stärke)	Chancen, Interessen	Risiken, Konfliktpotentiale	Maßnahmen
Unternehmensführung	unterstützt Projekt	Interesse: hoch Einfluss: hoch	möchte Wissensmanagement im Unternehmen fördern; Kostensparnisse	hohe Erwartungshaltung	fortlaufende Information über Projekt-Ergebnisse und Projekt-Fortschritte
Leiter der Fachabteilungen	effiziente und effektive Arbeit in den einzelnen Funktionsbereichen sicherstellen	Interesse: vermutlich vorhanden; Einfluss: hoch	bessere Führungsinfos; verbesserte Wissensorganisation und Workflow im Unternehmen führt zur Leistungssteigerung bei der Sachbearbeitung; Instrument der Mitarbeiterqualifizierung	Unsicherheit über die Kultur des Wissensmanagements bei Mitarbeitern und im Management	Informationsgespräche mit den Abteilungsleitungen; vertrauensbildende Maßnahmen durch gemeinsames Treffen und lfd. Information
betroffene Sachbearbeiter in den Fachabteilungen	hervorragende Arbeitsleistungen erbringen	Interesse: muss geweckt werden Einfluss: mittel	Neue Möglichkeiten eröffnen neue Informationschancen, Mittel zur Aktualisierung von Wissensbeständen (individuell, kollektiv)	technische Voraussetzungen müssen gegeben sein; Interesse wahrscheinlich sehr unterschiedlich, Hemmschwellen denkbar	Information und Schulung, Vorteile der neuen Möglichkeiten darstellen, Anforderungen abfragen
Personalabteilung	Personalmanagement und Personalentwicklung,	Interesse: hoch Einfluss: mittel bis hoch	besondere Profilbildung für die Personalentwicklung, effizientes Instrument der Personalentwicklung	Unsicherheit, was das Projekt bringt	vertrauensbildende Maßnahmen, enge Kooperation suchen, Vorteile darstellen
Betriebsrat	Sicherheit und Datenschutz („Wer darf welche Daten sehen?“)	Interesse: hoch, da Personalfragen unmittelbar betroffen Einfluss: mittel bis hoch	Information und Einwilligung der Mitarbeiter	Mitbestimmungspflicht bei Mitarbeiterqualifizierung, Arbeitszeitausgleich/Überstundenregelung, Rationalisierungseffekte/ Stellenabbau	Einbezug bei bestimmten Entscheidungen und Information über Projektfortschritte

ABBILDUNG 5.10 Stakeholdertabelle (Beispiel)



Praxistipps:

Da die Umfeldanalyse eine Momentaufnahme ist, müssen Sie den Betrachtungszeitpunkt festlegen, weil sonst die Meinungen im Team sehr stark auseinander gehen. Unter Umständen ist die Stakeholderanalyse in späteren Projektphasen zu wiederholen.

Formulieren Sie den als Ergebnis einer Umfeldanalyse entstehenden Maßnahmenkatalog so operativ wie nur möglich. Jede Maßnahme sollte einer Person oder Gruppe zur Erledigung bis zu einem definierten Zeitpunkt übertragen werden.

Es empfiehlt sich, die Umfeldanalyse in jedem Fall zum Projektstart als Teil der Projektplanung durchzuführen (Basisanalyse). Nach Abschluss wichtiger Projektphasen (zu den Meilensteinterminen) ist es außerdem nützlich, wenn die Umfeldanalyse aktualisiert wird. Der Vergleich zwischen den Ergebnissen der Basisanalyse und den aktuellen Daten liefert auch wertvolle Informationen für eine aktive Projektsteuerung.

5.3.4 Projektziele präzisieren

Bereits in der Phase der Projektvorbereitung wurde eine grobe Zielplanung vorgenommen. Um ein Projekt erfolgreich durchführen zu können, ist diese Zielvorgabe aber oft zu unpräzise. In der Startphase müssen deshalb für die weitere Projektarbeit die Ziele nun weiter konkretisiert und in Kommunikation mit dem Projektteam vereinbart werden.

Wie gelangt ein Projektteam zu den „richtigen“ Zielen? Wichtig ist, dass das Bilden von Zielen als ein dynamischer und sozialer Prozess gesehen wird. Ziele müssen gemeinsam zwischen Beteiligten und Betroffenen erarbeitet und mit dem Erkenntnisfortschritt angepasst werden; nur dann können sie wirksam als Handlungsgrundlage für alle Projekt-Beteiligten vereinbart werden. Dabei sind – wie die Erfahrungen der Praxis zeigen – folgende Teilschritte und **Grundsätze** zu beachten:

1. Sammeln Sie die mit dem Projektergebnis angestrebten Ziele! (Wichtig: Projektziele sollen lösungsneutral sein, denn grundsätzliche mögliche Lösungen sollen nicht von vornherein ausgeschlossen werden.)
2. Gliedern Sie die Ziele, und entwickeln Sie damit ein entsprechendes Zielsystem! (Aber nicht mehr als 20 Ziele in einem Zielsystem!)
3. Formulieren Sie die Ziele möglichst operational, und fixieren Sie diese schriftlich! (Ziele müssen eindeutig nachvollziehbar, präzise, verständlich und leicht messbar formuliert sein. Die schriftliche Fixierung zwingt zu einer bewussten Entscheidung; lässt den Problemlöser nicht im „Regen“ der Beweisnot stehen.)
4. Prüfen Sie, ob die formulierten Ziele machbar sind! Ziele müssen realisierbar sein, gleichzeitig aber auch eine Herausforderung darstellen. (nicht überfordernd, aber auch nicht unterfordernd; unerreichbare Ziele können Handlungen nicht leiten).
5. Ziele sollen in ihrer Präferenz erkennbar sein. (Wichtiges soll im Vergleich zu Unwichtigem deutlich werden; Trennung von Muss- und Kann-Zielen ist mitunter sinnvoll.)



Beachten Sie:

Einmal vereinbarte Ziele müssen auch während der Projektabwicklung immer wieder überprüft werden, ob sie weiter verfolgt werden sollen oder ob eine Veränderung der Zielsetzungen sinnvoll ist. Gerade bei IT-Projekten mit längerer Projektdauer sind Veränderungen in den Rahmenbedingungen des Projektes nicht untypisch; diese können auch eine neue Vereinbarung bzw. Revision von Projektzielen erforderlich machen.

5.3.5 Phasengliederung und Meilensteine festlegen

Erfahrungen zeigen, dass sich für die **Planung und Steuerung der meisten IT-Projekte eine Gliederung** in Phasen als sinnvoll erweist. Abhängig vom Projektgegenstand können unterschiedliche Vorgehensmodelle sinnvoll sein. Jede Phase wird durch einen so genannten Meilenstein beendet. Die jeweiligen Meilensteine definieren klare Checkpoints, die letztlich sicherstellen, dass die im Projekt zu leistenden Aktivitäten zielgerichtet und zeitgerecht in der gewünschten Qualität abgewickelt werden.

Typische Projektphasen bei verschiedenen IT-Projekttypen sind im Folgenden skizziert:

Software-Entwicklungsprojekte:

- Visioning
- Ist-Aufnahme und Bedarfsermittlung (Anforderungsspezifikation)
- Grobplanung der Lösung
- Pilot-Realisierung
- Test und Abnahme

Software-Einführungsprojekte:

- Projektierung
- Fachliches Soll-Konzept (Plan)
- Design
- Realisierung (Build)
- Test
- Technische Implementierung und Integrationstest
- Organisatorische Implementierung (Run)

IT-Infrastrukturprojekte:

- Projektvorbereitung
- Ist-Analyse
- Zielplanung
- Soll-Konzeption
- Pilotanwendung
- Evaluierung der Pilotanwendung
- Umsetzung des Gesamtkonzeptes
- Schulung und Gesamt-Evaluation

Netzwerkprojekte:

- Projektplanung
- Konzepterstellung
- Vorbereitung
- Durchführung
- Nachbereitung

Welche Bedeutung haben Meilensteine im Projekt? Um wichtige Aufgaben und Termine (reviews) herauszuheben, sollten so genannte Meilensteine (milestones) definiert und gesondert dargestellt werden. Es handelt sich dabei um markante Zeitpunkte im Projektablauf, die üblicherweise keine Dauer besitzen. Es sind typischerweise Entscheidungssitzungen, die als Einschnitte zwischen Projektphasen die Projektarbeit strukturieren. Sie kennzeichnen – wie aus dem Namen schon hervorgeht – den Weg, den das IT-Projekt bereits genommen hat bzw. der noch vor ihm liegt. Damit liefern sie eine hervorragende Orientierung für die Projektbeteiligten, für den Projekt-Auftraggeber und auch für die Projekt-Stakeholder.

Durch Überprüfen der Meilensteine erhält der Projektleiter rasch einen Überblick über die zeitliche Abstimmung der einzelnen Phasen des gesamten Projektes. Gleichzeitig können Meilensteine auch dazu dienen, vor einem Projektklenkungsausschuss Rechenschaft darüber abzulegen, inwieweit das Projekt noch richtig auf Kurs ist.

Wie werden Meilensteine ausgewählt?

- Meilensteine sollten wichtige Ereignisse in dem Terminplan bilden. Dies ist beispielsweise der Abschluss einer umfangreichen Projektphase, der mit einer Präsentation oder einer Entscheidungssitzung repräsentiert sein kann.
- Meilensteine können außerdem eine wesentliche Zäsur beinhalten, indem sie logische Abschnitte kennzeichnen, wo auch inhaltliche Entscheidungen (beispielsweise „Stop or Go“-Entscheidungen des Auftraggebers) zu treffen sind oder Verantwortlichkeiten wechseln.
- Um aussagefähige Projekt-Statusberichte zu ermöglichen, ist es hilfreich, wenn die ausgewählten Meilensteine ein überprüfbares Ergebnis beschreiben (beispielsweise ein Zwischenprodukt zu definierten Kosten an einem bestimmten Termin).



Beispiel:

Die Verteilung der Meilensteine könnte am Beispiel des Projektes „Aufbau eines Mitarbeiterportals“ wie folgt aussehen:

1. Meilenstein:
Präsentation des genehmigten Projektvorschlages und Startup-Meeting
(großer Meilenstein)
2. Meilenstein:
Anforderungen analysieren; Bedarfe ermitteln; Konzept entwickeln; Abschluss der Konzept- und Designphase (kleiner Meilenstein)
3. Meilenstein:
Customizing durchführen; Abschluss der Produktionsphase (kleiner Meilenstein)
4. Meilenstein:
Entscheidung über die Maßnahmenplanung; Freigabe der Budgetmittel
(großer Meilenstein)
5. Meilenstein:
Testphase und Evaluation der entwickelten/adaptierten Softwaremodule zum Wissensmanagement und Workflow (kleiner Meilenstein)
6. Meilenstein:
Entwicklung weiterer Module; Abnahme der Ergebnisse (kleiner Meilenstein)
7. Meilenstein:
Projektabschlusspräsentation und Freigabe des Gesamtproduktes
(großer Meilenstein)

■ 5.4 Projektbeteiligte und Projektorganisation

Die vertrauensvolle Zusammenarbeit von Auftraggeber, Projektleitung, Projektteam, Entscheidungsträgern sowie den künftigen Nutzern der Projektergebnisse ist eine unverzichtbare Basis für eine erfolgreiche Projektarbeit. Dazu ist eine entsprechende Organisation erforderlich, die die Form der Koordination, Kommunikation und Kooperation zwischen den verschiedenen Beteiligten festlegt.

Zu Beginn eines jeden IT-Projektes ist deshalb die **organisatorische Einbindung** zu klären. Dazu zählen:

- eine Definition der wichtigsten Projektrollen (Auftraggeber des IT-Projektes, Projektleitung, Projektteam, am Projekt beteiligte Bereiche);
- eine Beschreibung der wesentlichen projektbezogenen Rollen;
- die Bildung des Projektteams (Zuordnung von Personen zu den Rollen);
- Darstellung der Projektaufbauorganisation (Projektorganigramm) sowie
- Vereinbarungen zum Informationsfluss im Projekt.

Kern eines jeden IT-Projektes ist eine **Projektgruppe**, die von Projektbeginn bis zur Auflösung des Projektes existiert. Die Projektgruppe arbeitet letztlich unter der Hauptregie des **Auftraggebers** für ein Projekt. Zu ihr gehören

- der IT-Projektleiter/die IT-Projektleiterin,
- Projektmitarbeiter (in Voll- oder Teilzeit) sowie
- eventuell externe Personen (wie Berater und andere Fachleute).

Bereits bei der Stakeholderanalyse wurde aber auch deutlich, dass ergänzend weitere Personen bzw. Personengruppen in die Projektarbeit einzubeziehen sind. So ist für den Projekterfolg auch eine Koordinierung und Abstimmung der oftmals unterschiedlichen Interessenten und Interessen notwendig. Neben dem Projektteam sind in jedem Fall von besonderer Bedeutung:

- Vertreter der Fachabteilungen
- Mitglieder der Unternehmensleitung
- abhängig vom Projektauftrag evtl. auch Beteiligte aus anderen Unternehmen (Kunden, Lieferanten, Logistikdienstleister, Agenturen etc.)

Entsprechend kann deshalb ergänzend die Bildung bestimmter Gremien (Lenkungsausschuss, Projektbeirat) notwendig sein. Hinzu kommt in größeren Organisationen die **Einrichtung spezieller Unternehmensinstanzen**; etwa ein so genanntes **Project Office** (mitunter auch als **Project Management Office** – kurz PMO – bezeichnet) zur Koordinierung verschiedener Projekte.

Eine Orientierung zu den **Beteiligten bei Projekten** zeigt Abbildung 5.11.

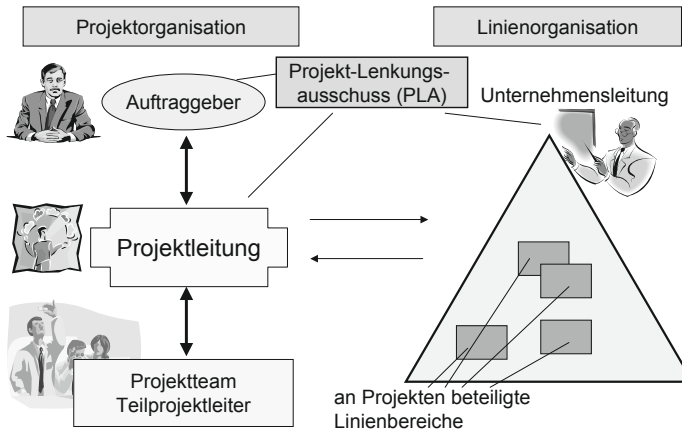


ABBILDUNG 5.11
Beteiligte im Projektmanagement

5.4.1 Der IT-Projektleiter – Aufgaben, Anforderungen und Befugnisse

Projekte – gleich welcher Art – benötigen eine Projektleitung, die die Hauptverantwortung für das Projektmanagement und die Projektdurchführung übernimmt. Die **Projektleitung** ist letztlich **verantwortlich**

- für das Erreichen der im Projektauftrag formulierten Projektziele;
- für das Einhalten des festgelegten Zeit- und Kostenrahmens;
- für den sach- und termingerechten Einsatz der Projektressourcen sowie
- für das Bereitstellen der Projektergebnisse gemäß den gesetzten Qualitätsanforderungen.

Die Projektleitung fungiert als Hauptansprechpartner für das jeweilige Projekt und stellt ein Bindeglied zwischen Auftraggeber, dem Projektteam und den übrigen am IT-Projekt beteiligten Personen und Bereichen dar.

Bezüglich der **Anforderungen an die Projektleitung** ist festzuhalten, dass ein Projektleiter in erster Linie nicht immer der beste Fachmann seines Projektteams sein muss. Er sollte vielmehr in der Lage sein, als integrierende und motivierende Kraft die beste Leistung mit dem Team zu bringen, Fachleute sachgerecht einzubeziehen und das Projektziel gradlinig zu verfolgen.

Bezüglich der wahrzunehmenden **Aufgaben** sowie der dabei erforderlichen **Befugnisse** soll Tabelle 5.6 auf der nächsten Seite eine Orientierung geben.

TABELLE 5.6 Aufgaben und Befugnisse der Projektleitung

Aufgaben eines IT-Projektleiters	Mindestbefugnisse eines IT-Projektleiters
▪ Abstimmung mit dem Auftraggeber des IT-Projektes ▪ Projektvorbereitung: ▪ Vorbereitung und Durchführung von Ausschreibungen ▪ Mitwirkung bei der Einrichtung der Projektorganisation ▪ Durchführung der Projektplanung (in Kooperation mit dem Projektteam) ▪ Abstimmung des Arbeitseinsatzes und der Arbeitsaufträge mit den Mitgliedern des Projektteams ▪ Vorbereitung, Durchführung und Leitung von Projektsitzungen ▪ Vorbereitung von Sitzungen des Steuerungsgremiums ▪ Projektsteuerung und Kontrolle des Projektfortschritts (Termine, Kosten, Arbeitsfortschritt, Qualität) ▪ Koordination des Projektablaufs ▪ Berichtswesen ▪ Organisation der Abnahme der Projektergebnisse	▪ Fachliche Anweisungsbefugnisse gegenüber Projektmitarbeitern ▪ Disziplinarische Anweisungsbefugnisse (wenn ein Projektleiter mit denselben Mitarbeitern über Jahre hinweg in Folgeprojekten zusammenarbeitet) ▪ Vorschlags- und Mitspracherecht für die Auswahl der Teammitglieder ▪ Übertragen von Projektaufgaben an die Projektmitarbeiter ▪ Mitspracherecht bei der Abwesenheitsplanung (beispielsweise Urlaubsplanung der Teammitglieder) ▪ Vorschlagsrecht für Aus- und Weiterbildung der Projektmitarbeiter ▪ Einleiten von Korrekturmaßnahmen bei Planabweichungen ▪ Lösung von Konflikten innerhalb der Projektgruppe



Beachten Sie:

Der **IT-Projektleiter** ist als **Schlüsselperson für den Projekterfolg** dem Projektlenkungsausschuss und über ihm den Auftraggebern verantwortlich. Er führt die Projektgruppe bzw. das Projektteam, unter Umständen mit Hilfe von Teilprojektleitern.

5.4.2 Das Projektteam – Rollenkonzept und Teambildung

Wer auf Dauer die Anforderungen erfüllen möchte, die an erfolgreiche Projektarbeit und die zu liefernden Projektergebnisse gestellt werden, wird die Ressourcen eines Projektteams benötigen. Gegenüber der Einzelarbeit hat das **Arbeiten im Team** gerade bei Projekten nämlich zahlreiche **Vorteile**:

- Durch Hinzuziehen unterschiedlicher Fachkräfte können fachübergreifende Aufgaben überhaupt erst gelöst werden.
- Ein gut funktionierendes Team erzielt Leistungen, die die Mitglieder für sich allein nicht fertigrbringen würden. Es ergibt sich eine bessere Problemlösung durch den kumulierenden Effekt unterschiedlicher Denkleistungen (Ausnutzung so genannter Synergieeffekte).

- Die Gruppe gibt einzelnen Teammitgliedern auch eine höhere Sicherheit und bedeutet damit oft eine verstärkte Motivation und größeres Engagement für jeden einzelnen.
- Wichtige Entscheidungen lassen sich im Team auf einer fundierten Basis treffen, sodass das Risiko von Fehlentscheidungen reduziert wird.

Nehmen Sie als Beispiel das Projekt „Aufbau eines Mitarbeiterportals“: Hier arbeiten Fachleute aus extrem unterschiedlichen Wissensgebieten zusammen: Fach- und Führungskräfte aus dem Personalwesen, Web-Designer, Texter/Content-Manager, Datenbankexperten und Programmierer sprechen jeweils eine eigene Sprache und betrachten das Projekt aus völlig unterschiedlichen Perspektiven. Das Team ist also in starkem Maße interdisziplinär „aufgestellt“, sodass das Projektmanagement die Zusammenarbeit von Menschen verschiedener Denkart ermöglichen muss.

Das Projektteam sorgt letztlich für die Ausführung der verschiedenen Teilaufgaben im Projekt, wobei jedes Teammitglied seinen ihm gemäßen Beitrag dazu leisten muss. Typische **Aufgaben der Mitarbeiterinnen und Mitarbeiter im Projektteam** sowie vorhandene **Befugnisse** zeigt Tabelle 5.7.

TABELLE 5.7 Aufgaben und Befugnisse von Projektteammitgliedern

Das Projektteam	
Typische Aufgaben	Befugnisse/Verantwortung
▪ Selbstständige und verantwortliche Bearbeitung von Arbeitspaketen ▪ Sachlich qualifizierte Fertigstellung der übernommenen Arbeiten im vereinbarten Terminrahmen ▪ Regelmäßige Statusmeldungen zum Stand der übernommenen Arbeitspakete ▪ Unverzügliche Mitteilung an den Projektleiter bei sachlichen oder zeitlichen Abweichungen von der Planung ▪ Unterstützung der Projektleitung durch Mitwirkung bei der Projektplanung ▪ Erarbeitung von Entscheidungsvorlagen ▪ Erstellen der zur Projektsteuerung notwendigen Berichte (Tätigkeitsberichte, Arbeitsaufträge und Arbeitsauftragserledigung).	▪ Mitwirkung bei der Sicherstellung der Projektziele ▪ Termin- und kostengerechte Erledigung der Arbeitsaufträge ▪ Mitbestimmung bei Entscheidungen und Vereinbarungen zur Projektarbeit ▪ Aktive Mitarbeit bei den Teamsitzungen ▪ Rechtzeitiges Einfordern von Personal, Sachmitteln (Kapazitäten) und Finanzen bei der Projektleitung

Für die **Teambildung** ist es zunächst hilfreich, sich zu vergegenwärtigen, welche Funktion einem Team zukommt. Eine der Entscheidungsgrundlagen für die Teamzusammensetzung, aber auch für Personalentwicklungsmaßnahmen ist dann die Mitarbeiter-Potenzialanalyse. Neben vorhandenen Personaldaten (etwa einer Skill-Datenbank) gehören dazu auch die laufende Beobachtung der Mitarbeiter, ihre Stärken und Schwächen, die Kommunikation mit anderen, der Umgang mit Verantwortung, das Verhalten in Krisen und vieles mehr. Die Informationen und Ziele werden aus Mitarbeiter-Gesprächen, den Erfahrungen in der täglichen Projektpraxis durch die Projektbegleitung, mögliche Teamanalysen durch die Teammitglieder sowie eine Projektnachbetrachtung gewonnen und in weiterer Folge für die Gewinnung eines Mitarbeiter-Profiles (Stärken, Schwächen und Potenzial des Mitarbeiters) genutzt.

Ein leistungsfähiges und ausgewogenes Projektteam zusammenzustellen, ist in den meisten Fällen jedoch keine einfache Aufgabe. Bei der Bildung des Projektteams sollte deshalb auf Erfahrungen zurückgegriffen werden. Wir haben einige „**Regeln zur Teambildung**“ nachfolgend zusammengestellt:



Regeln zur Teambildung:

- Teams sollten nicht zu groß sein. Ein arbeitsfähiges Team umfasst zwischen fünf und sieben Personen. Bei dieser Gruppenstärke wird die bestmögliche Team-effizienz erreicht.
- Bei Projekten mit einer größeren Zahl von Projektmitarbeitern (etwa mehr als sieben Personen) wird sinnvollerweise ein Kernteam gebildet. Außerdem ist es dann notwendig, verschiedene Teilprojekte zu bilden.
- Es sollte darauf geachtet werden, dass möglichst jede Gruppe von Hauptbetroffenen im Projektteam repräsentiert ist. Auch sollte versucht werden, Machttträger und Promotoren in das Projektteam einzubinden.
- Im Projektverlauf können sich die Anforderungen an die Teamgröße und -zusammensetzung je nach Bedarf ändern.
- Da im Projektteam unterschiedliche Rollen zu besetzen sind, werden auch Personen unterschiedlicher Qualifikation benötigt. Dabei ist darauf zu achten, dass die Personen die Rollen übertragen bekommen, die sie auch ausfüllen können.
- Bei der Auswahl der Personen spielen Qualifikationsanforderungen (fachlich/methodisch) ebenso eine Rolle wie Interesse, Motivation und Identifikation mit dem Projekt sowie rein personenbezogene wie soziale Kompetenzen.
- Eine Mischung des Projektteams aus unterschiedlichen Persönlichkeiten kann für ein Projekt oft gewinnbringend sein. Denn: Kontroversen können – so sie sachlich ausgetragen werden – zu fortschrittlichen, unkonventionellen Lösungswegen führen.

5.4.3 Projekt-Auftraggeber und unterstützende Gremien

Unabhängig von der existierenden Organisationsform und der Größe der Organisation, in der das IT-Projekt durchgeführt wird, sind verschiedene Instanzen notwendig, um die Projektdurchführung zu begleiten und zu unterstützen. So ist durch eine entsprechende Koordination und Abstimmung sicherzustellen, dass oftmals unterschiedliche Interessen harmonisiert werden.

5.4.3.1 Der Auftraggeber im Projektmanagement

Der **Auftraggeber eines IT-Projektes** ist in der Praxis vielfach mit dem Initiator des Projektes identisch und zählt meist auch zu den unmittelbaren Nutzern der Projektergebnisse (Tabelle 5.8). Er übergibt dann in der Regel den unterzeichneten Projektauftrag an die Projektleitung und das Projektteam.

TABELLE 5.8 Aufgaben und Befugnisse des Projekt-Auftraggebers

Der Projekt-Auftraggeber	
Aufgaben	Befugnisse/Verantwortung
▪ Rahmenbedingungen für die Projektarbeit festlegen ▪ Projektrelevante Informationen bereitstellen ▪ Planungen der Projektleitung begleiten ▪ Regelmäßige Überwachung der Projektarbeit (etwa über Statusberichte) ▪ Mitwirkung im Lenkungsausschuss	▪ Übernahme des finanziellen und unternehmerischen Risikos ▪ Projektgenehmigung ▪ Entscheidungskompetenz bei wichtigen Projektabschnitten (Milestones) und Zwischenreviews ▪ Finanzielle Freigaben ▪ Projektabnahme

Zu unterscheiden sind in der Projektpraxis zwei Varianten:

- **Interner Auftraggeber:** In Unternehmen ist die Unternehmensführung oder eine Hauptabteilung als Auftraggeber denkbar. Im Beispielprojekt „Aufbau eines Mitarbeiterportals“ ist die zentrale Unternehmensführung der Projekt-Auftraggeber.
- **Externer Auftraggeber:** Führt eine Unternehmensberatung oder eine Softwarefirma ein Projekt für einen Kunden durch, handelt es sich bei den Kunden um externe Auftraggeber.



Beachten Sie:

Der Auftraggeber ist letztlich der „Hauptentscheider“ zu allen Fragen der Umsetzung und Abnahme des IT-Projektes. Er trägt das unternehmerische und finanzielle Risiko.

5.4.3.2 Die Rolle der Unternehmensführung

Der Einfluss der Unternehmensführung auf den Erfolg von IT-Projekten ist nicht unerheblich. Dies gilt vor allem für strategisch orientierte IT-Projekte und für solche, in denen die Unternehmensführung die Rolle des Auftraggebers innehat. Nicht unerheblich ist auch die Promoterfunktion, die dem Management bei vielen IT-Projekten zukommt. Nur mit Unterstützung von solchen Machtpromotern bzw. Sponsoren lässt sich oft der Erfolg eines IT-Projektes – wie die Erfahrungen zeigen – sicherstellen. Wichtig ist deshalb eine gut funktionierende Zusammenarbeit, Kommunikation und Abstimmung der Unternehmensführung mit der Projektleitung und dem Projektteam.

Die Führungsebene muss natürlich auch selbst dafür sorgen, dass die Projektarbeit erfolgreich verläuft und eine hohe Akzeptanz gegeben ist. Beispiele für **unterstützende Maßnahmen und hilfreiche Leitlinien seitens der Unternehmensführung** zeigt Tabelle 5.9.

TABELLE 5.9 Unterstützung der Projektarbeit durch die Unternehmensführung

Hilfreiche Rahmenbedingungen	Leitlinien (Projektmanagementkultur)
Ausreichende Freiräume für das Projektteam sind gewährleistet.	Mindestens ein Mitglied der Unternehmensführung ist inhaltlich (als „Sponsor“) beteiligt.
Die Bedingungen für eine optimale Informationsbasis der Teammitglieder sind geschaffen.	Niemand im Unternehmen sollte Projektarbeiten als Bedrohung ansehen, sondern als Chance, innovativ tätig zu werden und etwas zu verbessern.

Hilfreiche Rahmenbedingungen	Leitlinien (Projektmanagementkultur)
Ein positives Betriebsklima für die Zusammenarbeit von Projektteam und Fachabteilungen ist sichergestellt.	Projekte werden nach modernen mitarbeiterorientierten Prinzipien geführt. Dabei herrscht vor allem Offenheit gegenüber neuen Arbeits- und Lösungswegen.
Es ist sichergestellt, dass synergetische Arbeitsteams eingebunden werden können.	Kompetente Mitarbeiter sind auf entsprechenden Wunsch für die Projektarbeit freizustellen/bereitzustellen. Eine laufende Fortbildung zur Förderung der Mitglieder des Projektteams ist zu gewährleisten.
Der Projektleitung und dem Projektteam wird ausreichende administrative Unterstützung gewährt.	Zwischen dem Projektmanagement im Unternehmen und den anderen Führungskräften sollte keine Rivalität bestehen, sondern die Bereitschaft, voneinander zu lernen und sich gegenseitig zu unterstützen.

Insgesamt lässt sich festhalten, dass die Unternehmensführung (bzw. der Auftraggeber des Projektes) unbedingt dafür Sorge treffen muss, die notwendige Organisationskultur (die Werte und Leitlinien der Unternehmung) und die strukturellen Voraussetzungen für ganzheitlich-situative Projektarbeit zu schaffen. Wird sie dieser Aufgabe nicht gerecht, kann das Projekt schon zum Scheitern verurteilt sein, noch bevor es begonnen hat.

5.4.3.3 Der Projektlenkungsausschuss

Bei mehreren und bei größeren Projekten hat sich die Einrichtung von Ausschüssen als sinnvoll erwiesen. Als Entscheidungs-, Koordinations- und Kontrollgremium ist die Einrichtung eines **Projektlenkungsausschusses** (kurz PLA) auf gesamtorganisatorischer Ebene weit verbreitet (synonyme Begriffe dafür sind Entscheidungskommission, Steuerungsgruppe, Steering Committee). Er bildet letztlich die Schnittstelle zwischen

- Projekt, Projektleitung und Projektteam auf der einen Seite und
- Unternehmensführung und extern Beteiligten auf der anderen Seite.

Dieses Gremium überwacht das Projekt von Beginn an bis zur Umsetzung. Es ist das oberste Gremium für die Planung und Steuerung aller Projekte, die in einer Organisation realisiert werden. Hier werden letztlich die entscheidenden Weichen für weitere Projektfortschritte gelegt. So kann der Projektlenkungsausschuss in der Regel darüber entscheiden, ob das Projekt gestoppt oder gar abgebrochen wird, wenn sich abzeichnet, dass die Projektziele überhaupt nicht erreicht oder andere übergeordnete Ziele durch das Projekt sogar gefährdet werden.

Bezüglich der Zusammensetzung hat es sich als zweckmäßig erwiesen, in dieses Gremium hochrangige Führungskräfte zu entsenden. Da in dem Gremium Entscheidungen von erheblicher Tragweite getroffen werden, sollte in jedem Fall ein Mitglied der Geschäftsleitung sowie die IT-Leitung im Projektlenkungsausschuss vertreten sein. Die Projektleitung kann mitunter ebenfalls an den Sitzungen teilnehmen (bei unterschiedlichem Stimmrecht).

Es hat sich bewährt, dass sich die Mitglieder des Lenkungsausschusses in regelmäßigen Abständen (z. B. monatlich) treffen, darüber hinaus auch bei Bedarf außerplanmäßig. Bezüglich der Beschlussregeln gilt das „Einstimmigkeitsprinzip“, um so eine weitgehende Koordination zwischen den beteiligten Bereichen und für die spätere Umsetzung zu gewährleisten.

**Praxistipp:**

Lenkungsausschüsse sind in der Regel für mehrere Projekte in einem Unternehmen zuständig. Um die Verantwortlichkeit zu verdeutlichen, sollte in dem Lenkungsausschuss für jedes Projekt ein Mentor als Ansprechpartner festgelegt werden.

5.4.3.4 Das Projektbüro (Project Office)

Um ein optimales Multiprojektmanagement zu gewährleisten und eine übergeordnete Steuerung und Auswertung von Projekten zu realisieren, findet sich in größeren Organisationen zunehmend eine besondere Stelle: das Project Office. Diesem obliegt die Administration der Gesamtplanung aller Projekte zum Zwecke der übergeordneten Steuerung und Auswertung der Projekte.

Das Project Office erhält zu allen Projekten die aus der Projektvorbereitung resultierenden Entwürfe der Projektaufträge, nach der Auftragserteilung die definitiven Projektaufträge, die Projektpläne sowie zum gegebenen Zeitpunkt die Abschlussberichte. Das Project Office wird von den Fachabteilungen zum frühestmöglichen Zeitpunkt über sämtliche Ideen oder Initiativen zu möglichen Projekten informiert.

Den möglichen Zusammenhang zwischen den verschiedenen Mitarbeitern im Projekt (Teams, Teammitgliedern) und dem Projekt-Lenkungsausschuss bzw. einem Project Office verdeutlicht Abbildung 5.12.

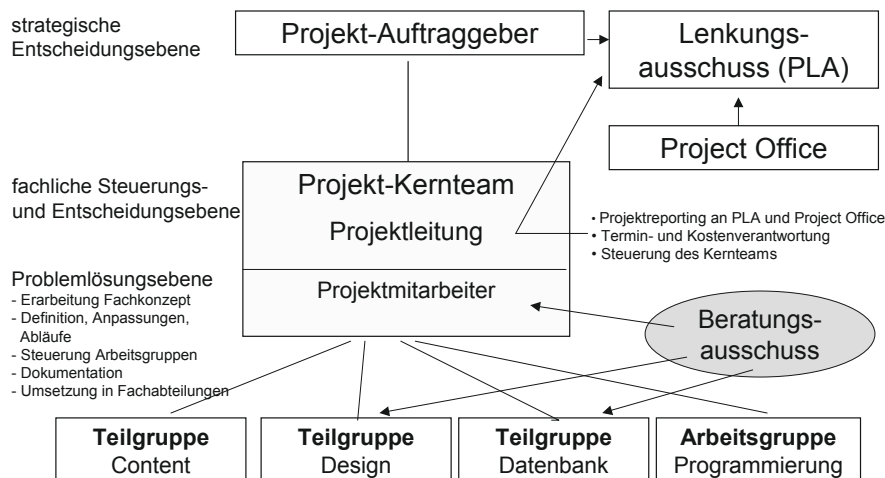


ABBILDUNG 5.12 Einordnung von Lenkungsausschuss und Project Office

5.4.3.5 Projektcontrolling und Projekt-Qualitätsmanagement als Sonderfunktionen

In größeren Organisationen kann es außerdem **besondere Stellen** geben, die eine übergreifende und wirtschaftliche Projektarbeit gewährleisten:

- IT-Projektcontrolling
- Projekt-Qualitätsmanagement

Zur Unterstützung des IT-Projektleiters kann das Einsetzen eines speziellen **Projektcontrollers** hilfreich sein. Ausgehend von den genehmigten Projektaufträgen werden hier folgende Aufgaben für sinnvoll angesehen:

- Prüfung und Aktualisierung von Projektplanungen (insbesondere der Kostenplanung)
- Einholen von Statusmeldungen und Prüfung der monatlichen Statusberichte
- Durchführen spezieller Soll-Ist-Vergleiche und von Projekt-Reviews
- Erstellen von Projektprognosen (insbesondere zu den Finanzmitteln)
- Ableiten von Handlungsempfehlungen für die Projektleitung

QS-Beauftragte: Für die Dauer des Projektes kann ein spezieller QS-Beauftragter die Projektleitung bei der Planung, Steuerung und Durchführung von projektbezogenen QS-Aktivitäten (beispielsweise die Entwicklung eines Projekt-QS-Plans) unterstützen.



Beachten Sie:

Welche Ausschüsse, Gremien und besondere Stellen zur Steuerung und Unterstützung der Projektarbeit vorhanden sind, hängt stark von den Rahmenbedingungen der betreffenden Unternehmung/Institution sowie der Projektgröße ab.

5.4.3.6 Beteiligung der Arbeitnehmervertretung

Es soll ehrgeizige Projekte geben, die nie über das Planungsstadium hinauskommen, weil man den Konflikt mit den Arbeitnehmervertretern scheut. Das muss nicht sein – zumindest nicht, wenn man zeitgemäßes Projektmanagement wörtlich nimmt.

Was die Einbindung des im Zusammenhang mit neuen Maßnahmen vielfach als Bremsklotz verschrieenen Betriebsrats angeht, sind drei Dinge angesagt:

- Anerkennung seiner Existenz und Arbeit;
- Einbeziehung in das „Benchmarking“ konkreter Projektphasen und
- gemeinsame Definition eines mit dem Projekt verbundenen langfristigen Ziels.

5.4.4 Kooperation mit externen Fachkräften

Firmenfremde Fachkräfte können für eine erfolgreiche Projektabwicklung aus mehreren Gründen unentbehrlich sein. Einmal kommt ihr Einsatz dann in Betracht, wenn die Kapazität der eigenen Mitarbeiter zur termin- und sachgerechten Projektdurchführung nicht ausreicht. Zum anderen fehlt oft das erforderliche Know-how zum Aufbau einer modernen Hardware- oder Datenbanklösung oder zur Anpassung einer komplexen Softwarelösung.

Bei **IT-Projekten** lassen sich **drei Kategorien von Fachkräften** unterscheiden, die in ein Projekt involviert werden können:

- Unabhängige Berater (Consultants) mit fachlichem Know-how oder spezieller Coaching-Kompetenz;
- Spezialisten einer Softwarefirma zur Anpassung und Einführung von Standardsoftware und
- Hardware-Systemspezialisten zur Mithilfe bei einer Netz-Konzeption oder der Architektur-entwicklung für IT-Infrastrukturen bzw. ihrer Komponenten.

Generell sollte auf externe Beratung dann zurückgegriffen werden, wenn „Neuland“ betreten werden soll, für das innerbetrieblich nicht das notwendige Know-how vorhanden ist. Speziell bei der Einführung von Computer- und Web-Anwendungen bietet sich Hilfe von außen für den Fall an, dass

- langfristige Planungen erforderlich sind (Strategie-Konzept);
- das übliche Maß überschreitende Finanzinvestitionen anstehen;
- völlig neue Technologien eingeführt werden sollen (Multimedia, Workflow, Portale, Wissensmanagement-Werkzeuge);
- größere Projekte mit vielen Schnittstellen zu realisieren sind oder
- zügige Programm-Anpassungen vorzunehmen sind.

Für ein IT-Projekt (so auch im Anwendungsbeispiel „Aufbau eines Portals“) gelten viele der genannten Anwendungssituationen gleichzeitig. Vielleicht ist es sogar unumgänglich, neutrale Kompetenz in derartige Projekte einzubeziehen. Dabei sollte sich die Aufgabe des Beraters nicht auf die Einbringung technischer Expertise beschränken. Er muss sich vielmehr rasch in das Unternehmen und dessen Probleme hineindenken können sowie als Katalysator für Projekte und zugleich als Konfliktlöser dienen.

**Beachten Sie:**

Die Entscheidung über die Art der in Frage kommenden Beratungsfirma dürfte in erster Linie vom Ziel des Beratungsauftrages abhängig sein. Während bei organisatorischen Problemen und Auswahlfragen „Herstellerneutralität“ besondere Bedeutung hat, kann für die Realisierung durchaus die Spezialisierung auf bestimmte Anbieter nützlich bzw. unumgänglich sein.

■ 5.5 Planungsaufgaben in IT-Projekten

5.5.1 Rahmenbedingungen moderner Projektplanung

Die Notwendigkeit einer klaren Projektplanung ist auf Managementebene nahezu unbestritten. Erfahrungen der Praxis zeigen nämlich, dass gerade eine schlechte Planungsarbeit eine Hauptursache für Projektfehlschläge und Zielabweichungen ist. Das folgende Beispiel zeigt, dass sich eine gut durchdachte Planung durchaus lohnt:

Untersuchungen haben erwiesen, dass die Kosten für die Planung von Projekten nur ca. 2% der gesamten Projektkosten ausmachen. Natürlich ist auch ein Planungskostenanteil von 2% noch zu hoch, sofern die Planung keinen Nutzen bringt. Auch hier gibt es Erfahrungswerte: So wurden ca. 22% Zeitersparnis und 15% Kostenersparnis ermittelt, die durch genaue Projektplanung erreichbar sind.

Die zuvor genannten Werte können natürlich nur eine grobe Schätzung liefern und sind in der Praxis von IT-Projekt zu IT-Projekt sehr verschieden. Dennoch: zeigen sie, dass Projektplanung aus betriebswirtschaftlicher Sicht sehr vorteilhaft sein kann.

Auch wenn die grundsätzliche Notwendigkeit einer Projektplanung aus Erfahrung bestätigt werden kann, stellt sich natürlich die Frage, was geplant werden muss. Im Wesentlichen werden in der Praxis heute bei der Projektplanung mehr oder weniger detaillierte Vorstellungen über den personellen, sachlichen und finanziellen Rahmen sowie für den zeitlichen Ablauf des Projekts entwickelt. Dabei wird nach dem Grundprinzip „Vom Groben zum Detail“ die konkrete Gesamtaufgabe in überschaubare Arbeitspakete zerlegt und mit ausgewählten Personen ein Projektteam gebildet. Das Ergebnis der Planungsarbeiten ist ein umfassendes Konzept mit verschiedenen **Teilplänen**, das die Grundlage für die Steuerung und Maßstab für die Kontrolle des Projekts ist.

Die verschiedenen Teilpläne für das Projektmanagement sind voneinander abhängig. So wäre beispielsweise eine noch so perfekte Zeitplanung wertlos, wenn sie Ressourcen unterstellt, die nicht vorhanden sind. Insoweit ist es notwendig, die Planungsmaßnahmen und die Planungsgrößen untereinander sowie in zeitlicher Hinsicht aufeinander abzustimmen.

Tabelle 5.10 skizziert – ausgehend von den wesentlichen Planungsgegenständen – die typischen Teilpläne und dabei zu lösende Fragestellungen.

TABELLE 5.10 Teilpläne im IT-Projektmanagement

Planungsgegenstand/ Ergebnisse	Fragestellungen, die durch die Teilpläne beantwortet werden können
Projektstruktur: Projektstrukturplan (PSP)	▪ Welche Aktivitäten sind für das Erreichen der Projektziele nötig? (Was ist im Einzelnen zu tun?) ▪ Welcher Zusammenhang besteht zwischen den Projektaufgaben? (Hierarchie der Teilaufgaben bilden) ▪ Wie lassen sich die Objekte und Tätigkeiten für das Projekt in Arbeitspakete aufteilen?
Projektablauf: Projektablaufplan	▪ In welchen Phasen soll das Projekt abgewickelt werden? ▪ In welcher Reihenfolge sind die Aktivitäten zu erledigen? Wo gibt es logische Abhängigkeiten? ▪ Welche Arbeitspakete können parallel ausgeführt werden?
Projekttermine (Zeiten): Terminplan	▪ Wie hoch wird der Zeitaufwand für die jeweiligen Aktivitäten geschätzt? ▪ Bis wann ist was zu erledigen? Sind bestimmte Meilensteine zu beachten?
Ressourcenbedarf, Ressourcen-Kapazität, Ressourcen-Einsatz: Ressourcenpläne	▪ Wie viel Personal wird für die einzelnen Arbeitspakete benötigt? ▪ Welcher Sachmittelbedarf ist gegeben? ▪ Welche Kapazitätsbegrenzungen bezüglich der Ressourcen sind zu berücksichtigen (Kapazitätsplan)? ▪ Wann ist die Verfügbarkeit der Ressourcen notwendig (Ressourcen-Einsatzplan)?

Planungsgegenstand/ Ergebnisse	Fragestellungen, die durch die Teilpläne beantwortet werden können
Kosten und Projektfinanzen: Kosten- und Finanzplan	▪ Welche Kosten(-arten) fallen wann bei welchen Arbeitspaketen an? Wie hoch sind die Gesamtkosten für das jeweilige Arbeitspaket? ▪ Was wird das Projekt insgesamt ungefähr kosten? Lässt sich die Summe durch eine Addition der Arbeitspaketkosten (so genannte direkte Kosten) und der Gemeinkosten ermitteln? ▪ Wie hoch sind die anfallenden Personalkosten? ▪ Wie erfolgt die Freigabe der Finanzmittel? (Zeitpunkt, Voraussetzungen)
Qualität: Qualitätssicherungsplan (QS-Plan)	▪ Welche Ergebnisse sollen in welcher Qualität/Form erarbeitet werden? ▪ Welche qualitätssichernden Maßnahmen sollen im Projektverlauf ergriffen werden? (projektinterne Richtlinien, QS-Schulungsmaßnahmen, Reviews, Tests)
Risikomanagement: Risikoplan	▪ Welche Projektrisiken sind denkbar, und wie groß ist die Wahrscheinlichkeit ihres Eintretens? ▪ Welche Auswirkungen sind im Risikofall möglich? ▪ Welche vorbeugenden Maßnahmen zur Risikominimierung können ergriffen werden (Prioritätsplan der Risiken)?
Projektorganisation: Organisationsplan, Berichtsplan	▪ Welche Rollen sind in dem Projekt gegeben? ▪ Welche Aufgaben, Kompetenzen und Befugnisse sind jeder Rolle zuzuordnen, und wie ist das Zusammenspiel zwischen den Projektrollen geregelt? ▪ Wie wird die Kommunikation zwischen Team, Auftraggeber und weiteren Beteiligten geregelt? ▪ Wie soll das Berichtswesen organisiert werden? ▪ Wie wird das Projekt dokumentiert?

**Praxistipp:**

Für die Abstimmung der Planungsgrößen empfiehlt sich ein iteratives Vorgehen. Ausgangspunkt ist eine (kritische) Größe, bei der ein Engpass vermutet wird. Häufig wird dies der festgelegte Finanzrahmen oder die begrenzte Personalkapazität sein. Auf die jeweilige Engpassgröße werden dann alle anderen Plangrößen ausgerichtet.

Stellt sich im Rahmen der weiteren Planung eine andere Größe als kritischer heraus, so muss diese zur Grundlage einer neuen Planungsrunde gemacht werden. Alle anderen Größen müssen nun hierauf abgestellt werden. Dieses Verfahren wird so oft wiederholt, bis alle Plangrößen miteinander in Einklang gebracht worden sind.

Der Zusammenhang zwischen den **Teilaufgaben bei der Planung von IT-Projekten** kann durch Abbildung 5.13 (nächste Seite) illustriert werden.

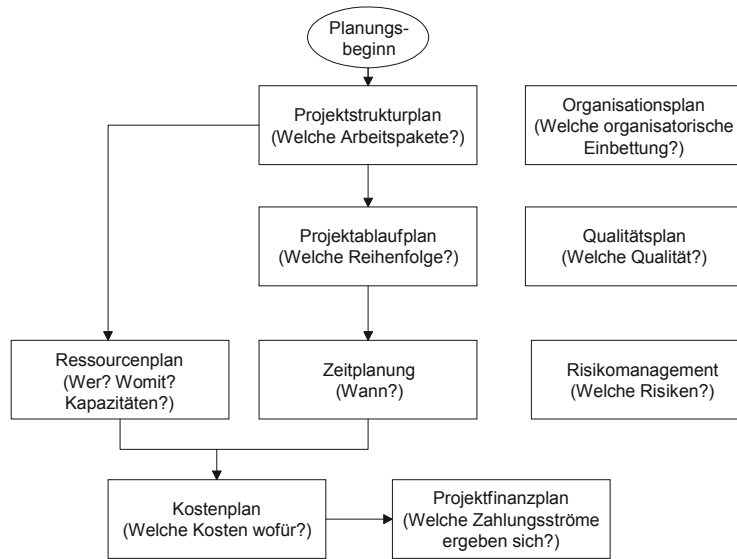


ABBILDUNG 5.13 Teilaufgaben bei der Projektplanung

Es ist sinnvoll, die Projektplanung von der eigentlichen Produktplanung zu unterscheiden. Soll ein hochkomplexes Produkt durch das IT-Projekt entwickelt werden, ist es erforderlich, zunächst eine intensive **Produkt-Strukturplanung** vorzunehmen. Sie gibt die technische Gliederung des zu entwickelnden Produktes wieder und stellt alle physischen Komponenten des Projektliefer- und -leistungsumfangs dar. Dies ist bei einem Projekt zum Aufbau eines Mitarbeiterportals beispielsweise das zu realisierende Portal mit den verschiedenen Teilbereichen und Funktionen.

5.5.2 Projektstrukturplan und Arbeitspakete

Die eigentliche Projektplanung beginnt – nach Vorliegen des unterschriebenen Projektauftrages – mit der Strukturplanung. Aufbauend auf dem Anforderungskatalog (dem Pflichtenheft) bzw. den im Projektauftrag formulierten Aufgabenstellungen, wird das Entwicklungsvorhaben technisch, aufgabenmäßig und kaufmännisch strukturiert. Ziel ist es, das Projekt zu Beginn in überschaubare und abgrenzbare Aufgaben zu zerlegen, um damit eine erste Übersicht über alle notwendigen Aktivitäten zur Projektrealisierung zu erhalten.

Für die Strukturplanung hat es sich als sinnvoll erwiesen, stufenweise vorzugehen und die gesamten Aktivitäten in einer hierarchischen Form zu ordnen. Ergebnis dieser Gliederung ist ein **Projektstrukturplan** (kurz PSP, engl. **work breakdown structure**), der meist in einer grafischen Form erstellt wird. Dieser Plan – auch als Aufgabenstrukturplan bezeichnet – gibt einen Überblick über die in der Projektabwicklung zu erledigenden Aufgaben.

Bei der Erstellung des PSP ist insbesondere darauf zu achten, dass alle Aktivitäten klar voneinander abgegrenzt und Überschneidungen vermieden werden. Ziel ist nicht, eine Reihenfolge von Aktivitäten darzustellen, sondern ausschließlich eine inhaltliche Zergliederung des Projektziels vorzunehmen. So dient der Projektstrukturplan dann auch als Basis für eine klare

Zuordnung aller Projektbeteiligten zu einzelnen Projektelementen. Zusammengesetzt müssen die Teilaufgaben und Arbeitspakete den Projektauftrag erfüllen.

Wie gelangt man in der Praxis zu einem Projektstrukturplan (kurz PSP)? Es gibt grundsätzlich zwei Wege (siehe Tabelle 5.11):

- die Orientierung am Projektziel (Objekt, Produkt) oder
- die Orientierung an Projektphasen (= Projektfunktionen).

TABELLE 5.11 Wege der Strukturplanerstellung

(1) objektorientierte Erstellung eines PSP (produktorientiert)	(2) prozessorientierte Erstellung eines PSP (funktionsorientiert, phasenorientiert)
Erläuterung: Das vereinbarte Projektziel (= das Produkt wie beispielsweise das Mitarbeiterportal) wird in wesentliche Bestandteile zerlegt.	Erläuterung: Es wird der Weg, der zum Erreichen des Projektziels zurückgelegt werden muss, in kleinere, meist auch chronologisch geordnete Teilziele zerlegt.
Beispiel: Das Projekt „Entwicklung des Mitarbeiterportals“ führt unterhalb der „Ist-Analyse“ zu den folgenden Einheiten: ▪ bisherige Intranet-Lösung (Inhalte, Design) ▪ Infrastruktur (Netze, Rechner) ▪ Daten- und Dokumentenorganisation ▪ Prozesse	Beispiel: Das Projekt „Aufbau des Mitarbeiterportals“ führt in der 2. Ebene zu den folgenden Einheiten: ▪ Projektvorbereitung und Analyse ▪ Soll-Konzept entwickeln ▪ System- und programmtechnische Realisierung ▪ Einführung der neuen Lösung (Run, Roll Out) ▪ Projektmanagement und Personalfragen

Das objektorientierte Vorgehen wird vor allem bei IT-Projekten gewählt, bei denen ein Überblick über die zu berücksichtigenden Objekte gegeben ist. Demgegenüber werden funktionsorientierte Gliederungen vorwiegend bei Dienstleistungsprojekten gewählt, da hier sehr gut erkennbar ist, welche Tätigkeiten anfallen.



Beachten Sie:

In der Regel werden in einem Projektstrukturplan beide Gliederungsprinzipien vorkommen (so genannter gemischtorientierter Projektstrukturplan). Steht die Einhaltung von Terminen im Vordergrund, dominieren phasenorientierte Gliederungen. Hat dagegen die Einhaltung von Kosten Priorität, erfolgt eher eine objektorientierte Gliederung.

Im Beispielfall wird für das Projekt „Aufbau eines Mitarbeiterportals“ der folgende Projektstrukturplan (Abbildung 5.14, nächste Seite) zugrunde gelegt.

Die einzelnen Äste im Projektstrukturplan werden – je nach Bedarf – unterschiedlich weit zu untergliedern sein. Bezüglich der Projektstrukturplanung wird im Allgemeinen davon ausgegangen, dass die Gliederung des Projekts nur so detailliert vorgenommen wird, bis sich Arbeitspakete als plan- und kontrollierbare Einheiten ergeben. Eine weitergehende Detaillierung verringert in der Regel die Übersichtlichkeit und verschlechtert so das Kosten-/Nutzenverhältnis der Projektplanung. Beachten Sie auch, dass das Ergebnis einer Projektstruktur-

planung unbedingt mit der zuvor festgelegten Projektdefinition (bzw. dem Projektauftrag) abgeglichen und quergeprüft wird.

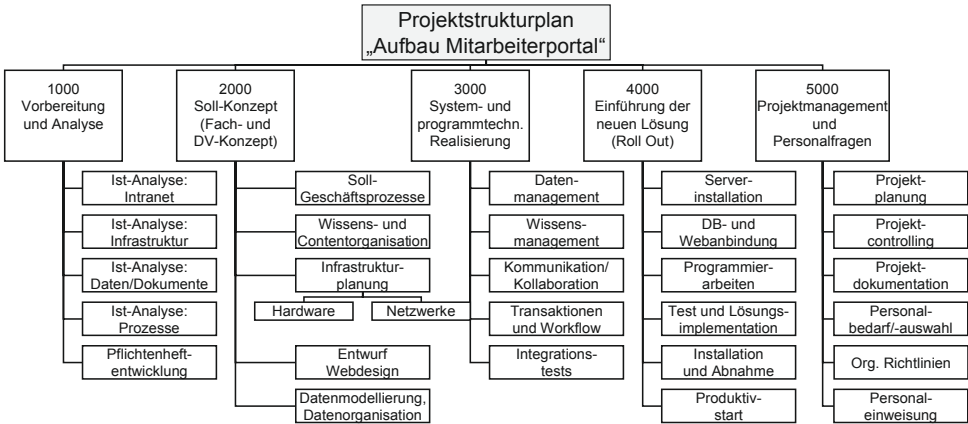


ABBILDUNG 5.14 Projektstrukturplan (Beispiel)

Der Projektstrukturplan stellt eine wichtige Basis dar, um einzelne Arbeitspakete planen zu können. Der Plan sollte ja so aufgebaut sein, dass jedes Strukturelement ein Arbeitspaket darstellt. Dies bedeutet: Ein **Arbeitspaket** umfasst in der Regel alle Vorgänge (Tätigkeiten, Aktivitäten) eines Projektes, die sachlich zusammengehören und in einer organisatorischen Einheit (von einer Stelle oder einer Teilgruppe) durchgeführt werden sollen.

Das in Tabelle 5.12 dargestellte Beispielformular aus dem Projekt PORTAL kann als Basis für eine Arbeitspaket-Beschreibung dienen.

Wichtig bei der Planung der Arbeitspakete ist: Die einzelnen Pakete sind exakt voneinander abgegrenzt (keine Überschneidung mit anderen Arbeitspaketen). Für jedes Paket ist als Zielgröße ein konkretes Ergebnis festzulegen. Dies können bestimmte Dokumente, fertige Programmelemente und Ähnliches sein. Die Arbeitspakete können somit gleichsam als isolierte Einzelaufträge innerhalb eines Projektes angesehen und zur Bearbeitung an Einzelpersonen, Arbeitsgruppen oder externe Projektpartner vergeben werden.

Im Rahmen der Planung der Arbeitspakete findet eine erste **Aufwandsschätzung** statt:

- Dazu ist für jedes Arbeitspaket ein **Zeitschätzwert** zu bestimmen. Dies ermöglicht später eine genaue Berechnung verschiedener Termine. Mögliche Zeitstufen sind: Jahre, Monate, Wochen, Tage, Stunden, Minuten oder Schichten. Grundsätzlich handelt es sich bei dem Schätzwert um eine Zeit, die unter normalen Umständen anzusetzen ist.

TABELLE 5.12 Beispiel einer Arbeitspaketfestlegung

Arbeitspaketplanung	
Projektbezeichnung:	PORTAL
Projektleiter:	Dipl.-Kfm. Friedrich Müller
Arbeitspaket (AP):	Ist-Analyse „Bisherige Intranet-Lösung“
AP-Verantwortliche:	Frau Frieda Käfer

Arbeitspaketplanung

1. Abgrenzung, Inhalt und Umfang (was zu tun ist):

Analyse des bisher realisierten Intranets unter Berücksichtigung der angestrebten Ziele und der Verbesserungs-/Erweiterungspotenziale durch den Ausbau zu einer Portallösung

2. Abzuliefernde Ergebnisse (z. B. zu erstellende Dokumente):

- Zusammenstellung der bisherigen Inhalte des Intranets (Dokumentation)
- Benutzerprofilanalyse (aufgrund einer Mitarbeiternutzungsanalyse)
- Bericht zur Akzeptanz des Designs
- Beschreibung und Beurteilung der bisherigen Funktionalitäten (Datenbankunterstützung, Verzeichnisse etc.)

3. Abstimmung mit anderen Arbeitspaketen:

soll eine Basis zur Entwicklung eines Soll-Konzeptes sein.

4. Einzuhaltende Spezifikationen:

- QS-Richtlinien für den Aufbau der Web-Sites im Unternehmen
- organisatorische Regelungen zur Abwicklung von Geschäftsprozessen
- Datenschutz- und Datensicherheits-Richtlinien

5. Kapazitätsbedarf/Aufwandsschätzung:

4 Personenwochen

6. Ecktermine:

geplanter Beginn der Arbeiten:

geplantes Ende der Arbeiten:

- Der Zeitschätzwert pro Arbeitspaket hängt natürlich vor allem davon ab, wie viel Ressourcen (Personen) für die Bearbeitung der einzelnen Arbeitspakete zur Verfügung stehen bzw. benötigt werden. Das ist auch der Grund dafür, dass die Werte oft als so genannte Personen-tage (bzw. Personenmonate, Personenjahre) angegeben werden (früher wurde auch von Manntagen, Mannmonaten oder Mannjahren gesprochen).

Hinsichtlich der für ein Arbeitspaket verplanten Zeit wird die Auffassung vertreten, dass diese – verglichen mit der gesamten Projektdauer – nicht zu groß sein sollte. In diesem Fall besteht nämlich die Gefahr, dass ein Terminverzug zu spät erkannt wird und keine wirksamen Maßnahmen zur Gegensteuerung mehr möglich sind.

Letztlich sollte für jedes Arbeitspaket auch die organisatorische Zuständigkeit geregelt sein. Dies ist am einfachsten bei der Zuordnung zu einer bestimmten Person, die zum Projektteam gehört. Es ist aber auch denkbar, dass ein Arbeitspaket von einer Fremdfirma übernommen wird.



Beachten Sie:

Die Aufwandsschätzung ist in der Praxis nicht immer ganz einfach. Außer dem eigenen Erfahrungspotenzial sollten die Erfahrungen außenstehender Experten sowie die Möglichkeiten spezieller Aufwandsschätzverfahren (gibt es beispielsweise bei IT-Projekten zur Softwareentwicklung) genutzt werden.

5.5.3 Projektablauf- und Terminplanung

Nachdem feststeht, was alles im Rahmen der Projektarbeit zu tun ist und welche organisatorische Einheit (Person) für die Erledigung der jeweiligen Arbeitspakete verantwortlich ist, kann die sinnvolle Reihenfolge der Abarbeitung der Arbeitspakete geprüft und festgelegt werden. Dazu wird ein Projektablaufplan (PAP) erstellt. Auf dieser Basis kann dann weiter ins Detail gegangen und eine Projektterminplanung vorgenommen werden.

5.5.3.1 Projektablaufplan erstellen

Zur Erstellung des Projektablaufplans müssen vor allem die folgenden Fragen geklärt werden:

- In welcher logischen Reihenfolge sind die Arbeitspakete (Vorgänge) auszuführen?
- Können bestimmte Arbeitspakete parallel ausgeführt werden? Wenn ja, welche?
- Ist es sinnvoll, die Arbeitspakete weiter in Vorgänge zu untergliedern?

Das Ergebnis der Ablaufplanung kann in einer Tabelle (als Vorgangsliste) oder in grafischer Form dargelegt werden. Aus dem Projektstrukturplan für das Projekt „Aufbau eines Mitarbeiterportals“ wurde eine Vorgangsliste (siehe Tabelle 5.13) erstellt.

TABELLE 5.13 Beispiel einer Vorgangsliste

Vorgangsbezeichnung	Dauer in Wochen	Vorgänger
1 Grobe Vorstudie	1	–
2 Ist-Analyse „Intranet“ u. a.	4	1
3 Pflichtenhefterstellung	2	2
4 Auftragserteilung	3	3
5 Entwurf „Geschäftsprozesse“	7	4
6 Entwurf „Wissens-/Content-Orga.“	3	5
7 Datenmodellierung und DB-Orga.	3	5
8 Entwurf „Web-Design“	2	5
9 Infrastruktur-Planung	4	6
10 Entscheidungssitzung	1 Tag	9; 8; 7
11 Teilprojekt „Datenanalyse/DB-Management“	6	10
12 Teilprojekt „Wissensmanagement“	8	10
13 Teilprojekt „Kommunikation/Kollaboration“	6	10
14 Teilprojekt „Transaktionen und Workflow“	10	10
15 Serverinstallation	3	11; 12; 13; 14
16 Datenbank- und Webanbindung	3	15
17 Programmierarbeiten	2	16
18 Test- und Lösungsimplementation	2	17; 14
19 Installation und Abnahme	4	18
20 Personaleinweisung	1	19; 18
21 Produktivstart	1	20; 18

Die Tabelle macht deutlich, dass eine Vorgangsliste für jeden Vorgang folgende Daten enthält:

- Vorgangsnummer
- Vorgangsbezeichnung
- Vorgangsdauer
- den jeweiligen Vorgänger (das sind die Vorgänge, die zum Beginn des betrachteten Vorgangs abgeschlossen sein müssen).

Beachten Sie folgende Hinweise für das Entwickeln einer Vorgangsliste aus einem vorhandenen Projektstrukturplan:



Hinweise für das Entwickeln einer Vorgangsliste:

- Die im Rahmen der Projektstrukturplanung festgelegten Arbeitspakete werden noch einmal in weitere Aktivitäten zerlegt und für die Terminplanung als Vorgänge übernommen.
- Tragen Sie die Vorgänge in einer Tabelle zunächst möglichst in der zeitlichen Reihenfolge der Abarbeitung ein!
- Die voraussichtliche Dauer eines jeden Vorgangs wird in der Spalte Dauer eingetragen. Hier sind unterschiedliche Zeiteinheiten möglich (je nach gewünschter Genauigkeit der Planung).
- Betrachten Sie danach den Beziehungszusammenhang zwischen den einzelnen Vorgängen. In der Spalte „Vorgänger“ der Vorgangsliste wird der Vorgang bzw. werden die Vorgänge, die erledigt sein müssen, eingetragen, um mit der Arbeit an dem jeweiligen Vorgang beginnen zu können. Beispiel: Die Datenbank- und Webanbindung (Vorgang 16) setzt voraus, dass die Serverinstallation abgeschlossen ist (Vorgang 15).
- Grundsätzlich kann es Vorgänge ohne notwendigen Vorgänger (gilt zumindest für einen Startvorgang), mit einem oder mehreren notwendigen Vorgängern geben.

5.5.3.2 Projektterminpläne (als Gantt- oder Netzplandiagramm) erstellen

In der Zeitplanung wird auf Ergebnisse der Ablaufplanung (Struktur der Ablauffolge) und evtl. der Bedarfsplanung (Anzahl und Zeitdauer der zur Verfügung stehenden Ressourcen) zurückgegriffen.

Um eine genaue Berechnung von Projektterminen zu ermöglichen, ist zunächst der Zeitpunkt festzulegen, an dem das Projekt starten soll (= **Startzeitpunkt**) oder alternativ der Zeitpunkt, an dem das Projekt spätestens beendet sein soll (= **Endzeitpunkt**).

Außerdem muss für jeden Vorgang eine Zeitdauer (in Arbeitsstunden bzw. Personentagen oder Personenmonaten) geschätzt werden. Auf dieser Basis können dann – unter Berücksichtigung der vorliegenden Meilensteintermine, der vorhergehenden Annahmen zur logischen Aufeinanderfolge und den Zeitschätzungen für die einzelnen Arbeitspakete – verschiedene Zeiten ermittelt werden. So kann man berechnen,

- wann das Gesamtprojekt abgeschlossen ist (frühester Endtermin);
- zu welchen Terminen bestimmte Vorgänge (Arbeitspakete) beginnen können und wann diese abgeschlossen sind;

- wann die festgelegten Meilensteine erreicht sein werden;
- wo mögliche Pufferzeiten liegen;
- wann von wem welche Arbeitsergebnisse vorliegen müssen und
- wo der kritische Pfad liegt.

Bei der Berechnung der Zeiten sind zwei Varianten denkbar:

- **Vorwärtsrechnung:** Ausgehend vom Projektbeginn werden die Termine für die einzelnen Arbeitspakete und damit auch der Projektendtermin ermittelt.
- **Rückwärtsrechnung:** Hier wird von einem vereinbarten oder gewünschten Endtermin ausgegangen und „rückwärts“ der Projektanfangstermin ermittelt.

In beiden Fällen werden die Zeiten anhand der Arbeitspakete, deren Dauer und deren logischen Abhängigkeit zueinander berechnet. Unter Nutzung einer Projektmanagementsoftware lässt sich die jeweilige Berechnungsart einfach auf die andere Variante umschalten.

Für die **Darstellung des zeitlichen Ablaufes** sind – je nach Komplexität des Projektes – unterschiedliche Instrumente geeignet:

- Tabellarische Terminliste
- Balkendiagramm (Gantt-Darstellung)
- Netzplandiagramm

Tabellarische Terminliste

Für einfache Projekte reicht eine tabellarische Liste, die die Arbeitspakete des Projektes in der Reihenfolge der Bearbeitung mit den Anfangs- und Endterminen (unter Umständen auch noch mit den zuständigen Ressourcen) enthält. Ein Beispiel hierfür liefert Abbildung 5.15.

	📌	Vorgangsname	Dauer	Anfang	Ende
1		Grobe Vorstudie	1 Woche	Fr 02.02.07	Do 08.02.07
2		Istanalyse "Intranet" u. a.	4 Wochen	Fr 09.02.07	Do 08.03.07
3		Pflichtenhefterstellung	2 Wochen	Fr 09.03.07	Do 22.03.07
4		Auftragserteilung	3 Wochen	Fr 23.03.07	Do 12.04.07
5		Entwurf "Geschäftsprozesse"	7 Wochen	Fr 13.04.07	Do 31.05.07
6		Entwurf "Wissens-/Contentorga"	3 Wochen	Fr 01.06.07	Do 21.06.07
7		Datenmodellierung und DB-Orga.	3 Wochen	Fr 01.06.07	Do 21.06.07
8		Entwurf "Web-Design"	2 Wochen	Fr 01.06.07	Do 14.06.07
9		Infrastrukturplanung	4 Wochen	Fr 22.06.07	Do 19.07.07
10		Entscheidungssitzung	1 Tag	Fr 20.07.07	Fr 20.07.07
11		TP "Datenanalyse/DB-management"	6 Wochen	Mo 23.07.07	Fr 31.08.07
12		TP "Wissensmanagement"	8 Wochen	Mo 23.07.07	Fr 14.09.07
13		TP "Kommunikation/Kollaboration"	6 Wochen	Mo 23.07.07	Fr 31.08.07
14		TP "Transaktionen und Workflow"	10 Wochen	Mo 23.07.07	Fr 28.09.07
15		Serverinstallation	3 Wochen	Mo 01.10.07	Fr 19.10.07
16		Datenbank- und Web-Anbindung	3 Wochen	Mo 22.10.07	Fr 09.11.07
17		Programmierarbeiten	2 Wochen	Mo 12.11.07	Fr 23.11.07
18		Test und Lösungsimplementation	2 Wochen	Mo 26.11.07	Fr 07.12.07
19		Installation und Abnahme	4 Wochen	Mo 10.12.07	Fr 04.01.08
20		Personaleinweisung	1 Woche	Mo 07.01.08	Fr 11.01.08
21		Produktivstart	1 Woche	Mo 14.01.08	Fr 18.01.08

ABBILDUNG 5.15 Tabellarische Terminliste (Beispiel)

Balkendiagramm

Mit der Balkendiagramm-Darstellung lassen sich verschiedene Projekt-Aktivitäten innerhalb einer Zeitspanne veranschaulichen und vergleichen. In diesem Fall wird jede Tätigkeit des Projektes (also jedes Arbeitspaket) durch einen waagrecht verlaufenden Balken über einer Zeitachse dargestellt, dessen Länge die Dauer kennzeichnet. Anhand der Zeitachse wird der zeitliche Ablauf eines Projektes auf einen Blick erkennbar. Abbildung 5.16 zeigt ein Beispiel für das Projekt PORTAL.

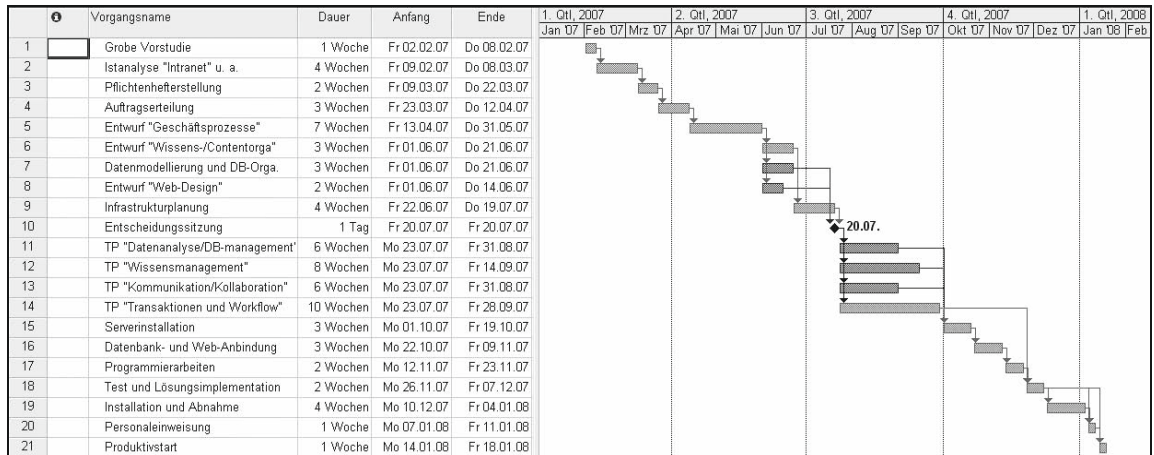


ABBILDUNG 5.16 Balkendiagramm-Darstellung (Beispiel)

Im Einzelnen kann dieser Darstellungsform entnommen werden,

- wie der zeitliche Ablauf eines Projektes geplant ist;
- wo zeitliche Überlappungen von Aktivitäten gegeben sind;
- welche Bedeutung die verschiedenen Aufgaben für die Einhaltung der gesetzten Termine haben (veranschaulicht durch unterschiedliche Farben und Symbole);
- wo sich der kritische Weg befindet.

Möglich ist eine unterschiedliche Skalierung der Zeitachse. Sie wird so festgelegt, dass ein „lesbares“ Diagramm entsteht.

Auswertungen und daraus folgende Maßnahmen sind daraufhin in verschiedener Weise aufgrund der ermittelten Meilensteine und des kritischen Pfades denkbar:

- Meilensteine werden im Balkendiagramm durch eine Raute gekennzeichnet (im Beispielfall der Vorgang 10 „Entscheidungssitzung“). Möglich sind dabei sowohl errechnete Meilensteine als auch individuell gesetzte Meilensteine.
- Der kritische Pfad ist von besonderer Bedeutung für das Projektmanagement, denn alle Aktivitäten, die auf diesem Pfad liegen, erfordern eine besondere Aufmerksamkeit durch die Projektleitung. Die zeitkritischen Vorgänge sind nämlich dadurch gekennzeichnet, dass eine Verzögerung bei diesen Vorgängen unmittelbar zu einem Zeitverzug für das gesamte Projekt führt. Alle anderen Aktivitäten haben einen zeitlichen Puffer. Eine wichtige Schlussfolgerung für das Projektmanagement: Es bietet sich an, die kritischen Vorgänge in kürzeren Abständen zu reviewen.

Netzplandiagramm

Die Netzplantechnik ist eine bereits längere Zeit bewährte Planungsmethodik, die eine Reihe von Verfahren zur Analyse, Beschreibung, Planung, Steuerung und Überwachung von Projektablaufstrukturen umfasst. Dazu werden die festgestellten Projektablaufstrukturen in eine grafische Darstellung gebracht, die die logische und zeitliche Abhängigkeit der Vorgänge verdeutlicht. Dabei werden Zeiten, Kosten, Ressourcen und weitere Einflussgrößen erfasst und Berechnungen dazu durchgeführt.

Es handelt sich in der Regel um ein **rechnergestütztes Verfahren**, da es sich bei der heute verfügbaren Software als viel zu aufwändig erweisen würde, das Erstellen der Diagramme und die Berechnungen (für die Ermittlung der Planungsdaten bzw. für Auswertungen) manuell durchzuführen.

Grundlage für das Erstellen eines Netzplanes ist die bereits erläuterte **Vorgangsliste**, die

- sämtliche Tätigkeiten des Projektes (Vorgänge) auflistet,
- die geschätzten Zeitwerte enthält sowie
- die Abhängigkeiten zu den Vorgänger- und Nachfolger-Vorgängen aufzeigt.

Es gibt verschiedene Verfahren der Netzplantechnik, wobei allerdings ein gemeinsames Grundprinzip vorhanden ist: Es werden alle Ablaufelemente und ihre Abhängigkeiten untereinander in einer grafischen Darstellungsform berücksichtigt, sodass sich eine vernetzte Darstellung sämtlicher Arbeitspakete ergibt. Die Varianten zeigt Abbildung 5.17.

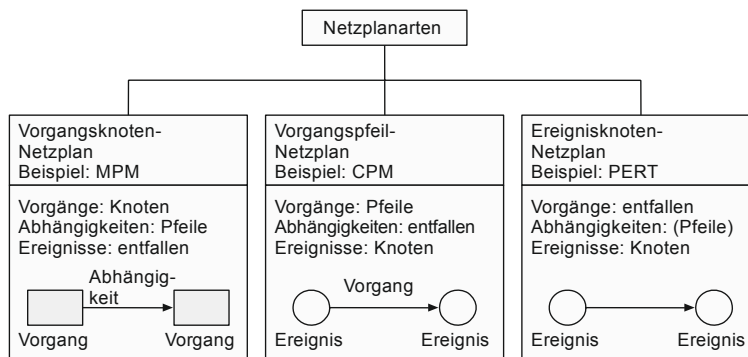


ABBILDUNG 5.17
Arten der Netzplan-technik



Beachten Sie:

Je nach verwendeter Netzplan-Methode lassen sich unterschiedliche Anordnungsbeziehungen darstellen. Einige Methoden (Programme) erlauben nur sog. Ende-Start-Beziehungen, andere können auch beliebige Überlappungen zwischen den Tätigkeiten darstellen.

Werden nach diesen Vorüberlegungen die geschätzten Zeiten hinzugenommen, lassen sich die geplanten Anfangs- und Endtermine der einzelnen Vorgänge ermitteln. Einen Ausschnitt aus einem entsprechenden Netzplan zeigt die Übersicht in Abbildung 5.18.

Die Berechnung der Zeiten erfolgt dabei in der Weise, dass – ausgehend von einem Startzeitpunkt für einen Vorgang – jeweils die geschätzte Vorgangsdauer addiert wird. Im Endergebnis ergibt sich für den letzten Vorgang des Projektes die Gesamtzeit bzw. der Endzeitpunkt des Projektes.

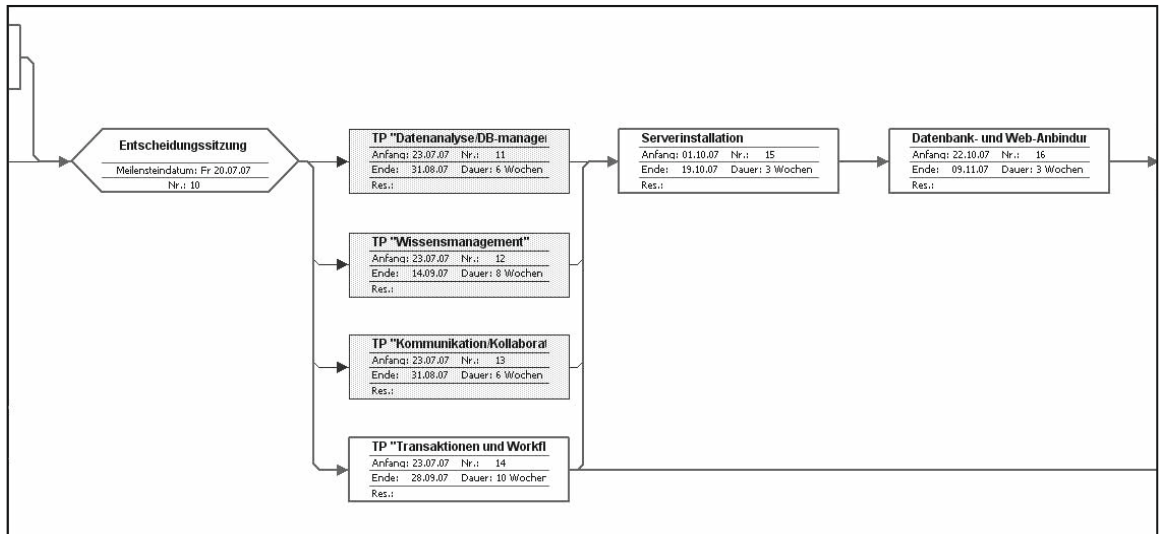


ABBILDUNG 5.18 Netzplan (Ausschnitt)

Ein besonderer Vorteil: Mit der Netzplantechnik lassen sich Zeitreserven für die Projektsteuerung ermitteln, indem der kritische Weg und Pufferzeiten für die einzelnen Vorgänge berechnet werden. Unterschieden werden folgende Pufferzeiten:

- **Gesamte Pufferzeit (GP):** Zeitspanne zwischen frühester und spätester Lage eines Ereignisses bzw. Vorganges.
- **Freie Pufferzeit (FP):** Zeitspanne, um die ein Ereignis bzw. Vorgang gegenüber seiner frühesten Lage verschoben werden kann, ohne die früheste Lage anderer Vorgänge bzw. Ereignisse zu beeinflussen.

Beachten Sie, dass bezüglich der Zeiten für einen Vorgang zu unterscheiden sind:

- **Vorgangsdauer** (Arbeitszeit, die ein Vorgang erfordert): Beispiel: Vorgang „Pflichtenheft erstellen“ benötigt 20 Tage
- **Arbeitsdauer** (= Zeit, die eine Ressource für einen Vorgang aufwendet): Beispiel: Bearbeiten 2 Mitarbeiter parallel den Vorgang „Pflichtenheft erstellen“, dann beträgt die Arbeitsdauer pro Mitarbeiter 10 Tage. Arbeiten 2 Mitarbeiter 50% ihrer Zeit parallel an der Aufgabe „Pflichtenheft erstellen“, dann beträgt die Arbeitsdauer 20 Tage.



Beachten Sie:

Bezüglich der realen Terminermittlung ist darüber zu berücksichtigen, dass für die beteiligten Personen neben der zur Verfügung stehenden Arbeitszeit auch noch die Urlaubszeiten und Feiertage einzurechnen sind.

Der effiziente Einsatz einer oder mehrerer Terminplanungsmethoden hängt von der Komplexität und Dynamik des jeweiligen Projekts ab. Einige Beurteilungen im Vergleich zeigt die Tabelle 5.14.

TABELLE 5.14 Vergleich von Terminplanungsmethoden für Projekte

Projekt-Terminplanungsmethoden im Vergleich			
Beurteilungsmerkmal	Terminliste	Balkendiagramm	Netzplan
Informationsbedarf bzw. bereitgestellte Informationen	Arbeitspaketliste Starttermine und/oder Endtermine der Arbeitspakete	Arbeitspaketliste Dauer je Arbeitspaket zeitliche Lagen der einzelnen Arbeitspakete	Arbeitspaketliste Dauer je Arbeitspaket technologische und ressourcenmäßige Abhängigkeiten zwischen Arbeitspaketen
Darstellung der Abhängigkeiten	nein	schlecht	gut
Übersichtlichkeit	gering	gut	sehr gut
Aufwand für die Erstellung	gering	mittel	hoch (Software-nutzung sinnvoll)
Einsatzbereich	für einfache Projekte	für kleinere bzw. mittlere Projekte	für komplexe und größere Projekte

5.5.4 Ressourcenbedarfsplan und Ressourceneinsatzplan

Zur Verdeutlichung, welche **Ressourcen** für ein IT-Projekt in Betracht kommen, kann folgende Differenzierung gewählt werden (siehe Tabelle 5.15):

TABELLE 5.15 Projektressourcen

Mögliche Ressourcen	Erläuterungen/Besonderheiten
Eigenpersonal	für das Projekt benötigte Personen (Einzelpersonen oder Personengruppen): Mitarbeiter der Abteilung, die das Projekt durchführt, Beteiligte aus anderen Fachabteilungen des Unternehmens.
Fremdpersonal	Hierzu zählt beispielsweise die Inanspruchnahme externer Beratungsleistungen im Projekt. Neben dem zeitlichen Einsatzplan sind vertragliche Vereinbarungen mit den externen Dienstleistern über die Kooperation wichtig.
Investitionsgüter und sonstige Sachmittel	Hierzu rechnen vor allem Anlagen der Informations- und Kommunikationstechnik (einschließlich der beschafften Applikationen bzw. Software-Lizenzen).
Räume	Projektmitarbeiter bzw. das Projektteam benötigen während der Projektlaufzeit besondere Räumlichkeiten.

Innerhalb dieser Gruppen kann eine weitere Klassifizierung sinnvoll sein, wenn das Ressourcenmanagement sehr viele Ressourcen umfasst und detaillierte Planungen und Auswertungen nötig sind.

5.5.4.1 Ressourcenbedarfsplanung

Im Rahmen einer **Ressourcenbedarfsplanung** haben Grenznutzenbetrachtungen eine große Bedeutung. Ein Projektvorgang, für den beispielsweise 24 Arbeitstage Aufwand angesetzt sind, kann von 3 Mitarbeitern in 8 Tagen genauso erfüllt werden wie von 4 Mitarbeitern in 6 Tagen. 24 Mitarbeiter werden aber kaum mit nur einem Tag auskommen. Sie werden sich vermutlich gegenseitig im Wege stehen, und der Koordinationsaufwand dürfte unangemessen ansteigen.

Ergebnis der **Ressourcenbedarfsplanung** sollte eine Übersicht über den **Bedarf an Personen und Sachmitteln pro Arbeitspaket und für das gesamte Projekt** sein. In einer Tabelle werden die so ermittelten Mengen den Arbeitspaketen zugeordnet. Aus ihr können dann sowohl der Bedarf pro Arbeitspaket wie auch der Gesamtbedarf abgelesen werden. Das Ergebnis der Bedarfsplanung ist eine Bedarfsübersicht für jedes Arbeitspaket und für das gesamte Projekt (siehe Abbildung 5.19).

Aufgabe	Anzahl Mitarbeiter	Qualifikation	Zeitdauer	Sachmittel	Organisations- mittel	Raumbedarf
Σ						

ABBILDUNG 5.19 Ressourcenbedarfsplanung (Planungstabelle)

5.5.4.2 Ressourcenkapazitätsplanung

In engem Zusammenhang mit der Ressourcenbedarfsplanung steht die Kapazitätsplanung. Die benötigten Ressourcen können **Restriktionen** in zeitlicher und kapazitativer Hinsicht aufweisen. Auch dies lässt sich berücksichtigen. Eine Zeitplanung unter der Annahme unbegrenzt verfügbarer **Kapazitäten** wäre in der Praxis ja oft unrealistisch. Es bedarf vielmehr der Einbeziehung zusätzlicher Restriktionen; etwa die Berücksichtigung einer beschränkten Verfügbarkeit von Personal und Einsatzmitteln (Beispiel: Herr X aus der Fachabteilung arbeitet nur zu 30% seiner Arbeitszeit an dem Projekt „Aufbau des Mitarbeiterportals“ mit).

Der Leitgedanke einer jeden Planung lautet „nach Engpass planen“:

- Entweder stehen die Termine eines Vorgangs fest. Dann sind die Kapazitäten so einzuplanen, dass dieser Termin auch erreicht wird.
- Alternativ liegen die personellen Kapazitäten fest, dann sind hieraus resultierend die Termine zu bestimmen.



Beachten Sie:

Die zur Projektarbeit erforderlichen Ressourcen werden in einer **Kapazitätsplanung** auf die verfügbaren Mitarbeiter, Maschinen und Ressourcen aufgeteilt. Das Ergebnis ist eine Gesamtübersicht aller zur Abarbeitung des Projektes erforderlichen Kapazitäten zu geplanten Terminen während der Projektlaufzeit.

Bei der Kapazitätsplanung werden also die während des Projektablaufs benötigten Personalbedarfe zeitlich eingeplant. Für jeden Projektmitarbeiter wird so ermittelt, wie groß die Kapazitätsauslastung innerhalb eines Zeitraumes ist, und in Form eines Belastungsprofils erstellt. Damit ist ersichtlich, ob die für das Projekt verfügbare Personalkapazität eines Mitarbeiters unterschritten wird und für andere Aktivitäten eingeplant werden kann oder überschritten wird und somit ein Belastungsausgleich erforderlich ist.

Die Ressourcenbedarfs- und -kapazitätsplanung erfordert gleichzeitig eine Planung der Ressourcenbeschaffung. Dabei geht es vor allem um die zeitgerechte Anforderung von Sachmitteln (inklusive Fremdpersonal und Beratungsleistungen) und Investitionsgütern (z. B. benötigte Hard- und Software). Bezüglich der Projektplanung ist zu beachten, dass mitunter bei den Beschaffungsvorgängen längere Vorlaufzeiten durch eventuell erforderliche Ausschreibungen nötig sind.

5.5.4.3 Ressourceneinsatzplanung

Aus den im Rahmen der Terminplanung errechneten Zeiten kann eine Ressourceneinsatzplanung (z. B. Personaleinsatzplanung) vorgenommen werden. Den verschiedenen Arbeitspaketen im IT-Projekt können jetzt konkrete Ressourcen zugeordnet werden, die zu ihrer Ausführung erforderlich sind. Für die Einsatzplanung kann dabei von zwei Ansätzen ausgegangen werden:

- Es wird ein gleichmäßiger zeitlicher Einsatz über die zeitliche Dauer eines Arbeitspaketes vorgesehen.
- Es wird ein unterschiedlicher Einsatz an verschiedenen Arbeitstagen/Arbeitswochen festgelegt.



Teilschritte der Personaleinsatzplanung:

- Ermitteln des Vorrats an Ressourcen (qualifikationsgerecht, zeitgerecht)
- Errechnen des Bedarfs (Arbeitspakete und Teilbarkeit als Rahmendaten, ermittelt aus Anzahl der Mitarbeiter pro Projekteinheit bzw. Zeitvorgabe)
- Gegenüberstellen von Bedarf und Vorrat (Personalmaßnahmen, Verteilzeiten, Grundlasten)
- Optimieren der Auslastung
- Aufgaben, Kompetenzen und Verantwortlichkeiten zuteilen
- Planung des Personaleinsatzes im Zeitablauf

Möglichkeiten, um vorhandene Überlastungsprobleme zu lösen, sind:

- Verlängerung des Zeitraumes, der zur Erledigung ausgewählter Arbeitspakete zur Verfügung steht
- Erhöhung der Kapazität für bestimmte Ressourcen
- Priorisierung von Tätigkeiten
- Veränderung von Ablauffolgen durch entsprechende Umstrukturierung des Ablaufplans.

**Beachten Sie:**

Zusätzliche Probleme ergeben sich für die Personaleinsatzplanung, wenn die Mitarbeiter in unterschiedlichen Projekten zum Einsatz kommen können. Hier ist eine umfassende **Multiprojektplanung** notwendig. Die Planung muss dann berücksichtigen, dass mehrere Projekte eines Unternehmens auf die gleichen knappen Ressourcen zugreifen.

5.5.5 Projekt-Kostenplanung

Für die Durchführung von Projekten werden mehr oder weniger umfangreiche Finanzmittel benötigt. Dazu zählen die Kosten für Personal, Materialien, Investitionen sowie externe Personal-Dienstleistungen. Zunächst zwei Hinweise:

- Ohne eine detaillierte Planung und Betrachtung der Finanzdaten können die Projektkosten schnell „aus dem Ruder“ geraten. Wichtig ist neben einer möglichst exakten Kostenplanung auch die permanente Prüfung der Wirtschaftlichkeit eines Projektes.
- Kosten können zum Teil darüber entscheiden, wie schnell Vorgänge erledigt und wie Ressourcen (etwa Sachmittel und Arbeitskräfte) eingesetzt werden. Steht beispielsweise bei fehlenden Ressourcen ein entsprechendes Budget zur Verfügung, kann etwa für Spezialfragen besonderer Sachverstand von außen „eingekauft“ werden.

Ausgangspunkt der Kostenplanung sind die Daten aus der Aufwandsschätzung und Terminplanung. Sie werden mit geeigneten Multiplikatoren (z.B. Arbeitswerte, Stundensätze, Verrechnungspreise, Einkaufspreise) in Werteinheiten umgerechnet. Ergebnis sind die voraussichtlichen Kosten für das Gesamtprojekt sowie der Kostenverlauf auf der Zeitachse.

Es empfiehlt sich, eine möglichst umfassende Vollkostenrechnung zu erstellen, in der alle direkten und indirekten Kosten für das Projekt erfasst werden. Die Gliederung der kalkulationsrelevanten Teileinheiten sollte auf der vorliegenden Projektstruktur aufbauen (vgl. Tabelle 5.16).

Die Umlage der unterschiedlichen Formen der Gemeinkosten erweist sich oftmals als problematisch. Ein Teil dieser Kosten ist in den Stundenverrechnungssätzen eingearbeitet, andere Kostenelemente müssen zusätzlich pauschal umgelegt werden.

TABELLE 5.16 Projektkostenermittlung

Checkliste zur Ermittlung der Projektkosten (Projektkostenarten)	
Einzelkosten	Beispiele
Personalkosten	▪ Gehälter (entsprechend dem Zeiteinsatz) ▪ Löhne ▪ Personalnebenkosten ▪ Prämien ▪ Fort- und Weiterbildung

Checkliste zur Ermittlung der Projektkosten (Projektkostenarten)	
Einzelkosten	Beispiele
Materialkosten	▪ Büromaterial (Papier etc.) ▪ Archivierungsmedien (konventionell, elektronisch) ▪ Folien, Flipchartblocks ▪ Moderationsmaterial (Karten, Stifte etc.)
Reisekosten	▪ Kilometergeld (Fahrtkostenerstattung) ▪ Bahn- und Flugreisen ▪ Übernachtung (Hotel) ▪ Spesen (Verpflegung)
Fremdleistungen	▪ Beratung ▪ externe Mitarbeiter
Versicherungen	direkt abgeschlossene Versicherungsleistung
Raumkosten	▪ Miete (direkt bzw. kalkulatorisch) ▪ Raumnebenkosten (Strom, Gas, Wasser) ▪ Einrichtungskosten
Gemeinkosten	Beispiele
Verwaltungskosten	▪ Geräte (anteilige Abschreibungen für Computer, Kopierer und anderes) ▪ Kommunikationskosten (Telefon etc.) ▪ Projektmanagement (Software etc.)
zentrale Dienstleistungen	▪ Personalwesen (Personalbeschaffung etc.) ▪ Finanz- und Rechnungswesen ▪ Qualitätsmanagement
Raummiete	anteilig für: ▪ Büroräume ▪ Schulungsräume ▪ Besprechungsräume ▪ Lagerräume

Die beste Grundlage für eine exakte Kostenplanung ist ein gut strukturierter Projektstrukturplan mit genau definierten Arbeitspaketen. Mit den darin zur Verfügung stehenden Daten kann eine so genannte **Schätzklausur** durchgeführt werden. Bei dieser Methodik geht das Projektteam (zuweilen auch mit Unterstützung von anderen Fachleuten) so vor, dass die einzelnen Arbeitspakete im Detail analysiert und betrachtet werden. Hierfür werden die jeweiligen Mengenangaben (= Personentage bzw. Personenwochen je Arbeitspaket) festgestellt. Diese Mengenwerte werden dann aufgrund der kalkulatorischen Lohn-/Gehaltsdaten in Personalkosten umgesetzt. Ähnliches gilt für die anderen Kostenarten.

Es bietet sich an, die Kosten in der beschriebenen Weise für jedes Arbeitspaket einzeln zu ermitteln. Diese Kosten werden anschließend als gesamte Projektkosten zusammengefasst (vgl. Abbildung 5.20).



Beachten Sie:

Verschiedene Studien zeigen, dass die Zufriedenheit des internen oder externen Auftraggebers weit mehr von der Qualität des gelieferten Produktes abhängt als etwa von der Einhaltung der zugesagten Termine und Kosten. Dies gilt sicher einige Zeit nach Projektabschluss, denn der Ärger mit überzogenen Terminen und erhöhten Kosten lässt mit der Zeit nach, im Gegensatz zum Ärger über ein Produkt, das sich im mehr oder weniger regelmäßigen Einsatz befindet.

Wesentlich für die **Qualitätsplanung** ist die Festlegung der Qualitätsmaßstäbe. Diese Festlegung ist gerade bei Projektergebnissen, die ja immer eine gewisse Neuartigkeit beinhalten, nicht einfach und hängt unmittelbar von den Produkten und Leistungen ab, die als Ergebnis der Projektarbeit herauskommen sollen. Jede Leistung muss so beschrieben werden, dass eine eindeutige Messung bei der Abnahme des Ergebnisses möglich ist.

Qualität – sowohl die objektiv messbare als auch die subjektiv wahrgenommene – wird durch sehr viele Faktoren bestimmt. Notwendig ist, dass sich die Projektleitung rechtzeitig mit dem Auftraggeber oder dem Kunden des Projektes über die erwarteten Qualitätsmerkmale abstimmt. So kann sichergestellt werden, dass nicht an den Vorstellungen des Auftraggebers vorbeientwickelt wird.

Im Ergebnis sollte ein **Projekt-Qualitätsplan** (kurz **Projekt-QS-Plan**; vgl. Tabelle 5.17) erstellt werden, der eine Aufstellung der im Projekt vorgesehenen qualitätssichernden Maßnahmen mit Aktivitäten, Verantwortlichkeiten und Zeiten (was, wer, wann) beinhaltet.

TABELLE 5.17 Beispiel für einen Projekt-QS-Plan

QS-Maßnahmen	Verantwortlichkeiten	Zeiten/Termine
▪ Richtlinien erstellen ▪ Design-Richtlinien ▪ Organisations-Richtlinien		
▪ Reviews ▪ QFD-Workshops (Quality Function Deployment) ▪ Zwischenergebnisse prüfen ▪ Realisierte Inhalte (Abschlussreview)		
▪ Tests ▪ Funktionstests ▪ Ergonomietests		
QS-Schulungsmaßnahmen		

In der praktischen Umsetzung der Qualitätsplanung wird in der Regel so vorgegangen, dass der Projekt-QS-Plan gemeinsam vom Projektleiter mit dem Projekt-Auftraggeber, dem Projektteam sowie einem im Projektauftrag festgelegten QS-Beauftragten erarbeitet wird. Grundlage dafür sind die Projektanforderungen, es besteht eine Abhängigkeit von den übrigen Projektplänen.

Um Spitzenqualität im Projekt zu erreichen, müssen mögliche Fehler permanent bzw. in sinnvollen Abständen analysiert und korrigiert werden. Eine entsprechende Orientierung gibt die folgende Checkliste.



Vorgehen zur Qualitätssicherung

- Qualitätsziele für das Produkt/Projektergebnis festlegen
(z. B. einfache Bedienbarkeit, ...)
- Mängel erkennen und analysieren
(beispielsweise komplizierte Benutzung bestimmter Funktionen, u. a.)
- Korrekturen/Maßnahmen entwickeln und verfeinern
(z. B. moderneres Produktdesign, ...)
- Wirksamkeit der neuen/veränderten Produktmerkmale messen
(beispielsweise Benutzerakzeptanz anhand eines Prototyps evaluieren)
- Neue Qualitätsziele setzen

Die Bestandteile der Qualitätssicherung der Projektergebnisse zeigt im Zusammenhang die Abbildung 5.22.

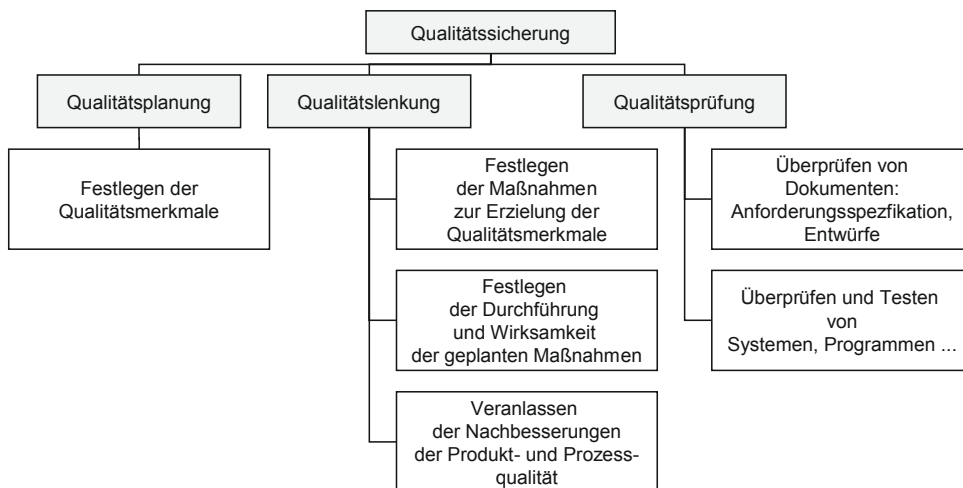


ABBILDUNG 5.22 Bestandteile der Qualitätssicherung in Projekten

Abschließend einige Hinweise auf wichtige **Grundsätze zur Qualitätssicherung** in Projekten:

- Bei der Auftragsvergabe sollten möglichst schon Abstimmungen zur Qualitätsplanung und Qualitätssicherung erfolgen. Eine präzise Projektdefinition erleichtert später das Herstellen der gewünschten Produktqualität.
- Bereits in der Anfangsphase von Projekten ist die Einhaltung der Qualitätsmaßstäbe konsequent zu verfolgen.
- Ein projektbegleitendes Qualitätsmanagement sollte vorbeugend von Anfang an dafür sorgen, dass die dem Kunden zugesagte oder vom Markt verlangte Qualität erreicht wird. Ein

neueres, aber bereits bewährtes Instrument sind QFD-Workshops (Quality Function Deployment), in denen die wichtigsten Anforderungen des Kunden erfasst und in technische Produkteigenschaften umgesetzt werden können. Ein anderes, neues Verfahren ist die Conjoint-Analyse, mit der die Qualitätsmerkmale gefunden werden können, die für den Kunden kaufentscheidend sein können.

- Bereits in frühen Phasen des Projekts werden die entscheidenden Weichen für die Qualität eines Produktes gestellt. Deshalb sollten immer wieder in Zwischenreviews die Zwischenergebnisse bei der Produktentwicklung geprüft werden (Meilensteine).

5.5.7 Projekt-Risikoplanung

Projektarbeit und Projektplanung sind aufgrund der Einmaligkeit und der hohen Komplexität der Projekte nicht frei von Risiken und so großen Unsicherheiten unterworfen. Diese machen sich oft im ungünstigsten Zeitpunkt bemerkbar und können den geplanten Projektverlauf empfindlich stören.

Eine nicht unwichtige Aufgabe besteht deshalb im Rahmen der Projektplanung darin, zu untersuchen, welche möglichen Risiken und Schwierigkeiten bei der Projektdurchführung auftreten können. Mit Risiko wird in diesem Fall die Möglichkeit bezeichnet, dass es im Projektverlauf zu negativen Auswirkungen kommt. Ein solches Risiko setzt sich zusammen aus:

- den möglichen Problemen;
- der Wahrscheinlichkeit ihres Auftretens;
- der Tragweite (Auswirkungen) beim Auftreten der Probleme sowie
- der Aufwände, die betrieben werden müssen, um das Risiko zu mindern.

Hier ist das Projektmanagement gefordert, ein vorbeugendes Risikomanagement zu betreiben. So muss die Projektleitung unter Einsatz bestimmter Techniken und Verfahren versuchen, Probleme vorherzusehen, ihnen vorzubeugen und damit das Projektrisiko zu mindern.

Die folgende Übersicht soll zeigen, dass **Risikomanagement** verschiedene **Tätigkeiten** umfasst, die in vier Abschnitte unterteilt werden können:

- die Identifikation der Risiken,
- die Bewertung der Risiken,
- die Klassifizierung sowie
- die Behandlung der Risiken.

Den Zusammenhang skizziert Abbildung 5.23.

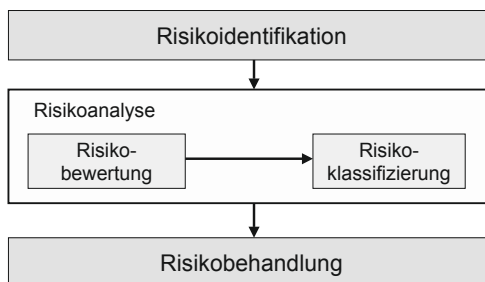


ABBILDUNG 5.23

Aktivitäten im Risikomanagement von Projekten

In der Praxis beschränkt sich Risikomanagement oft auf die Risikoanalyse. Wichtig ist aber auch die Risikobehandlung, bei der mögliche Reaktionen auf die erkannten Risiken zusammengestellt werden.

Ausgehend von den identifizierten Projektrisiken kann eine Bewertung der bestehenden Risiken vorgenommen werden (beispielsweise hinsichtlich der Wahrscheinlichkeit des Eintretens). Schließlich sind die Ursachen für die Risiken und Konsequenzen (bei Eintritt des Risikos) zu beschreiben.

Aber nicht nur das Erkennen und Bewusstmachen der Risiken im Projekt ist wichtig, sondern vor allem das Minimieren dieser Projektrisiken. Deshalb sollten bereits in der Planungsphase des Projektes Strategien entwickelt werden, wie die Risiken beseitigt, verringert oder im Fall des Eintretens beherrscht werden können.

Im Ergebnis sind – ausgehend von den identifizierten Risikofaktoren – **Maßnahmen zur Risikovorsorge (= Risikobehandlung)** zu formulieren. Ein Beispiel zeigt Tabelle 5.18.

TABELLE 5.18 Maßnahmen im Risikomanagement von Projekten (Beispiel)

Risikofaktoren im Projekt	Mögliche Maßnahmen zur Risikovorsorge	Verantwortlich, Termin
Mangel an geeignetem Teampersonal	▪ Schulungen durchführen ▪ Fördermaßnahmen zur Teamentwicklung ▪ „Einkauf“ externer Spezialisten	NN, xxxx.05.01
Unrealistische Kosten- und Zeitpläne	▪ Ausarbeitung detaillierterer Pläne ▪ Durchführung von Schätzklausuren ▪ Hinzuziehen von Experten	
Unzureichende Benutzerakzeptanz	▪ frühzeitige Einbindung der Endbenutzer in der Entwicklungsphase (QFD-Workshops) ▪ Prototyp erstellen ▪ konsequentes Change-Management	

Bei den in der rechten Spalte eingetragenen Maßnahmen kann noch eine Differenzierung dahingehend vorgenommen werden, ob es sich um **vorbeugende Maßnahmen** oder **Eventualmaßnahmen** handelt. Vorbeugende Maßnahmen werden im Vorfeld ergriffen, um das Risiko zu mindern. Dies geschieht in der Regel in der Form, dass Maßnahmen geplant und anschließend auch realisiert werden, die das Eintreten der auslösenden Ursachen und damit das Auftreten des möglichen Problems verhindern oder zumindest die Wahrscheinlichkeit des Eintretens senken.



Es empfiehlt sich, für alle Maßnahmen, die durchgeführt werden sollen, noch festzulegen,

- wer für die Durchführung der Maßnahme verantwortlich ist;
- welche Stelle mit der Durchführung der Maßnahme beauftragt werden soll und
- bis zu welchem Termin die Maßnahme realisiert bzw. vorbereitet sein muss.

5.5.8 Nutzung von Projektmanagement-Software für die Projektplanung

Projektmanagementprogramme bieten vielen Projektleitern die Chance, eine effizientere Planung und Steuerung der zu betreuenden Projekte zu realisieren. Auch Projektmitarbeiter profitieren davon, indem

- klar orientierende und motivierende Zielvorgaben erstellt,
- Aufgaben präzise zugewiesen und damit
- gleichzeitig die Rahmenbedingungen für eine positive Teamarbeit geschaffen werden.

Eine Orientierung, in welchen Phasen der Projektarbeit welche Teilaktivitäten des Projektmanagements durch Softwareeinsatz unterstützbar sind, gibt Abbildung 5.24.

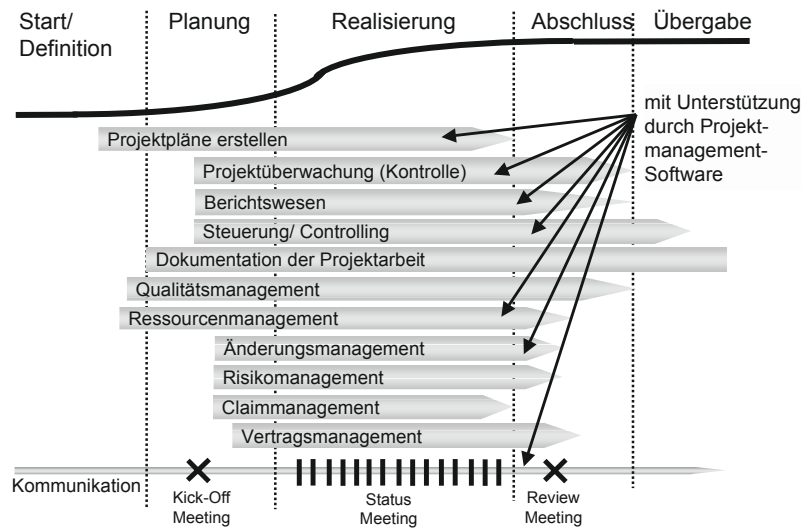


ABBILDUNG 5.24 Software-Unterstützung für Projektmanagementaktivitäten

Die Übersicht zeigt, dass ein Computerprogramm in der Startphase eines Projektes wenig hilfreich ist. Die Zieldefinition und die Analyse der Rahmenbedingungen für die Projektarbeit muss der Projektleiter in Zusammenarbeit mit dem Projektteam und dem Auftraggeber vornehmen. Demgegenüber kann gerade in der Planungs- und Steuerungsphase ein Projektmanagementprogramm wertvolle Unterstützung leisten.

Durch Einsatz eines Projektmanagementprogramms in der Planungsphase

- lässt sich die Projektstruktur in übersichtlicher Weise aufzeigen (mittels Balkendiagramm und Netzplan) und daraufhin eine genauere Projektplanung vornehmen;
- kann man automatisch eine Vielzahl wichtiger Plan- und Kontrolltermine ermitteln;
- werden wichtige Daten zur Budget- und Ressourcenplanung zur Verfügung gestellt;
- können auftretende Planänderungen schnell ohne großen Aufwand im Projektplan berücksichtigt werden;
- können im Planungsstadium verschiedene Möglichkeiten (etwa unterschiedlicher Personaleinsatz) durchgespielt werden, um herauszufinden, welche Auswirkungen diese auf das Gesamtprojekt haben (What-If-Analysen).

**Praxistipp:**

Vor der Entscheidung über ein geeignetes Programm sollten Sie sich erst einmal vergegenwärtigen, wie Programme dieser Kategorie arbeiten. Denn: Unabhängig vom eingesetzten Programm gibt es hinsichtlich der Arbeitsweise viele Gemeinsamkeiten.

■ 5.6 Kontrolle und Steuerung von IT-Projekten

Während der eigentlichen Projektumsetzung sind auch zahlreiche Management-Aktivitäten notwendig. Waren zuvor vor allem planende Aktivitäten gefragt, sind nun primär **überwachende und steuernde Funktionen durch das Projektmanagement** wahrzunehmen.

Wichtige Teilaktivitäten zur Realisierung einer ausreichenden **Projektsteuerung** zeigt im Zusammenhang die Abbildung 5.25.

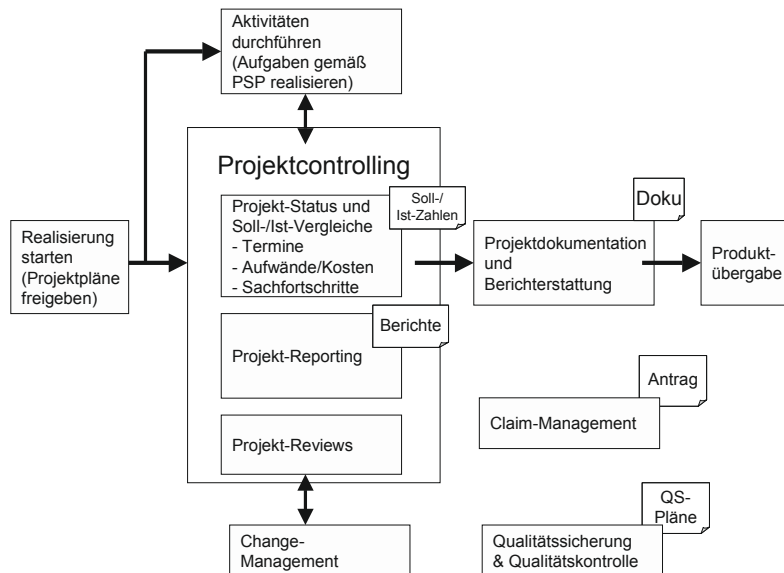


ABBILDUNG 5.25 Aufgaben bei der Projektsteuerung

Abbildung 5.25 zeigt, dass die Grundlage der Projektsteuerung die freigegebenen Projektpläne sind. Die Projektleitung muss nun sicherstellen, dass alle Mitarbeiterinnen und Mitarbeiter im Projektteam ab diesem Zeitpunkt auch über die aktuellen Daten als Orientierungsgrundlagen für ihre Arbeiten verfügen.

Mit der Umsetzung der Arbeitspakete können dann erste Ist-Daten (Ist-Anfang, Ist-Ende, tatsächlich benötigte Arbeitsstunden, Ist-Kosten) ermittelt und erfasst werden. Zur Feststellung

des Projektstatus sind diese Ist-Daten mit den Plandaten im Vergleich zu analysieren. Bei Abweichungen sind ggf. Steuerungsmaßnahmen notwendig. Dieser permanente Steuerungsprozess wird so lange durchgeführt, bis das Projekt erfolgreich beendet ist. Parallel erfolgt eine Projektdokumentation, die Aufbereitung von Projektinformationen sowie die Bereitstellung von Reports für unterschiedliche Berichtsempfänger.

Im Wesentlichen ist natürlich die Projektleitung gefordert, mit Unterstützung des Projektteams und eventuell eines Controllers oder eines Qualitätsmanagementbeauftragten, Steuerungsmaßnahmen festzulegen, zu diskutieren, zu beschließen und einzuleiten.

5.6.1 Varianten der Projektüberwachung

In Projekten ist eine permanente Fortschrittsüberwachung zu den Vorgängen, Ressourcen (Personaleinsatz, Materialverbrauch), Qualitäten und Kosten nötig. Voraussetzung zur Durchführung von Kontrollen ist in vielen Fällen, dass messbare oder genau beschriebene Soll-Werte vorhanden sind. Dies bedeutet beispielsweise, dass dem Mitarbeiter im Projekt genau klar ist, worauf es ankommt, um den Erwartungen zu entsprechen. Nur so können die für Kontrollen typischen Soll-Ist-Vergleiche durchgeführt werden. Dies ist natürlich bei den „harten“ Daten einfacher als bei den „weichen“.

Tabelle 5.19 gibt einen Überblick über typische Kontrollgrößen, Kontrollzeitpunkte sowie Kontrollverfahren in Projekten.

TABELLE 5.19 Kontrollgrößen, -zeitpunkte und -verfahren

Kontrolldaten (Kontrollgrößen)	Kontrollzeitpunkte	Kontrollverfahren
Harte Daten:		
▪ Ist-Termine	▪ ereignisgebunden	▪ Meldung
▪ Ist-Zeiten (Ist-Aufwand)	▪ periodisch (monatlich oder wöchentlich)	▪ Zeitaufschreibung
▪ Ist-Kosten	▪ ereignisgebunden/periodisch	▪ Buchhaltungsdaten
▪ Ist-Leistungsfortschritt	▪ periodisch	▪ Meldungen
▪ Qualität der Produkte	▪ ereignisgebunden	▪ Prüfung, Review
Weiche Daten:		
▪ Leistungsbereitschaft einzelner Teammitglieder	▪ permanent	▪ Beobachtung, Interview
▪ Teamatmosphäre (Stimmungen etc.)	▪ permanent oder bei Meetings	▪ Beobachtung, Befragungen
▪ Effektivität von Meetings	▪ bei Meetings	▪ Beobachtung, Befragung
▪ Akzeptanz des Projektes	▪ ereignisgebunden	▪ Befragungen

Welches Verfahren zur Kontrolle sollte gewählt werden? Grundsätzlich kann bezüglich des Verfahrens unterschieden werden,

- ob die Kontrolldaten mündlich, schriftlich oder elektronisch erfasst werden und
- ob sie vom Projektmitarbeiter gemeldet (Bringschuld) oder vom Projektleiter selbst erhoben werden (Holschuld).

**Praxistipp:**

Bei komplexeren Projekten hat es sich bewährt, die Ist-Daten von den verantwortlichen Personen bzw. von allen Projektmitgliedern einzuholen. Diese haben dann in regelmäßigen Abständen die Daten zu melden bzw. einen Bericht über den Vorgangsfortschritt (mit genau fixierten Ist-Daten) vorzulegen. Um ein Projekt zu verfolgen, müssen außerdem die geplanten Ressourcendaten abgeglichen werden. Jeder Mitarbeiter an einem Projekt muss dazu seine Arbeitstage (oder Stunden), die er am Projekt gearbeitet hat, laufend festhalten und an das Projektcontrolling melden.

5.6.2 Statuserfassung für Projektvorgänge

Zur erfolgreichen Durchführung von IT-Projekten ist eine laufende Erfassung der Projektfortschritte erforderlich. Dazu werden in regelmäßigen Zeitabständen die Ist-Daten zum Projektlauf gesammelt. Wichtige **Projektstatus-Daten**, die es zu erfassen und zu verfolgen gilt, sind:

- Zeitdaten (Termine, geleistete Stunden/Arbeitsaufwand)
- Fertigstellungsdaten (Fertigstellungsgrad einzelner Arbeitspakete)
- Kostendaten (Höhe und Art der angefallenen Kosten)

Liegen die aktuellen Fortschrittsdaten vor, müssen diese systematisch erfasst und der bisherige Projektplan ggf. fortgeschrieben werden. Im Rahmen der Terminkontrolle ist durch die Projektleitung oder durch das Projektteam die Fortschreibung der Anfangs- und Endtermine sowie der verbrauchten Zeiten für Teilvorgänge möglich. Ergänzend erforderlich ist in vielen Fällen außerdem eine Kontrolle und Fortschreibung des Ressourceneinsatzes sowie der angefallenen Kosten.

Die **Überwachung** und der **Statusabgleich** der tatsächlichen **Anfangs- und Endtermine** sind von besonderer Bedeutung. Die Termine beeinflussen den erfolgreichen Projektverlauf unmittelbar; die entsprechenden Daten sollten deshalb vorrangig überwacht werden. Beachten Sie:

- Vorgänge, die zu spät beginnen oder enden, können das gesamte Projektziel beeinflussen. Dies ist vor allem dann der Fall, wenn sich die darauf unmittelbar folgenden Vorgänge verzögern.
- Vorgänge, die früher als geplant beginnen oder enden, schaffen zusätzliche Freiräume. So können die dadurch frei werdenden Kapazitäten der Ressourcen für die Arbeit an anderen Vorgängen eingeplant werden.

Bei überschaubaren Projekten können die Termine im Balkendiagramm gut verfolgt werden, indem man den Balken dem erreichten prozentualen Leistungsanteil entsprechend ausfüllt.



Beachten Sie:

Die Terminkontrolle und Terminsteuerung sind bei größeren Projekten nur mit Unterstützung der Netzplantechnik praktikabel durchführbar. Nur sie erlaubt einen Gesamtblick auf die zahlreichen Einzelaufgaben mit ihren vielen Abhängigkeiten im Projekt. Das Durchrechnen der Termine zum Bestimmen des kritischen Pfads ist am einfachsten mit einem Software-gestützten Netzplanverfahren möglich.

Zur Zeit- und Aufwandserfassung, die möglichst durch die Mitarbeiter selbst erfolgen sollten, kann das Formblatt aus Tabelle 5.20 verwendet werden.

TABELLE 5.20 Formular zur Zeit- und Aufwandserfassung von Projektarbeiten

Zeit- und Aufwandserfassung										
Projektbezeichnung: PORTAL							Arbeitspaket:			
Projektleiter: Dipl.-Kfm. Friedrich Müller							Ist-Analyse „Bisherige Intranet-Lösung“			
Projektmitarbeiter: Frieda Müller							Kalenderwoche: 43			
Aktivitäten	Zeitaufwand (Stunden)						Summe Aufwand Woche	Plan-Aufwand Gesamt	Tats. Aufwand Gesamt	Restl. Aufwand
	M	D	M	D	F	S				
Dokumentation der Intranet-Inhalte	8	8	4				20	25	20	5
Benutzerprofil-analyse			4	8	4		16	20	20	0

Wenn die so erfassten Daten danach computergestützt weiterverwendet werden sollen, können organisatorisch folgende Varianten in Betracht kommen,

- Alle Projektmitarbeiter führen einen „Stundenzettel“ nach der oben abgebildeten Vorlage. Die Daten des Stundenzettels werden danach zentral in das Projektcontrollingsystem übertragen.
- Für das Arbeiten mit Zugriff auf einen Projekt-Server wird den Projektmitarbeitern vom Programmsystem eine Erfassungsmaske für die Arbeitszeiten dezentral zur Verfügung gestellt. Die Erfassung erfolgt so unmittelbar im Programm durch die Mitarbeiter.

Die Projektleitung fasst die gemeldeten Ressourcendaten schließlich zu einem Projekt-Statusbericht zusammen. In der Statusmeldung werden dann letztendlich die angefallenen Personentage (kurz PT) jeweils für die einzelnen Projektphasen nachgehalten und kumuliert. Hier werden auch kurz der jeweilige Ist-Stand geschildert, Schwierigkeiten beschrieben und eingeleitete Maßnahmen erläutert. Des Weiteren sollte das geplante Vorgehen kurz dargestellt werden.

5.6.2.1 Kostenerfassung

An die Erfassung und Kontrolle der Kosten, die im IT-Projekt anfallen, werden oft besondere Anforderungen gestellt. Für die Projektleitung ergeben sich typischerweise folgende Fragen:

- Wie hoch sind die bisher angefallenen Kosten?
- Welche Personen im Projektteam haben welche Kosten verursacht?
- Wie sind die angefallenen Kosten im IT-Projekt auf die einzelnen Projektphasen bzw. einzelnen Arbeitspakete verteilt? (Vorplanung, Entwurfsplanung, Ausführungen etc.)
- Wie weit ist das Projekt abgerechnet und sind die Kosten gedeckt?

Für Auswertungen ist von Interesse, welche **Aufteilung** bezüglich der Kostenerfassung möglich ist. Dies betrifft einmal genaue Auswertungen über die Personalkosten eines Projektes. Dabei ist die Ermittlung und Erfassung der Zeiten eine wichtige Basis für gezielte Auswertungen und weitere Verrechnungen (neben den Lohnkosten bzw. einem Anteil an allgemeinen Geschäftskosten). Üblich ist die Erfassung der einzelnen Personalstunden (unterschieden werden bei den Personalkosten zwischen Normalzeit, Dienstreise, Gleitzeit, Krankheit, Urlaub und Sonderurlaub) und etwaiger Kosten, wie Materialkosten oder Aufwendungen für Unterauftragsnehmer, sowie deren Verteilung auf die einzelnen Projekte. Ergänzend wäre die Zuordnung zu Kostenstellen- bzw. Abteilungsdaten von Interesse.

5.6.2.2 Sachfortschritte im Projekt erfassen

Die Fortschrittskontrolle stellt für die Projektleitung sicherlich die wichtigste und schwierigste Kontrollaufgabe dar. Die Sachfortschrittskontrolle zerfällt in eine produkt- und eine projektbezogene Kontrolle:

- **Produktfortschrittskontrolle:** Hier muss die Frage beantwortet werden, inwieweit bestimmte Leistungsmerkmale der zu erstellenden Projektprodukte bereits erreicht sind. Dies äußert sich beispielsweise in dem Erreichen bestimmter technischer Daten sowie im Vorliegen von Qualitätssicherungsdokumenten (z. B. Testberichte).
- **Projektfortschrittskontrolle:** Hier geht es um die Bestimmung des Fertigstellungsgrades bzw. des Fertigstellungswertes.

Als Messgrößen für den Sachfortschritt werden Fortschrittsberichte der einzelnen Mitarbeiter sowie Zwischenpräsentationen verwendet. Grundsätzlich ist es empfehlenswert, während der Projektdurchführung in bestimmten Abständen Restzeitschätzungen vorzunehmen.

Bei einer integrierten Projektsteuerung sollten neben den Terminen und den geleisteten Arbeitsstunden auch das inhaltliche Projektergebnis überwacht und bewertet werden. Damit wird letztlich der Fertigstellungsgrad eines Projektes ermittelt. „Der Fertigstellungsgrad bezeichnet das Verhältnis der zu einem Stichtag erbrachten Leistung zur Gesamtleistung eines Vorgangs, Arbeitspakets oder Projekts“ (gemäß DIN 69903).

Zur Ermittlung des Fertigstellungsgrades können in der Praxis unterschiedliche Messtechniken eingesetzt werden. Beispiele sind:

- Mengen- und Zeitproportionalität: Es werden in diesem Fall die angefallenen Mengen- und Zeiteinheiten mit den geplanten Mengen- und Zeiteinheiten verglichen. Daraus wird dann der Fortschritt der einzelnen Vorgänge ermittelt.
- Schätzung: Dieses subjektive Verfahren (Angabe eines Schätzwertes in %) sollte immer dann zur Anwendung gelangen, wenn andere (präzisere) Verfahren nicht möglich sind.

Hier gibt es ein besonderes Problem, nämlich das „Fast-schon-fertig“-Syndrom. Damit wird ausgedrückt, dass die Projektmitarbeiter den erreichten Fertigstellungsgrad ihrer Aufgaben meist als zu hoch bewerten. So werden beispielsweise für die letzten 10% einer Aufgabe meist mehr als 40% der Zeit benötigt. Gründe für solche Fehleinschätzungen sind:

- Der Aufwand für die noch zu leistende Arbeit wird unterschätzt.
- Der Anteil der bereits erbrachten Leistung wird überschätzt.
- Schwierigkeiten, die in der Zukunft bevorstehen, werden verharmlost.
- Bereits eingetretene terminliche Planüberschreitungen werden ignoriert und verdrängt.
- Das Drängen der Projektleitung beeinträchtigt die Realitätstreue der Aussagen der Projektmitarbeiter.

Grundsätzlich benötigt jedes Arbeitspaket eines Projektes zur Fertigstellung einen bestimmten Zeitaufwand und verursacht damit Kosten. Um den Wert von geleisteten Arbeiten zu einem bestimmten Stichtag zu ermitteln, wird der so genannte Fertigstellungswert berechnet. Nach DIN 69903 werden unter Fertigstellungswert „die dem Fertigstellungsgrad entsprechenden Kosten eines Vorgangs, Arbeitspakets oder Projekts“ verstanden. Die Formel zur Ermittlung lautet:

$$\text{Fertigstellungswert} = \text{geplante Kosten} \times \text{aktueller Fertigstellungsgrad}$$

5.6.3 Plan-Ist-Vergleiche und Reviews

Eine besondere Aufgabe der Projektleitung ist es, Abweichungen zu erkennen und den Projektfortschritt für jeden Vorgang zu verfolgen. Dazu lassen sich konkrete **Vergleiche von Plan- und Ist-Daten** vornehmen. Durch diesen Vergleich der geplanten Daten mit aktuellen Daten können mögliche Probleme schon bei der Entstehung erkannt und frühzeitig gelöst werden.

In der Praxis gibt es natürlich zahlreiche Gründe dafür, dass **Abweichungen zwischen Plan und Ist** auftreten:

- unvorhergesehene Änderungen im Projektverlauf (neue Schwerpunktsetzungen bei der Projektaufgabe, unerwartete Auswahl von Personal)
- unrealistische Planung (Einplanung von zu wenig Reiseaufwand, etc.)
- Fehler in der Arbeitsausführung
- nicht planmäßige Durchführung durch fehlende Qualifikation bzw. unzureichende Motivation der Beteiligten
- Spannungen im Projektteam
- falsche Einschätzungen von Umweltbedingungen und den damit verbundenen Auswirkungen (beispielsweise finanzielle Bedingungen, Preisentwicklungen auf den Märkten etc.).

Grundsätzlich werden drei **Arten von Abweichungen im Projektmanagement** unterschieden:

- Terminabweichungen
- Ergebnis-/Sachfortschrittsabweichungen
- Kostenabweichungen.

Ausgehend von den vorliegenden Ist-Daten und ihrer Analyse sind dann im Bedarfsfall geeignete Korrekturmaßnahmen einzuleiten. Während kleinere Abweichungen oft ohne großen Aufwand korrigiert werden können, sind größere Abweichungen möglich, die auch eine Korrektur der Pläne oder sogar der Projektziele auslösen können. Durch ein entsprechendes Projektcontrolling müssen diese Abweichungen frühzeitig erkannt und daraufhin Maßnahmen überlegt und ergriffen werden, die die Abweichungen wieder ausgleichen.

**Beachten Sie:**

Ständige Soll-Ist-Vergleiche sind wichtige Instrumente eines modernen Controlling. Im Projekt kann so früh eine gravierende Abweichung erkannt werden, um durch geeignete Steuerungsmaßnahmen entweder das Projekt wieder „in den Plan“ zu holen oder die Projekt-Planvorgaben zu ändern.

Liegen keine Terminabweichungen aufgrund der Plan-Ist-Vergleiche vor, sollte eventuell noch ergänzend eine **Termin-Trendanalyse** durchgeführt werden. Damit können künftige Verzögerungen aufgezeigt werden. In diesem Fall werden ältere Planwerte mit neuen Plandaten verglichen und – ausgehend von eventuell in Angriff zu nehmenden Korrekturen – entsprechende Trends ermittelt.

Ein besonderes Verfahren ist die **Meilenstein-Trendanalyse**. Sie vermag aufzuzeigen, inwieweit Arbeitspakete zur Erreichung eines Meilensteins (voraussichtlich) fristgerecht abgearbeitet werden. Damit lassen sich frühzeitig Verzögerungen erkennen und entsprechende Korrekturmaßnahmen einleiten; etwa Fremdvergaben organisieren oder zusätzliche Kapazitäten bereitstellen. Die Meilenstein-Trendanalyse erfolgt am besten grafisch: dazu wird eine Grafik angelegt, die etwa links den Planungszeitraum und rechts den Projektfortschritt (und damit den Berichtszeitraum) angibt.

Werden Leistungs- und Qualitätskontrollen vorgenommen, so erstrecken sich die auf die Arbeitsergebnisse eines Projektes. Damit soll aufgezeigt werden, ob die jeweils erzielten Ergebnisse dem Zeit- und Kostenaufwand entsprechen. Bei komplexen Entwicklungsprojekten hat es sich bewährt, bei Erreichen ganz bestimmter Meilensteine die Projektprodukte einem umfassenden Überprüfungsverfahren – einem **Review** – zu unterziehen. Zur Durchführung solcher Reviews wird meist eine spezielle Reviewgruppe zusammengestellt. Diese sollte über eine kollektive Fachkompetenz verfügen, die größer ist als die der Projektgruppe, deren Arbeitsergebnisse überprüft werden.

5.6.4 Kostencontrolling in Projekten

Bei der Kostenüberwachung werden die bis zu einem bestimmten Zeitpunkt geplanten Kosten den bis dahin angefallenen Kosten gegenübergestellt. Dies gibt bereits erste Anhaltspunkte, ob eventuell gegengesteuert werden muss. Eine Beispiel-Aufstellung eines **Soll-Ist-Kostenvergleiches** gibt Tabelle 5.21 wieder.

TABELLE 5.21 Beispiel für einen Soll-Ist-Kostenvergleich

Kostenarten	Soll-/Ist-Vergleich		Abweichungsanalyse	Beurteilung
	Soll	Ist		
Personalkosten	140	144	- 4	geringe Überschreitung
Materialkosten	24	20	+ 4	gute prozentuale Einsparung
Reisekosten	16	36	- 20	enorme Überschreitung der Kosten
Fremdleistungen	4	2	+ 2	Einsparung von 50%
Raumkosten	6	6	-	ausgeglichen
Gemeinkosten	10	12	- 2	Überschreitung um 20%
Summe	200	220	- 20	Überschreitung um 10%

Liegt keine Kostenüberschreitung vor, kann eine so genannte Kosten-Trendanalyse hilfreich sein, um künftige Abweichungen aufzuzeigen.

5.6.5 Projektreporting

Entscheidungsträger – seien es der Auftraggeber, das Projektbüro, die Unternehmensleitung oder der Kunde des Projektes – benötigen zur zielgerichteten Steuerung der Projektarbeit in regelmäßigen Abständen geeignete Informationen. Dabei gilt der Grundsatz, dass nicht alle Empfänger dieselben Projektinformationen in demselben Detaillierungsgrad erhalten müssen. Bei der Planung der Projektberichterstattung und der Projektdokumentation müssen deshalb vorweg einige Fragen geklärt werden, die letztlich darüber entscheiden, was im Detail zu tun ist. **Gestaltungsfragen der Projektberichterstattung** betreffen

- den Inhalt (was?),
- die Person des Berichterstatters und des Berichtsempfängers (wer?),
- die Form (wie?) sowie
- den Zeitpunkt der Berichterstattung (wann?).

Inhalte von Projektberichten:

Anhand der Checkliste Tabelle 5.22 können Sie die wichtigsten Aspekte für die Inhalte eines Projektberichtes zusammenstellen (abhängig von der Empfängergruppe).

TABELLE 5.22 Checkliste: Inhalte eines Projektberichtes

Hauptbereiche	Spezifikationen
Stand der Projektarbeiten laut Strukturplan	▪ fertiggestellt (erledigte Arbeitspakete) ▪ in Arbeit (inkl. vorliegender Zwischenergebnisse) ▪ in Unterbrechung ▪ noch zu arbeiten

Hauptbereiche	Spezifikationen
Terminplan der Projektaktivitäten/-ergebnisse	▪ Soll-Termine ▪ Ist-Termine
Kostenplan der Projektaktivitäten/-ergebnisse	▪ Soll-Kosten ▪ Ist-Kosten
Übersicht der Kapazitätsbelastungen	Personentage
Abweichungsanalysen	▪ Beschreibung der zu erkennenden Auswirkungen von Abweichungen ▪ mit Kommentaren und Vorschlägen für Steuerungsmaßnahmen
Stand des Projektbudgets	▪ Planansatz ▪ bisher verbraucht ▪ noch verfügbar ▪ Abweichungen gegenüber dem Planansatz
Hinweise auf Probleme, Risiken	▪ aktuelle Engpässe in der Projektarbeit ▪ Sachverhalte, die einer Änderung bedürfen ▪ ggf. Risikobewertung (wenn es sich um gravierende Änderungen handelt)
Handlungsbedarf	notwendige Maßnahmen
Projektbezogene Kennzahlen	▪ Kosten (Wie hoch? Welche Restkosten sind noch zu erwarten?) ▪ Termine ▪ Meilensteine ▪ Kapazitäten u. a.

**Beachten Sie:**

Ohne vereinbarten Berichtsplan ist ein modernes Projektmanagement und Projektcontrolling nicht denkbar. Darin ist beispielsweise festzulegen, welche Berichte in dem jeweiligen Projekt von wem erstellt werden und wer als Empfängerkreis zu berücksichtigen ist. Ergänzend kann angegeben werden, zu welchen Zeitpunkten und in welcher Form (Papier, online per E-Mail und auf der Online-Arbeitsplattform des Projektes) die Berichtsinformationen zu übermitteln sind.

5.6.6 Claim-Management

Trotz einer guten Projektvorbereitung und aller gründlichen Vorüberlegungen zu Projektbeginn können im Projektverlauf immer wieder Änderungswünsche an das Projektteam herangetragen werden. Die **Gründe** dafür sind vielfältig:

- Es werden zusätzliche Wünsche von dem internen oder externen Auftraggeber bzw. auch von anderen Stakeholdern des Projektes formuliert.

- Neue technische Erkenntnisse und Entwicklungen machen ein Überdenken der bisherigen Ziele und Projekt-Anforderungen notwendig.
- Es werden zusätzliche behördliche Auflagen gemacht, die zu berücksichtigen sind.
- Es wurden Fehler oder unpräzise Angaben in der ursprünglichen Spezifikation für das Projektergebnis gemacht.

In der Vergangenheit – so zeigen Erfahrungen aus zahlreichen IT-Projekten – wurde auf ein konsequentes Management von eingehenden Änderungen weitgehend verzichtet. Die Folge war, dass die Wünsche entweder ohne Überprüfung ihrer Auswirkungen (hinsichtlich Aufwand, Kosten und Zeiten) akzeptiert wurden oder dass jede weitere Änderung rigoros abgelehnt wurde. Beides ist sicherlich keine gute Reaktion; denn

- einerseits muss genügend Flexibilität gegeben sein, um neuen Herausforderungen gerecht zu werden und
- andererseits muss natürlich gesehen werden, dass häufige und unkontrolliert eingebrachte Änderungen nicht nur zusätzlichen Arbeitsaufwand verursachen, sondern auch den Planungs- und Koordinierungsaufwand im Projekt erhöhen.

Heute setzt sich immer mehr die Erkenntnis durch, dass eingehende Änderungsnotwendigkeiten systematisch geprüft und entsprechend entschieden werden. Für diesen Tätigkeitsbereich hat sich mittlerweile der Begriff „**Claim-Management**“ etabliert (abweichend finden sich aber auch Begriffe wie „Konfigurationsmanagement“ oder „Umfeldmanagement“). Damit wird quasi ein klares Verfahren vereinbart, wie mit solchen Änderungswünschen umzugehen ist. So kann erreicht werden, dass

- das Projektmanagement aufkommende Änderungswünsche im Griff behält;
- Eigenclaims (Anforderungen aus dem Projektteam) und Fremdclaims (Anforderungen des Kunden) rasch erfasst und berücksichtigt werden sowie
- ein aktives Gestalten der Umfeldbeziehungen ermöglicht wird.

Ein Änderungsantrag (bzw. eine veränderte Spezifikations- oder Fehlermeldung) ist – sobald die Notwendigkeit erkannt worden ist – durch die Verantwortlichen auszufüllen und an die Projektleitung weiterzuleiten. Wichtig ist, dass dieser Änderungsantrag dem Grundsatz Rechnung trägt, dass nur kontrolliert geändert werden darf. Die Auswirkungen auf andere Arbeitspakete und auf die Komponenten des Projektgegenstandes sowie auf Termine und Kosten müssen zunächst systematisch überprüft werden.



Beachten Sie:

Die Prüfung erfolgt im Wesentlichen durch die Projektleitung (evtl. auch unter Hinzuziehung weiterer Fachleute), die die Auswirkungen schriftlich im Change Request-Formular festhält. Danach kann eine Entscheidung getroffen werden. Bei kleineren Projekten entscheidet die Projektleitung bezüglich Änderungen eventuell selbst. Bei größeren Projekten gibt es oft einen „Change Control Board“ (besonderes Gremium zur Überwachung und Steuerung von Änderungswünschen), in dem auch der Auftraggeber vertreten ist.

Den gesamten Ablauf eines solchen Änderungsverfahrens gibt Abbildung 5.26 wieder.

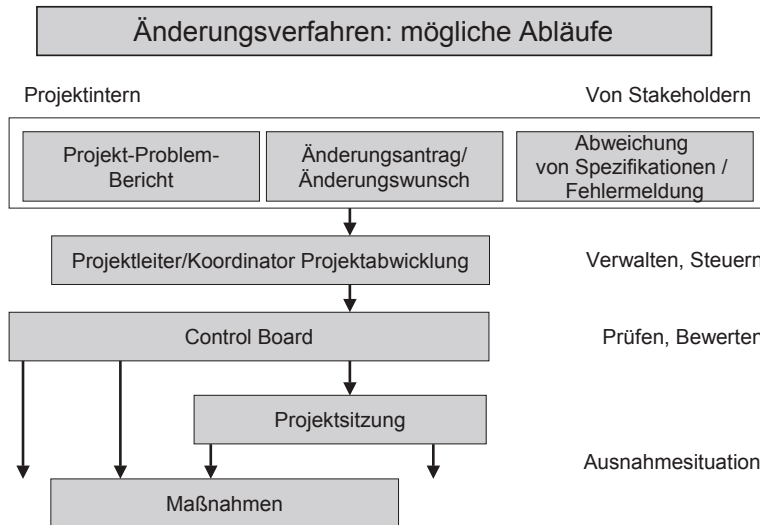


ABBILDUNG 5.26 Ablauf eines Änderungsverfahrens

5.6.7 Projekt-Marketing

Um den Projekterfolg nachhaltig zu sichern, muss ein IT-Projekt bereits im Vorfeld, während der Durchführung und im Rahmen der Umsetzung der Ergebnisse „vermarktet“ werden. Mit einem sorgfältig dosierten **Marketing-Mix** kann die Anerkennung und der Erfolg für ein Projekt erheblich verbessert werden. Die Wirkungen eines professionellen Projekt-Marketings sind weitreichend:

- Aktuelles aus der Projektarbeit wird zielgerichtet weitergegeben (abhängig von den Interessen der Stakeholder). Der verbesserte Informationsgrad zum Projekt geht Hand in Hand mit vermehrter Anerkennung der Projekt-Mitarbeiter und der Projektergebnisse.
- Bei einem hohen Informationsgrad lassen sich Entscheidungen durch den Auftraggeber im Projektverlauf leichter durchsetzen. Der Hauptgrund liegt in dem verbesserten Informationsstand und dem sich daraus ergebenden höheren Vertrauen in die Qualität der Projektarbeit.
- Der Projekt-Erfolg wird bekannt, sodass die verdiente Anerkennung der Projektarbeit laufend gegeben ist und die Motivation des Projektteams weiter gesteigert wird.

Die **Maßnahmen für ein Projektmarketing** sind vielfältig. Dazu zählen

- Informationsveranstaltungen (Marketing-Veranstaltungen für künftige Nutzer u. a.);
- Informationsbroschüren (beispielsweise periodisch als Projekt-Newsletter);
- Präsentation und Kommunikation via Intranet (E-Newsletter, Informationsforen, Projekt-Intranetsite mit aktuellen Infos rund um das Projekt, etc.).



Beachten Sie:

Marketingmaßnahmen für das im Projekt hergestellte Produkt sollten schon während der Projektumsetzung betrieben werden. Natürlich wird die Intensität gegen Ende der Umsetzung ansteigen. Im Ergebnis soll so eine hohe Akzeptanz des hergestellten Produktes beim Kunden/dem Projekt-Auftraggeber und im sonstigen Projektumfeld (den Stakeholdern) erreicht werden.

Durchführen und Steuern von Projektmarketingaktivitäten heißt nicht nur, die zuvor vereinbarten Maßnahmen des Projektmarketings umzusetzen, sondern auch, den gesamten Prozess zu kontrollieren und zu steuern. Dabei werden die einzelnen Teilprozesse „Analyse des Projektumfeldes“, „Planung von Zielen, Strategien und Maßnahmen“ sowie „Durchführung und Steuerung“ iterativ durchlaufen.

Abbildung 5.27 illustriert den skizzierten Projektmarketingprozess.

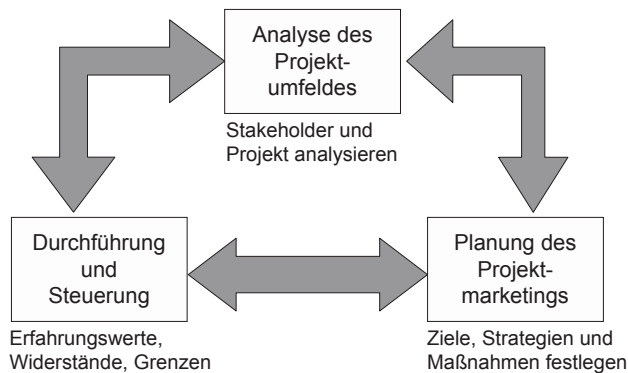


ABBILDUNG 5.27
Schritte im Projektmarketing

Als Fazit ist festzuhalten: Das Projektumfeld bedarf einer permanenten Analyse, um zu geeigneten Kommunikationsinstrumenten und -wegen zu kommen. Dies bedeutet für die Praxis, dass die Projektmarketing-Maßnahmen nicht nur durchzuführen, sondern auch ihre Auswirkungen im Umfeld zu beachten sind. Demzufolge handelt es sich beim Projektmarketing um einen Prozess, bei dem die Planung der Maßnahmen regelmäßig die Änderungen im Projektverlauf berücksichtigen muss.

5.6.8 Nutzung von Projektmanagement-Software für die Projektsteuerung

In der **Realisierungsphase** liefert ein Projektmanagementprogramm wichtige Steuerungsinformationen:

- Tatsächlich realisierte Werte (Zeiten, Ressourceneinsatz, Kosten) können für die einzelnen Arbeitspakete erfasst werden.
- Es sind permanente Soll-Ist-Vergleiche möglich. Diese liefern wertvolle Informationen für die Steuerung der Projektarbeit.

Nach dem Projektstart verlagert sich der Aufgabenbereich des Projektleiters auf die **Kontrolle und Steuerung des Projektes**. Zu diesem Zweck müssen die jeweiligen Projektfortschritte erfasst werden. Dies sind:

- die benötigten Ist-Zeiten,
- der tatsächliche Ressourcenverbrauch sowie
- die tatsächlich angefallenen Kosten.

Diese Daten müssen kontinuierlich oder in regelmäßigen Abständen (wöchentlich oder monatlich) erfasst werden.

Nach Eingabe von Ist-Terminen, tatsächlicher Ressourcennutzung und der Ist-Kosten lassen sich verschiedene **Soll-Ist-Vergleiche** anstellen. Beispiele sind:

- Projektstatus-Übersichten
- Soll-Ist-Vergleichlisten zu Terminen und Ressourceneinsatz
- Kostenentwicklungsübersichten
- Ressourcen-Auslastungs-Diagramme

Aus diesen Werten, die wertvolle Projektkontroll-Hilfen bieten, kann eine fortlaufende Fortschreibung der Anfangs- und Endtermine vorgenommen werden. Außerdem geben sie Anregungen, ob bei Abweichungen Maßnahmen zur Gegensteuerung ergriffen werden müssen.

Den Zusammenhang mit den wesentlichen **Grundarbeiten mit einem Projektmanagementprogramm** verdeutlicht Abbildung 5.28.

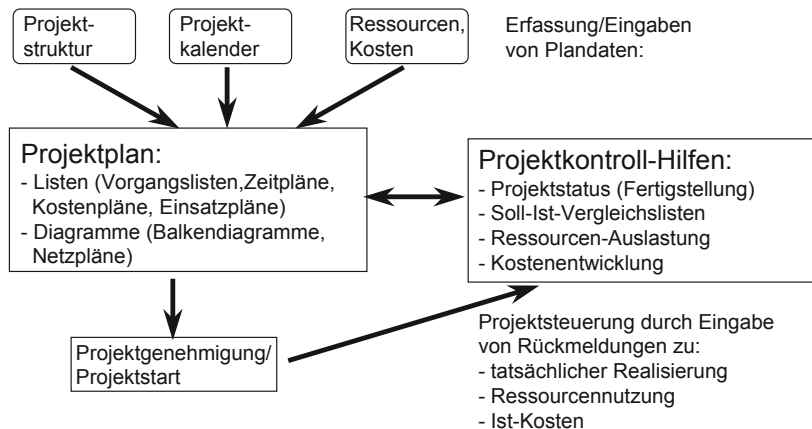


ABBILDUNG 5.28 Arbeiten mit einem Projektmanagementprogramm

Die angebotenen Projektmanagementprogramme sind darüber hinaus einer permanenten Weiterentwicklung unterworfen. Der Trend geht dabei immer stärker dahin, dass ein Projektmanagementprogramm nicht nur für die Projektleitung hilfreich ist, sondern auch das Projektteam selbst sowie ein Projekt-Office (Unterstützung von Multiprojektmanagement-Funktionen) und das Management (etwa für ein spezielles Projektcontrolling) ein solches Programm sinnvoll nutzen kann. Die Entwicklungslinien verdeutlicht Abbildung 5.29 (nächste Seite).

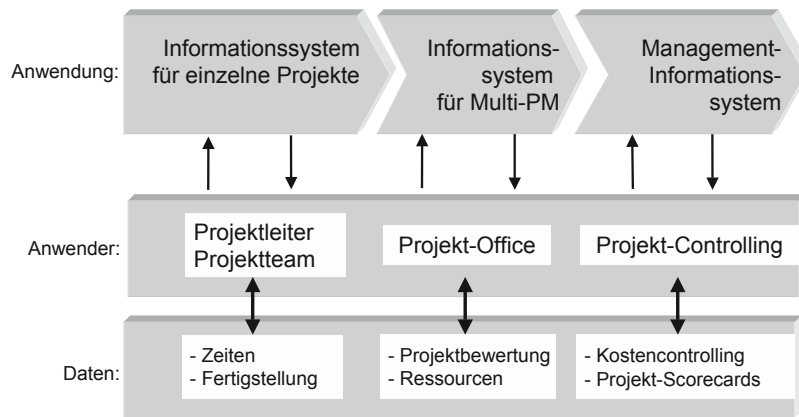


ABBILDUNG 5.29 Entwicklungslinien von Projektmanagementsoftware

■ 5.7 Multiprojektmanagement und Projektportfoliomanagement

IT-Verantwortliche und ihre Mitarbeiter führen in der Regel nicht nur ein Projekt durch. In der Praxis müssen meist mehrere IT-Projekte gleichzeitig gesteuert und umgesetzt werden. Diese Projekte können eine sehr unterschiedliche Ausrichtung hinsichtlich der angestrebten Projektergebnisse haben (seien es Software-Entwicklungsprojekte, IT-Infrastrukturprojekte oder strategische IT-Projekte) sowie eine unterschiedliche strategische Relevanz für das Unternehmen haben. Dies gilt es bei Auswahlentscheidungen ebenso wie bei der Durchführung zu berücksichtigen. Mit Methoden und Instrumenten des Projekt-Portfoliomanagements lassen sich die vielfältigen Aufgaben zur Bewertung, Qualifizierung und kontrollierten Steuerung sämtlicher IT-Projekte ganzheitlich erfolgreich realisieren, von der Anforderungsanalyse und Priorisierung bis hin zur Realisierung und Produktivsetzung der jeweiligen IT-Projekte.

Eine erfolgreiche Umsetzung der genehmigten IT-Projekte setzt in jedem Fall eine entsprechende Multiprojektmanagement-Organisation voraus. Dabei ist zu beachten, dass sich IT-Projekte durch eine relativ hohe Komplexität sowie einen nicht unerheblichen Innovationsgehalt der Aufgabenstellung auszeichnen. Mitarbeiter aus unterschiedlichen Abteilungen und Kulturen sind einzubeziehen sowie externe Mitarbeiter in die Projektarbeit zu integrieren. Während der Projektlaufzeit kommen diverse Änderungen der zuvor festgelegten Projektziele und Kunden-Anforderungen hinzu.

Während das Einzelprojektmanagement die zur erfolgreichen Durchführung eines singulären IT-Projekts notwendigen Projektmanagementprozesse beinhaltet, also den Projektstart (Projektplanung), das regelmäßige Projektcontrolling, die kontinuierliche Projektkoordination und den Projektabschluss (vgl. [Ste06], S. 121), geht es im Multiprojektmanagement um die Planung und Steuerung der Abwicklung von mehreren, ggf. miteinander verknüpften IT-Projekten. Dabei wird Multiprojektmanagement als summarischer Oberbegriff für ein Set an

Methoden und organisatorischen Einrichtungen gesehen und umfasst Prozesse wie Projektbeauftragung, Multiprojektcontrolling sowie Projektanbahnung und -evaluierung.

Abbildung 5.30 zeigt einen Überblick über die **Prozesse im Projektmanagement**.

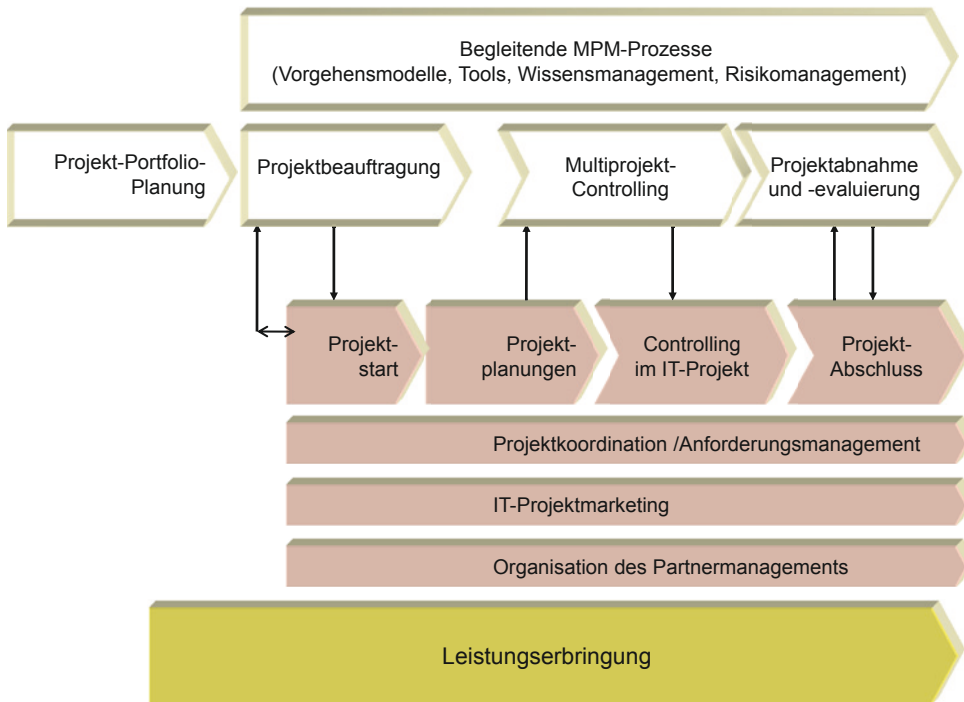


ABBILDUNG 5.30 Prozesse im Projektmanagement

5.7.1 Zielsetzungen und Erfolgsfaktoren im Multi-Projektmanagement

Zur erfolgreichen Umsetzung von Multiprojektmanagement bietet sich das Instrumentarium „Projekt-Portfoliomanagement“ an. Dieses leistet unter anderem einen Beitrag, um eine sachgerechte Anforderungsdefinition für IT-Projekte vorzunehmen und daraufhin die „richtigen IT-Projekte“ auszuwählen. In der Planungsphase für die beschlossenen IT-Projekte kann eine ganzheitliche Ressourcen- und Kostenplanung erfolgen. Darüber hinaus ist eine projektübergreifende Steuerung systematisch und zielgerichtet möglich, so dass beispielsweise angemessene Reaktionen auf unvorhergesehene Ereignisse möglich sind. Die erwähnten Methoden helfen dann auch, möglichst viele IT-Projekte in der geplanten Zeit und innerhalb des festgelegten Budgetrahmens abzuschließen.

Um die Herausforderungen des IT-Portfoliomanagements zu verdeutlichen, liegt es nahe, die Merkmale einer Multi-Projektmanagement-Umgebung für den IT-Bereich in Erinnerung zu rufen:

- Es gibt mehrere parallel laufende IT-Projekte.

- Die verschiedenen IT-Projekte greifen auf die gleichen Ressourcen (Personal, Sachmittel) zu.
- Mitunter bestehen Beziehungen bzw. Vernetzungen zwischen den verschiedenen Projekten. So sind IT-Projekte oft mindestens über die Ressourcen miteinander verbunden (Zugriff etwa auf gemeinsames Personal).
- Die Einzelprojekte werden nach anerkannten Regelungen und Vorgehensweisen zum Projektmanagement abgewickelt.



Beachten Sie:

IT-Portfoliomanagement bedeutet letztlich, Kosten und Nutzen, Risiken und Chancen von IT-Investitionen (IT-Projekten) gemeinsam zu betrachten und eine kohärente Strategie konsequent umzusetzen! Konsequent eingesetzt, wird der Aufwand um 5 bis 10% reduziert.

Angesichts parallel laufender Projekte gewinnt die **übergeordnete Steuerung aller Projekte** auf der strategischen Ebene des Unternehmens eine herausragende Bedeutung. Eine **Abgrenzung zwischen Multiprojektmanagement und Einzelprojektorganisation** zeigt Tabelle 5.23:

TABELLE 5.23 Multiprojektmanagement versus Organisation einzelner Projekte

Ausrichtungen	Multiprojekt-Umgebung	Einzelprojektorganisation
Kernfrage	Arbeiten wir an den richtigen IT-Projekten?	Machen wir mit dem Projekt alles richtig?
Merkmale	▪ Mehrere parallel durchgeführte IT-Projekte ▪ Für die verschiedenen IT-Projekte stehen – zumindest teilweise – gleiche Ressourcen zur Verfügung. ▪ Eine übergeordnete Projektsteuerung wäre sinnvoll.	▪ Ein mehr oder weniger komplexes IT-Projekt ▪ „Einmaligkeit“ ▪ Die Lösung der Projektaufgabe erfordert ein abgestimmtes Teamworking.
Zielsetzungen	▪ Hohe Effektivität bei der Abwicklung der verschiedenen IT-Projekte ▪ Übergreifend hohe Kapazitätsauslastung	▪ Hohe Effizienz der jeweiligen Projektabwicklung ▪ Beachtung des magischen Dreiecks von Qualität, Kosten und Zeit
Organisation/ Instrumente	▪ Ggf. Einrichtung eines zentralen Projektbüros (Project Office) ▪ Steuerungsinstrumente für übergreifenden Personaleinsatz sowie für Kapazitätsausgleich ▪ Gemeinsame Regeln für das Berichtswesen	▪ Projektmanagement-Instrumente ▪ Planungswerkzeuge (Termine, Kosten, Arbeitspakete etc.) ▪ Controlling-Instrumente

Aus den Problemen und Herausforderungen lassen sich wesentliche **Ziele eines modernen IT-Portfoliomanagement** ableiten:

- Die „richtigen“ Projekte durchführen.
- Die den diversen Projekten zugeteilten Ressourcen voll auslasten (Kapazitätsabstimmung).
- Eine hohe Vergleichbarkeit der Informationen herstellen.

Wesentliche **Zielsetzungen** und daraus abgeleitete **Hauptaktivitäten im Multiprojektmanagement für IT-Projekte** skizziert Tabelle 5.24.

TABELLE 5.24 Multiprojektmanagement – Zielsetzungen und Aktivitätsfelder

Zielsetzungen	Aktivitätsfelder im Multiprojektmanagement
Die richtigen Projekte	Auswahl für IT-Projekte: ▪ geeignete Priorisierungsverfahren bereitstellen und anwenden ▪ Projektanträge/zur Wahl stehende IT-Projekte bewerten
Entscheidungsfindung im gesamten Unternehmensinteresse abstimmen	Organisationsgestaltung für IT-Projekte: ▪ Anwendung und Pflege eines Projekt-Managementhandbuchs ▪ Entscheidungsverfahren und Wissensmanagement vereinbaren
Projektaufträge bei optimierter Kapazitätsauslastung zeitgerecht erfüllen	Kapazitätsabstimmungen für IT-Projekte: ▪ Personal- und Zeitplanungen vornehmen ▪ Verfahren zum Kapazitätsabgleich vereinbaren
Transparente Abläufe während der Durchführung sicherstellen	Überwachung und Steuerung der IT-Projekte: ▪ Steuerung mit Portfolios ▪ Project-Office als Institution ▪ abgestimmtes Berichtswesen und Scorecards vereinbaren



Beachten Sie:

Beim Multiprojektmanagement geht es nicht um die Optimierung der Durchführung eines einzelnen Projektes, sondern um eine Vorgehensweise und Methodik für die Abwicklung vieler parallel laufender Projekte. Außerdem soll eine Begleitung durch ein oder mehrere Genehmigungsgremien (Boards) erfolgen, die auch den Fortschritt der Projekte beobachten und Hilfestellungen bei Eskalationen geben.

5.7.2 Projektauswahl mittels IT-Portfolioanalyse

Im Rahmen des IT Portfolio-Managements empfiehlt es sich, alle anstehenden bzw. beantragten Projekte einer gemeinsamen Bewertung zu unterziehen. Dabei besteht die Aufgabe des Portfoliomanagements darin, Projektideen oder -anträge zu identifizieren und zu priorisieren, indem eine entsprechende Prüfung und Bewertung des Kosten-/Nutzenverhältnisses für das Unternehmen erfolgt.

Im Rahmen des Portfoliomanagements können bezüglich der Auswahlentscheidung mehrere **Projekttypen** unterschieden werden: Muss-Projekte, Soll-Projekte und Standard-Projekte.

- **Muss-Projekte** sind in jedem Fall durchzuführen, etwa aufgrund gesetzlicher Vorgaben oder unausweichlicher Tatsachen (Nichtmehrverfügbarkeit von Services etc.). Ein Beispiel sind die Softwareprojekte anlässlich der Euro-Umstellung (Gesetz).
- **Soll-Projekte** sind wünschenswerte, etwa von der Unternehmensführung aus unternehmenspolitischer Sicht „gesetzte“ Projekte. Sie werden deshalb im Regelfall auch keiner besonderen Bewertung unterzogen.

- **Standard-IT-Projekte** durchlaufen einen standardisierten Bewertungsprozess, z. B. hinsichtlich ihres Kapitalwertes und Risikos oder ihres Beitrages zur Erreichung von Unternehmenszielen (Nutzwertanalyse). Ein Beispiel wäre die Einführung eines CRM-Systems oder die Umgestaltung des Personalwesens inkl. Softwareumstellung.

Die Einbeziehung von Muss-Projekten in den Bewertungsprozess ist nicht notwendig, doch aus informatorischen Gründen möglich. Das Management ist aufgefordert, die entsprechende Unterstützung für die genehmigten Projekte zu gewährleisten. Die Experten der Organisation stehen außerdem in der Pflicht, die *überarbeitungswürdigen* Kandidaten in die entsprechende bessere Position zu bringen oder die Entscheidung für die Nichtdurchführung zu bestärken.



Beachten Sie:

Die Dimensionen für ein Portfolio sind individuell zu definieren. Mögliche Dimensionen: *Wirtschaftlichkeit* des jeweiligen IT-Projektes, *Risikoeinschätzung* im Sinne der Erreichbarkeit des Projektziels sowie die *strategische Bedeutung*. Das allgemeine Ziel eines Portfolios besteht darin, die Gesamtheit aller geplanten, aktuellen und beendeten IT-Projekte darzustellen. Auf diese Weise soll die Effektivität und Koordination der Projekt-Ressourcen und -Budgets sichergestellt werden.

5.7.3 Planungsaktivitäten im Multiprojektmanagement

Um das **Optimum der Multiprojektplanung** zu erreichen, ist eine Optimierung der Planungen nach verschiedenen Dimensionen erforderlich:

- **Zuordnung von Ressourcen zu den einzelnen Projekten.** Bei einer Multiprojektplanung wird die insgesamt für IT-Projekte verfügbare Kapazität (Ressourcen, Budgets) auf die einzelnen IT-Projekte verteilt. Dabei gilt es zu berücksichtigen, welche besonderen personalen Kompetenzen in den einzelnen IT-Projekten gefragt sind, und – vor allem – dafür zu sorgen, dass die Verteilung des verfügbaren Personals auf die Projekte so erfolgt, dass es in der Lage ist, seine Projektbeiträge optimal zu bewältigen, ohne Engpässe oder gar Überbelastung entstehen zu lassen.
- **Zuordnung von Ressourcen über die Zeit.** Die übergeordnete Kapazitätsplanung für die Ressourcen wird so optimiert, dass den einzelnen Projekten die angeforderten Ressourcen in ausreichender Menge zur Verfügung stehen.
- **Planoptimierung der einzelnen Projekte über die Zeit:** Einzelne Projekte sind so anzuordnen, dass sachlogische Abhängigkeiten untereinander berücksichtigt sind. Projekte liefern z. B. Vorergebnisse, die erst bereitstehen müssen, bevor ein anderes Projekt beginnen oder in eine bestimmte Phase eintreten kann. Weitere Abhängigkeiten können entstehen, wenn etwa das Ergebnis eines bestimmten Projektes nicht zeitgleich mit dem Ergebnis eines anderen Projektes bekannt sein sollte.

Die Ressourcenbedarfs- und -kapazitätsplanung in der Multi-Projektumgebung erfordert gleichzeitig eine Planung der Ressourcenbeschaffung. Bei einer Kapazitätsplanung plant man die während des Projektablaufs benötigten Personalbedarfe zeitlich ein. Für jeden Projektmit-

arbeiter wird auf diese Weise in Form eines Belastungsprofils ermittelt, wie groß die Kapazitätsauslastung innerhalb eines Zeitraumes ist. Damit ist ersichtlich, ob die für das Projekt verfügbare Personalkapazität eines Mitarbeiters unterschritten wird und für andere Aktivitäten eingeplant werden kann oder überschritten wird und somit ein Belastungsausgleich erforderlich ist. Im Rahmen des **Multiprojektmanagements** findet dann ein **projektübergreifender Belastungsausgleich** statt.

Aus der Einplanung von Ressourcen zu bestimmten Arbeitspaketen können sich im Ergebnis auch Überlastungen für ausgewählte Ressourcen ergeben. Um dennoch eine optimierte Auslastung zu planen, sind Auslastungsdiagramme hilfreich. Sie zeigen auf einer Zeitachse die Einplanung der Ressourcen zu geplanten Terminen während der Projektlaufzeit. In den Auslastungsdiagrammen wird ein Bezug zur Kapazitätsgrenze der Ressourcen hergestellt. Starke Einsatzspitzen sind oft mit erhöhten Kosten verbunden. Deshalb wird jede Projektleitung bemüht sein, eine gleichmäßige Auslastung der Kapazitäten zu gewährleisten.

**Beachten Sie:**

Ein Kapazitätsausgleich kann beispielsweise dadurch geschaffen werden, dass nicht kritische Vorgänge zu einem späteren Zeitpunkt gestartet werden. Jede andere Kapazitätsoptimierung oder -glättung hat entweder eine Terminverschiebung des Projektes oder einen höheren Ressourcenaufwand (durch Einstellung neuer Projektmitarbeiter oder externe Auftragsvergabe) zur Folge.

5.7.4 Steuerung des IT-Projekt-Portfolios

Für die Steuerung der Projektportfolios und der Projektdurchführung bieten sich meist spezielle Stellen an; insbesondere ein Projektlenkungsausschuss (PLA) sowie ein besonderes Projektbüro (Project Office) für Multiprojektsteuerung.

Im Rahmen der Durchführung der IT-Projekte übernimmt ein **Project Office** die Ausarbeitung des Projektgesamtstatus. Die Zusammenstellung basiert in der Regel auf den periodischen Statusberichten der IT-Projekte. Diese können auch in Form eines außerordentlichen Zwischenberichts oder des Abschlussberichts eines Projekts erfolgen. Das Project Office fertigt eine aktuelle Übersicht, den Projektgesamtstatus, an, übergibt sie zwecks weiterer Behandlung dem Lenkungsausschuss und stellt sie den IT-Projekten als Information zur Verfügung.

Der inhaltliche Fortschritt der IT-Projekte wird anhand der **Statusmeldungen** evaluiert. Abweichungen von den Zielvorgaben sowie daraus resultierende Maßnahmen werden im Projektgesamtstatus aufgezeigt und dienen dem Projektlenkungsausschuss als Diskussionsgrundlage.

Eine wichtige Forderung ist darüber hinaus, dass das Berichtswesen zu jedem Zeitpunkt die aktuelle Situation des Projekte-Portfolios widerspiegelt. Um dies zu erreichen, werden einige grundsätzliche Anforderungen an das Reporting in der Multi-Projektumgebung gestellt.

Ein „gutes“ Reporting im Multiprojektmanagement kennzeichnen folgende Merkmale:

- Empfängergerichte Informations-Aufbereitung. So benötigt etwa die Geschäftsführung in der Regel die Informationen in einer höheren Verdichtung als beispielsweise der Steuer-

kreis (der Projektlenkungsausschuss). Letzterer benötigt etwa Detail-Informationen, um direkt steuernd in das Projekte-Portfolio eingreifen zu können.

- Aktualität der Projektreports. Jede Form von Reporting sollte so aktuell wie möglich sein. Um Steuerungsmaßnahmen einleiten zu können, müssen aktuelle Daten vorliegen. Wenig hilfreich sind beispielsweise seit zwei oder drei Wochen veraltete Informationen.
- Geeignete Darstellungsform. Jedes Reporting präsentiert die Information in einer Form, die die aktuelle Situation unmittelbar widerspiegelt. Zu überlegen ist, in welcher Form die jeweilige Information dargestellt wird: Zahlentabellen, Grafiken, Symbole, freier Text. Hilfreich sind – unter anderem – Scorecards und Ampelgrafiken.

■ 5.8 IT-Projekte abschließen

Formal wird ein Projekt mit seiner Abnahme durch den Auftraggeber sowie der Übergabe der Projektergebnisse an die Projektnutzer (bzw. den Kunden des Projektes) abgeschlossen. Gleichzeitig wird die Projektgruppe vom Auftraggeber aufgelöst.

Um dahin zu gelangen, sind im Wesentlichen folgende **Schritte in der Abschlussphase eines Projektes** zu durchlaufen:

- Projektabnahme und Produktübergabe
- Durchführung einer Projektabschlussanalyse
- Erstellen eines Projektabschlussberichtes und einer Ergebnisdokumentation
- Aufbereitung der Lessons-learned zwecks Erfahrungssicherung Bekanntmachung der Ergebnisse in Form einer Abschlusspräsentation
- Emotionaler Projektabschluss (evtl. mit Prämienregelung für das Projektteam) sowie
- eigentliche Projektauflösung mit Freigabe der Mitarbeiter für andere Projekte und Rückgabe der erhaltenen Projektsachmittel.

Aktivitäten, die Teil eines guten Projektabschlusses (Project Closing) sind, zeigt Abbildung 5.31 im Zusammenhang.

Letztlich geht es mit einem sorgfältig organisierten Projektabschluss darum, verschiedene **Ziele** zu erreichen:

- Formal kommt es darauf an, durch eine entsprechend dokumentierte Unterlage eine ordnungsgemäße Abnahme der Projektprodukte bei dem Auftraggeber des Projektes sicherzustellen.
- Funktional ist es wichtig, eine umfassende Akzeptanz und konsequente Umsetzung der Ergebnisse bei den von den Projektergebnissen betroffenen Personen und Institutionen zu erreichen.

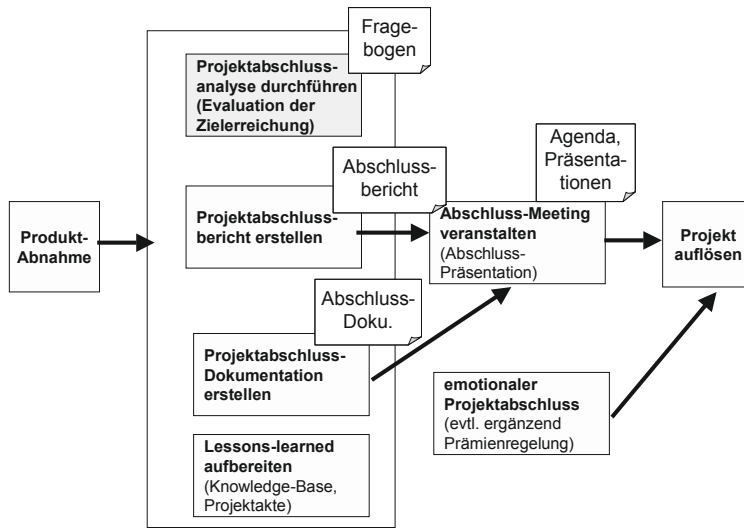


ABBILDUNG 5.31
Aufgaben zum
Projektabschluss

- Für künftige Projekte kommt es darauf an, aus den Erfahrungen, die im Projekt gesammelt wurden, zu lernen. Diese Chance sollte nicht verpasst werden.
- Am Projektende heißt es für die Mitglieder im Projektteam Abschied nehmen. Wichtig ist ein emotionales Beenden bei gleichzeitiger Rückkehr zu den ursprünglichen Kernaufgaben bzw. der Inangriffnahme neuer Projekte.

5.8.1 Projektabnahme und Produktübergabe

In der Regel wird ein Projektabschluss mit der Produkt-Übergabe eingeleitet. Projektleitung und Projektteam werden natürlich am konkreten Erfolg bzw. am Projektergebnis gemessen. Ein „korrekter“ Projektabschluss mit einer klar definierten Produktabnahme und Übergabe der Ergebnisse an den Auftraggeber ist immer dann unerlässlich, wenn – wie in der Praxis üblich – dem Projekt ein verbindlicher Auftrag zugrunde liegt.

Um die Projektabnahme zu erreichen, findet typischerweise eine **Projekt-Abschluss-sitzung mit dem Projekt-Auftraggeber** statt. Neben der Projektleitung und Vertretern des Projekt-Auftraggebers können an dieser gesonderten Abschluss-sitzung auch weitere Mitglieder des Projektteams beteiligt werden.

Im Normalfall wird der Projektleiter beim Auftraggeber dann um die Projektabnahme nachsuchen, wenn die in der Projekt-Aufgabenbeschreibung festgelegten Pflichten erfüllt und die Produkte (bzw. das Produkt) fertiggestellt sind. Hierbei muss als Erstes das Entwicklungsergebnis einen (vorgeplanten) Abnahmetest durchlaufen. Übergabe an den Auftraggeber und Übernahme durch denselben sind in einem Produktabnahmebericht festzuhalten. Typische Fragestellungen einer Projektabschluss-sitzung zeigt Tabelle 5.25.

Schwerpunkt der Abschluss-sitzung ist natürlich die Prüfung und Diskussion, ob die Projektziele erreicht wurden. In einer gemeinsamen Sitzung gilt es dann evtl. noch offene Aufgaben und Restarbeiten zu klären bzw. Verantwortliche für die Durchführung festzulegen.

TABELLE 5.25 Im Rahmen der Projekt-Abschlussitzung mit dem Auftraggeber zu klärende Fragenkreise

Themenbereich	Fragenkreise
Projektziel- erreichung	▪ Inwiefern wurden die Projektziele erreicht? Gegebenenfalls ist der Grad der Zielerreichung anzugeben! ▪ Welche Projektziele wurden verfehlt? Worin werden die Hauptgründe für das Nichterreichen gesehen?
Aufgaben- bearbeitung und Qualität der Arbeits- ergebnisse	▪ Sind noch Restarbeiten zu erledigen? Wenn ja, ist eine Einigung über noch zu erbringende Leistungen bzw. offene Aufgaben nötig. ▪ Wie wird die vorliegende Qualität der Arbeitsergebnisse bewertet? ▪ Ergeben sich von Seiten des Auftraggebers neue Anforderungen nach Vorlage der Projektergebnisse?
Produktabnahme durch den Auftraggeber	▪ Ist eine fachliche Abnahme der Projektergebnisse sichergestellt, und wer wird daran beteiligt? ▪ Ist eine technische Abnahme der Projektprodukte sichergestellt, und wer wird daran beteiligt? ▪ Welche Dokumente sind bis wann an wen zum Projektabschluss zu übergeben?
Produktauslie- ferung an den Projektkunden	▪ In welcher Form soll die Übergabe der Produkte (Resultate) an die Betroffenen bzw. den Fachbereich erfolgen? ▪ Wie kann die weitere Umsetzung der Ergebnisse (Verstetigung der Projektergebnisse) sichergestellt werden?
Projektteam- Bewertung	▪ Wie wird die Arbeit des Projektteams grundsätzlich eingeschätzt? ▪ Wie soll die Verabschiedung vom Projektteam erfolgen?

Im Fall einer Ablehnung der Projektabnahme (etwa weil schwerwiegende Mängel vorliegen) ist eine Nachbesserung der Projektergebnisse erforderlich. Wichtig ist, dass im Rahmen der Projekt-Abschlussitzung dafür ein realistischer Zeitrahmen vereinbart und fixiert wird. Dies führt dazu, dass die Abnahmeprozedur erneut zu durchlaufen ist.

**Beachten Sie:**

Wenn mit dem Auftraggeber ein Leistungserfolg – etwa die Realisierung eines Pflichtenheftes – vereinbart ist, sieht schon das Gesetz die Abnahme der Leistungen durch den Auftraggeber vor. Nach der gesetzlichen Regelung ist erst mit der unterzeichneten Abnahmeerklärung eine etwa anfallende Vergütung zu leisten und erst dann beginnt die Gewährleistung.

5.8.2 Projektabschlussanalyse durchführen – Evaluierung und Auswertung der Projektarbeit

Zu den wesentlichen Abschlussarbeiten am Projektende gehört auch eine gründliche Evaluierung und Auswertung der Projektarbeit. Für diese umfassende Projektauswertung sollten neben dem Projektteam sämtliche Stakeholder (Kunden, Lieferanten etc.) in die Erfassung und Analyse einbezogen werden.

Die Wahl der Methode hängt unter anderem von der Zielsetzung ab. Für die Erfassung, Zusammenstellung und Bewertung der Projekterfahrungen gibt es mehrere **methodische Herangehensweisen**:

- Projekt-Abschlussworkshop mit dem Projektteam
- informelles Gespräch mit den Teammitgliedern
- schriftliche Befragung (Fragebogen) der Teammitglieder und der Kunden (Abnehmer der Projektergebnisse)

An einem **Projekt-Abschlussworkshop** sollten in jedem Fall alle Mitglieder des Projektteams beteiligt sein, auch wenn einige Personen bereits mit völlig anderen Projekten und Aufgaben befasst sind.

Im Rahmen einer Abschluss-Evaluierung sollte die Projektleitung bzw. das Projektteam das Projekt vor allem daraufhin untersuchen, ob und inwieweit die vereinbarten Projektziele erreicht wurden. Dabei ist nicht nur das Projektprodukt zu evaluieren, sondern auch der gesamte Projektverlauf.

Bei der **Besprechung im Projektteam** kommt es vor allem darauf an, dass alle Beteiligten offen und ehrlich zum Feedback bereit sind. In Ergänzung zur mündlichen Feedback-Runde ist auch das Einholen eines **schriftlichen Feedbacks von den Projektmitgliedern** sinnvoll.

Eine weitere Erhebung richtet sich auf die **Zufriedenheit beim Kunden**. Dies kann mittels eines informellen Gesprächs, durch einen Projekt-Abschlussworkshop oder als schriftliche Befragung erfolgen.

5.8.3 Projekt-Abschlussbericht und Projekt-Gesamtdokumentation erstellen

Wichtig für den Auftraggeber ist außerdem der **Projekt-Abschlussbericht**. Hier kann es in Organisationen, die regelmäßige Projekte durchführen, klare Gliederungsvorgaben geben.

Der Projektabschlussbericht

- muss formal und inhaltlich dem festgelegten Standard entsprechen (erreichte Projektergebnisse, dokumentierte Abweichungen);
- enthält auch präzise Angaben über die laufenden Kosten des Produkts);
- wird einvernehmlich von Projektbeauftragtem und Projektleiter verfasst und
- muss vom Auftraggeber und vom Projektleiter unterschrieben sein.

Wichtig ist, dass das Erreichen der Projektziele innerhalb des Teams bzw. mit dem Auftraggeber festgestellt ist. Außerdem ist der Termin-, Aufwands- und Kostenplan (bzw. die dazu gehörenden Abrechnungen) auf dem letzten Stand. Abweichungen von der ursprünglichen Planung sind vollständig und korrekt berechnet und dokumentiert.

Der Projekt-Abschlussbericht ist letztlich Bestandteil einer umfassenden **Projektdokumentation**. Darin werden alle wesentlichen Fakten und Ergebnisse des Projektes gesammelt und zusammenfassend dargestellt. Ein wesentlicher Bestandteil kann auch eine Produktdokumentation sein (wenn auch die Ablieferung eines Produktes Gegenstand des Projektauftrages war).

**Eine „saubere“ Projektdokumentation umfasst beispielsweise:**

- Projektauftragsinformationen
- Verträge mit Kunden, Lieferanten und externen Beteiligten
- Vereinbarungen zur Projektorganisationsstruktur
- Projektplanungsunterlagen (Projektstrukturplan, Zeitpläne, Ressourcenplan, Kosten- und Finanzierungsplan, Risikoplan)
- Erzeugte Dokumente (beispielsweise angefallene Korrespondenz und Sitzungsprotokolle)
- Berichte (Prüf- und Abnahmeberichte, Projektstatusberichte, Projektabschlussbericht)
- Produktdokumentation

5.8.4 Projekterfahrungen sichern

Zunehmend wird in der Praxis auch die Notwendigkeit erkannt, Projekterfahrungen so aufzubereiten und zu sichern, dass sie auch zur Akquisition und Bearbeitung neuer, ähnlicher Projekte genutzt werden können. Findet keine Sicherung der Projekterfahrungen statt, hat dies zur Folge, dass

- wesentliche Informationen verloren gehen;
- wichtige Trends unerkannt bleiben;
- Wiederholungen von bereits an anderer Stelle erledigten Aufgaben vorkommen und
- wertvolle Erfahrungen aus früheren Projekten nicht zur Verfügung stehen.

In der Praxis ist für eine professionelle Sammlung, Speicherung und Nutzung des vorhandenen Wissens der Begriff des **Wissensmanagements** etabliert. Um ein verstärktes Wissensmanagement im Projektumfeld zu etablieren, sind vor allem einige Voraussetzungen zu schaffen:

- **Wissensmanagement** funktioniert nur dann, wenn in dem Unternehmen insgesamt und in dem Projekt eine hinreichende Vertrauenskultur herrscht. Diese lässt sich aber nicht verordnen. Durch ein zuverlässiges, aufrichtiges und berechenbares Handeln von Management, Projektleitung und eines jeden Teammitgliedes wird diese Vertrauenskultur entwickelt und gefördert. Denn nur wo die Projektmanagement-Kultur frei von jeder Geheimniskrämerei ist, kann Wissensmanagement funktionieren.
- Erfahrungen zeigen, dass es ganz hilfreich ist, Erfahrungswissen jeweils am Ende einer jeden Projektphase (Meilenstein-Sitzung) zu sichern, indem festgehalten wird, wie die jeweilige Phase „gelaufen“ ist und dann geprüft wird, was davon als Erfahrungswissen weitergegeben werden sollte.



Beachten Sie:

Erfahrungen, die bei der Projektarbeit gesammelt wurden, sind das Wissenskapital einer jeden Organisation, die nicht in den Köpfen einzelner Mitarbeiter oder bei der Projektleitung verkümmern sollten. Aus Erfahrungen kann man lernen, sie ermöglichen künftig einen Informations- und Wettbewerbsvorteil für andere Projekte.



Das Wichtigste – zusammengefasst

- **Favorisieren Sie einen ganzheitlichen Ansatz im Projektmanagement! Überlegen Sie dabei, welche Grundsatzentscheidungen getroffen werden sollten!**

Wichtig ist ein situativer Ansatz beim Treffen der Grundsatzentscheidungen im Projektmanagement. Die einseitige Ausrichtung des IT-Projektmanagements auf methodische, budgetäre oder personelle Fragen oder auf bestimmte Vorgehensmodelle birgt Gefahren. Überlegungen zum IT-Projektmanagement sollten alle wesentlichen Aspekte und Vorgehensmodelle gleichgewichtig einbeziehen.

- **Beachten Sie, dass eine gründliche Kenntnis der Ausgangssituation zum Projektgegenstand hilfreich ist!**

Ein offizieller Projektstart sollte erst erfolgen, wenn die wesentlichen Rahmenbedingungen geklärt und die notwendigen Voraussetzungen geschaffen worden sind. Dies ist in der Regel in einem konkreten Projektauftrag fixiert.

- **Organisieren Sie die Projekt-Startphase in besonderer Weise, denn diese ist eine wichtige Grundlage für den späteren Projekterfolg!**

Wichtig für eine erfolgreiche Abwicklung von IT-Projekten ist eine Integration dieser Projekte in die strategische Ausrichtung der Gesamtorganisation (Makro-Ebene). Die Erarbeitung einer Vision Map (Visioning) sowie die Durchführung von Startveranstaltungen und einer Projektumfeldanalyse (u. a. Stakeholderanalyse) sind wichtige Aktivitäten sein zu Projektbeginn.

- **Arbeiten Sie auf der Grundlage von Zeit- und Kostenplänen!**

Pläne sind notwendig, damit die Projektleitung dem Team eine Richtung vorgeben kann. Aber seien auch Sie flexibel! Prüfen Sie insbesondere, inwiefern Risikopläne und Qualitätsplanungen professionell erstellt und in die Projektarbeit integrativ eingebunden sind!

- **Ermitteln Sie im Rahmen von differenzierten Projektkontrollen den Ist-Zustand der Projektdurchführung, so dass ein Plan-Ist-Vergleich erfolgen kann!**

Bei Abweichungen müssen durch die Projektleitung bzw. den Projektleitungsausschuss (PLA) Korrekturmaßnahmen eingeleitet werden. Prüfen Sie, ob zusätzliche Ressourcen eingesetzt werden müssen, um den Projekttermin einhalten zu können!

- **Projektcontrolling ist heute quasi die Lebensversicherung des Projektverantwortlichen!**

Ein straffes Projektmanagement und insbesondere stringentes Projektcontrolling gewinnen an Bedeutung. Dies gilt sowohl für das Einzelprojektmanagement als auch für die Organisation des Multiprojektmanagements.

- **Bestimmen Sie, bevor Sie Controlling-Werkzeuge wie Scorecards oder Reports einsetzen, zunächst die typischen Controlling-Prozesse für Ihre IT-Projekte.**

Im IT-Projekt-Controlling können Sie Kennzahlen und Reports als wesentliche Instrumente nutzen. Dabei ist es unerlässlich, dass Sie die Kennzahlen für Ihre Projekttypen und organisatorischen Anforderungen spezifisch auswählen und festlegen. Außerdem müssen Sie ein auf die Empfänger abgestimmtes Reportingssystem vereinbaren und umsetzen.

- **Legen Sie die Inhalte der Projektreports unter Beachtung der Adressaten fest!**

Standardreports enthalten vor allem Statusinformationen zu den verbrauchten Zeiten, Ist-Termine, Ist-Kosten sowie den Fertigstellungsgrad des Projekts. Ergänzend können vorliegende Kennzahlen (etwa zur Kundenzufriedenheit) sowie Analyseinformationen „einfließen“.

- **Sorgen Sie durch die Inangriffnahme und Steuerung von definierten Teilprozessen für einen systematischen Projektabschluss!**

Kein IT-Projekt sollte ohne systematischen Projektabschluss enden. Dazu müssen Sie die für Ihre IT-Projekte wesentlichen Teilprozesse identifizieren und konsequent umsetzen. Hilfreich ist dafür auch eine spezifische Prozessbeschreibung (zumindest aber eine abgestimmte Checkliste).

- **Sichern Sie Ihre Projekterfahrungen, um sie für künftige Projekte nutzbar zu machen!**

Für künftige IT-Projekte kommt es darauf an, aus Erfahrungen zu lernen. Diese Chance sollten Sie nicht verpassen und Ihre Projekt-Erfahrungen in geeigneter Weise dokumentieren sowie kommunizieren.

- **Nutzen Sie die Instrumente und Organisationsformen des Multiprojektmanagements, wenn die Zahl der gleichzeitigen IT-Projekte in Ihrer Organisation ein gewisses Maß übersteigt!**

Wesentlich beim „Aufsetzen“ von Multiprojektmanagement für eine IT-Organisation ist die Beachtung der Unterschiede zum Einzel-Projektmanagement. So handelt es sich beim Multiprojektmanagement eher um eine dauerhafte Aufgabe, während das Managen und Leiten von Einzelprojekten zeitlich begrenzt ist. Darüber hinaus hat der Multiprojektmanager keine Ergebnisverantwortung, sondern nur eine projektübergreifende Koordinationsfunktion.

- **Sobald mehrere IT-Projekte gleichzeitig gemanaged werden müssen, wachsen die Herausforderungen und Aufgabenfelder für alle Beteiligten!**

Je mehr gleichzeitige IT-Projekte, umso größere Schwierigkeiten beim Setzen von Projektprioritäten; Koordinationsbedarf und Ressourcenkonflikte treten auf. Hierfür benötigen Sie angepasste Instrumente, wenn Sie die Projektarbeit erfolgreich gestalten wollen. Diese helfen der Unternehmensleitung oder dem Projektlenausschuss, alle Informationen zu liefern, die für Entscheidungen über IT-Projekten notwendig sind, sowie eine gemeinsame Infrastruktur und einheitliche Managementprozesse zu etablieren, um IT-Projekte besser planbar, steuerbar und mittels Scorecards vergleichbar zu machen.

■ 5.9 Literatur

- [Br02] *Brand, Th.*: Projektcontrolling. Projektwirkungen analysieren und bewerten. Hanser; München 2002
- [DL91] *DeMarco, T., Lister, T.*: Wien wartet auf Dich! Der Faktor Mensch im DV-Management. Hanser; München 1991
- [DM98] *DeMarco, T.*: Der Termin. Ein Roman über Projektmanagement. Hanser; München 1998
- [DM01] *DeMarco, T.*: Spielräume. Projektmanagement jenseits von Burn-out, Stress und Effizienzwahn. Hanser, München 2001
- [Fi01] *Fiedler, R.*: Controlling von Projekten. Projektplanung, Projektsteuerung und Risikomanagement von Projekten. Vieweg; Braunschweig, Wiesbaden 2001
- [Gar06] *Gareis, R.*: Happy Projects – Projekt- und Programmmanagement, Projektportfolio – Management, Management der projektorientierten Organisationen. (3 Auflage). Manz Verlag, Wien 2006
- [Ge03] *Geipel, P.*: Der IT-Projektmanager. Arbeitstechniken, Checklisten und soziale Kompetenz. Addison-Wesley; München 2003
- [Gr98] *Grupp, B.*: Qualifizierung zum Projektleiter. DV-Projektmanagement im Wandel. 4. Aufl. IDG; München 1998
- [Gr03] *Grupp, B.*: Der professionelle IT-Projektleiter. mitp; Bonn 2003
- [Ke01] *Kellner, H.*: Die Kunst, IT-Projekte zum Erfolg zu führen. Hanser; München 2001
- [Ki04] *Kitz, A.*: IT-Projektmanagement. Galileo Press; Bonn 2004
- [Li96] *Litke, H.-D.*: DV-Projektmanagement. Zeit und Kosten richtig einschätzen. Hanser; München 1996
- [Li01] *Litke, H. D., Kunow, I.*: Projektmanagement. Einfach. Praktisch. Haufe; Freiburg 2001
- [PJ91] *Page-Jones, M.*: Praktisches DV-Projektmanagement. Grundlagen und Strategien. Hanser; München 1991
- [RT01] *Reimann, M., Tiemeyer, E.*: Project 2000, Computerpraxis Schritt für Schritt. Europa-Lehrmittel; Haan 2001
- [Sc99] *Schelle, H.*: Projekte zum Erfolg führen. Projektmanagement systematisch und kompakt. Beck-Wirtschaftsberater im dtv; München 1999
- [Sch04] *Schreckeneder, Berta C.*: Projektcontrolling – Projekte überwachen, steuern und präsentieren. Haufe Verlag, Planegg/München 2004 [Ste06] *Sterrer, C.; Winkler, G.*: Let your projects fly. Goldegg Verlag, Wien 2006
- [Ti02] *Tiemeyer, E.*: Projekte erfolgreich managen. Methoden, Instrumente, Erfahrungen. Beltz; Weinheim, Basel 2002
- [Ti04] *Tiemeyer, E.*: Projekte im Griff – Tools und Checklisten zum Projektmanagement. Mit CD-ROM. WBV Bertelsmann; Bielefeld 2004
- [Ti08] *Tiemeyer, E.*: IT-Projekte erfolgreich managen. Zeit, Kosten und Ziele im Griff. rauscher.Verlag. Haag i. Obb. 2008.
- [Ti10] *Tiemeyer, E. (Hrsg.)*: Handbuch IT-Projektmanagement – Vorgehensmodelle, Managementinstrumente, Good Practices. Hanser-Verlag. München 2010.
- [Tu01a] *Tumuscheit, K. D.*: Überleben im Projekt. 10 Projektfallen und wie man sie umgeht. Moderne Verlagsgesellschaft; Landsberg 2001
- [Tu01b] *Tumuscheit, K. D.*: Immer Ärger im Projekt. Wie Sie die Projektkiller austricksen. Orell Füssli; Zürich 2001

- [WC04] *Weixlbaumer, E. (Hrsg.); Ciresa, M.:* IT-Projekte in Österreich. Management in time, in budget, in quality. Manz; Wien 2004
- [WM04] *Wieczorrek, H. W., Mertens, P.:* Management von IT-Projekten. Von der Planung zur Realisierung. Xpert.press. Springer; Berlin 2004

6

Organisation und Führung im IT-Bereich

Ernst Tiemeyer



Fragen, die in diesem Kapitel beantwortet werden:

- Welche grundlegenden Organisationskonzepte für den IT-Bereich gibt es (organisatorische Ausrichtung als Cost- oder Profitcenter)?
- Welche wichtigen Prozesse sind für eine IT-Organisation zu unterscheiden, und wie können diese in einer Prozesslandkarte dokumentiert sein?
- Welche Rollen und Skills sind aktuell im IT-Umfeld von Bedeutung, wie sind diese einzuordnen und welche Perspektiven (zukünftige Rollen) zeichnen sich ab?
- Welchen Einfluss hat ein zunehmendes Outsourcing von IT-Aufgaben, IT-Services und IT-Prozessen für die Positionierung der IT-Organisation?
- Inwiefern stellen IT-Kennzahlen (Scorecards) und Reports ein wichtiges Instrumentarium für das Management und die Führung im IT-Bereich dar?
- Welche Führungsaufgaben sind heute unverzichtbar, um erfolgreich und nachhaltig als Führungskraft im IT-Bereich tätig zu sein?
- Welche Phasen kennzeichnen die typische „Entwicklung“ von IT-Teams, und welche Möglichkeiten der Optimierung und Maßnahmensteuerung für die Teamleitung gibt es?

■ 6.1 Organisation und Führung – Basis für den Erfolg der IT-Abteilung

In verschiedenen Kapiteln dieses Buches wird immer wieder auf die gravierenden technologischen Veränderungen hingewiesen, die den IT-Bereich kennzeichnen (vgl. etwa Kapitel 3 „Enterprise Architecture Management“). Technologische Innovationen haben meist auch gravierende Auswirkungen in organisatorischer und personeller Sicht. Nicht selten sind grundlegende **Veränderungen der Organisation** die Folge:

- So ist in der letzten Zeit ein **Wandel der IT-Abteilung** im Unternehmen vom internen Lieferanten für technische Lösungen (Hardware und Software) hin zum umfassenden Dienst-

leister für die Lauffähigkeit von Systemen und Anwendungen sowie zu einem Komplettanbieter für IT-gestützte Geschäftsprozesse feststellbar.

- Parallel zu den Veränderungen findet sich eine umfassende Diskussion über die **Rolle und Bedeutung der IT** für die Unternehmen. Unabhängig davon, wo und von wem die IT-Leistungen für ein Unternehmen erbracht werden, ist die zunehmende Abhängigkeit der Unternehmensleistungen von einer funktionierenden IT unbestritten.

Geht man davon aus, dass die Bedeutung der IT weiter zunimmt – was etwa an Diskussionen wie IT-Governance sowie der feststellbaren zunehmenden Abhängigkeit der Geschäftsprozesse von effizienter und sicherer IT-Unterstützung erkennbar ist (Stichwort „Business-IT-Alignment“) –, ist eine stärkere Einbeziehung externer Gruppen (Stakeholder) sowie eine intensivere Kundenorientierung in der IT unverzichtbar. All diese Aspekte sind von der **IT-Führung** zu koordinieren.

Die Erwartungen und Anforderungen an Führungskräfte in Wirtschaft und Verwaltung sind nach wie vor besonders hoch. Zum einen wird von ihnen erwartet, sich im Produktumfeld auszukennen, auf der anderen Seite sollen sie ihre Mitarbeiter motivieren und als Führungskraft überzeugen. Dieser Spagat fällt oftmals schwer, besonders wenn man als „Bereichsspezialist“ aufgrund hervorragender Leistungen wenig vorbereitet in eine Führungsposition aufgestiegen ist. Gerade bei vielen **Führungskräften im IT-Bereich** ist dieses Phänomen häufig anzutreffen.

Die besondere Bedeutung einer erfolgreichen Führung – insbesondere im IT-Bereich – verdeutlichen folgende Argumente:

- motivierte Mitarbeiterinnen und Mitarbeiter
- ein hervorragendes Arbeitsklima
- weniger Mitarbeiterfluktuation
- die erfolgreiche Durchsetzung von Veränderungen
- eine hohe Ergebnisqualität der IT

■ 6.2 Elemente und Einflussfaktoren moderner IT-Organisation

Den Begriff „Organisation“ kann man institutionell – das Unternehmen hat eine Organisation – oder als Gestaltungsaufgabe – es werden organisatorische Maßnahmen in der Unternehmenspraxis geplant und umgesetzt – eingeordnet werden. Hier soll **Organisation** als **ganzheitliches Gestalten von Beziehungen zwischen Aufgaben, Menschen, Sachmitteln und Informationen** in sozialen Systemen verstanden werden (vgl. [Ti96]):

- **Aufgaben** sind dabei primär Verrichtungen an Objekten. Die grundsätzliche Forderung an die Festlegung und Verteilung besteht darin, Arbeiten dort zu erledigen, wo es sinnvoll ist. Dabei können Gestaltungsmaßnahmen dazu führen, dass ggf. Verrichtungen hinzukommen, wegfallen, sich ändern, und es können Änderungen bei den Objekten vorgesehen werden (Einzelfolge, Gruppierungsfolge, andere Objekte, weniger Objekte etc.).

- Der Leistungsbeitrag des **Menschen** ergibt sich im Rahmen beruflich-betrieblicher Tätigkeiten aus einer Kongruenz von Leistungsfähigkeit, -bereitschaft und -möglichkeit. Eingesetzt in betrieblichen Geschäftsprozessen, ist der Wertschöpfungsbeitrag jedes Einzelnen unmittelbar festzustellen. Das Prinzip der Kongruenz aus Aufgabe, Kompetenz und Verantwortung fordert eine eindeutig festgelegte Aufgabenzuordnung für den gesamten Arbeits- und Geschäftsprozess und Teile von ihm.
- Neben der Kongruenz aus Aufgabe, Kompetenz und Verantwortung bestimmen die **Sachmittel** und **verfügbaren Informationen** die Leistungsmöglichkeit der Menschen im jeweiligen Geschäfts- und Arbeitsprozess. Ob Teamarbeit und entsprechende Sachmittelunterstützung (mobile Systeme, Webzugang, Groupware, Workflow) von Vorteil sind, ist entsprechend zu prüfen und zu entscheiden.



Beachten Sie:

Für den IT-Bereich müssen verschiedene grundlegende Entscheidungen getroffen werden:

- Welche Prozesse gibt es im IT-Bereich, und wie hängen diese Prozesse miteinander zusammen (Dokumentation in einer Prozesslandkarte und Vereinbarung einer Process Policy)?
- Wie lassen sich die Arbeitsprozesse im IT-Bereich (IT-Prozesse) optimiert gestalten?
- Welche IT-Aufgaben fallen an, wie können diese systematisiert werden, und wo werden die identifizierten Aufgaben sinnvollerweise erledigt?
- Welche Rollen sind in den identifizierten und vereinbarten IT-Prozessen nötig, um die Aufgaben optimal zu erledigen?
- Welche Stellen werden im IT-Bereich benötigt, und wie werden die Stellen besetzt?
- Welche organisatorischen Regelungen (bzw. Richtlinien) müssen entwickelt, vereinbart und hinsichtlich ihrer Einhaltung geprüft werden?

Dabei ist zu beachten, dass die jeweils festgelegte IT-Organisation maßgeblich in Größe und Struktur von den Geschäftsaktivitäten des Unternehmens geprägt wird. So hat beispielsweise ein Unternehmen der Versicherungsbranche eine IT-Organisation mit anderen Schwerpunkten als ein großes Chemieunternehmen oder ein mittelständischer Handelsbetrieb.

Einen Einfluss auf die Größe des IT-Bereichs sowie auf seine Struktur haben natürlich vor allem die **Anforderungen aus den Geschäftsaktivitäten** des Betriebes. Als Beispiel kann hier angeführt werden, dass ein Betrieb, der rund um die Uhr ein großes Logistiksystem betreibt, typischerweise auch einen 24h-Betrieb im IT-Bereich erfordert.

Weiterhin hat die **regionale Verteilung eines Unternehmens** einen gewissen Einfluss auf die Organisation der IT. So ergibt sich beispielsweise die Notwendigkeit, jede Region spezifisch zu bedienen und damit ggf. Zeitverschiebungen und Sprachprobleme aufzufangen. Natürlich müssen darüber hinaus kulturelle Eigenarten und ggf. religiöse Besonderheiten berücksichtigt werden. Beides sind auch Faktoren, die in der Personalführung besondere Berücksichtigung finden müssen.

Unter Beachtung der allgemeinen wirtschaftlichen Lage kann man heute außerdem davon ausgehen, dass nicht nur die tatsächlichen Bedürfnisse hinsichtlich IT-Support bei den Unternehmen und Organisationen eine Rolle bei der Ausgestaltung der IT spielen, sondern auch die wirtschaftliche Situation gewisse Maßstäbe setzt. Die Konsequenz besteht darin, mit den vorhandenen Mitteln die bestmögliche IT-Unterstützung des Unternehmens zu gewährleisten. In solchen Situationen bekommen der Umgang mit Risikoabwägungen, Einsparpotenziale und Aufwandsreduzierung natürlich ein ganz anderes Gewicht. Auch die Entscheidungswege und die Reportingstrukturen werden davon beeinflusst und sind der Situation anzupassen.

Um **zu einer zukunftsfähigen Ausrichtung der IT-Organisation** zu gelangen, empfiehlt sich in der Regel ein stufenweises Vorgehen. Dabei sollten – ausgehend von den bestehenden Rahmenbedingungen, der vorhandenen Kundenstruktur sowie dem Leistungsportfolio des IT-Bereichs – folgende Teilschritte „angegangen“ werden:

- Identifikation und Präzisierung der IT-Prozesse (in Form einer Prozesslandkarte)
- Systematisierung der anfallenden Aufgaben im IT-Bereich
- Vereinbarungen zu den Rollen im IT-Bereich und Definition dieser Rollen
- Konsequenzen für die Stellen- und Abteilungsbildung

Wesentliche Fragenkreise/Entscheidungen, die in den einzelnen Teilschritten „in Angriff“ genommen werden müssen, zeigt Tabelle 6.1.

TABELLE 6.1 Stufen der organisatorischen Gestaltung

Stufen/Ausrichtungen	Fragenkreise/Teil-Aktivitäten
Stufe 1: Rahmen- und Grundsatzentscheidungen: Kunden der IT, Leistungen und Erwartungen an den IT-Bereich	Ist die IT-Abteilung ein reines Cost-Center, oder findet eine Kosten- und Leistungsverrechnung statt? Ist ggf. eine Positionierung als Profit-Center gegeben? Wie werden die vom IT-Bereich bedienten Kunden eingeordnet? Inwieweit lassen sich die Kunden systematisieren (mögliche Kundensegmente), um daraus differenzierte Lösungswege ableiten zu können? Welche Erwartungen haben die Kunden an die IT (Anforderungsmanagement)? Welche IT-Produkte und welche IT-Dienstleistungen werden für die verschiedenen Kundensegmente erbracht?
Stufe 2: Prozesse identifizieren und gestalten	Welche IT-Prozesse können identifiziert und müssen organisiert werden, um die gewünschten IT-Leistungen zu erbringen? Welches Optimierungspotenzial haben die vorhandenen IT-Prozesse?
Stufe 3: Aufgaben analysieren und zuordnen	Wie werden die IT-Produkte und IT-Dienstleistungen erbracht (Make-or-Buy)? Wie können die Aufgaben analysiert werden?
Stufe 4: Rollen und Skills bestimmen	Welche Rollen sind in den jeweiligen Prozessen nötig, um die Aufgaben optimal zu erledigen? Sind die Skills im Unternehmen vorhanden, um die identifizierten und definierten Rollen entsprechend erfolgreich ausführen zu können?
Stufe 5: Struktur der IT-Organisation und Verfahrensfestlegungen	Wie kann/muss die IT strukturell organisiert sein (Abteilungs- und Stellenbildung)? Welche organisatorischen Regelungen müssen vereinbart und getroffen werden?

■ 6.3 Grundausrichtung und Konzepte zur Organisation der IT

Die Festlegungen zur IT-Organisation hängen stark von ihrem organisatorischen Umfeld ab, d. h. von der Gesamtorganisation des Unternehmens, in das sie eingebettet ist. So wie die IT als Unternehmensteil mittels IT-Mission und Vision die Unternehmensziele auf den eigenen Zuständigkeitsbereich herunterbricht, sollte sich auch eine IT-Organisation vor allem an der Unternehmensstruktur (z. B. Grad der Zentralisierung, Anzahl der Mitarbeiter, Diversität von Geschäftseinheiten und Prozessen, Unternehmenskultur) ausrichten.

Zudem ist eine Vielzahl externer Faktoren zu beachten, u. a. rechtliche Regelungen (Regulatives), die Markt- und Wettbewerbssituation, das soziale Umfeld oder die allgemeine technologische Entwicklung. Weil die Gestaltung einer IT-Organisation meist eine Umgestaltung sein dürfte, spielt schließlich auch die bestehende IT eine Rolle (z. B. durch die vorhandene Sourcing-Strategie, die Leistungsfähigkeit und das Know-how).

6.3.1 Gestaltung und Optimierung der IT-Prozesslandschaft

Eine effektive und effiziente Organisation der IT erfordert in jedem Fall adäquate Abläufe in Form von IT-Geschäftsprozessen. Über ihre Ausgestaltung werden auf der operativen Ebene Möglichkeiten und Grenzen der IT im Hinblick auf Innovationen, Veränderungen, Service-Leistungen, Beziehungen zu Fachabteilungen und zu Lieferanten/Sourcing-Partnern, Skills (Potenziale von IT-Mitarbeitern und IT-Tools) und Administration (z. B. IT-Controlling, Lizenzierung) festgelegt. Im Zusammenhang mit IT-Prozessen bietet sich eine Differenzierung in primäre und sekundäre (unterstützende) IT-Prozesse (analog zur Geschäftsprozessmanagement-Systematik) an. Diese werden im Sinne von übergeordneten (operativen und strategischen) IT-Management-Prozessen koordiniert und gesteuert.

Durch die Prozessorientierung rückt aus organisatorischer Sicht die Betrachtung der gesamten IT-Prozesslandschaft in den Mittelpunkt. Ein Beispiel einer Systematisierung zeigt Abbildung 6.1 (nächste Seite).



Die IT-Prozesslandschaft enthält

- Management- und Führungsprozesse (Strategie, Enterprise-Architektur-Management etc.)
- Kernprozesse (Kundenmanagement, Projekt-Portfolio-Management, Applikationsentwicklung und Bereitstellung, Betrieb etc.),
- Prozesse zum Ressourcen-Management (Finanz- und Rechnungswesen, Einkauf und Beschaffung, Personalmanagement etc.) und
- Evaluationsprozesse (Sicherheits- und Risikomanagement, Innovationsmanagement).

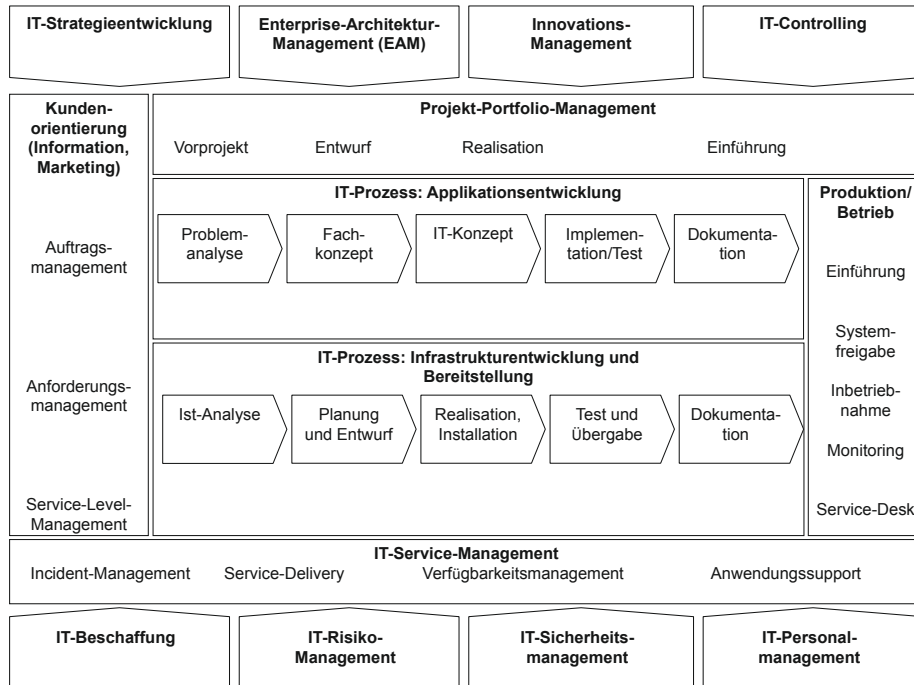


ABBILDUNG 6.1 Prozesslandschaft (IT-Prozesse)

Eine wichtige **Voraussetzung für die Einführung moderner IT-Organisationsformen** ist die Bereitschaft zum Wandel der IT in Richtung Kunden- und Serviceorientierung sowie eine ständige Gewährleistung der IT-Services und deren Überwachung. Auf diese Weise kann kontinuierlich die Effizienz, die Qualität und die Wirtschaftlichkeit der jeweiligen IT-Organisation verbessert werden. Die Dienstleistungsorientierung führt zu systematischer Kommunikation mit den Kunden und der Ableitung und Spezifikation von Leistungsangeboten der Informationsverarbeitung.

Die stark wachsende Bedeutung des **IT-Servicemanagements** wird offensichtlich, wenn man sich vergegenwärtigt, dass eine funktionierende IT heute in Unternehmen und Verwaltungen gewissermaßen das Rückgrat für die Geschäftsprozesse bildet. Ausfälle von IT-Systemen führen zu erheblichen Konsequenzen und wirtschaftlichen Schäden, die nicht zuletzt auch das Image der IT und des Unternehmens insgesamt gefährden.



Beachten Sie:

Notwendig dazu ist die Identifikation, Beschreibung und Optimierung der IT-Prozesse. Durch **Prozessorientierung** soll gewährleistet werden, dass die so erkannten Erwartungen der Kunden und die ihnen zugesicherten Dienstleistungen zuverlässig und optimiert erbracht werden.

Zur Unterstützung bei der Erfassung, Beschreibung und Dokumentation von IT-Serviceprozessen wurden **Rahmenwerke** (auch als **Frameworks** bezeichnet) entwickelt. Die bekannten

Rahmenwerke **IT Infrastructure Library (ITIL)** und **Control Objectives for Information Technology (CobiT)** beinhalten Anleitungen, die erläutern, wie eine IT-Service-Organisation aufgebaut und strukturiert sein sollte, um die laufenden Geschäftsanforderungen optimal unterstützen zu können.

Rahmenwerke wie ITIL sind nicht als Normen, sondern als Baukasten zu verstehen, der aus realen Erfahrungen (best practices) entwickelte Elemente enthält. ITIL ist international als Instrument für Betriebe unterschiedlicher Größe mittlerweile als De-facto-Standard akzeptiert. Weitere Rahmenwerke stellen dazu eine interessante, oft hilfreiche Erweiterung dar. Üblich ist eine **Einteilung der IT-Service-Prozesse** in

- **IT-Service-Supports** (= operationelle Management-Prozesse mit den Teilprozessen Incident-Management, Problem-Management, Change-Management, Configuration-Management und Release-Management) sowie der
- **IT-Service-Delivery** (= planende Management-Prozesse mit den Teilprozessen Service-Level-Management, Financial-Management, Capacity-Management, Service-Continuity-Management, Availability-Management).

Ausführliche Informationen zum IT-Servicemanagement finden Sie in Kapitel 4.

Besonderheiten sind die beiden weiteren Elemente des IT-Servicemanagements: der Service-Desk (als Funktion) sowie das IT-Security-Management (übergreifende Unterstützung der jeweiligen IT-Serviceprozesse). Sie haben – im Gegensatz zu den zuvor genannten IT-Serviceprozessen – entweder funktionalen Charakter oder sind funktionsübergreifender Natur.



Praxistipp:

Wichtige Voraussetzung für die Einführung moderner IT-Organisationsformen sind die Bereitschaft zum **Wandel der IT in Richtung Kunden- und Serviceorientierung** sowie eine ständige Gewährleistung der IT-Services und deren Überwachung. Auf diese Weise können Effizienz, Qualität und Wirtschaftlichkeit der jeweiligen IT-Organisation kontinuierlich verbessert werden. Die **Dienstleistungsorientierung** führt zu systematischer Kommunikation mit den Kunden und zur Spezifikation von Leistungsangeboten der Informationsverarbeitung.

6.3.2 Aufbauorganisatorische Ausrichtung

Folgende aufbauorganisatorischen Fragen sind für die Gestaltung des IT-Bereichs zu beantworten:

- Welche Aufgabenbereiche der IT werden identifiziert und legen eine Abteilungsbildung nahe?
- Welche Stellen benötigt man im IT-Bereich?
- Wie viele Stellen welcher Art braucht der IT-Bereich?
- Benötigt der IT-Bereich Unterstützung von zentralen Stellen (z. B. Recht, Organisation, Personalabteilung, Controlling, Innovation)? Wenn ja, in welcher Form und in welchem zeitlichen Umfang?
- Wie ist die Prozessverantwortung (hier für IT-Prozesse) im Liniensystem einer Institution zu integrieren?

- Wie werden die einzelnen Arbeitsprozesse des IT-Bereichs zu einer gesamten Organisation verbunden?

Abteilungen ergeben sich, indem mehrere Arbeitsaufgaben eines segmentierten, aber zusammengehörigen Aufgabenkomplexes in einen Organisationsbereich unter Leitung einer Instanz zusammengefasst werden. In einer Abteilung besteht ein Mindestmaß an direkten Arbeitsbeziehungen, sodass von einem quasi-geschlossenen Untersystem einer Institution gesprochen werden kann. Wird das Mindestmaß überschritten, werden Abteilungen in der Regel zu „Hauptabteilungen“ gebündelt. Denkbar ist also die IT-Abteilung als Hauptabteilung (bei großen Organisationen) oder als „normale“ Abteilung.

Die **klassische Organisation der IT** war die Einrichtung und der Betrieb eines Rechenzentrums. Im Laufe der Zeit sind spezielle Arbeitsbereiche dazugekommen; etwa die Anwendungsentwicklung oder das Managen von IT-Projekten.

Heute ergeben sich sehr differenzierte Möglichkeiten. Hatte die starke Technikbezogenheit der Datenverarbeitung in der Vergangenheit dazu geführt, dass sich IT-Abteilungen von ihrem Selbstverständnis her als Lieferanten von Technik sahen, reicht es heute nicht mehr aus, nur Technologie bereitzustellen:

- Nachgefragt werden Leistungen wie beispielsweise das Implementieren und die umfassende Pflege einer betriebswirtschaftlichen Anwendung.
- Trotz steigender Komplexität der IT-Technologien (etwa gemischte Client-Server-Strukturen) sowie der geschäftskritischen Anwendungen müssen sowohl die Qualität der bereitgestellten Informationen als auch die Verfügbarkeit der Informationssysteme und Informationen selbst gesichert werden.
- Der wachsende Kostendruck erfordert eine effektive Auslastung der Infrastruktur.

Oft untergliedern insbesondere größere Unternehmen ihre IT in eine **Nachfrageorganisation** (Informationsmanagement) und eine **Lieferorganisation** (interne IT-Abteilung und externe Kooperationspartner), um marktorientierte Verhaltensstrukturen zu etablieren. Die IT steuert dabei stellvertretend für die nachfragenden Fachbereiche (Einkauf, Personal, Rechnungswesen usw.) die Beschaffungsprozesse sowie zahlreiche Serviceleistungen für den laufenden Betrieb. Eine solche **Einordnung des IT-Bereichs** zeigt Abbildung 6.2.

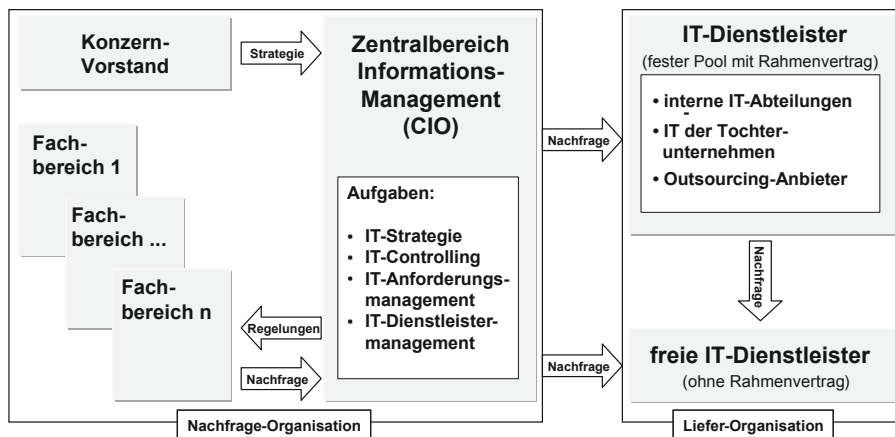


ABBILDUNG 6.2 Mögliche organisatorische Einordnung des IT-Bereichs (Quelle: [Ga05])



Ein typisches Phänomen moderner IT-Organisationen: Das IT-Management erarbeitet im Team die IT-Strategie für das Unternehmen, legt technische Standards fest, die von den internen und externen IT-Dienstleistern zu beachten sind. Diese können die Leistungen selbst erbringen oder wiederum Dritte beauftragen. Eine weitere Aufgabe ist das Anforderungsmanagement, also die Nachfragebündelung und das Management der Lieferantenbeziehungen.

Mittlerweile findet im IT-Bereich ein weiteres Umdenken statt: Jahrelang haben sich IT-Abteilungen auf die Einführung und Unterstützung von Technologien und deren fachliche Beherrschung konzentriert. IT-Abteilungen müssen heute ergänzend zahlreiche leistungsfähige Services erbringen, deren Ziel es in Zeiten von Kundenorientierung und Kostenbewusstsein ist, die bestmögliche Unterstützung der Geschäftsprozesse sicherzustellen. Die IT wird damit immer mehr Bestandteil des eigentlichen Geschäfts (vgl. dazu auch Kapitel 1).

Ein **Hauptziel der IT-Abteilung** lautet daher nicht mehr „Beherrschung und Unterstützung der Technik“, sondern „bestmögliche Unterstützung der Geschäftsprozesse (und Kunden) im Unternehmen“. In dieser Formulierung findet auch der Servicegedanke immer mehr Berücksichtigung bei der Gestaltung der IT-Organisation. **Zentrale Forderungen**, die organisatorisch der Berücksichtigung bedürfen, sind beispielsweise:

- Orientierung des Handelns am Leitbild der Organisation sowie des IT-Bereichs
- klare (zentrale) Ansprechpartner für bestimmte Aufgaben und auftretende Probleme
- umfassende Übersicht über den Status der Bearbeitung laufender Projekte
- Gewährleistung eines störungsfreien IT-Betriebs
- nachvollziehbarer und zielorientierter Informationsfluss im IT-Bereich und nach außen
- geregelte Abwicklung von Veränderungen in der IT (Changes)
- Sicherstellung der Wirtschaftlichkeit in der IT bei hoher Kosten- und Leistungstransparenz
- einheitliche Vorgaben für Dokumente aller Art (Projektdokumentation, Prozessdokumente etc.)

■ 6.4 Rollen und Aufgabenstellungen im IT-Bereich

Um die Führungs- und Fachaufgaben im IT-Bereich zu systematisieren und sinnvoll zu bündeln, lassen sich für ausgewählte Ausprägungen konkrete Rollen festlegen. Diese Rollen können in der Praxis eine oder mehrere Personen wahrnehmen. Es ist aber auch üblich, dass eine Person mehrere Rollen übernimmt. Letztlich geht es hierbei um das organisatorische Problem der Stellenbildung, das wir zum Schluss dieses Abschnitts darstellen.

6.4.1 Typische Rollen im IT-Bereich

Welche **Rollen** sind nun im **IT-Bereich** konkret festzustellen? Im Wesentlichen unterscheidet man die folgenden Segmente:

- **Rollen mit Führungsfunktionen** (CIO, IT-Leitung, RZ-Management, IT-Serviceleitung, Leitung Project Office etc.)
- **Rollen im Bereich IT-Planung und IT-Controlling** (IT-Architekten, IT-Controller, IT-Quality-Manager, IT-Koordinatoren, IT-Beschaffung, Informations- und Wissensmanagement)
- **Rollen im IT-Betrieb** (Gruppenleiter, Prozessverantwortliche, Mitarbeiter im HelpDesk und IT-Support, Datenbank-Administratoren, IT-Security-Experte)
- **Rollen in der Anwendungsentwicklung und Applikationsintegration** (Programmierer/Software-Architekten, Systemintegratoren, Datenbank- und Systementwickler)
- **Rollen im Projektmanagement** (Projekt-Gruppenleiter, Arbeitspaket-Verantwortliche)
- **Rollen im Bereich der Verwaltung** (Assistenz u. ä.)

6.4.1.1 Führungsfunktionen

Die Erwartungen und Anforderungen an Führungskräfte im IT-Bereich sind heutzutage extrem hoch. Zum einen müssen sie sich im IT-Umfeld (mit IT-Produkten und mit IT-Prozessen) auskennen, auf der anderen Seite sollen sie ihre Mitarbeiter motivieren und als Führungskraft überzeugen.

Hinsichtlich der Orientierung bezüglich der Rollen mit Führungsfunktionen gilt es zunächst einen Blick auf die IT-Leitungs-Rolle zu werfen. Zu den eigentlichen IT-Aufgaben der **IT-Leitung** zählen:

- Planung und Organisation des IT-Bereichs (IT-Strategien und Architekturmanagement, Projekt-Portfoliomanagement)
- Planung und Umsetzung der Anforderungen des Unternehmens an die IT (Anforderungen managen)
- Durchführung und Sicherung des Betriebs
- Personalführung
- Sicherstellung der Einhaltung der gesetzlichen/behördlichen Vorgaben sowie der Vorgaben der Unternehmensführung

Im Führungsbereich hat sich als Ergänzung oder als Ersatz zum klassischen IT-Leiter in letzter Zeit die Rolle des **CIO** (für „Central Information Officer“) herauskristallisiert. Von seiner Stellung her ist der CIO normalerweise Mitglied der Geschäftsleitung oder des Vorstands oder dieser Ebene direkt zugeordnet. Ausschlaggebend hierfür ist die Bedeutung der IT im Unternehmen. Der **Aufgabenbereich eines CIOs** umfasst:

- Entwicklung und Umsetzung einer IT-Strategie für das Informationstechnik-, Wissens- und Informationsmanagement.
- Erarbeitung, Festlegung und Durchsetzung von IT-Standards.
- Unterstützung der Fachbereiche bei der Entwicklung und Optimierung von Lösungen für deren Geschäftsprozesse.

- Identifikation und Einführung so genannter „Best Practices“ für das Unternehmen.
- Förderung des Informationsflusses zwischen allen Gruppen des Unternehmens, die an IT-Lösungen arbeiten bzw. mit diesen arbeiten.
- Planung, Überwachung und Analyse der IT-Budgets und IT-Kosten sowie Initiierung und Überwachung von Kostensenkungsprogrammen in Zusammenarbeit mit dem IT-Controlling.

Eine Trennung zwischen CIO und IT-Leitung ist dann vorzunehmen, wenn es sich um große Organisationen handelt bzw. eine Trennung zwischen dem Unternehmen und der IT besteht. Dies kann durch Auslagerung, rechtlich selbstständige Einheiten u.ä. geschehen. In diesem Fall ist der CIO auf der Unternehmensseite der Ansprechpartner für den IT-Leiter. Bei integrierten Einheiten in Unternehmen und Verwaltung ist der Aufgabenbereich IT-Leitung und CIO auf eine Person konzentriert.

In der **Aufgabenstellung** und damit in der Organisation gibt es grundsätzlich zwei Ausprägungen (vgl. hierzu [GM05], S. 46 ff.):

- Der CIO ist der Verantwortliche des Unternehmens für alle Belange der Informationsverarbeitung und vertritt das Unternehmen gegenüber dem gesamten IT-Bereich. Diese Ausprägung ist Standard in sehr großen Unternehmen mit rechtlich eigenständiger IT oder mit durch Dritte betriebener IT (Outsourcing). In diesem Fall fungiert der CIO quasi als Auftraggeber für die IT-Bereiche.
- Der CIO ist der Verantwortliche des Unternehmens für alle Belange der Informationsverarbeitung und gleichzeitig Leiter der IT des Unternehmens. Dies ist eine übliche Ausprägung in kleinen und mittleren Unternehmen sowie in Bereichen des öffentlichen Dienstes. Der CIO ist damit der Auftragnehmer gegenüber dem Unternehmensmanagement, hat aber gleichzeitig auch aus seiner Verantwortung für die Unternehmensdaten eine eigenständige Rolle als Auftraggeber für interne IT-Projekte.

**Beachten Sie:**

Die Abgrenzung des CIOs zum klassischen IT-Leiter zeigt die Unterschiede zum bisherigen, eher technisch geprägten Denken auf. Der Aufgabenbereich des IT-Leiters besteht in der Softwareentwicklung und dem RZ-Betrieb. Er ist mit der Bereitstellung technischer Lösungen für aktuelle Geschäftsprozesse betraut und verfügt über technisches IT-Know-how. Der CIO konzentriert sich hingegen auf das Informations-, Wissens- und Technik-Management, erarbeitet Visionen und Konzepte für zukünftige technische Möglichkeiten und berät die Fachbereiche bei der Gestaltung ihrer Geschäftsprozesse.

6.4.1.2 IT-Planung und IT-Controlling

Im Bereich der IT-Planung und des IT-Controlling sind folgende Rollen typisch:

- IT-Architekten
- IT-Controller
- IT-Quality-Manager
- IT-Koordinatoren

- IT-Beschaffung
- IT-Marketing
- Informations- und Wissensmanagement

IT-Architekten: Sie strukturieren die vorhandenen Anwendungs- und Systemwelten systematisch und schaffen durch definierte Rahmenbedingungen die Basis für eine flexible Anpassung der Informationstechnologien an veränderte Marktanforderungen. Wichtige Eckpunkte der Tätigkeit sind die kontinuierliche Entwicklung und Pflege der IT-Architekturen (Fach-, Software- und Systemarchitekturen), die situationsabhängige Durchsetzung der gewünschten Architektur und die Institutionalisierung des Architekturmanagements.

IT-Controlling: Unabhängig von dem Unternehmenscontrolling als verlängerter Arm der Unternehmensleitung besteht die Notwendigkeit eines Controllings für die spezifischen Aktivitäten des IT-Bereichs. IT-Controller sollen letztlich dafür sorgen, dass das Management (Unternehmensführung, Management der Fachbereiche, IT-Management) die „richtigen“ Entscheidungen treffen kann. Sie sichern und optimieren die Informationsversorgung der Manager. Neben der Beschaffung und Aufbereitung der entscheidungsrelevanten Daten klären und präzisieren sie, wo IT-Entscheidungen nicht mehr durch Fakten abgesichert werden können und welche Risiken die Entscheidungsträger eingehen (müssen). Im Einzelnen lassen sich folgende Kernaufgaben für das IT-Controlling unterscheiden:

- IT-Controller sorgen für Strategie-, Ergebnis-, Finanz- und Prozesstransparenz in der IT und tragen somit zu höherer Wirtschaftlichkeit bei.
- IT-Controller koordinieren Teilziele und Teilpläne ganzheitlich (etwa für IT-Projekte oder IT-Services) und organisieren das Berichtswesen.
- IT-Controller moderieren und gestalten den Managementprozess der Zielfindung, der Planung und der Steuerung in der IT so, dass jeder Entscheidungsträger zielorientiert handeln kann. Dies betrifft etwa Informationen bezüglich der Beschaffung von IT-Produkten.
- IT-Controller leisten den erforderlichen Service der betriebswirtschaftlichen Daten- und Informationsversorgung für die IT-Beschäftigten.
- IT-Controller gestalten und pflegen die IT-Controlling-Systeme.

Zur Erfüllung der Aufgaben im IT-Controlling sind entsprechende **Prozesse** zu definieren, zu dokumentieren und in der Praxis permanent zu optimieren (vgl. hierzu Kapitel 7 „IT-Controlling“).

IT-Qualitätsmanagement: Ein integriertes spezialisiertes Qualitätsmanagement gehört zu jedem IT-Bereich. Man unterscheidet hier drei wesentliche Aufgabenfelder, die es zu erfüllen gilt:

- Sicherung der Qualität der Produkte/Leistungen des IT-Bereichs sowohl in der Anwendungsentwicklung als auch in der Produktion bzw. im laufenden Betrieb.
- Planung, Definition, Abstimmung und Einführung interner Standards (etwa die Fixierung und Fortschreibung von Prozessbeschreibungen, das Erstellen eines Projektmanagement-Handbuchs etc.).
- Einführung externer Standards wie eine Zertifizierung nach ISO 9001 oder ITIL-Standard für die Serviceprozesse. Hierzu zählt dann auch die Schulung der Mitarbeiter und die Überwachung der Einhaltung der Standards und der Vorgaben der Normen usw.

IT-Koordination: Es wurde bereits herausgestellt, dass die IT-Technologien und IT-Produkte bereitstellen muss, die die Geschäftsprozesse der jeweiligen Organisation optimal unterstützen. IT-Koordinatoren befassen sich unter anderem mit der Auswahl, Einführung und dem störungsfreien Betrieb geeigneter IT-Systeme. Dabei sind die Interessen des einzelnen Anwenders genauso zu berücksichtigen (durch systematisches Erheben und Bewerten der Anforderungen) wie die strategischen Ziele des Unternehmens insgesamt sowie daraus abgeleitete spezifische IT-Ziele (Qualität, Sicherheit, Wirtschaftlichkeit). Ein IT-Koordinator muss letztlich die Balance zwischen den begrenzten Ressourcen des Unternehmens und den vielfältigen Möglichkeiten, die die modernen Informationstechnologien heute bieten, täglich neu finden.

IT-Beschaffung: Hier gilt es vor allem, IT-Systeme kostengünstig zu beschaffen und gleichzeitig eine hohe Leistungsqualität bereitzustellen. Aufgabe ist es beispielsweise über ein koordiniertes Mengenmanagement eine Nachfragebündelung für zu beschaffende IT-Produkte dadurch zu realisieren, dass die Nachfragemengen für alle Unternehmenseinheiten zentral zusammengeführt werden. Anstelle pauschaler Plandaten stehen damit für die IT-Beschaffung Daten zur Verfügung, die detailliertere Planungen ermöglichen. Auf die IT-Lieferanten kann so auch ein gewisser Druck über Preise und Margenvorgaben ausgeübt werden. Damit verbunden sowie durch die Nachfragebündelung lassen sich Kostenreduktionen realisieren. Angestrebt werden sollte ein zentrales Vertragsmanagement, sodass für alle Arbeitsplätze gleiche Rahmenverträge gelten. So erreicht man eine langfristige Konditionen-Sicherheit und stellt Preistransparenz für den Endbenutzer her.

Marketing und Vertrieb: Dies sind zwei Rollen, die zu jedem gut geführten IT-Bereich gehören, egal, ob es sich um einen weitgehend autarken Bereich handelt oder ob man eine stark eingebundene Organisation betrachtet. Die IT muss, da sie in dem hier beschriebenen Kontext eine Serviceorganisation ist, ihre Bedeutung und den Mehrwert für das Unternehmen verdeutlichen und auch gegenüber dem tatsächlichen oder fiktiven Wettbewerb (denken Sie etwa an den Bezug von IT-Leistungen von außen) eine akzeptierte Stellung wahrnehmen. Wichtig ist, andere Abteilungen im Unternehmen für die Pläne der IT zu interessieren, Neugier zu wecken. Im Idealfall wissen die Fachabteilungen genau Bescheid, wie sie IT-Services der IT abrufen können und welche neuen Lösungen verfügbar sind.

6.4.1.3 IT-Betrieb

Der IT-Betrieb bzw. die Produktion von IT-Leistungen stellen wiederum eine Zusammenfassung verschiedener Rollen dar. Zu unterscheiden sind hier beispielsweise:

- Service-Desk (Help-Desk)
- Hardwareservice und Betrieb
- Netzwerkservice
- Peripherieservice usw.
- Service-Prozessverantwortliche
- Systemadministration
- Datenbankadministration

Die im Einzelfall nötige Aufteilung richtet sich nach der Größe des jeweiligen Bereichs.

Service-Desk (zuweilen auch **Help-Desk**): die zentrale Kontakt-Schnittstelle zwischen den Benutzern von IT-Systemen und den Mitarbeitern im IT-Servicemanagement. Die Mitarbeiter im Service-Desk sind bei allen Fragen und Schwierigkeiten rund um den IT-Arbeitsplatz erste Ansprechpartner für den Anwender von IT-Systemen (Single-Point-of-Contact). Der Service Desk hat sich aufgrund der erweiterten Aufgaben und vielschichtigen Funktionalitäten der IT aus dem früheren Help Desk entwickelt. Mittlerweile ist er nicht mehr nur eine Anlaufstelle für Probleme, sondern vielmehr eine Service-Organisation, die sich auch um Installationen oder IT-Übersiedlungen kümmert. Zu den wesentlichen **Aufgaben im Service-Desk** zählen:

- die Aufnahme und Klassifizierung von Störungen (Incident Management);
- die Bereitstellung von Soforthilfen (etwa über Fernwartung) sowie
- die Überwachung der Störungsbearbeitung bis zur Problemlösung.



Um die genannten Aufgaben erfolgreich bewältigen zu können, werden im Service-Desk Informationen über den aktuellen Bearbeitungsstand von Störungen in Datenbanken festgehalten. Zudem erbringen die Beschäftigten im Service-Desk für die Anwender bei Bedarf auch Beratungs- und Supportleistungen.

Netzwerkservice: Mittlerweile ist es für Unternehmen/IT-Bereiche mit eigenen Leitungsnetzen (etwa LANs bzw. WANs) nahezu selbstverständlich, dass sich spezielle Gruppen mit Netzhardware, Netzanbindungen und auch der Netzauslastung beschäftigen. Zunehmend ist jedoch auch die Nutzung der öffentlichen Netze ein wesentlicher Erfolgsfaktor bei der Abwicklung der Unternehmensaktivitäten. Auch dieser Bereich muss in einem internen Service organisiert sein. Die Aufgaben im öffentlichen Netz bestehen darin, sowohl die technischen Kontakte mit den Providern zu organisieren und die für den Betrieb optimalen Angebote zu identifizieren als auch die Bewertung der wirtschaftlichen Gesichtspunkte. Außerdem sind hier in Verbindung mit dem Security-Management die Sicherheit des Netzes und damit auch des Betriebs zu gewährleisten. Der Netzwerkservice wird in den betrachteten Unternehmen und Organisationen sowohl dem Betrieb zugeordnet als auch als selbstständiger Bereich (Gruppe, Abteilung etc.) geführt.

Entscheidungskriterien hierfür sind sowohl die Größe des Netzwerkbereichs (in Bezug auf die zugeordneten Personen) als auch die Bedeutung für den Unternehmensablauf insgesamt. So ist in den kommunikationsintensiven Betrieben wie im Internethandel der Netzwerkbereich eine separate Organisation.

Service-Prozessverantwortliche: Für jeden der definierten und zu implementierenden IT-Serviceprozesse sollte ein spezifischer Prozessmanager ernannt werden, der in der Einführungsphase in Vollzeit zur Verfügung steht. Er verfügt idealerweise über Erfahrungen aus dem jeweiligen Prozessumfeld und über Basis-Know-how im Bereich IT-Servicemanagement. Eine entsprechende Orientierung vermittelt Abbildung 6.3.

Prozessgruppe	Prozess/Status	Verantwortlichkeiten							
		Produktion	Infrastruktur	Competence Center	Business Intelligence	Competence Center	Competence Center	Projekt-Management	Account Mgmt./Controlling
Service Support	Incident Management	X							
	Problem Management	X	X	X	X	X	X		
	Configuration Management		X						
	Change Management							X	X
	Release Management					X			
Service Delivery	Service Level Management								X
	Financial Management								X
	Capacity Management		X						
	Continuity Management	X	X						
	Availability Management	X	X						

ABBILDUNG 6.3 Prozessverantwortung im IT-Betrieb



Beachten Sie:

Bei der Einführung eines IT-Servicemanagements sind unbedingt die Qualifikationen der IT-Mitarbeiter zu berücksichtigen. Dabei gilt es zu ermitteln, für welche Prozesse Qualifikationen vorhanden sind und wo sie noch fehlen. Bezüglich der fehlenden Qualifikationen ist ein Zeit- und Kostenplan zur Erlangung dieser Befähigungen zu erstellen. Dieser ist dann mit den allgemeinen Einführungsplanungen zu vergleichen, und die Lücken (GAPs) sind herauszuarbeiten. Daraufhin sind ggf. Schulungen zu organisieren, die es den Mitarbeitern ermöglichen, die neuen Anforderungen zu bewältigen.

6.4.1.4 Anwendungsentwicklung

Im Bereich der Anwendungsentwicklung sind folgende Rollen typisch:

- Systemanalytiker
- Anwendungs-Entwickler
- Software-Integratoren
- Webdesigner
- Datenbankentwickler

Unter Anwendungsentwicklung wurden hier die tatsächliche Entwicklung von Software und die Einführung von Standardsoftware zusammengefasst. Obwohl hinsichtlich der Projektabwicklung (Vorgehensmodelle) und der Behandlung der Produkte erhebliche Unterschiede bestehen, können die Bereiche organisatorisch gleich behandelt werden. Es hat sich bewährt, die Bereiche bei ausreichender Größe entsprechend der Software zu trennen.

6.4.1.5 Projektmanagement

Eine mögliche Rolle ist das Projekt-Portfoliomanagement. Hier geht es um die Planung und Verwaltung des Projekt- und Betriebsportfolios. Diese werden in jedem IT-Bereich als wesentliche Basis für die Führung des Bereichs und für die Abwicklung der anstehenden Aufgaben benötigt.

Auch die **IT-Projektleitung** nimmt in diesem Rahmen eine Sonderstellung ein, sie ist die Vermittlerin zwischen dem Anwendungsbereich und der IT sowie die Verwalterin eines Projektvolumens, das durchaus dem Volumen eines mittelständischen Betriebs entsprechen kann, und hat die Führung eines Projektteams zu realisieren. Eine klassische Zuordnung ist die Integration der Projekte in die Anwendungsentwicklung. Dies ist heute jedoch zu eng gegriffen.

Ausführliche Angaben zu den Projektrollen finden Sie in Kapitel 5.4.

6.4.1.6 Verwaltung

Jeder Bereich benötigt eine eigene Verwaltung. Es ist nachvollziehbar, dass die Stellenbemessung für die Verwaltung von der Größe der IT und der Eigenständigkeit des Bereichs abhängig ist. Unter der Rolle Verwaltung der IT sind viele Einzelrollen zu sehen, die sich alle dadurch auszeichnen, dass sie eigentlich Stabsaufgaben für die IT-Leitung bzw. den CIO wahrnehmen. Trotzdem sind sie für eine effektive IT-Organisation besonders wichtig.

So werden mit der IT-Verwaltung die Aufgaben eines Sekretariats bzw. einer Assistenz verbunden. Zum Aufgabenbereich gehören neben der Abwicklung des Schriftwechsels und der Terminverwaltung für die IT-Leitung auch wesentliche organisatorische Aufgaben der Ressourcenverwaltung und der Verfügbarkeitsplanung. Viele Aufgaben sind in enger Zusammenarbeit und als Ansprechpartner für die externe Rolle der Personalverwaltung zu sehen. Ein weiterer gesonderter Verwaltungsbereich könnte auch das Bestandsmanagement zu den installierten IT-Systemen bzw. zu den verfügbaren Lizenzen sein.

6.4.2 Stellenbildung und Personalbemessung

Die **Stellenbildung** ist eine unverzichtbare Technik in jedem Gestaltungsansatz, so auch bei der Gestaltung des IT-Bereichs. Systematische Grundlage ist in der Organisationspraxis eine mehr oder weniger differenzierte Aufgabenanalyse. Durch Stellenbildung entstehen „auf Dauer“ angelegte Systembestandteile, die übertragene Aufgaben erfüllen, solange sich diese Aufgaben in einem gültigen oder zu gestaltenden Arbeitszusammenhang bewegen.

Stellen sind elementare organisatorische Einheiten der betrieblichen Struktur (in diesem Fall des IT-Bereichs), denen die Erfüllung bestimmter, sachlich genau abgegrenzter Teilaufgaben (**Stellenaufgaben**) zugewiesen wird. Ein bestimmter Aufgabenkomplex aus der Sammlung der Teilaufgaben kennzeichnet jede Stelle im IT-Bereich.

Zu jeder Stelle sollte es eine **Stellenbeschreibung** geben. Diese dokumentiert die vertikale und horizontale Eingliederung von Stelleninhabern in einer Organisationsstruktur, die zu erfüllenden Aufgaben (Stellenbildung), die zu erreichenden Ziele und die notwendigen Informationen zur Aufgabenerfüllung. Wesentlich für den Stelleninhaber sind:

- Aufgabenbild und Ziele,
- Anforderungsprofil und
- Kommunikationsbild (notwendige Informationen).



Praxistipp:

In der Aufgabenanalyse für den IT-Bereich sind Teilaufgaben zu bilden, deren Umfang durch Zerlegen so weit reduziert wird, bis jede Teilaufgabe deutlich unter der Auslastung einer Person – oder einer sich selbst weiter organisierenden Gruppe – liegt. Die Stellen werden gebildet, indem jeweils einige dieser Teilaufgaben gebündelt und in der Regel einer „gedachten“ Person, einer (teil-)autonomen Arbeitsgruppe oder einem sachlichen Aufgabenträger zugeordnet werden.

In engem Zusammenhang mit der Stellenbildung steht die Personalbemessung. Die **Personalbemessung** (oder auch Stellenbemessung) ist als **quantitative Stellenbildung** Teil der aufbauorganisatorischen Gestaltung. Grundlage der Personalbemessung sollte ein bereits von Schwachstellen befreites Strukturkonzept sein. Andernfalls werden organisatorische Mängel mit einem häufig überhöhten Personalbedarf festgeschrieben.

Folgende **Ziele** können für Überlegungen zur **Personalbemessung im IT-Bereich** zu beachten sein:

- begründeter Personalumfang und begründete Personalkosten,
- Gewährleistung einer zeitgerechten Aufgabenerfüllung,
- angemessene und gleichmäßige Arbeitsbelastung der Mitarbeiter,
- Anpassungsflexibilität gegenüber Veränderungen in der Aufgabenerledigung (z. B. Aufgabemengen-Schwankungen, Arbeitsablaufänderungen).

Zur Ermittlung des zur Aufgabenerfüllung erforderlichen Personalbedarfs werden verschiedene sich ergänzende Verfahren genutzt:

- Aufgabenorientierte Kennzahlen werden analytisch ermittelt. Dazu werden für jede Aufgabenart gesondert der Arbeitszeitbedarf (Bearbeitungszeit) sowie die Aufgabenmenge festgestellt.
- Dieser Prozess lässt sich vereinfachen, wenn für die Bearbeitungszeit je Aufgabenart aus Erfahrungswerten gebildete Richtzahlen vorliegen. Diese Richtzahlen geben die Aufgabenmenge an, die von einem Menschen innerhalb einer bestimmten Zeit geleistet werden kann.



Praxistipp:

Bei der Verwendung von Richtzahlen ist zu prüfen, ob die bei der Ermittlung der Richtwerte zugrunde gelegte Situation (Soll-Situation) der Ist-Situation entspricht. Da die Soll-Situation vielfach nicht bekannt ist, muss davon ausgegangen werden, dass die Richtzahlen einer „Normalsituation“ gerecht werden.

■ 6.5 Outsourcing von IT-Leistungen

Outsourcing von IT-Leistungen ist mittlerweile ein wesentliches Entscheidungsfeld für die Gestaltung der IT-Organisation. Die Idee dahinter ist einfach: Eine Unternehmung soll sich auf ihre Kernkompetenz konzentrieren. Alles, was darüber hinausgeht, hindert eine Privatunternehmung lediglich am finanziellen Erfolg und treibt intern die Kosten. Deshalb erwartet man Kostenreduktionen, wenn Firmen, deren Kernkompetenz eben IT ist, diesen Betrieb für mehrere andere Firmen übernehmen.

Outsourcing (Abkürzung für „outside resourcing“) ist in der IT-Welt umstritten. Letztlich geht es um die mittel- und langfristige Übertragung einzelner oder aller bisher innerbetrieblich erfüllten IT-Aufgaben an ein rechtlich unabhängiges Dienstleistungsunternehmen.

Betrachtet man heute die IT-Organisationen großer Unternehmen und öffentlicher Bereiche, so ist festzustellen, dass die Verlagerung von Aktivitäten des Bereichs auf fremde Firmen und Organisationen ständig zunimmt. Grundsätzlich kommen mehrere Optionen einer Zusammenarbeit mit Dritten in Betracht: Einzelpersonen, Partner-Unternehmen, Offshore-Unternehmen (als Sonderfall externer Unternehmen) sowie Outsourcing-Partner.



Beachten Sie:

Grundsätzlich wird das Verhältnis zwischen Dritten und der eigenen IT-Organisation ausschließlich durch die bestehenden Verträge und Gesetze geregelt. Zu regeln ist unter anderem auch die Integration in die Aufbau- und Ablauforganisation sowie in Know-how-Transfer und Reporting.

6.5.1 Entscheidung über IT-Outsourcing

Eine wesentliche Grundsatzentscheidung, die in allen Bereichen von Betrieben und Verwaltungen heute zu treffen ist, ist der **Grad des Outsourcing** (IT-Outsourcing ja/nein? Was wird outgesourced?). Neben anderen Überlegungen (wie Sicherheit, Flexibilität etc.) spielen natürlich vor allem Kostenüberlegungen eine Rolle. Als wesentliche **Entscheidungsgründe für IT-Outsourcing** werden genannt:

- Kurzfristig erforderliche Kapazitäten werden möglicherweise nicht auf Dauer benötigt. Dies gilt etwa bei der Einführung einer neuen ERP-Lösung. Nach der Einführungsphase wird IT-Personal zwar für den Betrieb bzw. die Weiterentwicklung der Lösung denkbar sein, aber weniger für die Entwicklung bzw. das Customizing von Lösungen.
- Die rasche Entwicklung in den Informationstechnologien lässt immer wieder neue Tätigkeitsfelder im IT-Bereich entstehen, bei denen die zugehörigen Personal-Ressourcen (zunächst) knapp sind. Die innerbetriebliche Aneignung sehr spezieller Kenntnisse mit geringer Wiederverwendungsmöglichkeit ist nicht wirtschaftlich, sodass auf externe Ressourcen zurückgegriffen wird.
- Um innerbetriebliche Fachkompetenz im IT-Bereich aufzubauen, sind in der Regel externe Schulungs- und/oder Beratungsleistungen erforderlich.

- Im Rahmen von IT-Projekten werden oft unternehmenspolitisch heikle Veränderungen vorgenommen, die mit externer Unterstützung durch namhafte Beratungsunternehmen leichter durchsetzbar sind als ausschließlich intern erarbeitete Vorschläge.

Abbildung 6.4 illustriert grundsätzliche Motive für IT-Outsourcing.

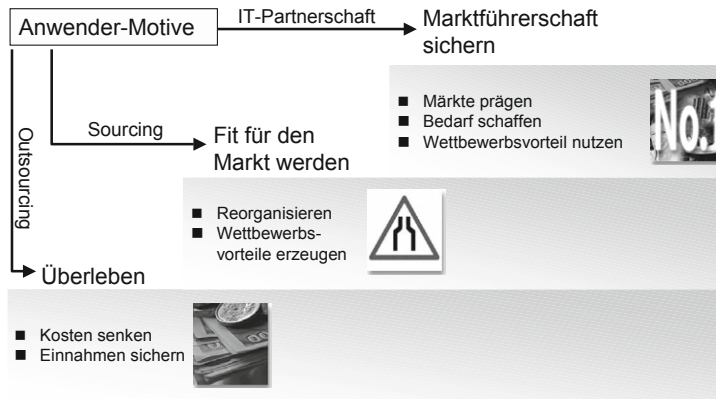


ABBILDUNG 6.4
Anwender-Motive für IT-Outsourcing

Aus der Definition zu IT-Outsourcing wird auch deutlich, dass es unterschiedliche Formen des Outsourcing gibt. Einen Überblick über **typische Partnerschaftsmodelle für das IT-Outsourcing** zeigt Abbildung 6.5.

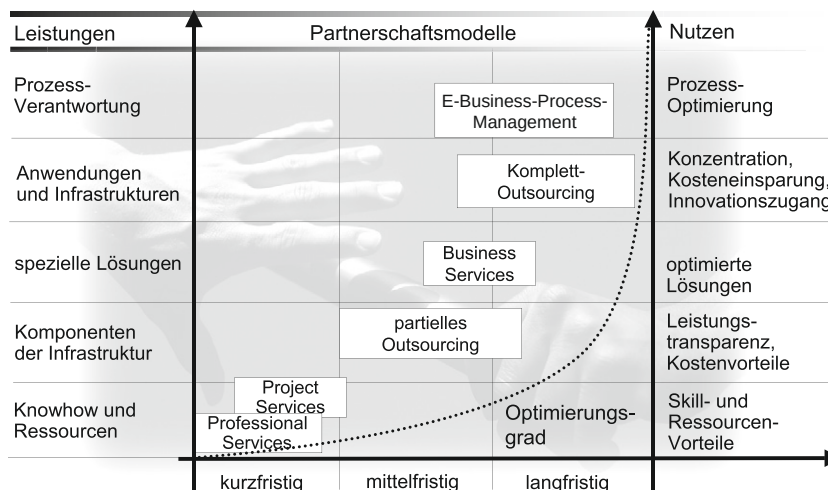


ABBILDUNG 6.5 Partnerschaftsmodelle des IT-Outsourcing

Einige erläuternde Hintergrundinformationen zu Abbildung 6.4:

- Bei kurzfristigen Lösungen (sog. Project-Services oder Professional Services) werden bestimmte IT-Projekte außer Haus durchgeführt bzw. IT-Leistungen durch Externe erbracht, beispielsweise IT-Beratung, Systementwicklung, Systeminstallationen, Programmierung und IT-Schulungen. Letztlich werden externes Know-how sowie externe Personalressourcen in Anspruch genommen.

- Werden auch Komponenten der IT-Infrastruktur ausgegliedert, spricht man von partiellem Outsourcing. In diesen Fällen müssen beispielsweise keine Extra-Server vor Ort eingesetzt werden, um bestimmte Anwendungen zu nutzen. Das Outsourcing kann dabei die Bereiche Storage und Archivierung, Back-up und Systemmanagement einschließen.
- Werden spezielle Lösungen übertragen und somit auch Anwendungen (etwa Lohn- und Gehaltsabrechnungen) außer Haus erledigt, spricht man von Business Services durch Outsourcing.



Mittlerweile hat sich für viele Organisationen die Auslagerung von IT-Infrastrukturen etabliert. Neue Konzepte sind das Business-Process-Outsourcing (BPO), etwa in den Bereichen Personalwesen, Controlling/Rechnungswesen und Einkauf. Diese hochwertigen Services sollten einer genauen Prüfung unterzogen werden. Gleiches gilt für ein Application-Management, das primär für größere Organisationen von Interesse ist.

Eine besondere Rolle spielt auch die **Wahl des Outsourcing-Partners**. Die Anbieter unterscheiden sich meistens hinsichtlich ihres Portfolios: Applikations-Outsourcing steht neben Infrastruktur-Outsourcing und Business Process Outsourcing. **Entscheidungskriterien** können sein:

- Erfahrung, Reputation, Zuverlässigkeit und Garantien des Anbieters der Outsourcing-Leistungen
- Globalität und lokale Präsenz sowie Unternehmenskultur des Anbieter-Unternehmens
- Finanzielle Situation und Marktstellung des Anbieters
- Referenzen
- Branchenkenntnisse
- Innovationsfähigkeit
- Vorhandene Technologie- und Personal-Ressourcen
- Flexibilität in Vertragsverhandlungen, Fairness in der Vertragsgestaltung
- Zusammenarbeit und Kommunikation
- Kostenkriterien (Einmal- und lfd. Kosten)
- Datensicherheit und Datenschutz

Eine beispielhafte Beurteilung der Sourcing-Strategie nach den Kriterien Kosten, Flexibilität, Geschäftsstrategie, Innovation, kritische Masse und Qualität zeigt Abbildung 6.6.

		Selbstbetrieb	Partnerschaft	Externer Betrieb
Kosten		++ ↩	+	–
Qualität	Kundenzufriedenheit	+	++ ↩	+
	Akzeptanz	+	++ ↩	+
Flexibilität	Spitzenzeiten	–	+	++ ↩
	Neue Anforderungen/ Anwendungen	–	+	++ ↩
Strategie	Planung/Steuerung	+	+	–
	Operativ	+	+	–
	Know-how fachlich	+	++ ↩	–
	Know-how Software	++ ↩	+	–
	Schnittstellen	+	++ ↩	–
Innovationen	Markttrends	+	++ ↩	

ABBILDUNG 6.6 Entscheidungskriterien für das Outsourcing

6.5.2 Projektierung von IT-Outsourcing

Outsourcing ist eine Strategie, welche die Tätigkeiten im Unternehmen auf Kernkompetenzen beschränkt, indem Nicht-Kernkompetenzen an externe Dienstleister vergeben werden und so die Produktivität gesteigert und Kosten gesenkt werden. Das Auslagern gewachsener Strukturen erfordert jedoch eine detaillierte Planung, damit man die angestrebten Ziele nicht verfehlt (vgl. ausführlich [So02]).

Wie kann eine **Projektierung von IT-Outsourcing** aussehen? 80 Prozent der Unternehmen, die Dienste wie Anwendungsentwicklung und -wartung bereits von einem externen Provider beziehen, haben Probleme. Dies ist das Ergebnis einer Studie. Diese zeigt nämlich, dass 60 Prozent der Unternehmen strategisch wichtige Bereiche auslagern, aber 80 Prozent der Befragten keine Management-Techniken, keinen Rechtsschutz und keine Maßnahmen etabliert haben, um die Einhaltung von Spezifikationen zu gewährleisten. Obwohl Kontrolle und Management des Outsourcers die einzige Kompetenz ist, die nach dem Outsourcing im Haus bleibt, haben die Unternehmen nicht in das Management und die Kontrolle des Partners investiert.

Die Versäumnisse vieler Unternehmen beginnen vielfältigen Erfahrungen zufolge schon bei den Vorbereitungen zu einem Auslagerungs-Deal. Eine ausformulierte Strategie ist selten vorhanden, die Entscheidungsfindung folgt meistens einzig und allein der Vorgabe, das IT-Budget zu reduzieren. Dies ist umso erstaunlicher, als die tatsächlichen IT-Kosten des aktuellen Betriebs kaum bekannt sind und die angepeilten Ersparnisse einer echten Prüfung nicht standhalten.

Eine **fundierte Kostenbetrachtung** sieht anders aus. Ihr sollten nicht allein die in dem eigenen Betrieb und Unternehmen versteckten Kosten zugrunde liegen, sondern auch

- die Anlaufkosten für das Outsourcing-Projekt,
- die Aufwendungen für die Veränderungsprozesse im Hause,

- die erhöhten Preise für künftige Erweiterungs- und Änderungswünsche gegenüber dem Outsourcer sowie – natürlich –
- die laufenden Zahlungen an den externen Dienstleister.

Nüchtern und unvoreingenommen sollten die Anwenderunternehmen sich dem Outsourcing-Thema nähern und allen Entscheidungen eine Bestandsaufnahme vorausgehen lassen. Dazu zählt neben der Kostenbetrachtung nach dem Total-Cost-of-Ownership-(TCO-)Verfahren oder vergleichbaren Modellen möglicherweise auch ein Benchmark-Projekt und die Dokumentation der aktuellen Prozesse. Bei Letzterem helfen Best-Practice-Ansätze wie die IT Infrastructure Library (ITIL) sowie das vor allem von indischen Anbietern genutzte Capability Maturity Model (CMM) des Software Engineering Institute (SEI).

Obwohl nach dem Outsourcing zumindest eine Zeit lang die alten Systeme von bekannten Mitarbeitern betrieben werden, bleibt nach dem Betriebsübergang kaum etwas erhalten. Vormalig informelle Vereinbarungen weichen offiziellen Aufträgen. Dafür sorgen die Outsourcer sehr schnell, indem sie die übernommenen Mitarbeiter in ihre bewährten internen Delivery-Prozesse einbinden. Zu Problemen auf Anwenderseite kommt es immer dann, wenn sie diese Neuerungen organisatorisch nicht aufgreifen. Nur gut ausgebildetes Personal, das den Wert der IT für die Geschäftsprozesse kennt, die Anforderungen der Fachabteilungen in ein Pflichtenheft für den Outsourcer übersetzen sowie den externen Partner kontrollieren und steuern kann, ist ein Garant für ein funktionierendes Auslagerungsprojekt.

In jedem Fall ändert sich aber das Anforderungsprofil der Mitarbeiter. Sie müssen sich vom Handwerker zum Architekten entwickeln. Intern sind Projekt-Manager gefragt. Dem zum externen Anbieter wechselnden Arbeitnehmer zeigen sich ebenfalls neue Karrierepfade auf. Um sie erfolgreich beschreiten zu können, ist eine serviceorientierte Mentalität erforderlich.



Erfahrungswerte und Tipps zur Entscheidung und Organisation des IT-Outsourcing

- Erhalten Sie sich internes Wissen für die Konzeption und Strategieentwicklung.
- Vermarkten Sie den Veränderungsprozess „Outsourcing“ intern, denn IT-Outsourcing muss – soll es funktionieren – von den verschiedenen Kundengruppen und Stakeholdern akzeptiert werden.
- Versuchen Sie, geschäftsbezogene SLAs abzuschließen.
- Kennzahlen müssen für Sie interpretierbar und als Steuerungsgröße anwendbar sein.
- Klare Definition von Schnittstellen, gerade bei mehreren Outsourcing-Partnern.
- Sie werden es nicht schaffen, alles vertraglich zu fixieren. Streben Sie deshalb eine partnerschaftliche Zusammenarbeit an, und versuchen Sie, Ihren Outsourcing-Partner zur Innovation zu motivieren.
- Stellen Sie einen Knowledge-Transfer Ihrer internen Abläufe zum Outsourcing-Partner sicher. Stellen Sie gleichzeitig sicher, dass dieses Wissen auch bei Ihrem Outsourcing-Partner verbleibt.

■ 6.6 Information und Kommunikation mittels Kennzahlen und Reporting

Vielfältige Erfahrungen zeigen: Für die Umsetzung der IT-Prozesse (siehe die zuvor abgebildete Prozesslandschaft) und den damit verbundenen Planung-, Steuerungs- und Überwachungsaufgaben sowie von Projektaktivitäten sind für die IT-Verantwortlichen abgestimmte Informations- und Kommunikationstätigkeiten nötig. In vielen Organisationen verfügen IT-Verantwortliche noch nicht über entsprechende Instrumente, was verstärkt als eklatanter Mangel empfunden wird.



Beachten Sie:

Die Effektivität des IT-Bereichs, seine Reaktionsfähigkeit und seine Akzeptanz hängen ganz wesentlich von Kommunikation und Reporting ab. Wichtig ist deshalb der Aufbau eines geeigneten Informations- und Kommunikationssystems für das IT-Management.

6.6.1 Informationsbedarf der IT-Führung

Von besonderer Bedeutung für den Aufbau eines Informationssystems für das IT-Management sind zunächst die genauen Inhalte und eine Festlegung, welche Informationen notwendig sind. Informationen sind die Basis für jedes Führungshandeln, so auch im IT-Bereich. Deshalb gilt es erst die Anforderungen, die ein Informationssystem für das IT-Management erfüllen soll, zu analysieren und zu formulieren. Maximal-**Anforderungen** sind durch folgende Merkmale gekennzeichnet:

- hoher Aussagegehalt (genau, eindeutig)
- aktuelle und zeitgerechte Bereitstellung
- Vollständigkeit
- leichte Zugänglichkeit und unmittelbare Verfügbarkeit
- sichere Speicherung (keine Zugriffsmöglichkeit für Unbefugte)
- attraktive Darstellung
- sinnvolle Informationsverdichtung

Moderne Management- und Steuerungsansätze fußen letztlich auf Kennzahlen. Auch die IT-Leitung bzw. der CIO benötigt heute ein individuell auf die Unternehmensanforderungen zugeschnittenes Kennzahlensystem. Mit Kennzahlen sollten ihr möglichst aktuelle und verdichtete Maßgrößen zu den wesentlichen IT-Dimensionen (IT-Produkte, IT-Prozesse, IT-Personal und IT-Projekte) bereitgestellt werden, um damit eine adäquate Grundlage für Entscheidungen im IT-Bereich zu haben.

In vielen Unternehmen sind die Kosten und Leistungen der IT erstaunlich intransparent. Ohne saubere Struktur und Erfassung der IT-Kosten sowie der IT-Leistungen und daraus abge-

leitete „richtige“ Kennzahlen gleicht die IT-Führung einem „zahnlosen Tiger“. Zu prüfen ist im Detail, welche IT-Kennzahlen im Einzelfall mit vernünftigem Aufwand erhoben werden können und welche den größten Nutzen haben.

Ausgehend von den genannten Anforderungen kann eine genauere Einordnung des Begriffs **IT-Kennzahlen** (gleichberechtigt finden sich auch die Bezeichnungen „Kontrollziffer“, „Schlüsselgröße“, „Messzahlen“) vorgenommen werden:

- IT-Kennzahlen sind ein wichtiges Handwerkszeug des Managements, des IT-Managements sowie des Controllings, mit denen Informationen in verdichteter Form bereitgestellt werden.
- Mit IT-Kennzahlen lassen sich komplexe Systeme abbilden und Ist- und Sollzustände beschreiben. Diese betreffen die Leistungsfähigkeit der installierten IT-Systeme ebenso wie die Betreuung von IT-Anwendungen, die Durchführung von IT-Projekten sowie den Einsatz von Ressourcen (Personal, Sachmittel).
- Jede Kennzahl erfasst natürlich nur einen engen Ausschnitt der komplexen Realität und stellt demzufolge ein grobes Abbild dieser Realität dar. Als Kennzahlen können jene Zahlen gelten, die quantitativ erfassbare Sachverhalte in konzentrierter Form erfassen.
- IT-Kennzahlen beinhalten heute nicht nur Informationen über technische und betriebswirtschaftliche Tatbestände, sondern auch zu den IT-Prozessen, Stakeholdern, Personen und Kunden.
- IT-Kennzahlen ermöglichen die Beurteilung von IT-Bereichen und die von ihnen erbrachten Leistungen.

Hinweis: IT-Kennzahlen werden unter anderem in Kapitel 7 „IT-Controlling“ vorgestellt.

6.6.2 Reporting im IT-Bereich

In engem Zusammenhang mit der Organisation von Information und Kommunikation für die Führungsebene steht das betriebliche Berichtswesen gegenüber der Unternehmensleitung. Hier liegt der Schwerpunkt auf der Bereitstellung von verdichteten Informationen. Außerdem kommt es ergänzend darauf an, die wertmäßigen IT-Erfolge zu verdeutlichen (im Sinne von IT als Wettbewerbsfaktor bzw. als Value-Management des IT-Bereichs).

Entscheidungssträger – seien es die Unternehmensleitung oder die IT-Leitung bzw. das IT-Management – benötigen zur zielgerichteten Steuerung der IT-Aktivitäten in regelmäßigen Abständen geeignete Informationen. Dabei gilt der Grundsatz, dass nicht alle Empfänger dieselben Informationen in demselben Detaillierungsgrad erhalten müssen.

Bei der Planung der Berichterstattung müssen deshalb vorweg einige Fragen geklärt werden, die letztlich darüber entscheiden, was im Detail zu tun ist. **Gestaltungsfragen der Berichterstattung** betreffen

- die Person des Berichterstatters und des Berichtsempfängers (wer?),
- den Inhalt (was?),
- die Form (wie?) sowie
- den Zeitpunkt der Berichterstattung (wann?).

Berichte aus dem IT-Bereich sollten kein Selbstzweck sein. Wichtig ist vielmehr, für spezifische Zielgruppen angepasste Berichte bereitzustellen, die zu einer erfolgreichen Durchführung aktueller und künftiger Aktivitäten im IT-Bereich beitragen.

Management-Informationen dürfen nicht „überfrachtet“ sein. Es kommt vielmehr darauf an, dass die entscheidungsrelevanten Informationen für das Management unmittelbar erkennbar und anschaulich aufbereitet sind. Ein Ansatz dazu ist das so genannte „**One Page Management**“ (OPM). Ziel dieser Konzeption ist es, die für einen Manager wichtigen Informationen so zu strukturieren, dass alles Wesentliche übersichtlich in drei Memos, die jeweils nicht länger als eine Seite sind, dargestellt werden kann. Ausgehend von zuvor definierten kritischen Erfolgsfaktoren, kann das Informationssystem des Managements auf den folgenden drei einseitigen Memos aufgebaut werden:

6.6.2.1 Schwerpunkt-Memo

Im Schwerpunkt-Memo sind die Schlüsselinformationen über den Tätigkeitsbereich des jeweiligen Managers enthalten. Für jeden definierten kritischen Erfolgsfaktor bzw. dessen Messgröße werden ein Minimalniveau, ein befriedigendes Niveau und ein hervorragendes Zielniveau bestimmt. Die Erreichung wird wöchentlich oder monatlich dokumentiert, wie dies Abbildung 6.7 beispielhaft zeigt.

Schwerpunkt-Memo für Karl Meiler für den Monat Februar					
1. Erfolgsbereich – IT-Projekte					
Projektbezeichnung	ANUBA	BEGIM	SEGEL	SELUBA	ZEILA
Fertigstellungsgrad	10%	65%	15%	80%	100%
Geplanter Endtermin	10. Oktober	30. Mai	15. Mai	1. April	–
2. Erfolgsbereich – IT-Services					
Servicebereich	RZ-Services	Web-Services	Daten-Services	Benutzer-Services	Software-Services
Servicegrad	92%	90%	95%	98%	65%

ABBILDUNG 6.7 Beispiel für ein Schwerpunkt-Memo

6.6.2.2 Feedback-Memo

Das Feedback-Memo beinhaltet die guten und schlechten Nachrichten zu den Arbeitsfeldern. Auf dieser Seite werden die kritischen Erfolgsfaktoren nach positiver bzw. mangelnder Zielerreichung getrennt. Dies soll einerseits eine motivationsfördernde Wirkung haben, andererseits den Blick auf jene Bereiche lenken, in denen sich durch frühzeitige Maßnahmen ein Misserfolg noch verhindern lässt.

6.6.2.3 Management-Memo

Im Management-Memo werden die positiven und negativen Leistungen der Mitarbeiter dokumentiert. Empfehlenswert ist ein Aufbau nach folgendem Schema:

Indirekte Mitarbeiter	Direkte Mitarbeiter
1. Positivzone	2. Positivzone
3. Negativzone	4. Negativzone

Als indirekte Mitarbeiter bezeichnen wir hier jene, die primär in den Fachabteilungen angesiedelt und der betreffenden IT-Führungskraft somit nicht unmittelbar unterstellt sind, aber in IT-Projekten mitwirken. Die Positivzonen beschreiben ausgezeichnete Leistungen, die Negativzonen anhaltende Probleme.

■ 6.7 Führung im IT-Bereich als Herausforderung

Warum ist eine erfolgreiche Führung so wichtig? Schlagwortartig einige Argumente:

- hohe Motivation der Mitarbeiterinnen und Mitarbeiter
- hervorragendes Arbeitsklima
- weniger Mitarbeiterfluktuation
- erfolgreiche Durchsetzung von Veränderungen (Führungskräfte als Change Manager)
- hohe Ergebnisqualität (bezogen auf die jeweiligen Arbeitsergebnisse der einzelnen Unternehmensbereiche).

Primäre Aufgabe der Führung ist, die Potenziale der anvertrauten Menschen (sowohl die Entwicklung der einzelnen Personen als auch die der Teams) so zu verändern und zu aktivieren, dass ihre Leistung und Leistungsbereitschaft erhöht werden. **Ziel der Führungsaktivitäten** des IT-Management sollte es folglich sein,

- die Mitarbeiterinnen und Mitarbeiter in der IT-Organisation zu befähigen, ihr Bestes für die Unternehmung zu geben und die übertragenen Aufgaben mit Freude zu erfüllen;
- Teammitglieder (z. B. IT-Projektteams, Serviceteams, Entwicklungsteams) dazu anzuleiten, Ziele gemeinsam zu erreichen;
- die Rahmenbedingungen so zu gestalten, dass die Teammitglieder effektiv arbeiten können, sowie
- die Problemlösungskompetenz der Teammitglieder (einzeln und als Gruppe) zu erhöhen.

Eine illustrative Einordnung der Herausforderungen zeigt Abbildung 6.8.

Ohne ausgefeilte Führungstechniken und ausgeprägtes Teamverhalten ist eine moderne IT heutzutage nicht mehr vorstellbar. Wie alle Führungsaufgaben im Unternehmen ist auch die bereichsorientierte Führung (etwas des IT-Bereichs) den Einflüssen aus den Veränderungen der allgemeinen Wirtschaftslage sowie den Veränderungen der Aktivitäten innerhalb der Unternehmensorganisation unterworfen. Zu beachten ist auch, dass Veränderungen bei den Anforderungen und Rahmenbedingungen zu beachten sind. Die Konsequenz daraus ist die Notwendigkeit, für die wesentlichen Prozesse Change-Verfahren zu definieren.



ABBILDUNG 6.8 Herausforderungen für Führungskräfte im IT-Bereich

Hierauf kann dann bei Veränderungen zurückgegriffen werden, was die Reaktionsfähigkeit entsprechend erhöht.

Als Führungskraft trägt man Verantwortung für eine Reihe von Aufgaben, die letztlich alle die Effektivität des Unternehmens betreffen. Konkret bedeutet dies: Man erwartet von der Führungskraft neue Fertigkeiten, neues Wissen und neue Verhaltensstrategien. Darüber hinaus stehen Effektivität und Organisation der eigenen Aufgaben im Zentrum. Klar definierte Ziele und Ergebnisse alleine reichen nicht aus. Wenn Sie effektiv sein wollen, müssen Sie als Führungspersönlichkeit überzeugen. Als derjenige, dem die Mitarbeiter aus Überzeugung folgen. Zudem gilt es, von Anfang an festzulegen, wofür und für wen man verantwortlich ist, sowie, welche Entscheidungsbefugnisse man hat.

Die einer Führungskraft übertragene Autorität muss mit fachlicher, methodischer und sozialer Kompetenz ausgefüllt werden. Sind diese drei Kernkompetenzen erfüllt, kann man mit einer erfolgreichen Arbeit als Führungskraft rechnen. Darüber hinaus sollte eine Orientierung an klaren Grundsätzen erfolgen, wie sie Abbildung 6.9 illustriert.

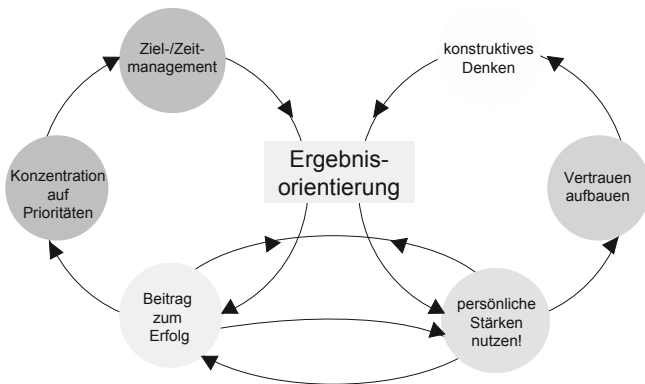


ABBILDUNG 6.9

Wirksame und klare Grundsätze für erfolgreiche Führungskräfte im IT-Bereich

**Beachten Sie:**

Erfahrungen aus der Praxis zeigen: Führungskräfte sind zunehmend gefordert, ein professionelles Führungsverhalten zu etablieren. Nur so können die Mitarbeiter ihre Leistungsfähigkeit voll entfalten und Teams erfolgreich arbeiten.

6.7.1 Führungsaufgaben – Einordnung und Teilaktivitäten

Zu den **typischen Führungsaufgaben** zählen sowohl interne Leitungsaufgaben, die sich aus den hierarchischen Zuständigkeiten ergeben, als auch die Führung in Teams, z. B.:

- Motivationsförderung und Coaching einzelner Mitarbeiter
- Unterstützung der Personalentwicklung
- Zielvereinbarungen und Mitarbeitergespräche
- Teambildung und Teamführung
- Optimales Change Management bei organisatorischen Veränderungen
- Konfliktmanagement (Verhalten in schwierigen Situationen)

Folgende Bereiche, die **typische Führungsaufgaben** darstellen, sollten nach dieser Orientierung auch von IT-Führungskräften gewissenhaft wahrgenommen und daraufhin geprüft werden, ob hier optimal gehandelt wird oder ob Verbesserungen nötig bzw. möglich sind:

- **Motivieren:** Die IT-Führungskraft sollte eigene Maßstäbe setzen, die zur Motivation der Mitarbeiterinnen und Mitarbeiter beitragen.
- **Koordinieren:** Die IT-Führungskraft sollte sicherstellen, dass die notwendigen beruflichen Tätigkeiten nach ihrem Wichtigkeits- und Dringlichkeitsgrad mit einem Minimum gegenseitiger Behinderung ausgeführt werden.
- **Personalauswahl:** Gerade bei der Zusammensetzung des Mitarbeiterteams muss die IT-Führungskraft maßgeblich mitwirken. Sollte dies nicht gegeben sein, gilt es zu prüfen, inwieweit eine Einflussmöglichkeit denkbar ist.
- **Delegieren:** Delegierbare Aufgaben und Zuständigkeiten sollte die IT-Führungskraft in geeigneter Weise Teammitgliedern übertragen. Wichtig ist dabei die Vorgabe von Zielen, aber auch eine entsprechende Kontrolle.
- **Lenken:** Bei der Ausführung von Arbeitsaufträgen durch die Teammitglieder sollte die IT-Führungskraft eine wesentliche Unterstützungsfunktion übernehmen. Nur so lässt sich sicherstellen, dass diese zeit- und qualitätsgerecht ausgefüllt werden.
- **Personalentwicklung:** Die Führungskraft kann sich viel Zeit und Nacharbeit sparen, wenn die Personen, die Aufgaben übernehmen sollen, ausreichend und zielgerichtet vorbereitet und geschult werden.



„Mitarbeiter motivieren zu können, ist der entscheidende Faktor beim Erfolg eines Managers.“

(Peter W. Schutz, Manager)

Eine wichtige Führungsaufgabe liegt darin, eine dauerhafte **Motivation** der Mitarbeiterinnen und Mitarbeiter sicherzustellen. Werden hier wichtige Einflussfaktoren vernachlässigt, führt dies oft zu einer besonders hohen **Demotivation**. Dazu zwei Beispiele:



Eine Hauptursache für demotivierte Mitarbeiter kann in der Unzufriedenheit mit dem Informationsverhalten im Unternehmen bestehen. Fühlen sich Personen ausreichend informiert, wird dies als Selbstverständlichkeit empfunden. Teammitgliedern, die sich schlecht über wichtige Belange informiert fühlen, vergeht hingegen schnell die Lust an der Arbeit. Deshalb ist dies ein recht guter Ansatzpunkt, den Sie vielleicht als Erstes in Angriff nehmen.

Mitarbeiterinnen und Mitarbeiter im Team fordern von der Leitung typischerweise eine hohe Fach- und Führungskompetenz. Steht es schlecht damit – müssen sie beispielsweise Weisungen von einer in ihren Augen unfähigen Führungskraft entgegennehmen und befolgen –, sinkt ihr Engagement erheblich. Umgekehrt wird die Einsatzbereitschaft nicht wesentlich erhöht, wenn die Fach- und Führungskompetenz bei der Führungsebene als unumstritten gilt.

Sind die demotivierenden Faktoren „ausgeräumt“, sollte die Führungskraft positiv überlegen, wie sie zur **Steigerung der Motivation** beitragen kann. Dazu einige Tipps:

- Entwickeln Sie neue Ideen für Ihren Arbeitsbereich. Prüfen Sie vor allem, welche zusätzlichen Funktionen die Arbeit bereichern können. So kann es Arbeitsaufgaben geben, die für Mitarbeiterinnen und Mitarbeiter gleichzeitig die Möglichkeit einer persönlichen Weiterentwicklung bieten.
- Achten Sie auf den Umgangston! Ein Lob oder ein Hinweis auf das bisher Erreichte ist häufig gut geeignet, um Mitarbeiterinnen und Mitarbeiter neu zu motivieren.
- Die IT-Leitung sollte jede Form von willkürlichem Verhalten unterlassen, gelegentlich ein Auge zudrücken und Fehler eines Mitarbeiters nicht zur Katastrophe hochstilisieren. Be- und verurteilen Sie nicht gleich alles! Lassen Sie – wenn möglich – etwas Zeit verstreichen, bevor Sie in einer Angelegenheit Stellung beziehen!
- Prüfen Sie Ihr eigenes Informationsverhalten. Suchen Sie nach Wegen, wie sich mit Hilfe einer ausgewogenen Informationspolitik Misstrauen vermeiden lässt. So können Sie einen wertvollen Beitrag zur Förderung der Motivation bei den Mitarbeiterinnen und Mitarbeitern leisten.
- Achten Sie darauf, auch künftig mit den „richtigen“ Personen zu kooperieren. Anerkennung, Entfaltungsmöglichkeiten, Freude daran, in einem „winning team“ zu arbeiten, diese Faktoren sind meist die entscheidenden, wenn die Arbeit Spaß machen und von Erfolg gekrönt sein soll.



Nicht vergessen:

Letztendlich kann – so meinen manche – niemand eine andere Person motivieren, sie muss und kann sich nur selbst motivieren. Selbstverwirklichung ist echte Motivation. „Engagement für eine gute Sache oder Aufgabe führt zur wahren Selbstverwirklichung“ (Hans P. Jansen).

„Wenn du entzünden willst, musst du selbst brennen.“ (Friedrich Nietzsche)

Eine weitere wesentliche Führungsqualität besteht in einer geschickten **Aufgabendelegation**. Hier einige Tipps, was IT-Führungskräfte beachten sollten:

- Jede Auftragserteilung an andere muss kurz und möglichst klar sein. Die Führungskraft sollte immer deutlich sagen, was sie unter professioneller Aufgabenerfüllung versteht.
- Es sollte für die Erledigung der übertragenen Aufgaben immer ein Endtermin festgelegt werden, unter Umständen sind ergänzend Termine für Zwischenberichte nötig. Arbeiten Sie bei umfangreichen Arbeitspaketen mit Etappenzielen.
- Die Führungskraft sollte immer den Stellenwert und die Bedeutung des Auftrags, den sie delegiert, klarmachen. Unter Umständen ist auch mit Hilfe von Fragen zu prüfen, ob der Auftrag tatsächlich verstanden wurde.
- Es empfiehlt sich das Führen einer Erledigungskartei: kein Auftrag ohne Erledigungsmeldung.

Exemplarisch sei noch auf die Funktion der **Personalentwicklung** hingewiesen, die als weitere wesentliche Führungsaufgabe gilt. Personalentwicklung umfasst dabei alle Maßnahmen, mit denen die Mitarbeiterinnen und Mitarbeiter ausgewählte Kenntnisse, Fähigkeiten und Verhalten erwerben, um die übertragenen Aufgaben und Arbeitspakete erfolgreich zu bewältigen. Als Teilaufgaben für IT-Führungskräfte können herausgestellt werden:

- Fordern und Fördern der IT-Mitarbeiterinnen und IT-Mitarbeiter
- Rahmenbedingungen für das Lernen schaffen bzw. schaffen lassen
- „Vorleben“, was Lernen im Beruf und im Projekt bedeutet
- Wahrnehmen der Verantwortung für die IT-Mitarbeiterinnen und IT-Mitarbeiter
- Umsetzen von IT-Strategien und Grundsätzen.

Zur **Realisierung einer wirksamen Führung** lassen sich beispielsweise die in Abbildung 6.10 enthaltenen Bereiche und Grundsätze unterscheiden.

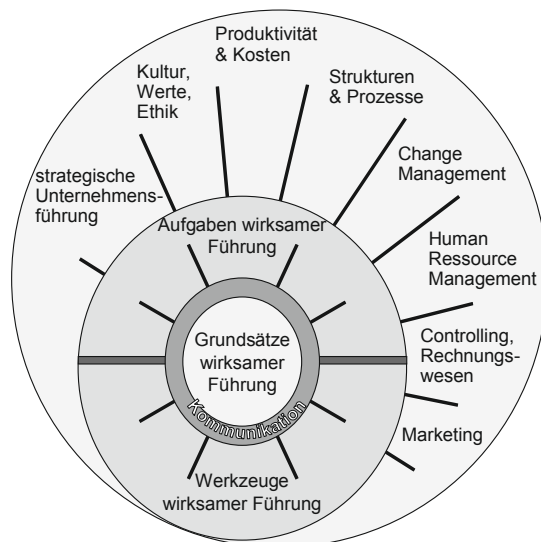


ABBILDUNG 6.10

Aufgaben wirksamer Führung

Checkliste „Erfolgreiches Führen“:**Führung durch Vertrauen:**

Eine wesentliche Voraussetzung für erfolgreiche Führung ist der Aufbau eines Vertrauensverhältnisses zu jedem Teammitglied. Beachten Sie deshalb immer genau die Distanz und das Distanzbedürfnis des anderen. Mit wachsendem Vertrauen des Partners wird sich zugleich die Distanz verringern.

Führung durch Emotionen:

Zu einer erfolgreichen Führung gehört auch das Produzieren von Emotionen. Denken Sie daran: Begeisterung reißt mit, Trauer und Niedergeschlagenheit stecken an, Sympathie weckt Sympathie. Deshalb sollten auch Sie lernen, Emotionen im Team zu produzieren.

Führung und gegenseitige Wertschätzung:

Voraussetzung für erfolgreiches Führen ist auch ein individualisiertes Menschenbild sowie die Wertschätzung der Mitarbeiterinnen und Mitarbeiter. Langfristig überzeugt in führender Position nur jemand, der seine Mitarbeiter „als Menschen“ akzeptiert. Dies kann er aber nur dann, wenn sein eigenes Verhalten dem entspricht. Denken Sie daran, dass Sie nur dann „menschlich“ wirken, wenn Sie (kontrolliert) zeigen, was und wie Sie empfinden.

Zukunftsorientiertes Führen:

Führung bedeutet auch, für die Zukunft Mut zu machen. Sie müssen sich bewusst sein, dass permanent Veränderungs- und Evolutionsprozesse zu bewältigen sind. Es gibt niemals eine endgültige Lösung. Alles bleibt immer im Fluss.

6.7.2 Führungsstile

Führung ist, im Gegensatz zur nackten Machtausübung, untrennbar verbunden mit den Bedürfnissen und Zielen der Geführten.

James MacGregor Burns, amerikanischer Politologe

Die Erfahrung aus der Praxis lehrt: IT-Führungskräfte sind zunehmend gefordert, ein professionelles Führungsverhalten zu etablieren. Nur so gelingt es ihnen, ihre Leistungsfähigkeit voll zu entfalten und Teams auf Erfolgskurs zu bringen.

In deutschen Unternehmen ist es mit modernem Führungsstil vielfach immer noch nicht weit her: Die Führungskraft sagt den Beschäftigten, was sie zu tun haben – und damit Schluss. In Wirklichkeit werden Mitarbeiterinnen und Mitarbeiter dann nicht geführt, sondern nur als Mittel zum Zweck eingesetzt. Zu diesem Ergebnis kommt eine in 180 Unternehmen mit 3000 Führungskräften durchgeführte Studie der Unternehmensberatung Oves Organisations-, Versorgungs- und Entgeltsysteme in Wiesbaden.

Im Detail: Grundlage der Autorität von Führungskräften sei laut Untersuchung in erster Linie der Wissensvorsprung, den sich Vorgesetzte vorbehalten. Schwierige Fälle wollen sie selbst bearbeiten, statt sie den nachgeordneten Mitarbeitern zu überlassen. Die Erklärung: Führungskräfte leiten davon ihr Selbstwertgefühl ab und können mit der Anerkennung durch die nächsthöhere Hierarchieebene rechnen. Somit bliebe, behauptet die Studie, für die eigentliche – meist nicht erlernte – Führungsaufgabe der Mitarbeiter keine Zeit. Dauerstress sei die Folge.

Fazit: Die Mitarbeiterführung ist in den meisten Unternehmen verbesserungswürdig, da eine professionelle Führung, die Mitarbeiter systematisch stärker einbezieht, enorme Reserven freisetzen könnte.

Wichtig ist deshalb, dass jede IT-Führungskraft ihren eigenen, adäquaten Führungsstil findet. Als Ausgangspunkt empfiehlt sich eine Analyse des persönlichen Führungsstils bzw. des in Ihrem Unternehmen praktizierten Führungsstils. Die folgende Tabelle skizziert typische Führungsstile in der Praxis. Tabelle 6.2 soll Sie bei Ihrer Analyse unterstützen!

TABELLE 6.2 Führungsstil-Varianten

Führungsstile (Merkmale)	Erläuterung
geringe Mitarbeiterorientierung + geringe Aufgabenorientierung	Laisser-faire, es findet fast keine Führung statt
geringe Mitarbeiterorientierung + hohe Aufgabenorientierung	stark sachbetonte Führung ohne Pflege zwischenmenschlicher Beziehungen
hohe Mitarbeiterorientierung + geringe Aufgabenorientierung	fürsorglich, Human-relation-Ansatz, dient der Pflege menschlicher Beziehung
hohe Mitarbeiterorientierung + hohe Aufgabenorientierung	gemeinsame Zielfindung und häufige Meetings

Überlegen Sie, ob Sie mit der Zuordnung für Ihre Situation zufrieden sind und damit „gut zurechtkommen“. Anderenfalls sollten Sie Änderungsmaßnahmen in Angriff nehmen! Natürlich gibt es keinen generell „richtigen“ Führungsstil. Es gibt nur einen subjektiv/situativ richtigen, authentischen Stil, den Sie permanent weiterentwickeln sollten. Der geeignete Führungsstil ist situationsbedingt; Abbildung 6.11 verdeutlicht die dabei wirksamen wesentlichen Einflussgrößen.

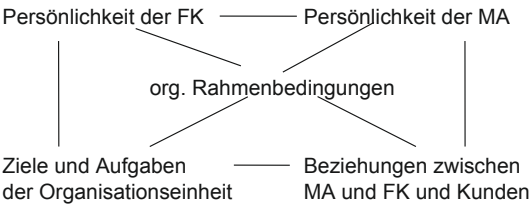


ABBILDUNG 6.11
Der situative Führungsstil – Einflussfaktoren
des adäquaten Führungsstils
(FK = Führungskraft, MA = Mitarbeiter)

Eine Orientierung hinsichtlich der besonderen Akzentuierung des Führungsstils gibt Tabelle 6.3. Sie zeigt sechs verschiedene Ausprägungen eines Führungsverhaltens, wobei gegenseitige Abhängigkeiten bestehen. In der Praxis gilt es oft, sinnvolle Kombinationen zu schaffen:

TABELLE 6.3 Anwendung von Führungsstilen

Führungsstil	Besondere Merkmale (Führungsverhalten)	Anwendung bei ...
wertschätzender Führungsstil	▪ Eigene Wertschätzung äußern ▪ Erreichte Ziele anerkennen ▪ Lob in dosiertem Umfang spenden	Dieser Führungsstil sollte engagierten und ausgleichenden Personen gegenüber gewählt werden. Diese sind in ihrem Verhalten zu bestärken und dauerhaft zu motivieren.

Führungsstil	Besondere Merkmale (Führungsverhalten)	Anwendung bei ...
fördernder Führungsstil	▪ Zielorientierung und Leistungen herausstellen ▪ Ausdehnung von Aufgaben-, Kompetenz- und Verantwortungsbereichen analog zur Mitarbeiterentwicklung ▪ leistungsanreizende Motivationsfaktoren nutzen	Anwendung, um leistungsstarke Mitarbeiter zu motivieren, ihre Stärken zu erhalten bzw. noch zu steigern. Ist die Leistungsbereitschaft – bezogen auf die Aufgabe – hoch, die Fähigkeiten zur Problemlösung bei den Mitarbeitern aber noch unzureichend ausgeprägt, ist ein Anleiten und Fördern durch die Führungskraft hilfreich.
anspornender Führungsstil	▪ wenig aufgaben-, aber stark Mitarbeiter-bezogener Führungsstil ▪ deutlich Erwartungen rückkoppeln und mit Appellen zur Veränderung des Mitarbeiterverhaltens verbinden ▪ bewusst machen, dass Minderleistungen eines Einzelnen Mehrleistung für die Gruppe bedeuten	Bei Mitarbeitern mit Bequemlichkeitsmotiven („Drückeberger“) sollte ein anspornender Führungsstil gewählt werden, um sie entsprechend zu fordern. Mitunter verfügen Mitarbeiter über ein hohes Maß an Fähigkeiten und Fertigkeiten zur Aufgabenbewältigung, doch fehlt Ihnen oft das nötige Engagement.
integrierender Führungsstil	▪ klar definierte Ziele vereinbaren und häufigere Kontrollen der Zielerreichung durchführen ▪ „schützende Hand“ walten lassen, wenn Personen von anderen Teammitgliedern isoliert werden	Ist sinnvoll, um Neulinge zu integrieren und Außenseiter an die Gruppe heranzuführen.
ermutigender Führungsstil	▪ neue Hoffnungen geben und Zuversicht zeigen ▪ aktiv Zuhören und verstehende Anteilnahme zeigen ▪ unterlaufene Fehler nicht tadeln und kritisieren, sondern gemeinsam bereinigen	Schüchterne und in ernste Lebenskrisen geratene Mitarbeiter („Problembeladene“) können auf diese Weise gestärkt und neu motiviert werden.
bremsender Führungsstil	▪ vereinbarte Ziele fokussieren und keine Zielabweichungen zulassen ▪ persönliche Autorität einsetzen ▪ aufkeimenden Streit und aufwiegelndem Verhalten sofort und massiv begegnen	Zu lebhaft und stark extrovertierte Mitarbeiter (Profilneurotiker, Querulanten, Besserwisser) müssen mitunter in Schranken gewiesen und auf Leistungsziele hingesteuert werden.

Erfahrene Manager haben ihren eigenen Führungsstil. John D. Rockefeller sagte: „Was mich anbelangt, so zahle ich für die Fähigkeit, Menschen richtig zu behandeln, mehr als für irgendeine andere Fähigkeit auf der ganzen Welt.“

**Beachten Sie:**

Voraussetzung für alle Führung sind ein die Persönlichkeit respektierendes Menschenbild und die Wertschätzung der Mitarbeiter. Nur ein partnerschaftlich-dialogisches Führungskonzept entspricht dem neuen Selbstverständnis gut ausgebildeter, mündiger IT-Mitarbeiter und IT-Mitarbeiterinnen.

Moderne IT-Führungspersonen müssen in Zukunft ihre Macht teilen und „loslassen können“ bzw. ihren anvertrauten Mitarbeiterinnen und Mitarbeitern mehr zutrauen. Delegation ist zu wenig. Die neue Führungsaufgabe ist Hinführung und Entfaltung zum Mitunternehmertum. Persönliches Charisma und Glaubwürdigkeit sowie Offenheit der Führenden werden mitunter zu entscheidenden Prämissen für den Erfolg.

6.7.3 Ausgewählte Führungsinstrumente

Die Kommunikation der IT-Führungskräfte untereinander ist für den Unternehmenserfolg und für erfolgreiches Handeln unerlässlich. Kommunikation erleichtert Entscheidungen und das Lösen von Konflikten. Mit Kommunikation werden zudem Informationen beschafft. Kommunikation sorgt für Entspannung und macht Wissen verfügbar.

Die Notwendigkeit einer funktionierenden Kommunikation in Management- und Führungsprozessen ist unbestritten. Dazu zählen nicht nur die Besprechungen im Team. Notwendig sind auch persönliche Gespräche. So sollte gerade die IT-Leitung immer wieder das Einzelgespräch unter vier Augen suchen, da man nur dort erfährt, wie die Zusammenarbeit im Team beurteilt wird und wie die Motivationslage der Teammitglieder zu bewerten ist. Auch persönliche Einstellungen, Befürchtungen, Konkurrenzgefühle oder zwischenmenschliche Konflikte lassen sich nur im persönlichen Gespräch aufdecken.

**Beachten Sie:**

Sie können bei Ihrem Gesprächspartner kein Interesse für etwas wecken, wenn er Ihnen gar nicht zuhört. Ebenso wenig wird es Ihnen gelingen, Ihren Gesprächspartner zum Handeln zu bewegen, wenn er nicht auch innerlich und gefühlsmäßig von einer Sache überzeugt ist.

Nachfolgend sollen die wesentlichen Führungsinstrumente, die insbesondere auch Kommunikationsanforderungen an die IT-Führungskraft stellen, skizziert werden: Zielvereinbarungen, Mitarbeitergespräche und aktives Konfliktmanagement.

6.7.3.1 Zielvereinbarungen

Zielvereinbarungen sind auch für das IT-Management wesentlich, um verbindliche Absprachen mit den Mitarbeiterinnen und Mitarbeitern für einen festgelegten Zeitraum zu treffen (in der Regel ein Jahr). Sie enthalten Angaben zu den für den definierten Zeitraum zu erreichenden Wirkungen/Ergebnissen (Outcome) und/oder über die zu erbringenden Leistungen (Out-

put). Dabei werden die bereitgestellten Ressourcen und andere Rahmenbedingungen ggf. ausdrücklich skizziert.

Daraus lassen sich zwei wesentliche Funktionen von Zielvereinbarungen ableiten:

- Sie sind ein wesentliches Instrument, um Ergebnis- oder Prozessziele zu einer Tätigkeit in IT-Projekten bzw. innerhalb von IT-Prozessen zu definieren.
- Sie sind ein Instrument zur Förderung der Mitarbeiter-Motivation und können ggf. auch als Anhang des Arbeitsvertrags festgelegt sein.

Bei der Festlegung von Zielen im Rahmen von Zielvereinbarungen sind einige Grundregeln zu beachten. Die Ziele müssen sein:

- genau definiert und messbar (z. B. nach Menge, Qualität, Aufwand /Kosten, Zeiträumen/Fristen);
- umsetzbar in konkretes Handeln;
- überschaubar, also zeitlich und inhaltlich begrenzt;
- realistisch, d. h. herausfordernd, aber binnen eines Jahres erreichbar;
- aus übergeordneten strategischen Zielen ableitbar, jedenfalls mit ihnen vereinbar;
- ohne Widerspruch zu anderen Zielen;
- annehmbar, also auf die individuellen Möglichkeiten und Fähigkeiten bezogen;
- sie müssen Handlungsspielräume frei lassen.



Tipps für das Festlegen von Zielvereinbarungen:

Die Anzahl der zu vereinbarenden Arbeitsziele sollte nicht mehr als 15 bis 20 betragen. Arbeitsziele können aus allen Themenfeldern des Aufgabenbereiches entwickelt und gemeinsam erarbeitet werden. Die Ziele sollten möglichst zu Kernaufgaben im Zuständigkeitsbereich und damit zu Arbeitsschwerpunkten vereinbart werden. Zielvereinbarungen umfassen qualitative ebenso wie quantitative Aspekte.

Bezüglich der Entscheidung über eine Einführung oder Optimierung des Einsatzes von Zielvereinbarungen ist zu prüfen und herauszuarbeiten, welcher Nutzen damit verbunden ist. Als Vorteile von Zielvereinbarungen für den IT-Bereich können genannt werden:

- Die Entwicklung, Definition und Vereinbarung von Zielen schafft eine verlässliche Arbeitsgrundlagenbeziehung zwischen der IT-Leitung und den Mitarbeitern.
- Die strategischen Ziele der Unternehmensorganisation bzw. des IT-Bereichs werden durch Vereinbarungen zu Sach-, Arbeits- und Verfahrenszielen mit den Jahreszielen aus den konkreten Aufgaben der einzelnen Beschäftigten über alle Ebenen hinweg verknüpft. Das schafft mehr Transparenz.
- Die Vereinbarungen zu Arbeitszielen und zu persönlichen Zielen sind als Bestandteile des Mitarbeitergesprächs wichtige Voraussetzungen für ziel- und qualitätsorientiertes Handeln in der Praxis.
- IT-Leitung und Mitarbeiter werden in die Lage versetzt, sich eine detaillierte Vorstellung von den Aufgaben der Zielvereinbarungspartner zu erarbeiten. Gleichzeitig wird die Iden-

- tifikation mit den Aufgaben des IT-Bereichs erleichtert und mehr eigenverantwortliches Handeln im eigenen Zuständigkeitsbereich ermöglicht.
- Schließlich wird so die Aufgabenerfüllung im IT-Bereich durch klare Ziele gesteuert.

6.7.3.2 Mitarbeitergespräch

Das **Mitarbeitergespräch** ist ein vertrauliches „Vier-Augen-Gespräch“ und bietet die Chance, die Zusammenarbeit zwischen Vorgesetztem und Mitarbeiter zu verbessern. Es ist regelmäßig und mindestens einmal jährlich zwischen Vorgesetzten (hier der IT-Leitung) und Mitarbeitern als gleichberechtigte Partner zu führen. Es dient der wechselseitigen Rückmeldung über erlebtes und erwünschtes Verhalten und über die jeweiligen Zielvorstellungen zu den Sach- und persönlichen Zielen.

Auch soll das Mitarbeitergespräch den Informationsfluss und die Transparenz in der Arbeit verbessern, Störungen in der Zusammenarbeit aufdecken und beseitigen und die persönliche Entwicklung fördern. Daher sollen im Gespräch folgende Themenbereiche angesprochen werden: Zusammenarbeit und Führung, Arbeitsumfeld, Aufgaben und Rahmenbedingungen der Arbeit, berufliche Förderung und persönliche Entwicklung sowie Zielvereinbarungen zu Arbeits- und persönlichen Zielen.



Praxistipp:

Für eine optimale Gesprächsführung ist es wichtig, dass Führungskräfte sich bei Gesprächen im Vorfeld Gedanken über den möglichen Einfluss dieser Faktoren machen. Schwierige Gespräche erfordern zu Beginn eine sehr klare und differenzierte Zielformulierung.

Es gibt noch eine ganze Reihe weiterer Einflüsse, die den Gesprächsablauf bzw. das Verhalten des Gesprächspartners stark beeinflussen:

- Verhalten und Meinung von Vorgesetzten bzw. Kollegen
- gesellschaftliche Einflüsse
- private Situationen
- vorgegebene Verfahren
- rechtliche Regelungen bzw. Vorschriften
- Unternehmenskulturen
- Stimmungsschwankungen jedes Einzelnen

6.7.3.3 Konfliktmanagement

Unsere Aufgabe ist es nicht, den Konflikt – als existentiellen Spannungszustand – zu negieren, sondern ihn zu erkennen, zu untersuchen, zu bewältigen – und mit ihm zu leben, soweit er nicht zu bewältigen ist.

Hans L. Merkle, Manager

Dieses Zitat verdeutlicht die Bedeutung, die dem Konfliktmanagement für eine erfolgreiche Tätigkeit einer IT-Führungskraft zukommt. Die Vorstellung, konfliktfrei leben und arbeiten zu

können, ist sicher ein Mythos. Dazu eine wichtige Feststellung vorweg: Konflikte sind im Berufs- und Privatleben nicht unbedingt eine Katastrophe, sondern eigentlich normal, weil überall dort, wo Menschen mit Menschen umgehen, längerfristig Konflikte entstehen.

Auch in der IT-Praxis sind Konflikte nicht selten. Meist läuft im Team etwas schief, wenn Absprachen und Termine nicht eingehalten wurden, einzelne Teammitglieder sich überlastet fühlen, Rivalitäten im Projekt ausgetragen werden, strenge Planvorgaben die Arbeitsmotivation bremsen oder Informationen nicht weitergegeben wurden. Ein typischer Konflikt ist oft vorprogrammiert, wenn Mitglieder eines IT-Projektteams parallel in der Linienorganisation tätig sind und dann quasi zwei Vorgesetzte haben.

Wahrscheinlich verbinden auch Sie Konflikte mit etwas Unangenehmem, das vermeidbar ist. Das trifft sicher zu einem Großteil zu. Konflikte behindern Ihre Arbeit, kosten Zeit und belasten die Arbeitsatmosphäre. Dennoch sollten Sie Ihre Einstellung ein wenig relativieren: Konflikte können durchaus produktiv sein. Sie sind nicht selten der Motor von Dynamik und Weiterentwicklung. Wo keine Auseinandersetzung stattfindet, gibt es auch keine Veränderung. Als Beispiele für positive Erfahrungen im Umgang mit Konflikten seien genannt: Probleme werden aufgezeigt, Kreativität wird gefördert und der persönliche Horizont erweitert.

Aber aufgepasst: Die vorgenannten Feststellungen bedeuten nicht, dass Sie unbedingt und permanent auf Konfliktkurs gehen sollten. Wichtig ist der richtige Umgang mit Konflikten. Damit Konflikte nicht zum Ärgernis werden, müssen sie rechtzeitig **erkannt, richtig analysiert und konstruktiv bearbeitet** werden. Diese systematische Vorgehensweise fasst man unter dem Begriff **Konfliktmanagement** zusammen.



Beachten Sie:

Konflikte können einen sehr unterschiedlichen Verlauf nehmen: Sie können lange oder nur kurz andauern, sachlich oder aggressiv ausgetragen, offen angesprochen oder direkt angegangen werden. Trotz dieser Vielfalt gibt es Vorgänge, die für das Verständnis aller Konflikte wichtig sind.

Wie tragen Sie Konflikte gekonnt aus? Suchen Sie baldmöglichst das Gespräch, und vereinbaren Sie mit den Betroffenen einen Termin einige Tage im Voraus, um sich in Ruhe besprechen zu können.

- Wichtig ist für Sie, mehr über die Hintergründe Ihres Konfliktpartners zu erfahren bzw. sich diese zu vergegenwärtigen. Sprechen Sie das Problem gezielt an. Dabei helfen Ihnen die W-Fragen weiter, beispielsweise indem Sie interessiert nach dem Warum fragen.
- Zeigen Sie den Willen zur Konfliktlösung, und unterbreiten Sie einen oder mehrere Lösungsvorschläge. Lassen Sie auch andere Meinungen und Ansichten gelten. Legen Sie aber gleichzeitig Ihre eigene Sichtweise dar. Betonen Sie, dass beide Positionen gleichwertig sind.
- Beachten Sie außerdem, dass im Konfliktgespräch „Du-Aussagen“ nach dem Motto „Du bist ...“, „Du musst ...“ wenig hilfreich sind. Besser als solche Anklagen sind „Ich-Aussagen“ nach dem Motto „Ich bin der Meinung“ oder „Ich fühle mich verletzt“.

Da Konflikte in der Praxis wohl unvermeidlich sind, müssen Führungskräfte nach Wegen suchen, um ihre Konfliktfähigkeit langfristig zu verbessern. Dies bedeutet letztlich, dass sie die **Fähigkeit** entwickeln, künftig

- unnötige Konflikte zu **vermeiden**,
- unausweichliche Konflikte psychisch **durchzustehen** und
- vorhandene Konflikte zu **beheben**.

Um **unnötige Konflikte zu vermeiden**, sollten Sie die Konfliktpotenziale kennenlernen, die im Team und bei anderen Personen stecken können.



Praxistipps:

- Stellen Sie sicher, dass die Zusammenarbeit im IT-Bereich funktioniert. Signale über das Funktionieren erhalten Sie bei der Prüfung, inwieweit Aufgaben und Verantwortung übernommen werden und ob kreative Vorschläge zustande kommen.
- Formulieren Sie gemeinsam einen Verhaltenskodex für Führungskräfte! Auf diese Weise soll sichergestellt werden, dass sich niemand auf Kosten anderer profiliert.
- Prüfen Sie die Kommunikationskultur im IT-Bereich! Wichtig ist es, Probleme offen anzusprechen und wichtige Informationen rechtzeitig weiterzugeben.

Allerdings: Die soeben beschriebenen Gedanken sind hoffentlich gute Leitlinien für Ihr künftiges Verhalten. Patentrezepte können sie jedoch nicht sein. Wie Sie am besten vorgehen, sollten Sie in der jeweiligen Situation von Ihren persönlichen Erfahrungen und den aktuellen Rahmenbedingungen abhängig machen.



Nicht vergessen!

Sprechen Sie im Konfliktgespräch auch verbindende Elemente an. Wenn möglich, betrachten Sie die Sache auch mit einem humorvollen Auge (zumindest innerlich).

■ 6.8 Führung von Teams – Teambildung und Teammanagement

6.8.1 Teamentwicklungsprozesse identifizieren

*„Der Mensch für sich allein vermag gar wenig und ist ein verlassener Robinson;
nur in der Gemeinschaft mit den andern ist und vermag er viel.“*

Arthur Schopenhauer

Experten sehen die Teamentwicklung als einen Prozess an, der mehrere Phasen umfasst (vgl. Abbildung 6.12):

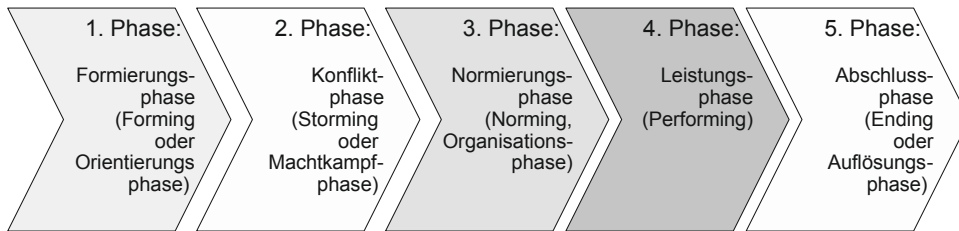
**ABBILDUNG 6.12** Phasen der Teamentwicklung

Tabelle 6.4 skizziert in übersichtlicher Form die verschiedenen Phasen sowie die Verhaltensweisen und Stimmungen der Teammitglieder in den jeweiligen Phasen.

TABELLE 6.4 Teamentwicklungsphasen analysieren

Teamentwicklungsphase	Erläuterungen zur Gruppenstruktur	Verhaltensweisen, Stimmungen
1. Phase: Formierungsphase (Forming oder Orientierungsphase)	In der Anfangsphase der Kooperation formiert sich das Team. Dabei bestehen noch Unsicherheiten hinsichtlich der konkreten Zielsetzungen der Kooperation sowie der Regeln und Formen der Zusammenarbeit.	höfliches, vorsichtiges und unpersönliches Verhalten der Teammitglieder, gegenseitiges Kennenlernen, mitunter gespannte Stimmungslage
2. Phase: Konfliktphase (Storming oder Machtkampfphase)	Im Verlauf der Zusammenarbeit kommen immer wieder Machtkämpfe und Konflikte im Team zum Vorschein. Wichtig ist, dass hier die Spielregeln festgelegt und Konflikte so „bewältigt“ werden, dass sie sich in positive Energie verwandeln.	Cliquenbildung, erste unerschwellige Konflikte brechen auf, mühsames Vorwärtskommen in der Sache (Ziele werden in Frage gestellt u. ä.)
3. Phase: Normierungsphase (Norming, Stabilisierungsphase)	Es bilden sich klare Teamregeln heraus, gegenseitige Unterstützung findet statt, ein Gruppengefühl entwickelt sich. Nun ist auch mehr Offenheit vorhanden. Mitunter entwickeln sich sogar Teamrituale.	Entwicklung neuer Umgangsformen und Verhaltensweisen, gegenseitiges Helfen in Problemsituationen
4. Phase: Leistungsphase (Performing, Produktionsphase)	Eine Konzentration auf die eigentliche Teamarbeit setzt sich durch, Teammitglieder können Aufgaben eigenständig bearbeiten. Kommunikations- und Entscheidungsprozesse laufen in geregelter und in von jedermann akzeptierter Form ab.	Energie wird für effektive Arbeit frei, die Gruppe ist ziel- und ergebnisorientiert; engagiertes, leistungsorientiertes Verhalten; Solidarität bei Problemen
5. Phase: Abschlussphase (Ending oder Auflösungsphase)	Das Ende der Kooperationsarbeiten bedeutet auch die Auflösung des Teams.	Umsetzungsbemühen, Auflösungserscheinungen

Natürlich werden die genannten Phasen nicht alle nacheinander linear durchlaufen. So können Störungen von außen immer wieder zur Folge haben, dass ein Team, das schon gute Fortschritte gemacht hat, wieder in die Konfliktphase zurückgeworfen wird.

Im Verlauf fast aller Teambildungen gibt es „Durststrecken“. Die Motivation der Teammitglieder kann im Laufe der Zeit nachlassen. In diesem Fall – aber auch zur Vorsorge – sind besondere Teamentwicklungsarbeiten nötig.

Die folgenden Symptome lassen auf **Störungen in der Teamentwicklung** schließen:

- **Interesselosigkeit** bei der Bearbeitung von Teamaufgaben: Das Team ist unkonzentriert und inkonsequent bei der Verfolgung der gemeinsamen Ziele und der sich daraus ergebenden Aufgaben. Die Vorbereitung auf Meetings erfolgt nur unzureichend, Diskussionen im Team verlaufen eher schleppend, anstehende Entscheidungen werden tendenziell aufgeschoben.
- Fehlende Übernahme von Verantwortung und **Unentschlossenheit** bei der Entscheidungsfindung: In Teammeetings wird oft abstrakt, auf einer theoretischen Ebene diskutiert, sodass konkrete Lösungsvorschläge ausbleiben. Gleichzeitig ist eine gewisse Angst vor den Folgen von Entscheidungen zu spüren. Im Extremfall weigern sich Teammitarbeiter sogar, Verantwortung zu übernehmen.
- **Konflikte im Team:** Feststellen lassen sich diese insbesondere dann, wenn permanent eine gespannte und aggressive Stimmung in den Teamsitzungen zu spüren ist. Typische Phänomene sind auch, dass Ideen schon angegriffen werden, obwohl sie noch gar nicht ausreichend dargelegt wurden oder Argumente äußerst emotional und heftig vorgetragen werden. Das Klären und Lösen solcher Konfliktsituationen ist dann der einzige Lösungsweg, um wieder zu einer konstruktiven Teamarbeit zu kommen.

Werden Störungen in der Teamentwicklung wahrgenommen, müssen die **Ursachen für die beschriebenen Störungen im Team** analysiert werden. **Mögliche Störfaktoren** sind:

- *Kompetenzprobleme:* Teammitglieder verfügen über einen höchst unterschiedlichen Kenntnisstand, etwa bezüglich der Fachkompetenz, sodass sich keine Synergieeffekte bei der Teamarbeit ergeben.
- *Entscheidungsprobleme:* Die Arbeit im Team geht nicht so recht voran, weil man sich nicht zu den notwendigen klaren Entscheidungen durchringen kann.
- *Kommunikationsprobleme:* Kooperationsziele sowie die erwarteten Ergebnisse bleiben vielen Teammitgliedern nach wie vor unklar.
- *Informationsprobleme:* Probleme bei der Kooperation sind mitunter nur auf Schwierigkeiten beim Informationsaustausch unter den Beteiligten zurückzuführen.
- *Organisationsprobleme:* Ein vereinbarter Arbeitsplan, aus dem insbesondere ein Zeit- und Aktivitätenplan hervorgeht, fehlt. Dieser muss entsprechend nachgearbeitet werden.
- *Rollenkonflikte:* Rollen und Funktionen sind oft nicht eindeutig festgelegt. In diesem Fall muss noch einmal über das Rollenkonzept diskutiert und eine klare Festlegung der Verantwortung und Kompetenzen von Leitung und Team getroffen werden.
- *Beziehungsprobleme:* Es finden beispielsweise „Dominanzspiele“ der Teammitglieder untereinander statt. Werden Beziehungsprobleme zwischen Teammitgliedern ignoriert, kann dies zu echten Krisen führen, wo auch sachlich angemessene Informationen und Argumente nicht mehr gehört und berücksichtigt werden.

Es empfiehlt sich, diese Störfaktoren im Einzelfall zu hinterfragen und daraufhin geeignete Maßnahmen zu ergreifen. Notwendig ist zumindest eine gewisse Sensibilität für die angeführten Störfaktoren.

Geeignete **Maßnahmen zur Bewältigung der genannten Störungen** bestehen primär in einem optimalen Beziehungsmanagement gegenüber allen Kooperationspartnern sowie in einem sorgfältig abgestimmten Informationsaustausch. Insofern liegt es natürlich nahe, dass – je nach Kooperationspartner – auch ein angepasstes und differenziertes Kooperationsverhalten notwendig ist:

- Die IT-Leitung sollte versuchen, die Merkmale von Top-Teams vorzuleben und das Umfeld im Team in regelmäßigen Abständen zu motivieren. Kundenorientierung sollte der wesentliche Leitsatz des Handelns im Team sein!
- Ein weiterer Erfolgsfaktor ist die Einstellung der einzelnen Teammitglieder. Positiv ist es, wenn jedes Teammitglied versucht, eine gemeinsame Wellenlänge mit dem Kooperationspartner zu erreichen. Da die jeweiligen Kooperationspartner naturgemäß höchst unterschiedlich sein können, ist dies nicht immer einfach. Teammitglieder benötigen in jedem Fall ein großes Repertoire an Verhaltensalternativen.
- Zur gemeinsamen Erreichung der Ziele ist außerdem immer wieder zu prüfen, ob die inhaltlichen Arbeitsschritte und Teillösungen dem Teamziel entsprechen. Daraufhin ist zu überprüfen, ob die Art der Zusammenarbeit (Rollen- und Aufgabenverteilung, Teamklima, Machtverteilung) und die Art des Vorgehens (Methodik) zielführend sind.
- Außerdem sollte jedes Teammitglied die Wirkung, die es beim jeweiligen Gegenüber erzeugt, zur Kenntnis nehmen und als Spiegelung des eigenen Verhaltens betrachten. Dies erfordert mitunter den Mut, eingefahrene Gleise zu verlassen, und die Bereitschaft, neue Verhaltensweisen zu erlernen. Solche Anstrengungen werden aber sicher belohnt, weil sich jedes Mal eine neue Gelegenheit bietet, die eigene Persönlichkeit weiterzuentwickeln.



Beachten Sie:

Eine wichtige Aufgabe der Teamleitung ist es, die **Teamentwicklung hinsichtlich der zu erreichenden Ziele zu steuern**. Weil die Teamarbeit zeitlich begrenzt ist, muss schnell eine funktionierende Arbeitsbasis geschaffen werden. Der IT-Leitung obliegt es, dazu in moderierender Weise das Team zu formen, Teamregeln zu vereinbaren und zu überwachen sowie die Verantwortlichkeiten zu regeln.

6.8.2 Teamkultur aufbauen und zielorientiert weiterentwickeln

Die Erfahrungen der Praxis zeigen: Die Unternehmenskultur bestimmt sehr stark auch den sozialen Orientierungsrahmen, den jedes Teammitglied entwickelt. Dennoch kann und sollte eine spezifische Teamkultur aufgebaut und gefördert werden.

Ein entscheidender Erfolgsfaktor von Teams ist die Zielorientierung. Ein Team kann nur dann eine optimale Leistung erbringen, wenn es eine gemeinsame Richtung einschlägt. Das „Wir“-Gefühl – der Teamgeist – muss immer an erster Stelle stehen.

Aufgabe der Teamleitung ist es, durch entsprechende Aktivitäten den Wirkungsgrad eines Teams positiv zu beeinflussen. Als wichtige **Orientierungen** werden heutzutage angesehen:



- Geben Sie möglichst strategische Richtlinien vor, keine taktischen! Jedes Team sollte eine gewisse „Mission“ haben.
- Richten Sie das Team auf die gemeinsamen Ziele aus!
- Die Teamleitung sollte über Charisma verfügen.
- Bringen Sie Vielfalt ins Team!
- Verhelfen Sie dem Team zu Erfolgen!
- Stärken Sie das Elitegefühl, und machen Sie Qualität zum Kult! Nützlich ist dabei ein sportlicher Teamgeist und das Herausstellen der „Einzigartigkeit“ der Aufgabe.
- Nehmen Sie möglichst geringe Veränderungen in der Teamzusammensetzung vor (nach dem Grundsatz „never change a winning team“).

In einem Team sind Menschen mit persönlichen Zielen für die Erfüllung einer gemeinsamen Aufgabe beschäftigt. Nur wenn es gelingt, die Mitarbeiter auf das gemeinsame Ziel auszurichten und an einem Strick ziehen zu lassen, kann das Team Höchstleistungen vollbringen.

Ein wichtiges Element einer modernen Teamkultur ist ausreichendes **Vertrauen** untereinander. Vertrauen ist die Basis für persönliche Kompetenz und beruflichen Erfolg. Eine gute Portion Vertrauen und Zuversicht fördert die Harmonie im Team.

Eine entscheidende Rolle spielt das Vertrauensverhältnis sowohl bei der Teamleitung-Team-Beziehung als auch bei den Beziehungen innerhalb des Teams. Jeder muss sich auf den anderen blind verlassen können! Einige wichtige Grundsätze für den **Aufbau und die Aufrechterhaltung von Vertrauen** zeigt die folgende Checkliste.



Checkliste Aufbau und Aufrechterhalten von Vertrauen

- Vertrauen entsteht durch die erfolgreiche Wahrnehmung von Verantwortung.
- Halten Sie Ihr Wort, wenn Sie anderen etwas versprechen.
- Achten Sie darauf, dass Sie Ihre Meinung immer ehrlich und offen äußern. Andere Menschen merken dann schnell, dass man Ihnen vertrauen kann.
- Achten Sie darauf, dass Sie zu Terminen (Teamsitzungen) und Verabredungen immer pünktlich erscheinen. Pünktlichkeit erzeugt bei manchen Menschen Vertrauen!
- Räumen Sie Ihrem Team administrative und organisatorische Hürden aus dem Weg. Teams kann man zeitweise völlig autonom arbeiten lassen bzw. in die Isolation „verbannen“ (Hotel, abgelegenes Büro, Ferienhaus).
- Arbeiten Sie an einer positiven Ausstrahlung, die auf Vertrauen gebaut ist.
- Akzeptieren Sie andere Menschen so, wie sie sind. Versuchen Sie nicht, sie zu ändern. Wenn Sie Vertrauen schaffen wollen, müssen Sie selbst dem anderen ebenfalls vertrauen können. Vertrauen ist die Grundvoraussetzung für ein motivierendes menschliches Miteinander.
- Achten Sie auf Ihre Wortwahl. Die richtige Kommunikation ist die „Brücke von Mensch zu Mensch“ und schafft gegenseitiges Vertrauen.

- Trauen Sie anderen Menschen mehr Verantwortung zu. Sie fördern auf diese Weise den harmonischen Umgang miteinander und schaffen gleichzeitig eine Atmosphäre des Vertrauens.
- Schieben Sie nie einen Fehler auf andere. Wer Fehler begeht, sollte diese auch zugeben. Anderenfalls merken Sie schnell, dass andere Ihnen misstrauen!



Beachten Sie:

Im Rahmen der Globalisierung nimmt die Zahl der internationalen Aktivitäten immer mehr zu. International orientierte Teams setzen beim Teamleader ein besonderes Know-how voraus. Dies betrifft insbesondere die Teamarbeit, da nun weitere Spielregeln überlegt werden müssen, um Mitarbeiter aus den verschiedenen Nationen und Kulturen in das Vorhaben einzubeziehen und zu einem harmonischen Team zu formen.



Das Wichtigste – zusammengefasst

- **Beachten Sie, dass IT-Organisation wesentlich auf das Schaffen geeigneter Prozesse und Strukturen ausgerichtet ist!**

Organisation kann grundsätzlich als das ganzheitliche Gestalten von Beziehungen zwischen Aufgaben, Menschen, Sachmitteln und Informationen eingeordnet werden. Dabei kommt es vor allem darauf an, die IT-Prozesse optimiert auszurichten und zu „leben“ sowie entsprechend abgestimmte Strukturen zu etablieren (Abteilungen, Gruppen, Stellen, Rollen).

- **Outsourcing von IT-Leistungen ist mittlerweile ein wesentliches Entscheidungsfeld für die Gestaltung einer zukunftsorientierten IT-Organisation!**

Dabei gilt es zu beachten, dass nur nach vorheriger gezielter Analyse und ganzheitlicher Bewertung aufgrund ausgewählter Kriterien eine Verlagerung von IT-Aufgaben, IT-Ressourcen bzw. IT-Prozessen erfolgt.

- **Demonstrieren Sie einen adäquaten Führungsstil, und setzen Sie Führungsinstrumente gezielt ein!**

Beachten Sie, dass es keinen generell richtigen Führungsstil gibt, sondern nur einen geeigneten, situationsadäquaten. Nur so kann eine „richtige“ Behandlung aller Mitarbeiterinnen und Mitarbeiter gewährleistet werden. Wichtige Führungsinstrumente sind Zielvereinbarungen, systematische Mitarbeitergespräche und erfolgreiche Teammeetings!

- **Notwendig für eine erfolgreiche Führung ist eine professionelle Organisation und Gestaltung der Arbeit im und mit dem Team.**

Teamentwicklung kann als Prozess angesehen werden, der mehrere Phasen umfasst: Forming, Storming, Norming, Performing, Ending. Das IT-Management sollte diese Phasen kennen und in der Lage sein, einzuschätzen, welche Maßnahmen zu bestimmten Zeitpunkten hilfreich sind, um erfolgreiche Teamarbeit und qualitativ hochwertige Ergebnisse der IT-Teams zu gewährleisten.

- **Aufgabe des IT-Managements ist es, eine förderliche Teamkultur aufzubauen und durch entsprechende Maßnahmen den Wirkungsgrad der Teams zu erhöhen.**

Ein positives Innovationsklima im IT-Team ist erreichbar durch eine klare Zielorientierung und klare Kommunikationsstrukturen.

- **Schaffen Sie optimale Voraussetzungen für ein motiviertes Arbeitsteam!**

Eine wichtige Quelle für den Arbeitserfolg sind die Mitglieder der IT-Teams und ihre Motivation. Je größer die Motivation, desto größer auch die Leistungsfähigkeit und desto besser die Ergebnisse.

■ 6.9 Literatur

- [HBR04] *Hodel, M., Berger, A., Risi, P.*: Outsourcing realisieren. Vieweg, Wiesbaden 2004
- [Ga05] *Gadatsch, A.*: IT-Controlling realisieren. Vieweg Verlag, Wiesbaden 2005
- [GM05] *Gadatsch, A.; Mayer, E.*: Masterkurs IT-Controlling. 2. Aufl., Vieweg, Wiesbaden 2005
- [GaTi06] *Gadatsch, A.; Tiemeyer, E. (Hrsg.)*: Betriebswirtschaft für Informatiker und IT-Experten, Elsevier-Verlag, Heidelberg 2006
- [Hu07] *Hungenberg, Harald; Wulf, Torsten*: Grundlagen der Unternehmensführung. Springer Verlag, Berlin; 3. Auflage 2007
- [Pa03] *Payr, Chr.*: IT-Organisation in KMU. Josef Eul Verlag GmbH, Köln 2003
- [So02] *Soebbing, T.*: Handbuch des IT-Outsourcing. Mitp, Bonn 2002
- [Ti96] *Tiemeyer, E. (unter Mitarbeit von R. Chrobok)*: OrgTools. AfürO-Softwareführer für die Organisationsarbeit. Band 1: Geschäftsprozeßorganisation. Schäffer-Poeschel, Stuttgart 1997
- [Ti05a] *Tiemeyer, E.*: IT-Servicemanagement kompakt. Elsevier/Spektrum Akademischer Verlag, Heidelberg 2005
- [Ti05b] *Tiemeyer, E.*: IT-Controlling kompakt. Elsevier/Spektrum Akademischer Verlag, Heidelberg 2005
- [Ti08] *Tiemeyer, E.*: IT-Projekte erfolgreich managen. Zeit, Kosten und Ziele im Griff. rauscher.Verlag. Haag i. Obb. 2008



Fragen, die in diesem Kapitel beantwortet werden:

- Wie lässt sich IT-Controlling im Rahmen des IT-Managements einordnen, und wie kann eine Positionierung in der Unternehmenspraxis erfolgen?
- Welche Möglichkeiten zur organisatorischen Einbindung des IT-Controllings in einer IT-Organisation bzw. einem Unternehmen gibt es?
- Welche Ziele werden mit der Einführung und Optimierung von IT-Controlling verfolgt?
- Welche Kernaufgaben des IT-Controllings sind zu unterscheiden?
- Wie hängen der Lebenszyklus von Informationssystemen und das IT-Controlling zusammen?
- Welche Methoden, Instrumente und Werkzeuge zur Unterstützung des IT-Controllings stehen zur Verfügung und haben sich in der Praxis bewährt?

■ 7.1 Begriff des IT-Controllings und konzeptionelle Aspekte

Mit dem sich wandelnden Verständnis der Rolle der Informationstechnologie (IT) in Unternehmen und Verwaltung hat sich auch das Verständnis bezüglich der Funktion des Controllings von IT und Informationssystemen (IS) verändert. Standen früher die von der IT verursachten Kosten im Mittelpunkt, so verschiebt sich der Fokus des IT-Controllings zunehmend auf die Darstellung von Leistungen, Wertbeiträge und Nutzen der IT (value management). Die Darstellung des IT-Controllings in diesem Kapitel folgt weitgehend den Darstellungen bei [AuKr99; Kü05; KeMüSc07; Kr10].

Wichtige Aufgaben des IT-Controllings bestehen darin, das Informationsmanagement (IM) einer Organisation zu koordinieren und das Management bezüglich der Effektivität und Effizienz der IT-Aktivitäten zu informieren, um gegebenenfalls rechtzeitig steuernd eingreifen zu können.

Ziele des Controllings umfassen daher Wirtschaftlichkeit, Effizienz und Effektivität von Planung, Steuerung und Kontrolle aller IT-Prozesse, deren Ressourcen und der Infrastruktur [Kr10 unter Verwendung von Kr90]

Die Beschäftigung mit IT-Controlling führt zu einer wirtschaftlichen Betrachtung der Resource Information. In Literatur und Praxis existieren diverse Controllingkonzeptionen, die je nach Einsatzziel verschiedene inhaltliche Schwerpunkte setzen. Im angloamerikanischen Raum wird der Begriff „Controlling“ nicht gerade häufig verwendet; er wird vielmehr durch die mit dem Controlling verbundenen inhaltlichen Fragestellungen ersetzt. Unterschieden wird zwischen IT/ IS (Information System) (investment) evaluation, IT/ IS (performance) measurement, measurement of IT/ IS costs and benefits oder IT/ business alignment [Sc06].

7.1.1 Funktionsbegriff und Institutionenbegriff

Hinsichtlich der begrifflichen Einordnung von IT-Controlling findet sich entweder die Positionierung als Funktionsbegriff oder als Institutionenbegriff.

Bei der Verwendung als **Institutionenbegriff** wird das IT-Controlling als Querschnittsfunktion im Unternehmen zur Unterstützung des organisationsweiten Informationsmanagements verstanden, weshalb Schnittstellen mit dem Linienmanagement sowie der Controlling-Abteilung benötigt werden. Da diese unternehmensinterne Stellung äquivalent zur Stellung anderer Controllingbereiche ist, kann auch das IT-Controlling als Stabstelle, Parallelorganisation oder als Kombination dieser Formen in das Unternehmen integriert werden [Kr10].

Legt man den **Funktionsbegriff** zugrunde, kann Controlling nach Vöhringer [Vö04] in drei Gestaltungsrichtungen unterschieden werden:

- Gewinnzielorientierung,
- Berichtswesen- bzw. Kennzahlenorientierung und
- Koordinationsorientierung.

Die gewinnzielorientierte Controlling-Konzeption ist auf die Gewährleistung der Gewinnerreichung ausgerichtet. Es werden überwiegend quantitative Kennzahlen zur Bewertung des Erfolgs eingesetzt.

Die berichtswesen- bzw. kennzahlenorientierte Konzeption konzentriert sich auf die Führungsunterstützung durch eine erhöhte Entscheidungsqualität. Diese soll durch die verbesserte Koordination der Beschaffung und Verarbeitung von Informationen gewährleistet werden. Es werden vorwiegend Informationen aus dem Rechnungs- und Berichtswesen verwendet.

Die koordinationsorientierte Controlling-Konzeption definiert die Sicherstellung von Koordinations-, Reaktions- und Anpassungsfähigkeit der Führung als Zweck des Controllings. Kernaufgabe des Controllings ist es demnach, die Systeme der Planung und Kontrolle sowie der Informationsversorgung zu koordinieren und zu steuern.

Die koordinationsorientierte Konzeption betrachtet das IT-Controlling als eigenständiges Subsystem der Führung und grenzt sich unter dem Gesichtspunkt des Institutionenbegriffs von den anderen Konzeptionen ab [Vö04]. [Vö04] beschreibt die Koordination von Führungssystemen als zentrale Funktion des IT-Controllings. Diese umfasst sowohl die Koordination innerhalb einzelner Teilsysteme als auch die Koordination zwischen unterschiedlichen Teilsystemen.

Des Weiteren kann die Koordinationsfunktion in Anlehnung an [Vö04] nach systembildender und systemkoppelter Koordination abgegrenzt werden. Die systembildende Koordination umfasst die Errichtung von Planungs-, Kontroll- und Informationssystemen sowie die Bildung von Organen zur Gewährleistung der Koordination und zielt auf die Abstimmung von Aufgaben ab. Die systemkoppelnde Koordination dient zur Problemlösung innerhalb existierender Systeme [Vö04].

Durch die gestiegene Bedeutung der Bewertung von Wertbeitrag, Leistungen und Nutzen der IT ist die koordinationsorientierte Konzeption zu einer vorherrschenden Stellung gelangt. Sie soll daher in der folgenden Betrachtung im Zentrum stehen.

Die Koordinationsfunktion umfasst im Sinne der unternehmensweiten Ziele den Lebenszyklus der Informationssysteme, der IT-Infrastruktur sowie den Informationseinsatz [Kr10]. Die Koordinationsfunktion dient neben der Versorgung des Unternehmens mit einheitlichen Methoden zur Informationsbeschaffung auch der Bereitstellung computergestützter Werkzeuge zur Verwaltung von Geschäftsprozessen in den Geschäftsbereichen [Kr10]. Zusammenfassend lässt sich IT-Controlling vor dem Hintergrund des koordinationsorientierten Ansatzes wie folgt definieren:



„IT-Controlling ist das Controlling der IT im Unternehmen. Das IT-Controlling soll die Formalziele Effizienz und Effektivität sowie die Sachziele Qualität, Funktionalität und Termineinhaltung der Informationsverarbeitung sicherstellen. Es wird hierbei nicht nur als reine Überwachungsfunktion verstanden, sondern hat eine Koordinationsfunktion für das gesamte Informationsmanagement.“ [Kr10]

7.1.2 Organisatorische Einbindung des IT-Controllings

Aus der Definition des IT-Controllingbegriffs ergibt sich, dass IT-Controlling und IT-Management Hand in Hand zusammenarbeiten müssen. Häufig wird jedoch nicht ausreichend zwischen originären Managementaufgaben und den Aufgaben des Controllings unterschieden. Die Folge sind Missverständnisse und falsche Verantwortlichkeiten.

7.1.2.1 Abgrenzung IT-Controlling und Management

Während das Management *ergebnis*verantwortlich ist (etwa in Form eines Cost- oder Profit-Centers), ist das IT-Controlling *transparenz*verantwortlich und bietet dem Management einen Informations-, Entscheidungs- und Koordinationsservice (vgl. [Kü06]). Im Rahmen dieser Führungsunterstützung übernimmt das IT-Controlling Entlastungsaufgaben, Ergänzungsaufgaben und Begrenzungsaufgaben [We04].

Entlastungsaufgaben sind nach [We04] Aufgaben, die theoretisch vom Management selbst wahrgenommen werden könnten (z. B. Berichtswesen, Abweichungsanalysen), die aber durch Delegation und Spezialisierung des Controllings von diesem besser, schneller und weniger aufwendig erfüllt werden können. Bei diesen Aufgaben ist das IT-Controlling dem Management unmittelbar nützlich.

Im Bereich der Ergänzungsaufgaben ist diese unmittelbare Nützlichkeit nicht gegeben [We04]: Das Management kann solche Aufgaben nicht mehr vollständig hinsichtlich Umfang, Inhalt und Ergebnis einschätzen – doch erkennt es die Wichtigkeit der Aufgabe und fordert einen zweiten Blick auf die eigene Einschätzung. Dies ist zum Beispiel der Fall, wenn eine höhere Führungsebene die Überprüfung einer Entscheidung durch das mittlere Management veranlasst.

Begrenzungsaufgaben stellen einen Sonderfall der Ergänzungsaufgaben dar – hier liegt ein „Wollensproblem“ seitens des Managers vor, beispielsweise das Verlassen eines von einer höheren Instanz gesetzten Rahmens [We04].

Darüber hinaus dient das Controlling der Rationalitätssicherung der Führung, beziehungsweise der Sicherung der Führungsqualität selbst: Es gibt in diesem Fall einen Rahmen zur Sicherung von Effizienz (richtige Mittel) und Effektivität (richtiger Zweck) des Managements vor [We04].

7.1.2.2 Zusammenhang zwischen IT-Controlling und IT-Governance

IT-Governanceformen lassen sich in Abhängigkeit von dem Ort, an dem die IT-Entscheidungen getroffen werden, und anhand der jeweils zugrunde liegenden Strukturen in sechs Entscheidungstypen von zentraler Entscheidung bis hin zu dezentraler Entscheidung klassifizieren [WeRo04]. Diese Entscheidungstypen sind:

- *Geschäftsmonarchie*: Entscheidungen durch ein Mitglied der Geschäftsleitung oder eine Gruppe von Geschäftsleitern;
- *IT-Monarchie*: Entscheidung durch den IT-Leiter oder eine Gruppe von IT-Verantwortlichen;
- *Föderalismus*: Entscheidung durch Führungskräfte der mittleren Führungsebenen aus allen operativen Geschäftsbereichen; dies berücksichtigt auch die Einbindung der IT-Leitung;
- *IT-Duopol*: Entscheidung durch IT-Leitung und eine Gruppe aus Mitgliedern der Geschäftsleitung;
- *Feudalismus*: Entscheidungen werden jeweils selbstständig auf Fachbereichsebene getroffen;
- *Anarchie*: Entscheidungsfindung selbstständig durch Nutzer oder eine Gruppe von Nutzern.

Diese Klassifikation ist nicht nur auf der Ebene der Entscheidungsfindung relevant, vielmehr kann die Klassifikation auch Auskunft über die Herkunft von Input für die Entscheidungsfinder geben [WeRo05].

Je nach Governance-Struktur entstehen unterschiedliche Anforderungen an die IT und folglich an das IT-Controlling (vgl. auch Kapitel 12 des Handbuches, das einen gesonderten Beitrag zu IT-Governance enthält).

7.1.2.3 Einbindung des IT-Controllings in die Organisation¹

In Abhängigkeit von der vorliegenden IT-Governance gibt es unterschiedliche Möglichkeiten der Einbettung des IT-Controllings in die Organisation, die sich mit folgenden Fragestellungen beschreiben lassen (vgl. [Kü05]):

¹ Quelle: Überwiegend [Kü05]

- Welcher Abteilung soll das IT-Controlling organisatorisch zugeordnet werden?
- Ist es sinnvoll, eine eigenständige IT-Controlling-Abteilung zu errichten, und wenn ja, wie soll sie personell besetzt werden?
- Wo soll die IT-Controlling-Abteilung im Unternehmen angesiedelt werden?
- Wie sollen IT-Controlling-Aufgaben aufgegliedert werden?

IT-Controlling sollte nahe bei den Managemententscheidern im Sinne der IT-Governance verortet werden. Folglich bietet es sich häufig an, das Controlling der IT-Leistungsverwendung dezentral in den Fachbereichen anzusiedeln, während organisationsweite Fragestellungen der IT-Leistungserstellung zentral in der IT-Organisation gesteuert werden sollten [Kü05].

So lässt sich zwar eine bedarfsgerechte Ausgestaltung des IT-Controllings erreichen, jedoch entsteht im Vergleich mit einer rein zentralen Organisation ein erhöhter Koordinationsaufwand, und Synergieeffekte können nur schwer genutzt werden.

Mögliche unterschiedliche Positionierungen des IT-Controllings in der Organisation stellt Abbildung 7.1 dar.

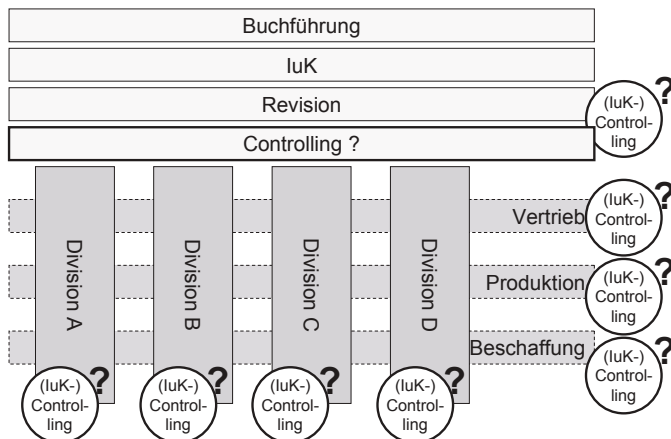


ABBILDUNG 7.1
Organisatorische Einbettung
des IT-Controllings

Wird das IT-Controlling als Querschnittsfunktion zur Unterstützung des unternehmensweiten Informationsmanagements aufgefasst, so sind entsprechende Schnittstellen mit dem Linienmanagement sowie der Controlling-Abteilung zu bilden [KrBu94]. Da diese unternehmensinterne Stellung äquivalent zur Stellung anderer Controlling-Bereiche ist, kann auch das IT-Controlling als Stabsstelle, Parallelorganisation oder als Kombination dieser Formen in das Unternehmen integriert werden. Jedoch muss man auf Grund der Querschnittsfunktion bei der Umsetzung festlegen, welche Entscheidungsbefugnisse für diesen Bereich gegeben sind und über welche Qualifikation der Mitarbeiter verfügen muss [KrBu94].

Die Entscheidung für die Errichtung eines eigenständigen IT-Controllings hängt im Wesentlichen vom Umfang und der Häufigkeit der IT-Nutzung, der strategischen Bedeutung der IT, der Art der IT-Leistungserstellung, der Unternehmensgröße sowie von existierenden Controlling-Konzepten ab [Kü05].

■ 7.2 Ziele, Objekte und Aufgaben des IT-Controllings



Startpunkt der Entwicklung eines IT-Controllingkonzeptes sind Vereinbarungen zu dessen Zielen. Die Ziele definieren die Objekte, mit denen sich das IT-Controlling beschäftigt. Aus den Objekten können dann konkrete Herausforderungen und Aufgabenfelder abgeleitet werden.

7.2.1 Ziele und Objekte für ein IT-Controlling

Die Ziele von IT-Controlling-Konzepten müssen mit den Zielen des unternehmensweiten Controllings abgestimmt werden. Dabei kann [Kr10] zwischen Formal- und Sachzielen unterscheiden werden:

- Zu den Formalzielen gehören die Effizienz und Effektivität der Planung, Steuerung und Kontrolle aller Informationsverarbeitungsprozesse, deren Ressourcen und der Infrastruktur im Unternehmen.
- Zu den Sachzielen zählen Qualität, Funktionalität und Termineinhaltung.

Ausgehend von den Aufgaben des Informationsmanagements, den Zielen allgemeiner Controllingkonzeptionen und des IT-Controllings, werden nachfolgend spezifische Controllingobjekte herausgearbeitet und in Teilbereiche untergliedert. Diese Aufteilung orientiert sich am Lebenszyklus der Informationssysteme [Kr10].



Grundsätzlich ist zwischen strategischem IT-Controlling und operativem IT-Controlling zu unterscheiden: Das strategische Controlling unterstützt die Koordinierung der IT-Strategieplanung und misst die IT-Strategieerreichung. Gegebenenfalls sind Abweichungsanalysen zu erstellen. Das operative Controlling koordiniert die Einzelplanungen von Ressourcen, Leistungen, Projekten und Maßnahmen. Es dient der systematischen Messung des Ist-Zustands im IT-Betrieb und bereitet die Informationen für die Entscheidungsträger auf.

Strategisches IT-Controlling

Das strategische IT-Controlling befasst sich nach [Kr10] mit der Integration der strategischen Ziele der Informationswirtschaft in die strategische Planung des Unternehmens. Auf diese Weise soll die Effektivität des Informationsmanagements gewährleistet werden. Die Wirtschaftlichkeit und die Versorgung des Unternehmens mit geeigneten Informationen stehen im Vordergrund. Weitere Ziele bzw. Aufgaben des strategischen IT-Controllings sind nach [Kr10] in der Qualitätssicherung der gelieferten Informationen, der Instandhaltung verwendeter Programme zur Gewährleistung der bereitgestellten Funktionalität sowie der Einhaltung von Terminen zu sehen. Die Strategie des Unternehmens und deren Gesamtziele sollen unterstützt

werden. Um die interne Akzeptanz des Controllings nicht zu gefährden, muss das Verhältnis von Aufwand und Nutzen im Auge behalten werden [Kr10]. Aus dieser Zielsetzung lassen sich die folgenden zu unterstützenden Controllingobjekte ableiten:

- IT-Strategieentwicklung;
- Planung, Kontrolle und Steuerung der IT-Architektur als Basis für die langfristige strategische Ausrichtung der IT-Landschaft an der Gesamtstrategie (vgl. dazu ausführlich Kapitel 3 dieses Handbuches);
- Planung und Priorisierung von (mittel- bis langfristigen) IT-Vorhaben (Grundlage für eine langfristige strategische Ausrichtung an den Geschäftsprozessen).

Operatives IT-Controlling

Die Ziele des operativen IT-Controllings werden aus dem Leistungsspektrum und den Leistungsprozessen der IT abgeleitet. Die Anwender der Fachbereiche nehmen Leistungen ab, die in Form sogenannter IT-Services seitens der IT (der IT-Abteilung bzw. des IT-Dienstleisters) angeboten werden. Die Leistungsbereiche entsprechen auch den Controllingobjekten. Die Controllingbereiche des operativen IT-Controllings resultieren aus dem Lebenszyklus der Informationssysteme und umfassen folgende Objekte [Kr10]:

- Portfolio (IT-Masterplan)
- IT-Projekte,
- IT-Produkte,
- IT-Infrastrukturen und deren Komponenten sowie
- IT-Prozesse.

7.2.2 Aufgaben im IT-Controlling

Analog zu den strategischen und operativen Zielen und Objekten des IT-Controllings kann zwischen strategischen und operativen Aufgaben für das IT-Controlling unterschieden werden.

Strategische Aufgaben

Die strategischen IT-Controllingaufgaben umfassen die Festlegung geeigneter Maßnahmen und Projekte, die die Organisation bei der Zielerreichung optimal unterstützt. Letztlich geht es auch um die Unterstützung der IT-Strategieentwicklung. Diese beschäftigt sich mit der Formulierung eines definierten Soll-Zustands und der Identifizierung des daraus abzuleitenden Handlungsbedarfs sowie der Ermittlung von Handlungsoptionen für den IT-Bereich [KrBuRe00]. Ein wesentlicher Bestandteil der IT-Strategie ist die langfristige Ausrichtung der IT an den Geschäftsprozessen. Sie definiert die Ist- und Soll-Struktur der IT-Landschaft und gibt die zukünftige Entwicklung der IT-Controllingobjekte vor (vgl. Kapitel 2 dieses Handbuches).

Mit der langfristigen Ausrichtung der IT an den Geschäftsprozessen liefert das strategische IT-Controlling den Entscheidungsträgern grundlegende Informationen zur Weiterentwicklung der IT-Architektur. Zur langfristigen Ausrichtung der IT an den Fachprozessen wird die Planung von IT-Vorhaben und IT-Projekten benötigt. Durch die übergeordnete Betrachtung aller Projekte, die Berücksichtigung des Gesamtnutzens beziehungsweise des Gesamtrisikos

sowie die Analyse auf eventuelle Abhängigkeiten kann die strategische Relevanz und Effektivität des IT-Portfolios für die Gesamtorganisation sichergestellt werden [KrBuRe00].

Operative Aufgaben

Die operativen Aufgaben des IT-Controllings stellen eine Kombination aus den Aufgaben des Informationsmanagements und den Aufgaben des Controllings dar [Kr10]: Das Controlling der Anwendungssysteme kann in Anlehnung an den Lebenszyklus von Informationssystemen in die Objektbereiche

- Portfolio-Controlling,
- Projekt-Controlling,
- Produkt-Controlling und
- Infrastruktur-Controlling

unterteilt werden. Diese Unterteilung ist in Abbildung 7.2 dargestellt.

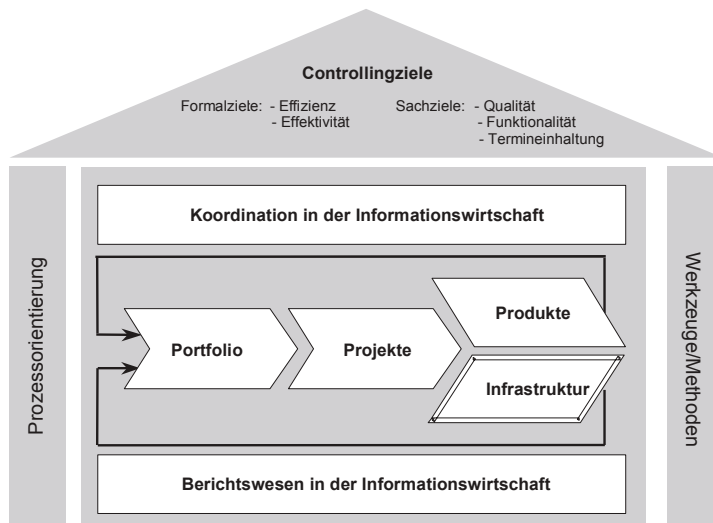


ABBILDUNG 7.2
IT-Controlling im
Unternehmen [Kr10]

Um das Controlling als Unterstützung bei der Entscheidungsfindung für das Management nutzen zu können, ist zusätzlich ein Berichtswesen notwendig, in dem adäquate Kenngrößen den IT-Controlling-Prozess zusammenfassend darstellen und somit zur Steuerung und Kontrolle des Informationsmanagements eingesetzt werden können [KrBu94]. Diese Teilbereiche werden im Folgenden näher erläutert.



Beachten Sie:

Orientierungspunkte im IT-Controlling sind Prozessorientierung (Geschäftsprozess-Unterstützung) sowie Werkzeuge und Methoden. Häufig angewandte Methoden sind beispielsweise Kennzahlensysteme und der Vergleich von Kennzahlen durch Benchmarking. Die Hauptaufgabe des IT-Controllings ist die Koordination der Informationswirtschaft, die sich als Koordination der Teilbereiche und Abstimmung einzelner Aktivitäten mit den Zielen versteht.

7.2.2.1 Portfolio-Controlling

Die Portfolio-Analyse dient zur Unterstützung des Informationsmanagements bei der strategischen Planung von IT-Projekten durch passende Verfahren der Planung und entsprechende Instrumente (vgl. dazu ausführlich Kapitel 5 in diesem Handbuch). Durch ein Portfolio-Controlling als Teil des IT-Controllings sollen die Beurteilung und Selektion von zukünftigen, geplanten oder existierenden Projekten erleichtert und die Transparenz bei laufenden IT-Projekten verbessert werden. Hierfür werden oft Projektdatenbanken erstellt und gepflegt sowie wichtige Eckdaten wie der Gesamtnutzen und das Gesamtrisiko der jeweiligen IT-Projekte anhand geeigneter Größen ermittelt und dargestellt [KrBuRe00](vgl. Abbildung 7.3).

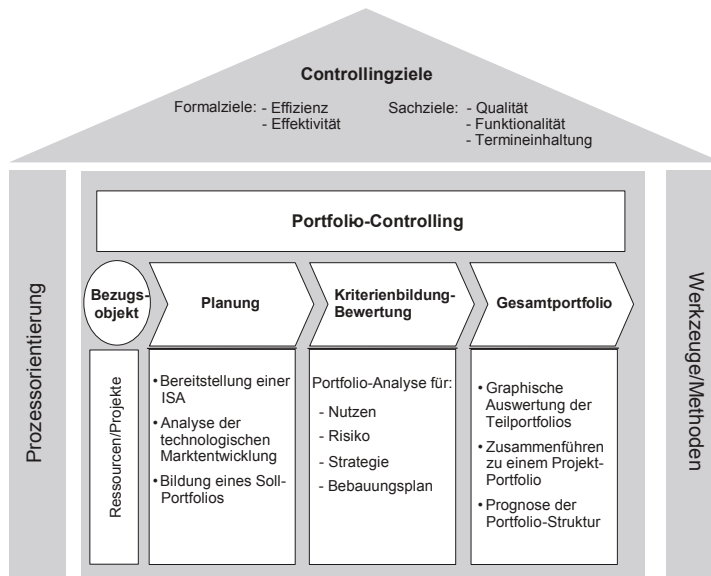


ABBILDUNG 7.3
Portfolio-Controlling
[Kr10]



Das Portfolio-Controlling muss nach [Kr10] strategische Relevanz und Wirtschaftlichkeit aller Anwendungen sicherstellen. Seine wichtigste Funktion ist demnach die Unterstützung des Informationsmanagements mit Planungsverfahren und Instrumenten für die Bewertung und Auswahl von Projekten. Als ein geeignetes Instrument zur Unterstützung des Portfolio-Controllings wird die Portfolio-Analyse angesehen.

7.2.2.2 Projekt-Controlling²

Kernaufgabe im Projekt-Controlling ist die Unterstützung des Projektmanagements bei der Durchführung der IT-Projekte: Es müssen geeignete Methoden ausgewählt, passende Instrumente zur Verfügung gestellt und notwendige Informationen bereitgestellt werden. Betrachtet man ein Projekt als die Erfüllung einer Aufgabe in einem festgelegten Zeitraum mit limitierten Ressourcen innerhalb einer bestimmten Organisation, so kann Projekt-Controlling als „integriertes System zur Planung, Steuerung und Kontrolle von Kosten, Terminen und Leistungen eines Projekts“ [Kr10] verstanden werden. Zwar existieren verschiedene Arten von

² Quelle: Überwiegend [Kr10]

Projekten, wie beispielsweise Software-Entwicklungs- oder Wartungsprojekte, doch unterliegen alle Informationssystem-Projekte einem Lebenszyklus. Während dieses Lebenszyklus ist es Aufgabe des Projekt-Controllings, die Durchführung des Projektes mit verschiedenen, der Art des Projektes angemessenen Instrumenten zu unterstützen. Soll der Ablauf des Projekt-Controllings genauer betrachtet werden, so ist eine Orientierung an den Projektphasen sinnvoll. Diese gliedern ein Projekt beispielsweise in folgende Abschnitte: Anforderungsanalyse, Fachspezifikation, IT-Spezifikation, Realisierung, Systemintegration und Einführung [So87].

Weitere Aufgaben des Projekt-Controllings sind die Planung, Steuerung und Kontrolle von Projekten, die Einrichtung einer Erfahrungsdatenbank sowie das Erstellen von Wirtschaftlichkeitsanalysen. Die Ziele für ein Projekt-Controlling lassen sich aus der Projektvorstudie und den im Ideen-Controlling entstandenen Projektzielen entwickeln.

Die Projektplanung stellt einen dynamischen Prozess dar, der sich über die gesamte Projektdauer erstreckt. Dieser Prozess lässt sich in die Teilprozesse Grobplanung und Detailplanung untergliedern: Während der Ablauf der unterschiedlichen Phasen des Software-Entwicklungsprozesses in der Grobplanung definiert wird, beschäftigt sich die Detailplanung mit der aktuellen und der jeweils nachfolgenden Phase. Dieses inkrementelle Vorgehen ist auf Grund der unzureichenden Informationslage am Anfang eines Projektes und des kontinuierlichen Zuwachses an Informationen erforderlich. Bei der Entwicklung von Software beispielsweise sind üblicherweise nicht alle Anforderungen der Benutzer von Anfang an bekannt, weshalb Planänderungen im Projektverlauf notwendig werden. Dies erfordert ein koordiniertes Zusammenspiel von Projekt-Controlling und Projektmanagement, um gemeinsame Ziele zu erreichen.

Als wichtigstes Instrument der Projektplanung gilt die Netzplantechnik, die auf der Graphentheorie basierend neben der Planung auch zur „Steuerung, Kontrolle und Disposition von Terminen, Kapazitäten und Kosten während der Projektabwicklung“ eingesetzt werden kann.

Die Projektsteuerung und Projektkontrolle erfolgt basierend auf der Projektplanung: Diese Teilaufgaben des Projekt-Controllings umfassen die Beratung, Systemvorbereitung und Entscheidungsunterstützung im Projektmanagement. Der Ablauf der Projektsteuerung folgt dem in Abbildung 7.4 beschriebenen Regelkreis, die betrachteten Objekte sind dabei der Projektfortschritt anhand von Meilensteinen, Terminen, Kapazitäten, Projektkosten, Qualität und Wirtschaftlichkeit.

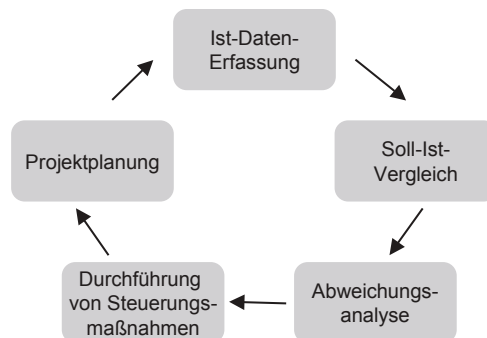


ABBILDUNG 7.4
Kreislauf der Projektsteuerung

Der Projektfortschritt wird anhand von Berichten der Projektmitarbeiter kontrolliert und gesteuert. Der aktuelle Stand des Projektes wird daraufhin durch die Auswertung der Ist-Daten ermittelt und dokumentiert. Außerdem wird die Terminsituation von Arbeitspaketen

überprüft, wobei gerade bei der Entwicklung von Software darauf zu achten ist, dass häufig Anforderungen ohne Beachtung von Qualitätsstandards als erreicht deklariert werden.

Um den Kapazitätsverbrauch festzustellen, werden verschiedene Verfahren zur Messung von Personalkapazitäten und der Rechnernutzung angewendet. Projektkosten können dabei mit Hilfe einer prozessorientierten Projektkalkulation überwacht werden.

Damit das Controlling eine unterstützende Funktion bei der Entscheidungsfindung übernehmen kann, ist die Errichtung einer Erfahrungsdatenbank vor allem bei der Planungsunterstützung des Informationsmanagements erforderlich. Auch das Berichtswesen basiert wesentlich auf Informationen aus dieser Datenbank. Durch die Bereitstellung einheitlicher Qualitätsstandards soll das Controlling die Qualitätssicherung von IT-Projekten gewährleisten. Die Qualitätssicherung muss unter dem Aspekt der Wirtschaftlichkeit stattfinden. Für das gesamte Projekt ist eine rollierende, projektbegleitende Wirtschaftlichkeitsanalyse durchzuführen, die unter anderem bei der nachträglichen Betrachtung von Projekten zur Erhebung von Kennzahlen und der Erweiterung der Erfahrungsdatenbank dient [Kr10] unter Verwendung von [So87].

Weitere Aufgaben des Projektcontrollings sind die Bereitstellung von Informationen für das Projekt Management Office und die Projektleitung, die Generierung von Berichten und die Dokumentation der IT-Projekte auf Basis der Erfahrungsdatenbank. Den kompletten Ablauf für ein Projekt-Controlling stellt Abbildung 7.5 dar.

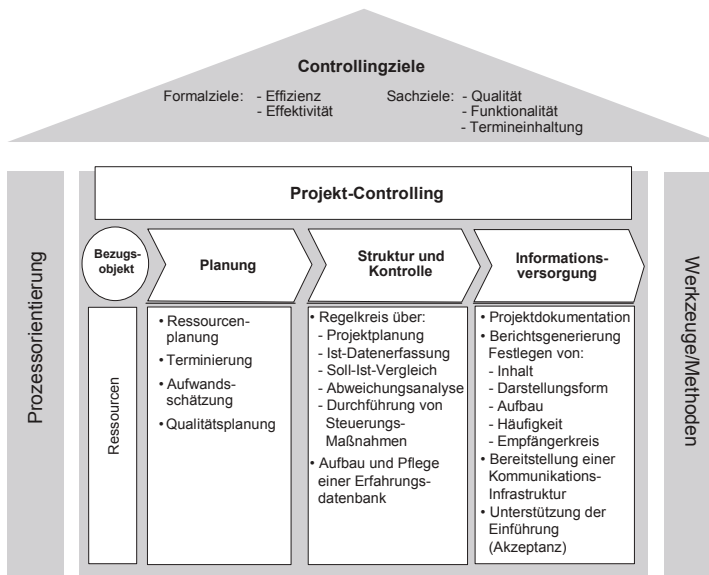


ABBILDUNG 7.5
Projekt-Controlling
[Kr10]



Beim Projekt-Controlling geht es um die Überwachung der Wirtschaftlichkeit, Qualität und Funktionalität einzelner Maßnahmen. Nachdem ein IT-Projekt ausgewählt worden ist, hat das Projekt-Controlling das Management mit den für die Projektrealisierung notwendigen Methoden, Instrumenten und Informationen zu versorgen. Zu den Teilaufgaben zählen dabei die Projektplanung, -steuerung, -kontrolle, der Aufbau einer Erfahrungsdatenbank und die Durchführung von Wirtschaftlichkeitsanalysen.

7.2.2.3 Produkt-Controlling³

Sobald ein Produkt fertiggestellt und eingeführt wurde, ist es Aufgabe des IT-Controllings, die effektive und effiziente Nutzung des Produkts über den gesamten Produktlebenszyklus zu koordinieren. Dabei sind die

- Betreuung,
- Wartung,
- Weiterentwicklung und
- Anpassung an neue Systemumfelder

als Aufgaben des Informationsmanagements zu beachten. Die Unterstützung dieser Prozesse durch das Controlling mit Instrumenten zur Koordination soll unter anderem helfen, die Folgekosten von Projekten gering zu halten. Weil die Kosten für Produkthanpassungen bis zu 80 Prozent der Kosten des gesamten Lebenszyklus betragen, muss das Controlling zur Kontrolle dieser Tätigkeiten passende Methoden und Werkzeuge zur Verfügung stellen. Um die Überwachung der Folgekosten zu ermöglichen, ist es ratsam, das Controlling an der Geschäftsprozessdefinition zu beteiligen, da sich aus den Prozessdefinitionen die notwendigen Tätigkeiten zur Produktmodifikation ableiten lassen.

Durch die Verwendung von Informationen über frühere Systeme aus der Erfahrungsdatenbank können Wartungszeiten verringert und Modifikationsprojekte verbessert werden. Mit Hilfe einer kontinuierlichen Kosten-Nutzen-Analyse kann das Produktmanagement bei der Entscheidungsfindung zur Durchführung von Modifikationsprojekten unterstützt werden. Somit fallen auch Produktmodifikationsprojekte in den Aufgabenbereich des Controllings, weshalb die Budgetierung und Verrechnung von Aufwänden bei bereichsübergreifend eingesetzten Produkten durch Kostenverrechnung stattfinden kann. Des Weiteren gehören die Wirtschaftlichkeitsbetrachtung des Anwendungseinsatzes sowie die Ermittlung der Akzeptanz eines Systems zu den Aufgaben des Produkt-Controllings. Auf dieser Basis müssen Entscheidungen über den Ersatz eines Produkts und dessen Zeitpunkt vorbereitet werden.

Beim Einsatz von Standardsoftware entstehen hohe Kosten für die individuelle Anpassung der Systeme an die unternehmensinternen Anforderungen und Gegebenheiten [AuKr99]. Durch die häufigen Release-Wechsel und den daraus resultierenden Implementierungsaufwand entstehen weitere Aufwendungen. Weil die Wartung und Weiterentwicklung der Standardsoftware größtenteils vom Hersteller übernommen wird, rückt die Planung und Steuerung des Gesamtaufwands und der internen IT-Kapazitäten in den Hintergrund. Durch externe Wartungs- und Serviceverträge erfolgt die Aktualisierung der eingesetzten Produkte zu festgesetzten Konditionen. Folglich steht die Wirtschaftlichkeitsbetrachtung der Systemanpassung an die sich ständig ändernden Bedürfnisse der Benutzer im Vordergrund [AuKr99; Kr10]. Der Produkt-Controllingablauf ist in Abbildung 7.6 zu sehen.

³ Quelle: Überwiegend [Kr10]

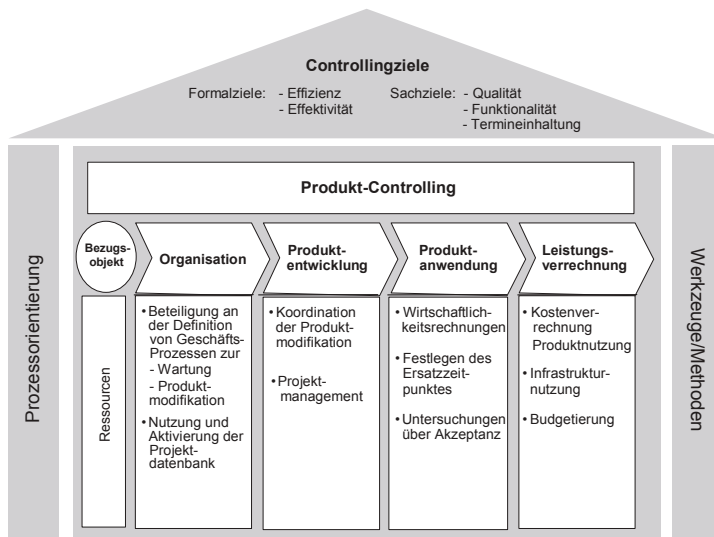


ABBILDUNG 7.6
Produkt-Controlling
[Kr10]



Das Produkt-Controlling hat die effektive und effiziente Nutzung fertiggestellter Produkte (Anwendungen) zum Ziel. Seine Aufgabe ist deshalb, das Produkt über den restlichen Produktlebenszyklus zu begleiten und seine Qualität und Funktionalität zu gewährleisten.

7.2.2.4 Infrastruktur-Controlling⁴

Durch die zunehmende Dezentralisierung von IT-Systemen wird die Steuerung der Gesamtheit aller IT-Systeme und Anwendungen in einem Unternehmen zu einer immer wichtigeren Aufgabe, die das Infrastruktur-Controlling übernimmt [AuKr99]. Zu den zentralen Aufgaben des Infrastruktur-Controllings gehören ([AuKr99]):

- die Mitwirkung bei der Gestaltung von Strukturen,
- die Bereitstellung adäquater Methoden und Werkzeuge zur Umsetzung,
- die Unterstützung bei der Konfigurationsanalyse mit geeigneten Methoden,
- die Gewährleistung einer strukturierten Systemdokumentation und
- die Bereitstellung von Techniken zur zentralen Steuerung und Kontrolle aller Systeme.

Weitere Aufgaben werden in Abbildung 7.7 dargestellt.

⁴ Quelle: [AuKr99]

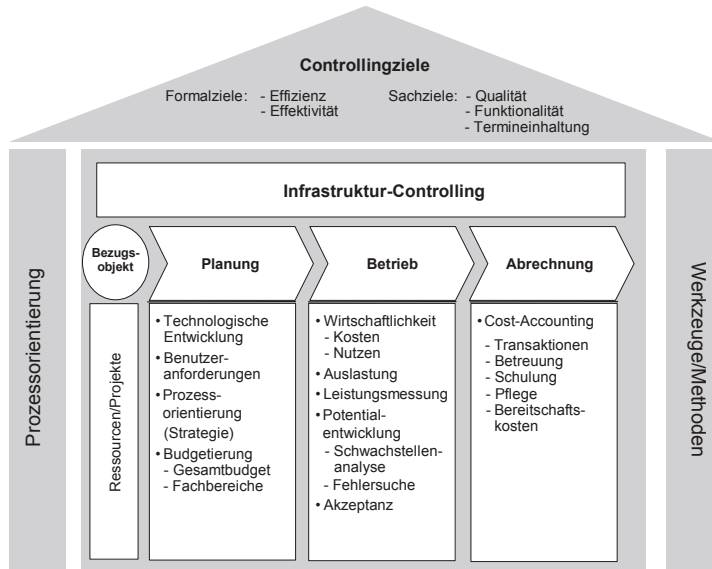


ABBILDUNG 7.7
Controlling der IT-Infrastruktur (nach [Kr05])

 Kernaufgabe des Infrastruktur-Controllings ist es, das Informationsmanagement bei der Gestaltung und Dokumentation eines Regelwerkes zu unterstützen, das alle wesentlichen Bestandteile einer IT-Infrastruktur im Unternehmen beinhaltet.

Abbildung 7.8 zeigt ein Rahmenkonzept, das Bestandteile einer IT-Infrastruktur exemplarisch darstellt. Das Rahmenkonzept bietet Unternehmen eine Strukturvorlage und Orientierungsmöglichkeiten zur bedarfsgerechten Ausgestaltung des eigenen Regelwerkes.

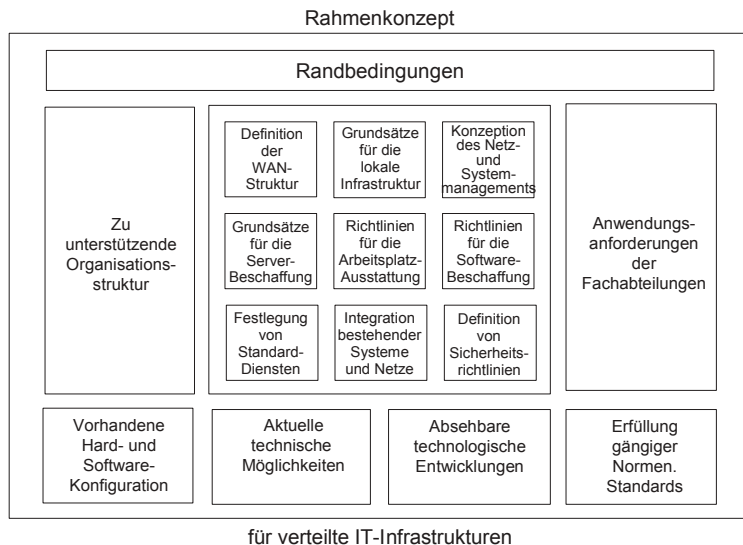


ABBILDUNG 7.8
Rahmenkonzept für verteilte IT-Infrastrukturen [AuKr99]

Die Anpassung des Rahmenkonzepts erfolgt anhand der spezifischen Randbedingungen des Unternehmens, deren Einhaltung das IT-Controlling überwacht [AuKr99]: Das IT-Controlling übernimmt die Dokumentation des angepassten Rahmenkonzeptes und sorgt für dessen unternehmensweite Verfügbarkeit, während für die inhaltliche Konzeption und die erforderlichen Grundsatzentscheidungen das Informationsmanagement zuständig ist. Zu den weiteren Aufgaben des Infrastruktur-Controllings zählen

- die Entscheidungsunterstützung,
- die Koordination und Abstimmung der Regelungsinhalte sowie
- die Aktualisierung und laufende Anpassung des Rahmenkonzeptes an die sich ändernden Anforderungen und technologischen Entwicklungen [AuKr99].

Außerdem müssen die unternehmensinternen Grundsätze und Richtlinien überwacht und kontrolliert werden.

[AuKr99] beschreiben die Ausrichtung der zu fällenden Infrastruktur-Entscheidungen an der strategischen IT-Planung als Ziel des Infrastruktur-Controllings. Hierbei ist auf die Berücksichtigung der Anwendungsarchitektur, des Datenhaltungskonzeptes, der Hardware- und Netzarchitektur, der Anwendungsentwicklung und des Sicherheitskonzeptes bei der Entscheidungsfindung zu achten. Darüber hinaus sind dem Informationsmanagement Informationen über die IT-Infrastruktur wie die Betriebskosten von IT-Systemen, die Verfügbarkeit von Systemen sowie die Verrechnungssätze für IT-Leistungen zur Verfügung zu stellen. Hierdurch kann das Informationsmanagement bei der Entscheidungsfindung unterstützt werden, die häufig durch eine große Zahl an Gestaltungsalternativen und eine hohe Komplexität der Infrastruktur-Entscheidungen geprägt ist.

Das Bestands-Controlling ist eine weitere Aufgabe des Infrastruktur-Controllings, die durch die Vielzahl der Komponenten einer IT-Infrastruktur mit einer hohen Heterogenität und einer starken räumlichen Verteilung notwendig ist. Auch die Verteilung in verschiedenen Netzwerken und die wechselseitige funktionale Abhängigkeit der Soft- und Hardware machen ein Bestands-Controlling unabdingbar. Dabei ist es gerade in stark verteilten IT-Infrastrukturen schwierig, den Überblick über den Bestand zu behalten und die entstehenden Kosten zu kontrollieren, weshalb vom IT-Controlling alle den Bestand betreffenden Informationen, die zur Entscheidungsfindung benötigt werden, dem Informationsmanagement zu liefern sind. Dies sind insbesondere Daten und Auswertungen über den IT-Bestand aus der Anlagenbuchhaltung, die Verwaltung existierender Verträge bezüglich des Kaufs, der Miete beziehungsweise des Leasings von Systemen sowie Lizenzverträge, Wartungs- und Versicherungsverträge. Damit verbunden ist die Anforderung an das Infrastruktur-Controlling, den Einsatz einheitlicher Releasestände zu gewährleisten, Entscheidungen über Releasewechsel vorzubereiten und Informationen über daraus resultierende Folgekosten bereitzustellen.

Durch die starke Delegation von IT-Aufgaben in die Fachabteilungen ergibt sich bei dezentralen Strukturen im Vergleich zu einer zentralen IT-Abteilung eine veränderte Ausgangslage in Bezug auf die Budgetierung [AuKr99]: Das Leistungsangebot, das den Anwendern zur Verfügung steht, ist nicht mehr auf die von der IT-Abteilung angebotenen Leistungen begrenzt, sondern kann durch Inanspruchnahme von unterstützenden Leistungen anderer Bereiche variieren. Außerdem werden Entscheidungen über die Verwendung von Anwendungen, Kommunikationsdiensten und Hardwaresystemen teilweise dezentral getroffen. Das IT-Budget wird auf verschiedene Fachbereiche verteilt und nicht mehr zentral der IT-Abteilung zugeordnet.

Durch die selbstständige Planung der Leistungen und Ressourcen, die in den Fachbereichen bezogen werden, ergibt sich das IT-Budget durch Konsolidierung der Budgets der Fachabteilungen und der Kosten der für die IT-Abteilung bezogenen Leistungen. Durch diese Aufteilung wird der Budgetierungsprozess komplexer und erfordert die Steuerung und Koordination durch das IT-Controlling unter Einbeziehung der Fachbereiche. Gleichzeitig entsteht dadurch aber auch die Chance, die IT-Budgets flexibler zu gestalten und den Fachbereichen die finanziellen Konsequenzen möglicher Infrastrukturalternativen darzulegen. Somit kann der Zusammenhang aus Leistungs- bzw. Ressourcenbeanspruchung und den daraus entstehenden Kosten verdeutlicht und somit die Effizienz der Gestaltung und Planung der IT-Infrastruktur durch die Budgetierung erhöht werden.

Bei der Gestaltung des Kostenverrechnungssystems ist dann auf die Transparenz und Gerechtigkeit der Verteilung zu achten, um eine effiziente und vertrauensvolle Zusammenarbeit der Kostenverantwortlichen und der zentralen IT-Abteilung zu gewährleisten. Eine möglichst gerechte Verteilung der Kosten lässt sich durch die verursachungsgerechte Zurechnung der entstandenen Kosten erreichen. Die in zentralisierten Strukturen rechnerisch nicht mehr zerlegbaren Fixkostenblöcke können in dezentralisierten Systemen direkt dem Verursacher zugeordnet werden, wodurch die Verteilungstransparenz erhöht wird. Bei den Kostenrechnungsverfahren müssen kausale Zusammenhänge so klar wie möglich dargestellt werden, um für die Kostenverursacher nachvollziehbar zu sein, wodurch die Akzeptanz des Verfahrens erhöht wird.

Durch die Anwendung eines nach den oben genannten Kriterien gestalteten Verrechnungssystems können neben Informationen für ein Budgetierungssystem auch Steuerungs- und Koordinationsaufgaben zwischen strategischer und operativer IT-Planung unterstützt werden.



Das Infrastruktur-Controlling beschäftigt sich mit der Steuerung der Verfügbarkeit und der Weiterentwicklung geeigneter Infrastruktur, wobei die Infrastruktur als Plattform für die Produkte verstanden wird. Zu den Aufgaben des Controllings gehören hier die Planung der IT-Infrastruktur, die Unterstützung der Umsetzung von Infrastrukturmaßnahmen und die Verrechnung entstandener Kosten.

■ 7.3 Methoden, Instrumente und Werkzeuge im IT-Controlling

Mit der steigenden Bedeutung des IT-Controllings wurde eine Vielzahl von Methoden, Instrumenten und Werkzeugen zur Erfüllung der Controllingaufgaben entwickelt. Das folgende Kapitel gibt einen Überblick über eine praxiserprobte und von der Literatur anerkannte Auswahl.

7.3.1 IT-Balanced Scorecard

Als zentrale Methode bei der Festlegung von Zielen ist in den Controllingkonzepten die Balanced Scorecard (BSC) zu sehen. Die Methode der BSC wurde im Umfeld der strategischen Unternehmenssteuerung entwickelt (vgl. [KaNo96]). Bei der BSC handelt es sich um ein Kennzahlensystem, das im Vergleich zu anderen Lösungen nicht nur finanzwirtschaftliche Kennzahlen betrachtet, sondern das Management auch hinsichtlich qualitativer Aspekte (zum Beispiel Durchlauf-/Antwortzeiten, Qualität, Zufriedenheit) informiert und bei der Entscheidungsfindung und Umsetzung unterstützt.

Durch die Berücksichtigung qualitativer Einflussgrößen gewährt die BSC nicht nur einen Überblick über vergangene Leistungen, sondern ermöglicht eine zukunftsorientierte Betrachtung wettbewerbsrelevanter Größen. Sie gewinnt daher im Zuge des gewandelten IT-Controllingverständnisses mehr und mehr an Bedeutung. Die operative und strategische Steuerung wird mit Hilfe der BSC umgesetzt, indem die Strategie beziehungsweise das Oberziel über Ursache-Wirkungszusammenhänge mit operativen Maßnahmeplänen verknüpft wird [GaMa05], das heißt, die Strategie wird mit konkreten Maßnahmen zu deren Umsetzung versehen. Die Balanced Scorecard ist dabei nicht auf die Darstellung der Gesamtorganisation beschränkt, sondern kann gleichzeitig zur Steuerung einzelner Organisationsbereiche, Abteilungen oder Projekte eingesetzt werden und bietet sich somit ideal für das hier betrachtete IT-Controlling an. Die BSC erfasst Kennzahlen aus unterschiedlichen Dimensionen, die als Perspektiven bezeichnet und über Ursache-Wirkungszusammenhänge miteinander verbunden werden [GaMa05].

Standardmäßig besteht eine BSC aus vier Perspektiven:

- Finanzwirtschaftliche Perspektive,
- Kundenperspektive,
- interne (Geschäfts-)Prozessperspektive und
- Lern- und Entwicklungsperspektive.

Je nach Bedarf können allerdings Perspektiven entfernt, hinzugefügt oder umbenannt werden. Die Entscheidung über die zu verwendenden Perspektiven ist in Abhängigkeit vom jeweiligen Anwendungsfall zu entscheiden. Bedeutsamer für eine wirkungsvolle Integration in die Führungs- und Steuerungssysteme sind letztendlich die gewissenhafte Ausarbeitung der Ursache-Wirkungszusammenhänge und deren Hinterlegung mit eindeutigen Kennzahlen, um die tatsächlichen Relationen zwischen Maßnahmen und Ergebnissen zu erfassen. Das Standardmodell kann also an die Verhältnisse eines IT-Bereichs in Abhängigkeit seiner organisationalen Einbindung angepasst werden. Dabei ist eine Verknüpfung mit der strategischen Positionierung der IT wichtig, da diese für die Bestimmung operativer Ziele und Auswahl der Maßnahmen relevant ist.

Ausgehend von der IT-Strategie werden für jede Perspektive auf jeder Controllingebene operative Ziele ermittelt und entsprechende Kennzahlen entwickelt [KeMüSc07]: Aus den IT-Zielen (zum Beispiel Leistungs- und Kostenziele) und der IT-Strategie werden für die einzelnen Perspektiven die strategischen beziehungsweise kritischen Erfolgsfaktoren (sogenannte Strategietreiber) definiert, die sich wesentlich auf die Zielerreichung (zum Beispiel Mitarbeitermotivation, Prozessqualität, hohe Kundenzufriedenheit) auswirken. Dabei ist darauf zu achten, dass die Ursache-Wirkungszusammenhänge korrekt abgebildet werden. Für jeden dieser

kritischen Erfolgsfaktoren sind im folgenden Schritt korrespondierende Kennzahlen (sogenannte KPI: Key Performance Indicators) zu bestimmen, die eine Überwachung und Steuerung der betreffenden Strategietreiber ermöglichen [Kü05] und mit Sollvorgaben und konkreten Maßnahmen zur Umsetzung sowie mit Verantwortlichkeiten zu hinterlegen.

7.3.2 IT-Kennzahlensysteme

Ein grundlegendes Instrument zur Überwachung und Steuerung der Zielvorgaben der Balanced Scorecard im Sinne eines IT-Controllings stellen Kennzahlen dar.



Kennzahlen sind quantitative Daten, die einen Ausschnitt der realen Situation einer Organisation zu einem bestimmten Zeitpunkt darstellen, und die festgelegten formalen Anforderungen genügen.

Kennzahlen entstehen erst durch Verdichtung (zum Beispiel durch Summenbildung).



Unter Kennzahlensystemen versteht man die Gesamtheit geordneter Kennzahlen, die die sachlogischen Zusammenhänge zwischen verschiedenen Größen aufzeigen und so betriebswirtschaftlich sinnvolle Aussagen über Unternehmungen und ihre Teile vermitteln [Glo1].

Kennzahlensysteme dienen der Analyse und Steuerung [Glo1]. Der grundlegende Gedanke hinter Kennzahlen und Kennzahlensystemen besteht darin, dem Management Informationen über kritische Erfolgsfaktoren der Zielerreichung in komprimierter und übersichtlicher Form zur Verfügung zu stellen. Bei den Kennzahlen lässt sich zwischen Kennzahlen im engeren Sinn, die in einer komprimierten Form über einen zahlenmäßig erfassbaren Sachverhalt berichten, und Indikatoren unterscheiden. Indikatoren sind komplementäre Kennzahlen, welche nur schwer abbildbare Zusammenhänge widerspiegeln. Dies kann zum Beispiel in Form von Ampeln oder Trendpfeilen geschehen (vgl. [Kü06]). Kennzahlen lassen sich in absolute und relative Kennzahlen unterscheiden. Bei den absoluten Kennzahlen geht es um grundlegende Sachverhalte in der Organisation. Beispielsweise können dies Einzelzahlen wie die Anzahl der Mitarbeiter, Summenzahlen wie die Bilanzsumme, Differenzen oder Mittelwerte sein. Relative Zahlen werden durch Quotientenbildung sinnvoller Sachverhalte erstellt, wobei der zu messende Wert als Zähler dient und der als Maß dienende als Nenner.

Die relativen Kennzahlen lassen sich wiederum in drei Gruppen einteilen:

- *Gliederungszahlen* geben den Anteil einer Größe an einer Gesamtmenge wider, beispielsweise den Anteil der IT-Personalkosten an den IT-Gesamtkosten.
- *Beziehungszahlen* sollen Zusammenhänge bei Zahlen mit unterschiedlicher Grundgesamtheit herstellen, bei denen ein Ursache-Wirkungs-Zusammenhang vermutet wird. Ein Beispiel dafür sind die Hardwarekosten pro Nutzer.
- *Indexzahlen* schließlich sind eine Aufbereitungsart, mit denen sich eine Veränderung von Daten über die Zeit deutlicher darstellen lässt. Dazu wird zu einem Zeitpunkt „t0“ als Grundwert „gleich 100“ gesetzt, und alle Änderungen können dann prozentual angegeben werden.

**Beachten Sie:**

„Es empfiehlt sich, neben absoluten Kennzahlen vor allem relative Kennzahlen zu verwenden. Durch die Verhältnisbildung zweier Kennzahlen lässt sich oftmals erst die erforderliche Aussagekraft erzielen“ [RuKüKro8].

Qualitative und quantitative Kennzahlen und Kennzahlensysteme bilden die Grundlage jeden IT-Controllings. Allerdings gibt es keine Kennzahlen, die sich – unabhängig vom Kontext – immer wieder einsetzen lassen. Je nach Zweck müssen daher für das IT-Controlling individuelle Kennzahlen definiert werden.

Eigenschaften, die grundsätzlich alle Kennzahlen erfüllen sollten, sind nach [Kü11] unter Verwendung von [Th94; Ha89]:

- **„Zweckeignung:**
Übereinstimmung des Informationsbedarfs mit dem durch die Kennzahl bereitgestellten Informationsangebot.
- **Genauigkeit:**
Zuverlässigkeit und Validität der Information.
- **Aktualität:**
Geringer Zeitraum zwischen Messung und Auswertung.
- **Kosten-Nutzen-Relation:**
Der Erkenntniswert der Kennzahl ist höher zu bewerten, als die Kosten der Erstellung.
- **Einfachheit und Nachvollziehbarkeit:**
Das Zustandekommen eines Kennzahlenwertes ist zurückverfolgbar und der Empfänger der Kennzahl kann das Messergebnis interpretieren“.

Oft sind Kennzahlen nur in einer Zusammenstellung in einem Kennzahlensystem sinnvoll. Ein solches Kennzahlensystem bildet möglichst genau den Zustand eines realen Systems als Modell ab und unterscheidet zwischen Soll- und Istzuständen [Kü05].

In der Literatur lassen sich Beispiele für Kennzahlensysteme mit unterschiedlichem inhaltlichen Fokus und für unterschiedliche Zielgruppen finden. So beschreiben etwa [RuKüKro8] ein Kennzahlensystem zur Messung der Qualität der IT-Servicebereitstellung im Kontext mittelständischer Unternehmen. Weitere Kennzahlen lassen sich etwa aus den Rahmenwerken der IT Infrastructure Library (ITIL) und der Control Objectives for Information and Related Technology (CobIT) ableiten.

Die wichtigsten Anforderungen an Kennzahlensysteme sind nach [Kü05]:

- Adäquate Beschreibung des aktuellen Systemstatus zu jedem Zeitpunkt;
- Beschreibbarkeit des Idealzustands des Systems anhand des Kennzahlensystems zu jedem Zeitpunkt;
- Erkennbarkeit der Stärke der Abweichung des Ist-Zustands vom Idealzustand;
- Existenz eines korrespondierenden Steuerungsmodells zur Beeinflussung des zu steuernden Objektes über passende Stellgrößen zu jeder Kennzahl.

Bei der Größe eines Kennzahlensystems ist nach [Kü05] auf die Anzahl der enthaltenen Kennzahlen zu achten, da beispielsweise durch die doppelte Anzahl an Kennzahlen gleichzeitig die

Betriebskosten für das Kennzahlensystem verdoppelt werden. Ebenso ist anzunehmen, dass durch die Erhöhung der Komplexität der Nutzen für den Verantwortlichen nicht unbedingt vergrößert wird. Zudem steigt die Schwierigkeit der Bewertung von Differenzen der Ist- und Sollwerte. Um mit Hilfe der Kennzahlen zu steuern und Entscheidungen zu treffen, ist es nötig, Kennzahlen entsprechend aufzubereiten. Vorgeschlagen wird, absolute Kennzahlen in Beziehung mit anderen Werten zu setzen [GaMa05]. Diese Normierung wird beispielsweise bei Strukturkennzahlen, Produktivitäten oder Wirtschaftlichkeiten verwendet, lässt sich aber auch bei anderen zeitraumbezogenen Größen einsetzen, wobei meist Mengen und Zeiträume in Relation gesetzt werden. Eine weitere Form der Normierung sind Erfüllungsgrade, bei denen der Istwert in Relation zum Zielwert gesetzt wird. Bei einem Erfüllungsgrad von 100 Prozent ist das Ziel erreicht.

Um die Akzeptanz eines IT-Kennzahlensystems zu gewährleisten, müssen die enthaltenen Informationen geeignet strukturiert und aufbereitet werden. Abhängig von der zu erfüllenden Steuerungsaufgabe und vom Umfeld können verschiedene Gliederungsansätze sinnvoll sein, etwa die Gliederung nach Zeitebenen, Sichten auf das Steuerungsobjekt oder nach Wertschöpfungsketten [Kü05; GaMa05]:

- Werden die IT-Kennzahlen nach Zeitebenen untergliedert, so lässt sich zwischen Tages-, Monats- und Langzeitkennzahlen unterscheiden.
- Bei einer Gliederung nach Sichten können die Kennzahlen in die Perspektiven Zeit, Kosten bzw. Aufwand, Leistung, Qualität und Risiko eingeordnet werden.
- Sollen die Kennzahlen anhand der Wertschöpfungskette strukturiert werden, ist eine Einteilung nach Kennzahlen über Lieferanten, Ressourcen, Prozesse, Produkte und Kunden möglich.

Kennzahlen und Kennzahlensysteme lassen sich außerdem wie folgt gliedern: Einzelkennzahlen, Analysekenzahlensysteme und Steuerungskennzahlensysteme.

Voraussetzung für die strategische Nutzung der Ergebnisse der Kennzahlendefinition ist nach [Ti05] ein fundiertes Berichtswesen, das Führungskräften, dem allgemeinen Controlling, der IT-Leitung und sonstigen Personen Informationen zur Verfügung stellt. Die Empfänger der Berichte treffen allerdings Entscheidungen in unterschiedlichen Bereichen und unterscheiden sich durch einen differenzierten Informationsbedarf. Die Berichtsform muss deshalb in Hinblick auf Berichtsinhalt, Zielgruppe und Berichtszeitpunkt angepasst werden [Ti05].

Bei der Einführung eines Berichtswesens für das IT-Controlling wird folgende Vorgehensweise vorgeschlagen [Ti05]:

- Ziele der Berichterstattung definieren;
- Adressatenkreis benennen (zum Beispiel Leitung, IT-Leitung, IT-Mitarbeiter);
- Informationsbedarf für die jeweiligen Empfänger ermitteln (Detaillierungsgrad, Verdichtungsstufen festlegen);
- Datenquellen analysieren (Daten aus Kostenverrechnung, Leistungsverrechnung, Risiko-Management, IT-Bestandsmanagement, vorhandene Berichte);
- Konzept ausarbeiten (Verantwortlichkeiten festlegen, Kennzahlen bestimmen, Darstellung etablieren);
- Werkzeuge auswählen (Ausgabemedien (Drucker, E-Mail, Software);
- Berichtssystem in Lasten- und Pflichtenheft spezifizieren.

7.3.3 Benchmarking⁵

Der Begriff IM-Benchmarking bezeichnet die Durchführung von Leistungsvergleichen im Informationsmanagement und ist ein fester Bestandteil des IT-Controllings. Durch den Vergleich mit anderen Organisationen, die Beobachtung von Erfahrungen, Methoden und Wissen und die Nutzbarmachung der gewonnenen Erkenntnisse auf Basis zentraler IT-Kennzahlen sollen Effizienz und Effektivität der Organisation gesteigert werden (vgl. [Kr10]).

Benchmarking beinhaltet einen Vergleich von Organisationen mit den jeweils „Besten“. Dieser Vergleich kann branchenabhängig oder branchenunabhängig erfolgen. Das Aufdecken von Schwachstellen in der eigenen Organisation steht im Vordergrund, Best Practices sollen übernommen werden: Die Identifikation und Adaption von Best Practices setzt eine große Erfahrung mit der Methode voraus. Oftmals ist es einfacher, einen Leistungsvergleich mit Orientierung und Ausrichtung an einem definierten Leistungsstandard (dem *Benchmark*) vorzunehmen. Häufig kann nämlich nicht eindeutig identifiziert werden, welche Lösung die Best Practice darstellt.

Die verschiedenen Formen des Benchmarkings werden in Abbildung 7.9 basierend auf [Le99] kategorisiert (vgl. [Kr10]): Die Vergleichspartner im Benchmarking können demnach entweder aus dem eigenen Unternehmen (intern) oder aus anderen Unternehmen (extern) stammen. Diese Unterscheidung wird als Vergleichshorizont bezeichnet. Stammen die Vergleichspartner aus der gleichen Branche, spricht man von konkurrenzbezogenem Benchmarking, während branchenunabhängiges Benchmarking auch als funktionales Benchmarking bezeichnet wird. Die Untersuchungsgegenstände des Benchmarkings können beispielsweise Prozesse, Produkte oder Strategien sein. Die Zielsetzung des Benchmarkings kann entweder die Leistungsmessung skalierbarer Zahlenwerte (quantitative Zielsetzung) oder das Erlernen von erfolgreichen Praktiken (qualitative Zielsetzung) sein.

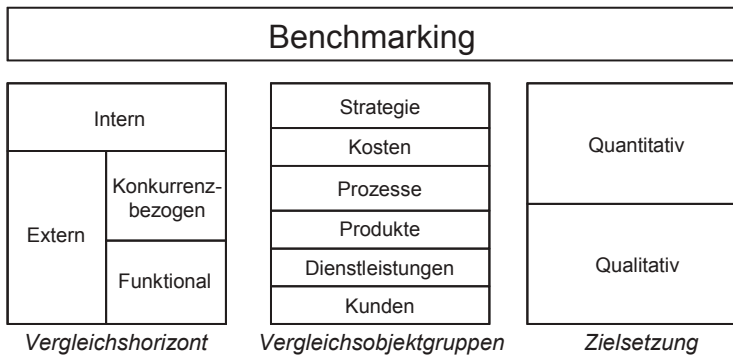


ABBILDUNG 7.9
Formen des Benchmarkings [Le99]

Eine wichtige Herausforderung beim Benchmarking besteht darin, sicherzustellen, dass die Vergleichsobjekte von allen Teilnehmern auch gleich definiert und erfasst werden: Grundlage des Vergleichs kann beispielsweise ein gemeinsam entwickeltes Kennzahlensystem sein. Weil das Informationsmanagement als Querschnittsfunktion in verschiedenen Unternehmen sehr unterschiedlich gestaltet sein kann, erweist sich die Definition und Operationalisierung von vergleichbaren Messgrößen in der Praxis oft als schwierig. Aus diesem Grund beschränken

⁵ Quelle: Überwiegend [Kr10]

sich Vergleiche im Benchmarking häufig auf die Informations- und Kommunikationsebene (zum Beispiel Benchmarks der Hardware, Infrastrukturgestaltung des Rechenzentrums). Sofern Prozesse als Vergleichsobjekte herangezogen werden, sind dies im Informationsmanagement meist Prozesse der Leistungserstellung und Unterstützung, da diese leichter zu vergleichen sind als die Prozesse der Leistungsverwendung.

Benchmarking hört nicht mit Abschluss des Vergleichs auf, vielmehr ist ein langfristiges Engagement seitens der beteiligten Organisationen erforderlich, um die identifizierten Best Practices für das eigene Unternehmen zu übernehmen.

Bei der Durchführung von Benchmarking-Vorhaben ist die Orientierung an vorhandenen Vorgehensmodellen wie etwa dem Phasenmodell von [Ca94] hilfreich. Diese Phasen werden mit den dazugehörigen Prozessschritten in Abbildung 7.10 dargestellt.

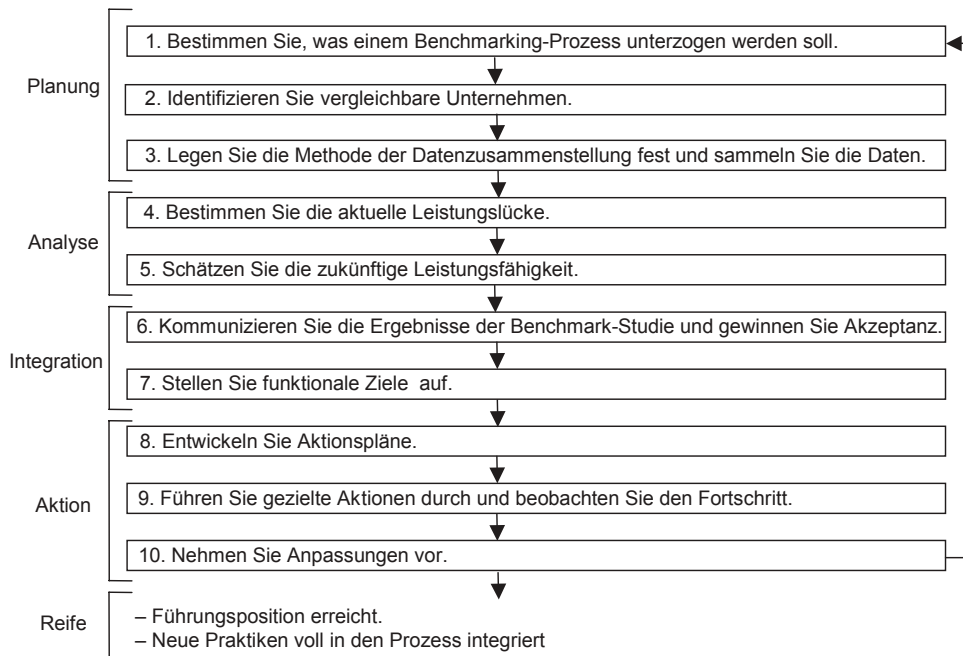


ABBILDUNG 7.10 Benchmarking-Prozessschritte [Ca94]

Die permanente Auseinandersetzung mit Best Practices erhöht das Verständnis der Benchmarking-Partner bezüglich ihrer Leistungsfähigkeit sowie ihrer Veränderungspotenziale beträchtlich.

7.3.4 Service-Level-Agreements (SLA)

Unter Service-Level-Agreements versteht man kennzahlenbasierte Vereinbarungen eines Dienstleistungsanbieters mit seinen Kunden bezüglich der zu gewährleistenden Servicequalität [Bu06]. Dabei wird der Grad der Leistungsqualität (Service-Level oder kurz SL) anhand der Definition der Leistung, der Darstellbarkeit der Leistung als Kennzahl, der Messmethode, des

Erstellers sowie des Empfängers der Leistung, als auch anhand der Erstellungsfrequenz und des Leistungsniveaus beschrieben [LeMa00].

Die Leistungsspezifikation durch die Definition von Service-Levels führt dazu, dass die Transparenz erbrachter IT-Leistungen erhöht wird. Daraus resultiert für den Dienstleistungsanbieter die Möglichkeit, Leistungszusagen verbindlich festzulegen. Diese Leistungszusagen verringern die Unsicherheit der Kunden bei Vertragsschluss bezüglich der Qualität der zu erbringenden Dienstleistung, welche auf Grund der fehlenden Inspektionseigenschaften zur Überprüfung der Qualität entsteht [OGC07].

Ein Service-Level bezieht sich nach [Bö04] immer auf ein Leistungsmerkmal einer IT-Dienstleistung, beispielsweise die durchschnittliche Verfügbarkeit eines Systems. Darüber hinaus wird festgehalten, mit welchen Systemen die Leistung gemessen wird und welche Verfahren dazu angewendet werden. Auch die Definition der Erhebungszeiträume ist fester Bestandteil eines Service-Levels. Außerdem muss spezifiziert werden, wie dem Kunden die erreichten Leistungsergebnisse mitgeteilt werden und welche Konsequenzen ein Unter- bzw. Überschreiten des Service-Levels nach sich zieht [Bö04].

Die für die Einhaltung eines Service-Levels relevante Größe bezeichnet man als Messgröße. Häufig verwendet werden hier Verfügbarkeitsquoten, Antwort- und Reaktionszeiten, Bearbeitungszeiten, der Personalaufwand zur Erbringung einer Leistung oder die Anzahl der Ausfälle pro Zeiteinheit [Sc00] in [Kr10]. Um die langfristige Vergleichbarkeit der erhobenen Daten zu gewährleisten, ist der Erhebungszeitraum zu definieren, also die Zeitpunkte beziehungsweise die Intervalle der Messungen [Sc00] in [Kr10].

Nach [Sc00] zitiert in [Kr10] müssen spezifische Anforderungen der Vertragspartner wie Mitwirkungs- und Beistelleistungen des Dienstleistungsnehmers in projektbezogenen Definitionen festgehalten werden. Hier können auch Ausnahmen definiert werden, die nicht Bestandteil der Messungen sein sollen. Außerdem muss spezifiziert werden, wie auf Änderungen im Umfang der zu liefernden Dienstleistung reagiert werden soll, um spätere Konflikte bezüglich des Vertrags zu vermeiden. Des Weiteren sind unter projektbezogenen Definitionen auch die Sanktionen genauer zu definieren, die bei Nichteinhaltung der SL verhängt werden [Sc00] in [Kr10].

Eine Einteilung von Beispielen für Service-Level-Agreements in Kategorien kann wie in Tabelle 7.1 dargestellt erfolgen [Bu06] in [Kr10]: Die ergebnisbezogenen beziehungsweise outputorientierten SLAs fordern eine gewisse Qualität der zu erbringenden Leistung und bilden diese auf Kennzahlen ab. Die prozessorientierten SLAs definieren Anforderungen an den Prozess der Leistungserstellung, während inputorientierte oder potenzialbezogene SLAs Ansprüche an die Inputfaktoren des Leistungsprozesses stellen.

**Beachten Sie:**

Ein Service-Level-Agreement muss auf Leistungen ausgerichtet sein, die für den Kunden von besonderer Relevanz sind, um auf beiden Seiten den Status der Verbindlichkeit zu erlangen [BöKro4].

TABELLE 7.1 Beispiele für ergebnis-, prozess- und potenzialbezogene Service-Levels [Bö04]

Service-Level	Erläuterung
1. Ergebnisbezogene Service-Levels	
Verfügbarkeit	Leistungsbereitschaft eines IT-Systems als Anteil eines Zeitraums (z. B. 98 Prozent/Monat)
Antwortzeit	Ausführungszeit für Benutzertransaktionen (z. B. durchschnittlich 1 sec im Tagesmittel oder 98 Prozent der Transaktionen < 1,5 sec)
Problem-lösungszeit	Maximale Zeit bis zur Lösung eines Problemfalls (in der Regel werden Probleme nach Schwere klassifiziert und danach abgestufte Zeiten vereinbart) (z. B. Behebung eines Störfalls der Stufe 1 (Totalausfall des Systems) innerhalb von vier Stunden)
Zuverlässigkeit	Einhaltung von Zusagen und Arbeitsqualität (z. B. Anteil kritischer Wartungsmaßnahmen, die zum zugesagten Zeitpunkt bereitgestellt werden, oder Anwendungen, die fehlerfrei in den Produktionsbetrieb übernommen werden)
Kunden-zufriedenheit	Zu erreichender Indexwert einer Kundenzufriedenheitsbefragung
2. Prozessbezogene Service-Levels	
Bereitschafts-zeit	Zeit, zu der der Nachfrager die Leistung anfordern kann (z. B. 07:00 – 24:00 Uhr)
Erreichbarkeit	Zahl der Fälle, in der Nachfrager den Anbieter in einem definierten Zeitfenster erreichen können (z. B. x Sekunden durchschnittliche/maximale Wartezeit für Anrufe am Help-Desk)
Reaktionszeit	Zeit, in der eine Leistung nach Anforderung erbracht werden muss (z. B. Einspielen von Sicherheitsupdates x Tage nach Verfügbarkeit)
Wiederhol-häufigkeit	Häufigkeit der Durchführung einer bestimmten Dienstleistung innerhalb eines festgelegten Zeitraums (z. B. Anzahl der Releasewechsel pro Jahr)
3. Potenzialbezogene Service-Levels	
Ressourcen-anforderungen	Anforderungen an Mitarbeiter und technische Ressourcen (z. B. (mitarbeiterbezogen) Sprachkenntnisse beim Help-Desk, Schulungsstand der Mitarbeiter oder (IT-bezogen) Verwendung eines bestimmten Hardware-herstellers, Betriebssystems oder Datenbanksystems)
Zertifizierung	Externe, dokumentierte Überprüfung des Leistungspotenzials des Anbieters nach festgelegten Standards (z. B. Zertifizierung als Microsoft-Gold-Partner oder nach ISO 9002, auditierte Einhaltung von Sicherheitsstandards bei der Ausstattung von Rechenzentren)
Kapazität	Vorhalten einer bestimmten Kapazität (z. B. Reservekapazität an Mitarbeitern)

Nach [BöKr04] gilt: Der Kunde ist zwar an der Verfügbarkeit und Performanz eines Anwendungssystems interessiert, nicht jedoch, ob diese auf Grund von Netzwerktechnik, Datenbanken oder Servern gewährleistet wird. Zwar ist es für den Dienstleistungsanbieter einfacher,

die Verfügbarkeit und Performanz der einzelnen Systeme zu messen, doch müssen diese Einzeldaten zu einem übergeordneten Service-Level aggregiert werden, um beim Kunden ein maximales Verständnis zu erreichen. Durch die zunehmende Verbreitung von Service-Level-Agreements wächst der daraus resultierende Aufwand zur Überwachung von Service-Levels stetig. Dabei sind die Anforderungen an die Infrastruktur zum Management und zur Überwachung der Service-Levels umso größer, je mehr Vereinbarungen getroffen werden und je größer die Anzahl der darin vorkommenden gemeinsamen Elemente ist.

7.3.5 Leistungsverrechnung

In den letzten Jahren sind die Kosten für IT in Unternehmen ständig gestiegen. Den gestiegenen Kosten steht das Unverständnis vieler Nutzer gegenüber, nach deren Wahrnehmung die Kosten für IT sinken müssten, weil die Preise für IT-Endgeräte niedriger werden [Di04]. Das IT-Controlling kann durch eine Steigerung der Transparenz bei der Ausgestaltung der Leistungsbeziehung zwischen IT-Servicegeber und IT-Servicenehmer dazu beitragen, diese Diskrepanz zwischen tatsächlicher Leistung und wahrgenommener Leistung der IT zu beseitigen. Als Controllinginstrument bietet sich hierbei die IT-Leistungsverrechnung an. Abbildung 7.11 zeigt eine praxisorientierte Darstellung der Aufgaben der IT-Leistungsverrechnung.

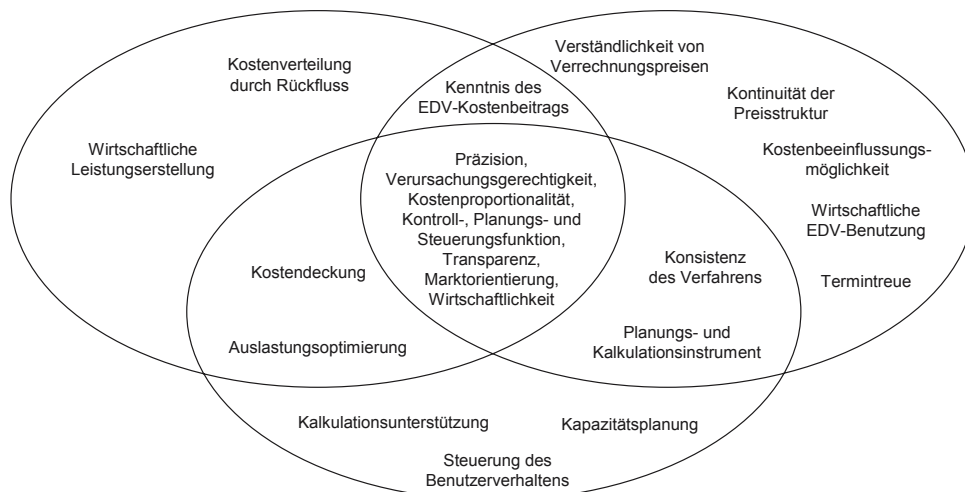


ABBILDUNG 7.11 Aufgaben der IT-Leistungsverrechnung [YuKoWe03]

Grundlagen der Kosten- und Leistungsrechnung⁶

In der Kostenrechnung wird zwischen Kostenarten, Kostenstellen und Kostenträgern unterschieden [Kü05]:

- Die Kostenartenrechnung ermittelt, um welche Kosten es sich handelt (beispielsweise Hardware- oder Softwarekosten).

⁶ Quelle: Überwiegend [Kü05]

- Die Kostenstellenrechnung beschäftigt sich mit der Frage, wo diese Kosten entstanden sind. „Orte“ der Kostenentstehung können zum Beispiel der ERP-Basisbetrieb oder der Service Desk sein.
- Die Kostenträgerrechnung zeigt, wozu die Kosten entstanden sind, etwa für einen bestimmten IT-Service.

Eine weitere Kostenklassifikation stellt die Unterscheidung in Fixkosten und variable Kosten dar [Kü05]: Fixkosten bleiben unabhängig von der Nutzungsintensität immer gleich hoch. Variable Kosten ändern sich in Abhängigkeit von der Nutzung. Außerdem existieren sogenannte intervallfixe Kosten, die innerhalb gewisser Intervalle fix sind, jedoch zwischen den Intervallen auf ein niedrigeres oder höheres Niveau fallen oder steigen. Die dritte Möglichkeit, Kosten aufzugliedern, sind Einzel- und Gemeinkosten: Einzelkosten lassen sich exakt auf Kostenträger zurechnen, Gemeinkosten müssen auf mehrere Kostenträger verteilt werden.

Methodisch unterscheidet man bei der Kostenrechnung zwischen Vollkostenrechnung und Teilkostenrechnung [Kü05]: Die Vollkostenrechnung verrechnet sämtliche Kosten auf die Kostenträger, die Teilkostenrechnung lediglich Einzelkosten.

Im Rahmen der Leistungsverrechnung wird zwischen Leistungsverrechnung durch Umlageverfahren, direkter, prozessorientierter und produktorientierter Leistungsverrechnung unterschieden [KeMüSc07].

Leistungsverrechnung durch Umlageverfahren

Das Umlageverfahren ist ein einfaches und schnell umsetzbares Verfahren, bei dem IT-Kosten über passende Bezugsgrößen – wie die Anzahl der Lizenzen oder die Anzahl der Arbeitsplatzrechner – pauschal verteilt werden. Diese Einfachheit hat jedoch zur Folge, dass Kosten nur sehr bedingt verursachungsgerecht verrechnet werden, worunter auch die Transparenz des Verfahrens leidet [KeMüSc07].

Direkte Leistungsverrechnung

Bei der direkten Leistungsverrechnung sollen hingegen Größen verwendet werden, die der realen Inanspruchnahme von IT-Leistungen entsprechen [KeMüSc07]. Beispiele aus der IT für direkte Leistungsverrechnung sind die Anzahl an gedruckten Seiten, Servicestunden oder die Dauer der Programmierung in Stunden.

Ist dieses Verfahren gut implementiert, können Kosten verursachergerecht und transparent verrechnet werden, wodurch das Kostenbewusstsein der Leistungsempfänger steigen soll. Jedoch bleibt anzumerken, dass bei einer vollständigen Verrechnung der Kosten Unwirtschaftlichkeiten der IT-Abteilung Preiserhöhungen zur Folge haben sowie der Verzicht auf IT-Leistungen zu Preisnachlässen führen müsste. Damit ist der Anreiz eines wirtschaftlichen Umgangs mit IT-Leistungen auf beiden Seiten nur sehr bedingt gegeben [KeMüSc07].

Prozessorientierte Leistungsverrechnung

Die prozessorientierte Leistungsverrechnung ist eine Methode, die durch das Paradigma der Prozessorientierung versucht wird, eine größtmögliche Transparenz herzustellen und der zunehmenden Komplexität der IT-Abteilungen gerecht zu werden [GeBuKr00]:

Das Ziel der Prozesskostenrechnung ist die transparentere Gestaltung der Gemeinkostenbereiche in Bezug auf die existierenden Aktivitäten und deren Inanspruchnahme von Ressourcen. Dadurch sollen die Kosten der einzelnen Gemeinkostenbereiche gezielter beeinflusst werden können. Durch eine prozessorientierte Kalkulation soll die Entscheidungsunterstützung verbessert werden. Wird eine strategische Kalkulation bereits in der Frühphase der Produktentwicklung durchgeführt, so können neue Kostensenkungspotenziale entdeckt werden. Letztendlich sollen Prozesse durch die Prozesskostenrechnung hinsichtlich ihrer Qualität, Zeit und Effizienz optimiert werden [GeBuKr00]. Abbildung 7.12 zeigt das Konzept der Prozessorientierung in Anwendung auf den IT-Bereich.

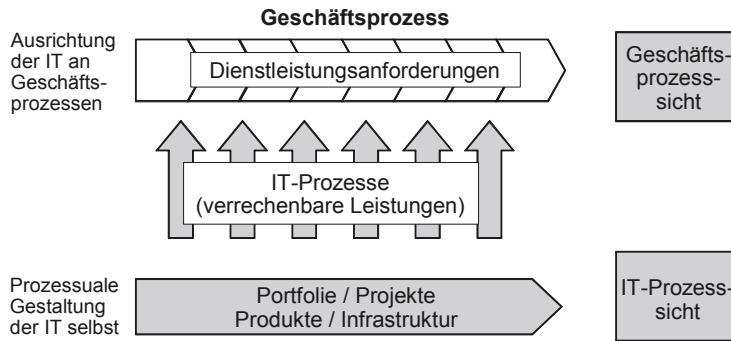


ABBILDUNG 7.12

Prozessorientierung
im IT-Bereich
[GeBuKr00]

Während üblicherweise die Gemeinkosten durch Zuschlagssätze auf die direkten Kosten verrechnet werden, ist dies bei IT-Dienstleistungen und IT-Produkten nicht sinnvoll, da der IT-Bereich als indirekter Leistungsbereich ausschließlich Gemeinkosten aufweist. Aus diesem Grund ist ein Vorgehen wie die Prozesskostenrechnung erforderlich, mit dem die Gemeinkosten weiter differenziert und verrechnet werden können [KaKü07].

Jedem Prozess wird nach [KaKü07] ein Kostentreiber zugeordnet, der sowohl als Messgröße für den Output der Leistung als auch für die Kostenverursachung herangezogen wird. Um die Prozesskostenrechnung zur Verrechnung von Kosten und Leistungen des IT-Bereichs nutzen zu können, müssen IT-Prozesse und Teilprozesse gebildet werden, in denen die Leistungen erbracht werden [KaKü07]. Den Teilprozessen können nun Kostentreiber zugeordnet und entsprechend die Prozesskosten ermittelt werden – es wird zwischen leistungsmengenabhängigen und leistungsmengenneutralen Teilprozessen unterschieden [KaKü07]: Teilt man die Summe der leistungsmengenabhängigen und leistungsmengenneutralen Prozesskosten durch die Menge der Kostentreiber, ergeben sich die Kostensätze der Prozesse [KaKü07].

7.3.5.1 Produktorientierte Leistungsverrechnung

Basis der produktorientierten Leistungsverrechnung sind die von der IT für die Leistungsabnehmer zur Verfügung gestellten IT-Produkte (IT-Services). Für solche IT-Services gilt [KeMüSc07]:

- Die Services müssen für die Kunden verständlich beschrieben werden, die Leistungsbeschreibung muss von den Kunden akzeptiert werden und sie müssen die Abnahme von Services beeinflussen können.

- IT-Services müssen voneinander abgrenzbar und standardisiert sein sowie in gleicher Qualität wiederholt angeboten werden können.
- IT-Services müssen auf die Unterstützung von Unternehmenszielen- und -strategien ausgerichtet sein.
- IT-Servicekosten sollten möglichst einfach messbar und kalkulierbar sein.
- Die Gestaltung von IT-Services sollte sich an externen und internen Angeboten weiterer Services orientieren, um einen Vergleich mit Marktpreisen zu ermöglichen.

Weil sich die Ausgestaltung des Servicekatalogs in der Praxis häufig als schwierig erweist, haben [RuScKr08] einen praxisorientierten Gestaltungsvorschlag für Servicekataloge erarbeitet. Der Vorschlag basiert auf der im IT-Servicemanagement üblichen Unterscheidung der Sichtweisen von Leistungsgeber und Leistungsnehmer. Die beiden Sichten werden durch die Gliederungsebenen

- IT-Services,
 - Servicemodule und
 - Serviceelemente
- miteinander verbunden.

Diese Gliederung ermöglicht es, den Abnehmern der IT-Leistungen auf Ebene der Services wahrnehmbare, verständliche und klar abgrenzbare Leistungsbeschreibungen zur Verfügung zu stellen, deren Leistungsumfang, Qualität und Menge auf Ebene der Servicemodule beeinflussbar sind (vgl. [RuBöKr08]). Die Servicestrukturierung kann als Grundlage für die Prozesse der Bedarfserhebung, Planung und Steuerung der IT-Servicebereitstellung eingesetzt werden [RuKr08].

Nach [Ru09] bestehen die Servicemodule aus für die Servicenehmer verständlichen Wahlmöglichkeiten in Bezug auf die angebotene Leistung. Die Serviceelemente beschreiben mehrfach kombinierbare Bündel von IT-Ressourcen zur technischen Umsetzung der Leistungen [Ru09]; Serviceelemente sind leistungsgebernah gestaltet sowie plattform- und herstellernabhängig formuliert. Sie können so auch zur Kommunikation mit (externen) Dienstleistern der IT eingesetzt werden [Ru09]. Abbildung 7.13 zeigt den Zusammenhang zwischen den Gliederungsebenen.

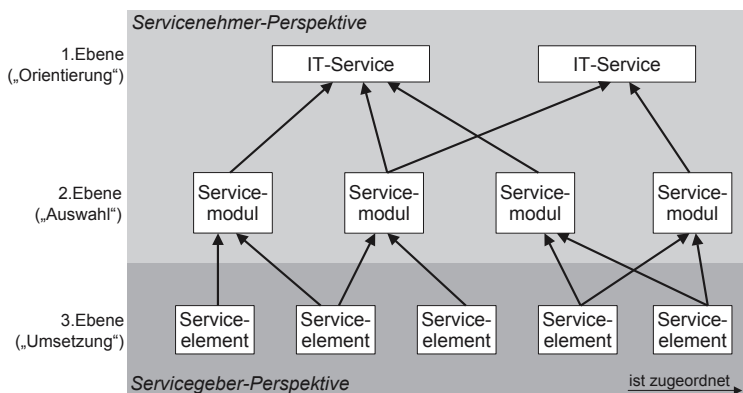


ABBILDUNG 7.13
Gliederungsebenen zur Strukturierung des Serviceangebots [RuBöKr08]

Abbildung 7.14 zeigt die musterhafte Ausgestaltung der Servicestruktur am Beispiel E-Mail.

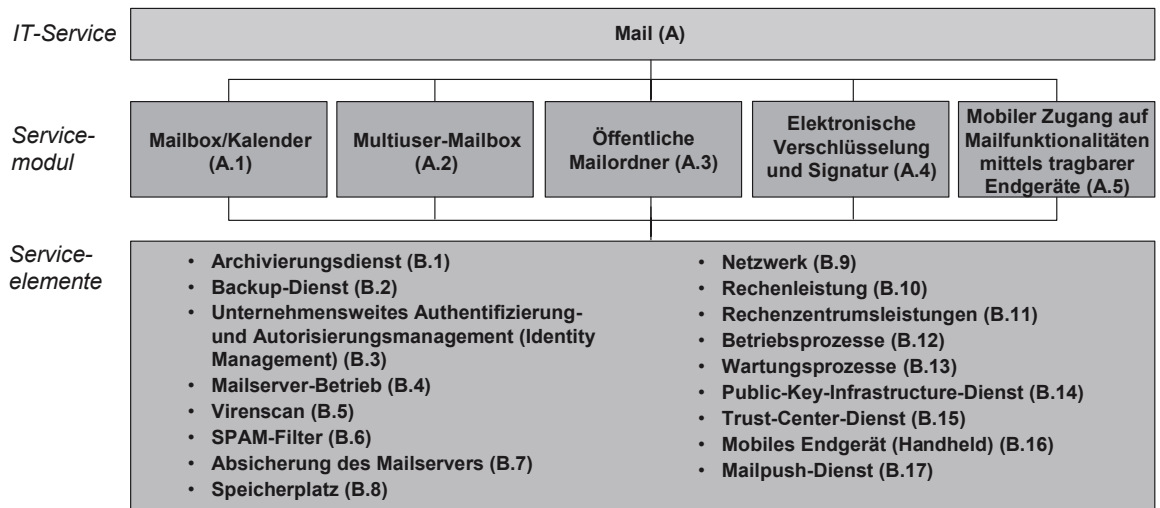


ABBILDUNG 7.14 Musterbeispiel Servicegestaltung E-Mail [RuBöKr08]

7.3.5.2 IT-Outsourcing⁷

Einen Sonderfall bezüglich der Leistungsverrechnung im IT-Controlling stellt das Outsourcing dar. Outsourcing wird in der Regel als Mittel zur Effizienzsteigerung und Kostensenkung gesehen. Viele Unternehmen gehen davon aus, dass Prozesse, die nicht zu den Kernkompetenzen der Organisation zählen und die keinen strategischen Wettbewerbsvorteil darstellen, von (externen) Spezialisten effizienter erbracht werden können. Dies wird auf die Vorteile der Spezialisierung und Economies of Scale zurückgeführt. Es verwundert daher nicht, dass der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) gerade im Jahr der Finanzkrise 2009 von einem Umsatzwachstum im Outsourcingbereich von 7,2 Prozent auf 14,6 Milliarden Euro ausgeht.

Darüber hinaus erhoffen sich viele Unternehmen durch Outsourcing eine Kostenreduktion im Zuge der Variabilisierung ihrer Fixkosten. Nicht zuletzt können auch weitere Gründe (politische Gegebenheiten, Durchsetzungsgründe) für Outsourcing sprechen (vgl. [Kr10]).



Beachten Sie:

Outsourcing ist eine Zusammensetzung der Wörter Outside, Resource und Using. Es bedeutet, dass einzelne Aufgaben der IT oder die gesamten IT-Aufgaben an ein anderes Unternehmen abgegeben werden. Es umfasst sowohl die Auslagerung (externes Outsourcing) und die Übertragung von Aufgaben an ein externes Unternehmen als auch die Ausgliederung (internes Outsourcing) an ein rechtlich verbundenes anderes Unternehmen [Krio].

In Outsourcingbeziehungen können unterschiedliche Formen der Koordination auftreten: Die schwächste Form des Outsourcings ist die Ausgliederung, bei der eine (konzerneigene) Firma

⁷ Quelle: Überwiegend [Kr10]

für die IT-Leistungen gegründet wird. Die nächste Outsourcingstufe liegt vor, wenn ein Unternehmen die Leistungen eines ausgegliederten Systemhauses beansprucht. Die größte Unabhängigkeit des Outsourcinganbieters ist bei Auslagerung an spezialisierte Fremdanbieter, etwa Hardwarehersteller oder Rechenzentren gegeben. Als Bindeglied zwischen Outsourcingnehmer und Outsourcinggeber kann auch eine Unternehmensberatung zwischengeschaltet sein.

Eine neue Form der Kooperation stellen so genannte Shared Service Center dar. Dabei werden Dienstleistungen wie zum Beispiel Rechenzentrumsleistungen zentral in gebündelter Form einer Gruppe von Abnehmern zur Verfügung gestellt. Shared Service Center vereinen in der Regel sowohl die Vorteile von Economies of Scope als auch die Vorteile der Economies of Scale auf sich. Kritisch anzumerken ist, dass bei Shared Service Centern auch Konstellationen denkbar sind, in denen konkurrierende Organisationen vom gleichen Anbieter mit Leistungen versorgt werden.

■ 7.4 Umsetzung von IT-Controlling

Die größte Herausforderung für das IT-Controlling liegt darin, das (strategische) Management mit Informationen über die Wirtschaftlichkeit der Leistungserstellung durch Informations- und Kommunikationstechnologie zu versorgen und insbesondere den Nutzen der Leistungsverwendung darzustellen. Eine große Gefahr dabei besteht darin, dass sich das IT-Controlling lediglich auf die Kostenseite beschränkt und Ausgaben und Nutzen nicht in geeignetem Ausmaß einander gegenübergestellt werden. In der Folge herrscht vielfach Angst davor, dass das Controlling lediglich als Vorwand für Budget- oder Personalkürzungen dienen soll. Diesem Umstand trägt das Controlling Rechnung, indem es den Spagat sowohl zwischen den Bedürfnissen der Anwender als auch den Ansprüchen der IT-Abteilung und den Bedürfnissen der Gesamtorganisation versucht.

Zur Erfüllung dieser Aufgabe stellen Literatur und Praxis dem IT-Controller einen ausgereiften Baukasten an Methoden und Instrumenten zur Verfügung.



Es kommt also in der Zukunft für Organisationen weniger darauf an, geeignete Instrumente und Werkzeuge des Controllings zu finden und diese aus dem Baukasten auszuwählen, sondern die ausgewählten Methoden richtig im organisationalen Kontext anzuwenden.

Das IT-Controlling muss sich daher in einem zyklischen Prozess immer wieder selbst auf seine Eignung als Instrument der Managementunterstützung hin evaluieren. Dazu bietet sich in Anlehnung an den DMAIC-Zyklus der Six-Sigma der Ablauf in Abbildung 7.15 an:

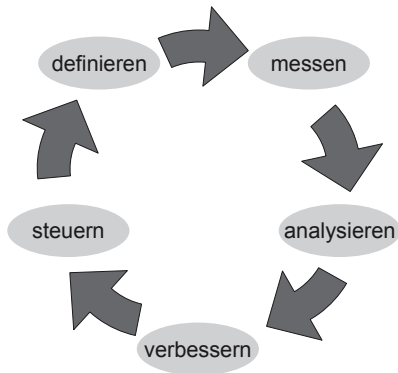


ABBILDUNG 7.15
Controllingablauf

- **Messen:** Im ersten Schritt werden die strategischen und operativen Ziele anhand geeigneter Kennzahlen gemessen.
- **Analysieren:** In Schritt 2 sind die gewonnenen Ergebnisse sowohl inhaltlich als auch hinsichtlich ihrer Realibilität und Validität zu analysieren.
- **Verbessern:** Auf Basis der Analyse erarbeitet man gegebenenfalls Verbesserungserfordernisse und Lösungsszenarien (Schritt 3). Die Verbesserungsanforderungen können sowohl die gemessenen Inhalte als auch die Kennzahlen selbst betreffen.
- **Steuern:** Die Erkenntnis aus Schritt 3 führt gegebenenfalls zu strategischen und/oder operativen Steuerungsmaßnahmen (Schritt 4). Die Umsetzung der Steuerungsmaßnahmen liegt in der Verantwortung des Managements.
- **Definieren:** Auf Basis der gewonnenen Erkenntnisse kann es zu Weiterentwicklungen und Neudefinitionen von Zielen und Kennzahlen kommen.



Das Wichtigste – zusammengefasst

- **Beachten Sie, dass es hinsichtlich der begrifflichen Einordnung und der Positionierung von IT-Controlling im Unternehmen unterschiedliche Ausrichtungen gibt!**

Als Primärziele eines IT-Controlling-Systems werden die Formalziele Effizienz und Effektivität sowie die Sachziele Qualität, Funktionalität und Termineinhaltung der Informationsverarbeitung herausgestellt. Dabei sollte IT-Controlling nicht nur als reine Überwachungsfunktion verstanden werden, sondern auch eine wesentlich Koordinationsfunktion für das gesamte Informationsmanagement wahrnehmen.

- **Die organisatorische Verankerung von IT-Controlling im Unternehmen sollte wohl überlegt sein; sie bestimmt zu einem hohem Maße das Erfolgspotenzial!**

In der Regel wird empfohlen, IT-Controlling möglichst nahe bei den Managemententscheidern im Sinne der IT-Governance zu verankern. Dabei kann es sich durchaus anbieten, das Controlling der IT-Leistungsverwendung dezentral in den Fachbereichen anzusiedeln, während organisationsweite Fragestellungen der IT-Leistungserstellung besser zentral in der IT-Organisation zu steuern sind. Bei einer Zuordnung als Querschnittsfunktion sind entsprechende Schnittstellen mit dem Linienmanagement sowie der Controlling-Abteilung zu beachten.

▪ **Berücksichtigen Sie bei der organisatorischen Ausgestaltung des IT-Controllings die zugrundeliegenden Entscheidungsstrukturen der IT-Governance!**

In Abhängigkeit von der Verteilung von Entscheidungsrechten und Zuständigkeiten bezüglich der IT zwischen zentralen und dezentralen Unternehmensbereichen sind auch unterschiedliche Ansprüche und Erwartungshaltungen an das IT-Controlling zu beachten. Durch eine entsprechende organisatorische Zuordnung des Controllings sowie eine geeignete Ausgestaltung von Berichtswesen und Kennzahlen können Sie diesem Umstand Rechnung tragen.

▪ **Beachten Sie den Zusammenhang zwischen dem Lebenszyklus der Informationssysteme und dem IT-Controlling!**

Es gibt kein allgemeines, in jeder Unternehmenslage identisches IT-Controlling. IT-Controlling setzt sich immer aus einer Mischung aus unterschiedlichen Methoden und Werkzeugen zusammen. Die Ausgestaltung des IT-Controllings kann sich dabei am Lebenszyklus der Informationssysteme orientieren. In Abhängigkeit vom Lebenszyklus (Portfolio, Projekte, Produkte und Infrastruktur) kann das Controlling spezifisch ausgestaltet werden.

▪ **Überlegen Sie, welche wesentlichen Teilbereiche bzw. Handlungsfelder das IT-Controlling in der Praxis umfassen sollte!**

Zu den strategischen IT-Controllingaufgaben gehören die Festlegung geeigneter Maßnahmen und Projekte (IT-Masterplanung), die die Organisation bei der Zielerreichung optimal unterstützen, sowie die Unterstützung der IT-Strategieentwicklung. Die operativen Controllingaufgaben umfassen etwa das Projekt-Controlling, das IT-Produkt-Controlling sowie das IT-Infrastruktur-Controlling.

▪ **Orientierungspunkte im IT-Controlling sind Prozessorientierung (Geschäftsprozess-Unterstützung) sowie Werkzeuge und Methoden.**

Zur Steuerung bieten sich insbesondere Kennzahlensysteme (z. B. auf der Basis einer Balanced Scorecard) an sowie der Vergleich von ausgewählten Kennzahlen durch Benchmarking.

▪ **Beachten Sie, dass eine innerbetriebliche Verrechnung der IT-Kosten und IT-Leistungen wesentliche Vorteile im Hinblick auf eine faire Kooperationskultur von IT-Bereich und -Fachbereich bringen kann!**

Durch den Einsatz eines entsprechenden IT-Controlling-Instrumentariums kann eine Steigerung der Transparenz bei der Ausgestaltung der Leistungsbeziehung zwischen IT-Servicegeber und IT-Servicenehmer erreicht werden und so die vielfach beobachtete Diskrepanz zwischen tatsächlicher Leistung und wahrgenommener Leistung der IT beseitigt werden.

▪ **Stellen Sie eine kontinuierliche Weiterentwicklung des IT-Controllings sicher!**

Aus der Erhebung von Kennzahlen und dem Controllingprozess können neben der Ableitung von inhaltlichen Erkenntnissen zur Steuerung auch Erkenntnisse zur Weiterentwicklung des Controllingprozesses und der Kennzahlen selbst gewonnen werden. Stellen Sie sicher, dass diese Erkenntnisse systematisch in das IT-Controlling eingebunden werden.

■ 7.5 Literatur

- [AuKr99] *Aurenz, H.; Krcmar, H.*: Controlling verteilter Informationssysteme. In (Von Dobschütz, L.; Baumöl, U.; Jung, R. Hrsg.): IV-Controlling aktuell. Gabler, Wiesbaden, 1999
- [Kü05] *Kütz, M.*: IT-Controlling für die Praxis. Konzeptionen und Methoden. dpunkt.verlag, Heidelberg, 2005
- [KeMüSc07] *Kesten, R.; Müller, A.; Schröder, H.*: IT-Controlling – Messung und Steuerung des Wertbeitrags der IT. Vahlen, München, 2007
- [Kr10] *Krcmar, H.*: Informationsmanagement. Springer, Berlin u. a., 2010
- [Kr90] *Krcmar, H.*: Informationsverarbeitungs-Controlling: Zielsetzung und Erfolgsfaktoren. In: Information Management, Vol. 5, Nr. 3, 1990; S. 6 – 15
- [Vö04] *Vöhringer, B.*: Computerunterstützte Führung in Kommunalverwaltung und -politik. Steuerung mit New Public Management und Informationstechnologie. Gabler, Wiesbaden, 2004
- [Kü06] *Kütz, M.*: IT-Steuerung mit Kennzahlensystemen. dpunkt.verlag, Heidelberg, 2006
- [We04] *Weber, J.*: Einführung in das Controlling. Schäffer-Poeschel, Stuttgart, 2004
- [KrBu94] *Krcmar, H.; Buresch, A.*: IV-Controlling – Ein Rahmenkonzept für die Praxis. In: Zeitschrift Controlling, Nr. 1994 Heft 5, 1994
- [KrBuRe00] *Krcmar, H.; Buresch, A.; Reb, M.*: IV-Controlling auf dem Prüfstand. Konzept – Benchmarking – Erfahrungsberichte. Gabler, Wiesbaden, 2000
- [So87] *Sokolovsky, Z.*: Projektcontrolling: Projektbegleitende Wirtschaftlichkeitskontrollen bei großen DV-Projekten. In: Zeitschrift für Organisation, Nr. 4, 1987; S. 261 – 268
- [KaNo96] *Kaplan, R. S.; Norton, D. P.*: Using the Balanced Scorecard as a Strategic Management System. In: Harvard Business Review, Vol. 74, Nr. 1, 1996; S. 75 – 85
- [GaMa05] *Gadatsch, A.; Mayer, E.*: Masterkurs IT-Controlling. Vieweg, Wiesbaden, 2005
- [Gl01] *Gladen, W.*: Kennzahlen- und Berichtssysteme – Grundlagen zum Performance Measurement. Gabler, Wiesbaden, 2001
- [RuKüKr08] *Rudolph, S.; Kütz, M.; Krcmar, H.*: Handlungsleitfaden IT-Kennzahlen und IT-Kennzahlensysteme für mittelständische Unternehmen. Books on Demand GmbH, Norderstedt, 2008
- [Kü11] *Kütz, M.*: Kennzahlen in der IT – Werkzeuge für Controlling und Management. dpunkt.verlag, Heidelberg, 2011
- [Th94] *Thaller, G. E.*: Software-Metriken einsetzen, bewerten, messen. Heise, Hannover, 1994
- [Ha89] *Haufs, P.*: DV-Controlling – Konzeption eines operativen Instrumentariums aus Budgets – Verrechnungspreisen – Kennzahlen. Physica, Heidelberg, 1989
- [Ti05] *Tiemeyer, E.*: IT-Controlling kompakt. Elsevier, München 2005
- [Le99] *Legner, C.*: Benchmarking informationsgestützter Geschäftsprozesse. Gabler, Wiesbaden, 1999
- [Ca94] *Camp, R.*: Benchmarking. Hanser, München, 1994
- [Bu06] *Burr, W.*: Service-Level-Agreements: Arten, Funktionen und strategische Bedeutung. In (Bernhard, M. G.; Mann, H.; Lewandowski, W.; Schry, J. Hrsg.): Praxishandbuch Service-Level-Management: Die IT als Dienstleistung organisieren. Symposium, Düsseldorf, 2006; S. 33 – 44
- [LeMa00] *Lewandowski, W.; Mann, H.*: Erfolgreiches Outsourcing – Eine gute Prozesssteuerung ist die halbe Miete. In (Bernhard, M. G.; Lewandowski, W.; Mann, H. Hrsg.): Service-Level-Management in der IT. Symposium, Düsseldorf, 2000; S. 215 – 234

- [OGC07] *Office of Government Commerce, G. B.:* Service Design. TSO (The Stationary Office), London, 2007
- [Bö04] *Böhmman, T.:* Modularisierung von IT-Dienstleistungen: Eine Methode für das Service Engineering. Gabler, Wiesbaden, 2004
- [Sc00] *Schrey, J.:* Ein Wegweiser für effektive vertragliche Regelungen – Fehlende gesetzliche Regelungen erfordern Absprachen. In (Bernhard, M. G.; Lewandowski, W.; Mann, H. Hrsg.): Service-Level-Management in der IT: Die IT als Dienstleistung organisieren. Symposium, Düsseldorf, 2000; S. 153 – 172
- [BöKr04] *Böhmman, T.; Krcmar, H.:* Grundlagen und Entwicklungstrends im IT-Servicemanagement. In: HMD – Praxis der Wirtschaftsinformatik, Nr. Band 237 (Juni 2004), 2004; S. S. 7 – 21
- [Di04] *Dietrichsweiler, L. A.:* Kostensenkung in der dezentralen IT-Infrastruktur. In (Dietrich, L. Hrsg.): IT im Unternehmen. Springer, Berlin 2004; S. 139 – 155
- [YuKoWe03] *Yurtkuran, S.; Kollorz, E.; Weber, M.:* Whitepaper zum IT-Controlling und IT-Leistungsverrechnung. Nicetec GmbH, Bissendorf, 2003
- [GeBuKr00] *Gerlinger, A.; Buresch, A.; Krcmar, H.:* Prozessorientierte IV-Leistungsverrechnung – Der Weg zur totalen Transparenz? In (Krcmar, H.; Buresch, A.; Reb, M. Hrsg.): IV-Controlling auf dem Prüf-stand: Konzept – Benchmarking – Erfahrungsbereichte. Gabler, Wiesbaden, 2000; S. 105 – 134
- [KaKü07] *Kargl, H.; Kütz, M.:* IV-Controlling. Oldenbourg, München, 2007
- [RuScKr08] *Rudolph, S.; Schwarzer, B.; Krcmar, H.:* Handlungsleitfaden IT-Services und IT-Servicekataloge für mittelständische Unternehmen. Books on Demand, Norderstedt, 2008
- [RuBöKr08] *Rudolph, S.; Böhmman, T.; Krcmar, H.:* Struktur von IT-Servicekatalogen: Ein praxisorientierter Gestaltungsvorschlag für die Dokumentation des IT-Leistungsangebots. GITO, S. 145 – 146
- [RuKr08] *Rudolph, S.; Krcmar, H.:* Prozessleitfaden zur Planung und Steuerung der IT-Servicebereitstellung für mittelständische Unternehmen. Books on Demand, Norderstedt, 2008
- [Ru09] *Rudolph, S.:* Servicebasierte Planung und Steuerung der IT-Infrastruktur im Mittelstand: Ein Modellansatz zur Struktur der IT-Leistungserbringung. Gabler, Wiesbaden, 2009

8

Herausforderung Lizenzmanagement – vom Risiko zum Wert

Torsten Groll



Fragen, die in diesem Kapitel beantwortet werden:

- Welchen Nutzen bringt die Einführung eines geregelten Lizenzmanagements? Welches Potenzial können Sie dadurch ausschöpfen?
- Welche Lizenzformen und Lizenzmodelle gibt es und sollten für die Entscheidungsfindung bekannt sein?
- Wie sehen die einzelnen Prozesse im Software-Life-Cycle aus?
- Welche Aufgaben erfüllt der Lizenzmanager, und welche weiteren Rollen sind im Unternehmen wichtig?
- Welche Daten sind für das Verwalten und Auswerten von Lizenzinformationen erforderlich?
- Wie identifizieren Sie die Komplexitätstreiber im Lizenzmanagement?
- Warum ist die Kenntnis der IT-Architektur für das Lizenzmanagement von Bedeutung?
- Wie finden Sie die beste Softwarelösung für die Unterstützung des Lizenzmanagements?
- Worauf sollten Sie bei der Einführung einer Lizenzmanagement-Lösung achten?

■ 8.1 Potenzial und Nutzen des Lizenzmanagements

Das Lizenzmanagement beschreibt Prozesse für den legalen Umgang mit Software und deren vereinbarten Lizenz- und Nutzungsbestimmungen. Das Lizenzmanagement hat primär eine wirtschaftliche Sichtweise. Für die natürlich gleichzeitig notwendige technische Verwaltung und Steuerung der einzusetzenden Software in einem Unternehmen – die jedoch nicht Gegenstand dieses Beitrags ist – wird der Begriff Software-Asset-Management (SAM) verwendet. Mit „SAM“ ist in Publikationen oft auch das Lizenzmanagement gemeint. Sie sollten diese Begrifflichkeiten vorab genau abklären und definieren, damit es zu keinen Missverständnissen kommt.

In den vergangenen Jahren haben sich IT-Manager selten ausreichend mit dem Thema Softwarelizenzen beschäftigt. In Abbildung 8.1 sehen Sie eine typische Verteilung der in einem Unternehmen eingesetzten bzw. vorhandenen Software und der damit einhergehenden Mehrausgaben: Für viele der installierten Software-Produkte fehlen Lizenzen, und an anderer Stelle werden installierte und lizenzierte Software-Produkte zum Teil gar nicht genutzt. Die Folge sind unnötige Mehrausgaben und keine Deckungsgleichheit von Software und Lizenzen.

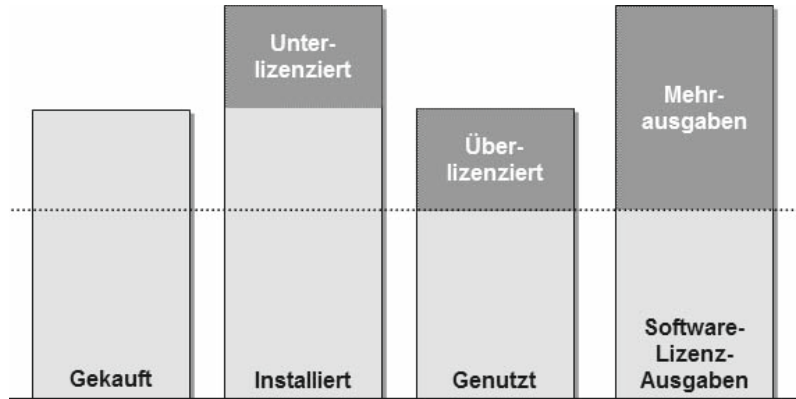


ABBILDUNG 8.1 Typische Unternehmenssituation bei Softwarelizenzen¹

Technisch ist es leicht: Eine einzige CD – oder ein über Ihr Unternehmensnetzwerk verteilbares Softwarepaket – würde ausreichen, um beliebig viele Installationen auszuführen. Rechtlich wird es schwieriger, denn für jede dieser „Installationen“ müssen Sie ein Nutzungsrecht (eine Lizenz) nachweisen. Diese erfolgt üblicherweise in Form von Lizenzverträgen mit den darin beschriebenen Nutzungsrechten. Diese Lizenzverträge beschreiben die erlaubte Anzahl der installierbaren Softwareversionen und müssen als Nachweise für einen Audit aufbewahrt werden.

So mancher erinnert sich bestimmt daran, dass es bei der Installation von Microsoft Office 4.2 genügte, bei der Abfrage des Lizenzkeys alle Felder mit einer Folge von 1 auszufüllen, und schon konnte man fröhlich weiter installieren. Einen wirksamen Schutz gegen das unrechtmäßige Kopieren der Softwaremedien gab es damals genau genommen nicht. Das Thema mit den Microsoft Office-Produkten hat auch heute nicht an Bedeutung verloren. Denn sollten Sie beispielsweise im Umgang mit den für Microsoft-Office-Produkten vereinbarten Nutzungsrechten nicht die notwendige Sorgfalt an den Tag legen, kann es schon vorkommen, dass mit einem Lizenzkey, der für das Microsoft-Office-Professional-Paket vorgesehen ist, ein unternehmensweiter Rollout für das Office-Standard-Paket vorgenommen wird (Paketierungsfehler). Da dies aber nicht den vereinbarten Nutzungsbestimmungen entspricht, hätten Sie spätestens bei einem Audit ein großes Problem und müssten schlimmstenfalls alle Desktops für das Office-Professional-Paket nachlizenzieren.

An diesem Beispiel sehen Sie schon, wie wichtig die Zusammenarbeit und Abstimmung zwischen dem Lizenzmanagement und den verantwortlichen technischen Fachbereichen ist.

¹ Alle Abbildungen in diesem Kapitel entnommen aus [Gr09, Kap. 2.3].

Die Ausgangssituation in den meisten Unternehmen

Es gibt kaum noch einen Unternehmensprozess, der von Software nicht – zumindest – unterstützt wird. Gleichzeitig unterschätzt man aber oft die Wichtigkeit einer aktuellen Übersicht über den aktiven und korrekt eingesetzten Softwarebestand. Gibt es diese Übersicht nicht, entsteht unerwünschter Wildwuchs, und die notwendige Transparenz geht verloren. Statistische Zahlen, die durch die Business Software Alliance (BSA) erhoben wurden, gehen davon aus, dass jede dritte Softwareinstallation illegal, d. h. nicht korrekt lizenziert im Einsatz ist.² Die häufigste Ursache dafür ist der leichtfertige Umgang mit dem Wirtschaftsgut „Software“ und mangelndes Software- und Lizenzmanagement.

Die Herausforderung

Die meisten Unternehmen haben keinen Überblick, welche Software wo und wie oft eingesetzt wird und ob sie auch ausreichend – entsprechend den vereinbarten Nutzungsbedingungen – mit Lizenzen kaufmännisch gedeckt ist. Diese Unkenntnis entbindet die Geschäftsleitung aber nicht von der Verantwortung, lizenzrechtliche Bestimmungen einzuhalten, um mögliche strafrechtliche und wirtschaftliche Konsequenzen abzuwenden.

Die handelsrechtliche Verantwortlichkeit verpflichtet die meisten Unternehmen zu Einführung und Betrieb eines Risikomanagementsystems, zu dessen Aufgaben auch die Überwachung der Lizenzkonformität der im Unternehmen eingesetzten Software gehört. Ein zu bewertendes Risiko kann dabei sein, für Lizenznachkäufe durch eine festgestellte Unterlizenzierung Rückstellungen zu bilden (vgl. hierzu auch den gesonderten Beitrag zum IT-Risikomanagement in diesem Handbuch, Kapitel 12). Die Risiken, die sich dabei auch auf das gesamte Unternehmen auswirken können (Stichwort: KontraG, Basel II, Sox), sind mit einem IT-basierten Software- und Lizenzmanagement-System minimierbar. Eine zentrale Verwaltung aller erworbenen Lizenzen und der dazugehörigen Verträge in Verbindung mit einer permanenten Analyse der installierten und aktiven Softwarebasis kann dabei helfen.



Praxistipp:

Hersteller lassen sich ständig neue Spielarten einfallen, Kunden mit immer komplexeren Lizenzbestimmungen zu verwirren. Dank einer effektiveren Verwaltung und Organisation Ihrer Softwarelandschaft können Sie diesen Herausforderungen gelassen begegnen. Dafür ist es jedoch notwendig, Spezialwissen über die Softwarelieferanten und deren Lizenzmodelle im Unternehmen aufzubauen. Dieses Wissen müssen Sie für den Aufbau und die Organisation des Lizenzmanagements nutzen. Dabei geht es auch darum, Rollen und Zuständigkeiten zu definieren und die damit verbundenen Prozesse abteilungsübergreifend im Unternehmen zu verankern.

In vielen Unternehmen erzeugen verteilte Interessen unklare Situationen bzgl. Verantwortlichkeiten, Rollen und Prozessen. Ein Überblick über die aktiven Softwareinstallationen (tech-

² http://portal.bsa.org/globalpiracy2010/downloads/study_pdf/2010_BSA_Piracy_Study-Standard.pdf
(Eight Annual BSA Global Software 2010 Piracy Study May 2011)

Pressemitteilung zur Studie zur Entwicklung von Softwarepiraterie http://portal.bsa.org/globalpiracy2010/downloads/press/pr_germany_german.pdf

nische Stückzahlen) und den tatsächlich vorhandenen kaufmännischen Lizenzbestand ist meistens nicht im geforderten Umfang und der benötigten Qualität vorhanden. Unternehmensspezifische Richtlinien zur Softwarenutzung existieren selten oder sind unzureichend. Vor diesem Hintergrund verwundert es nicht, dass einem anstehenden internen oder externen Software-Audit oft mehr mit „Glauben“ als mit „Wissen“ begegnet wird.

Folgende Fragen helfen Ihnen bei einer ersten Bestandsaufnahme in Ihrem Unternehmen:

- Können Sie auf Knopfdruck Ihren aktuellen Bestand an PCs, Servern und anderem IT-Equipment abrufen?
- Können Sie ermitteln, wie viele unterschiedliche Software-Anwendungen Sie haben, und werden diese auch alle eingesetzt und tatsächlich genutzt?
- Wird Ihre Software zentral oder dezentral beschafft?
- Werden die Vertragsunterlagen an einer Stelle geführt?
- Was passiert mit der Software, die nicht mehr genutzt wird? Wird das in den bestehenden Verträgen mit betrachtet?
- Kann Software von Mitarbeitern unerlaubt installiert werden?
- Besitzen Sie Richtlinien für den Umgang mit Software in Ihrem Unternehmen?
- Werden diese Richtlinien von jedem verstanden, „gelebt“ und ihre Einhaltung regelmäßig überprüft?

Vielleicht können Sie einige der gestellten Fragen mit „Ja“ beantworten, vielleicht müssen Sie sich aber auch eingestehen, dass Sie einige dieser Aspekte noch nicht ausreichend betrachtet haben, was bedeutet: Sie müssen handeln.



Tipp:

Auf dem Markt gibt es mittlerweile eine große Auswahl an Herstellern und Dienstleistern, die Tools für das Software-Asset-Management anbieten, in denen fast immer auch ein Lizenzmanagement mit integriert ist.

Aktives Lizenzmanagement – Potenzial und Nutzen

Allgemein wird die IT als Kostentreiber betrachtet, die nicht oder in nur geringem Ausmaß im Verlauf der Geschäftsprozesse zur Wertschöpfung beiträgt. Bei konsequenter Umsetzung eines Software-Lizenz-Managements wird aus dem Kostentreiber IT ein Wertschöpfer.

Die Einführung eines Software-Lizenz-Managements hilft Ihnen, mögliche Einsparpotenziale aufzudecken. Der Einsatz von Technologien zur Erfassung von Softwarelizenzen führt relativ kurzfristig zu einem beachtlichen Return on Invest (ROI). So können die durch eine Lizenzoptimierung aufgedeckten Sparpotenziale bei einem mittelständischen Unternehmen mit 3500 Mitarbeitern schon durchaus im 6-stelligen Bereich liegen. Durch Anpassung von Wartungsverträgen oder die Reduzierung von Lizenzstückzahlen ergeben sich weitere mittel- und langfristige Einsparmöglichkeiten.

Aktives Lizenzmanagement hilft Ihnen nicht nur Softwarekosten zu senken, sondern kann das Unternehmen unter Umständen vor einer strafbaren Unterlizenzierung und der Nutzung von Raubkopien auf den unternehmenseigenen Computern bewahren. Um die gesetzlichen

Anforderungen zu erfüllen und für Herstelleraudits gewappnet zu sein, ist es unerlässlich, ein Lizenzmanagement zu initiieren und auch dauerhaft zu betreiben.

**Tipp:**

In vielen Fällen ist der endgültige Auslöser, ein Lizenzmanagementprojekt zu starten, der angekündigte Besuch eines Auditors, der im Auftrag eines Softwareherstellers bei Ihnen vorstellig wird. Nur ist es dann meistens schon zu spät. Jetzt kostet es Sie unter Umständen richtig viel Geld, da Sie den „Schätzungen“ des Auditors keine eigenen belastbaren Zahlen entgegenhalten können. Zeigen Sie deshalb die Brisanz des Themas bei Ihrer Geschäftsleitung bzw. bei Ihrer Revision noch einmal eindringlich auf, um künftig bei anstehenden Audits besser gewappnet zu sein.

Neben den zuvor genannten vorrangigen Beweggründen gibt es aber noch eine Reihe weiterer Vorteile, die für die Einführung eines Lizenzmanagements sprechen:

- Die Sicherstellung der Einhaltung der Herstellervorgaben (Nutzungsbestimmungen);
- die Einhaltung der Volumenverträge, Beitritte sowie der übergeordneten Vereinbarungen, z. B. Software License Agreements (SLA);
- die Beachtung von Vorgaben zur transparenten Darstellung der Unternehmens-Situation (Revision);
- die Schaffung von Compliance (durch den Abgleich der erfassten technischen und kaufmännischen Daten);
- die Informationsbereitstellung für eine rechtzeitige, strategische Planung von Softwareeinkäufen;
- Aufzeigen möglicher Einsparungen durch aktive und proaktive Steuerung der Lizenz-Ausnutzung (Stichwort: SW-Nutzungsanalyse);
- Herstelleraudits lassen sich fast ohne Vorbereitungszeit – und damit ohne zusätzlichen Aufwand und Kosten – unproblematisch durchführen;
- Möglichkeit von Kosteneinsparungen durch Standardisierung und Lizenzpooling;
- Einsparungspotenziale durch Wiederverwendung ungenutzter bzw. freier Lizenzen innerhalb eines „Lizenzpools“;
- Prozesskostensenkung durch Optimierung des Lizenz- und Software-Handlings (z. B. interner Lizenz-Bestellvorgang, Lizenzverwaltung, Lizenzpooling);
- bessere Position gegenüber den Software-Herstellern oder Lieferanten bei Vertragsverhandlungen durch eine transparente und stets aktuelle Sicht auf die Lizenzierungssituation.

**Tipp:**

Erstellen Sie sich eine Argumente-/Vorteilsliste zum IT-Lizenzmanagement. Übernehmen Sie die hier aufgeführten Punkte, um eine Entscheidungsvorlage für die Einführung eines Lizenzmanagement-Projektes für Ihre Geschäftsleitung aufzubereiten.

Ein aktueller, transparenter und gepflegter Datenbestand kommt letztendlich auch den anderen Geschäftsprozessen zugute. Die Zukunft wird uns auch im Umfeld des Lizenzmanagements neue interessante Aufgaben bescheren. Die Hersteller werden weiterhin die Einhaltung ihrer Nutzungsrechte im Auge behalten, und nicht zuletzt werden neue Technologien wie beispielsweise „die Cloud“ das Lizenzmanagement vor neue Herausforderungen stellen.

■ 8.2 Was ist eine Softwarelizenz?

Begriffliche Klärung

Als in den 60er-Jahren, den Anfängen der Computerindustrie, die Großrechner aufkamen, war die Hardware das bestimmende Element. Die notwendige Software für den Betrieb stellte damals nur ein Nebenprodukt dar, das entweder von den Hardwareherstellern oder von den Anwendern selbst programmiert wurde. Heute bietet sich uns ein ganz anderes Bild. Computer sind sehr viel kleiner und leistungsfähiger geworden. Die darauf installierte Software unterstützt unseren Alltag im Geschäfts- und Privatleben mit den vielfältigsten Funktionen. Im Gegensatz zu den Anfängen des Computerzeitalters, als die Software immer für ein ganz spezielles Stück Hardware geschrieben wurde und nicht auf andere Computer so ohne Weiteres installierbar war, ist die heutige Software dafür gedacht, auf möglichst vielen Computersystemen eingesetzt zu werden.

Von der technischen Seite aus betrachtet, können Sie die Software nach der Installation auf Ihrem Computersystem anwenden und für Ihre Zwecke einsetzen. Nun ist aber die Software ein „Werk“, welches durch eine natürliche oder juristische Person (Hersteller) „erschaffen“ wurde. Der Urheber des Werks ist laut deutschen Urheberrechts untrennbar mit seiner „Schöpfung“ verbunden, d. h. nur er darf über die weitere Verwendung oder Verbreitung seines Werks bestimmen. Dieses Recht zur Verwendung (zur Nutzung) des Werks erteilt der Urheber in Form einer Lizenz. Der Duden beschreibt den Begriff „Lizenz“ folgendermaßen:

Li|zenz, die; -, -en (lat.) Erlaubnis, Genehmigung, bes. zur Nutzung eines Patents oder eines Softwareprogramms oder zur Herausgabe eines Druckwerks³

Der Begriff **Softwarelizenz** bezeichnet das Nutzungsrecht, das der Rechteinhaber (Urheber) dem Nutzer (Endanwender) an der von ihm erworbenen Software einräumt. In einem Lizenzvertrag wird der vom Urheber vorgegebene rechtliche und vertragliche Rahmen beschrieben. Erst mit dem Akzeptieren des Lizenzvertrags darf die Software in der vereinbarten Form bestimmungsgemäß genutzt werden.

Das Verwalten von Softwarelizenzen bedeutet also:

Die rechtskonforme sowie betriebswirtschaftlich optimierte Nutzung von Softwarelizenzen sicherzustellen, diesen Prozess permanent zu überwachen und zu steuern.

³ Duden, Band 1, Die deutsche Rechtschreibung, 24. Aufl., S. 649.

Die gebräuchlichsten Lizenzformen

Jeder Urheber, der Software entwickelt und in Verkehr bringt, legt mit der anzuwendenden Lizenzform fest, unter welchen Nutzungs- bzw. Lizenzbedingungen die Software verwendet werden darf. Sie werden in Ihrem Unternehmen sicherlich mit den unterschiedlichsten Softwareprodukten und deren Lizenzbestimmungen zu tun haben. Die dabei anzutreffenden Lizenzformen lassen sich prinzipiell in proprietäre Software (kommerziell) mit den Unterformen „Freeware“ und „Shareware“ sowie „Freie Software“ (Open Source, nicht kommerziell) unterteilen. Die „Public Domain“-Lizenzform als weitere Lizenzform der „Freien Software“ soll hier nur am Rande Erwähnung finden, weil nach deutschem Urheberrecht (im Gegensatz zum amerikanischen) kein Urheber auf seine Rechte zum Wohle der Gemeinheit verzichten darf. Somit kann ein Urheber in Deutschland seine Software nicht unter die Lizenzform „Public Domain“ stellen.



Hinweis:

Die vom Urheber gewählte Lizenzform bestimmt die Freiheiten bei der Benutzung oder Verbreitung seiner Software.

In den folgenden Abschnitten erhalten Sie einen kurzen Überblick über die am häufigsten von den Urhebern angewendeten Lizenzformen.

Proprietäre Software

Gemeinhin wird sämtliche Software, die nicht vom Urheber unter die Open-Source-Lizenzbedingungen (beispielsweise die GNU GPL) gestellt wird, als proprietäre Software eingestuft und auch als kommerzielle Software angesehen (also Software, die gegen Geld ge- und verkauft wird), wie beispielsweise Microsoft Office, Lotus Notes, Adobe Photo-Shop u. v. a. m. „Freeware“ und „Shareware“ sind zwei Lizenzformen, in die u. a. proprietäre Software eingeteilt werden kann. Gemeinsam ist allen, dass sie im Gegensatz zur Freien Software nicht verändert werden dürfen und der Quelltext der Software nicht offengelegt ist.

Freeware

Freeware bezeichnet im Allgemeinen proprietäre Software, deren Nutzung zwar kostenlos ist und frei kopiert bzw. weiterverbreitet werden darf, aber nicht mit so vielen Freiheiten ausgestattet ist wie Freie Software (Open Source). Die Nutzungsbedingungen werden durch den Urheber festgelegt und üblicherweise auch in der Form eines „End User License Agreement (EULA)“ beschrieben. Die Unterschiede zur Freien Software ergeben sich insbesondere daraus, dass der Quelltext nicht offen vorliegt und es beispielsweise dem Endanwender von den meisten Freeware-Programmen verboten wird, den Programmcode zu ändern und das geänderte Programm weiterzugeben.

Softwarehersteller vertreiben ihr Produkt häufig als Freeware, wenn die Verbreitung einen strategischen Marktvorteil erwirkt. Der Internet Explorer von Microsoft oder der Adobe Acrobat Reader sind bekannte Beispiele für Freeware.

**Tipp:**

Meist ist die kostenlose Nutzung von Freeware nur für den privaten Gebrauch zulässig, für die kommerzielle Nutzung erhebt der Autor Lizenzgebühren. Wenn Sie bei sich im Unternehmen Freeware einsetzen, dann lesen Sie sich bitte die Nutzungsbestimmungen der Software genau durch, damit Sie die rechtlichen Bedingungen einhalten.

Shareware

Shareware bezeichnet frei kopier- und weiter verbreitbare Softwareprodukte, die für einen bestimmten Zweck (beispielsweise für den privaten Einsatz) oder über einen gewissen Zeitraum hinweg kostenlos genutzt werden können. Zeitbegrenzungen enden oft nach 30 Tagen. In diesem Testzeitraum steht aber oftmals der komplette Funktionsumfang der Software zur Verfügung. Nach Ablauf der Testperiode muss der Endanwender, falls er die Software weiterhin nutzen möchte, eine Lizenzgebühr an den Autor zahlen. Die sonstigen Lizenzbedingungen entsprechen weitgehend der von proprietärer Software und werden oft mit einem in die Software integrierten „End User License Agreement (EULA)“ beschrieben.

Die Vertriebskanäle von Shareware sind in den meisten Fällen das Internet oder Software-sammlungen auf CD-ROMs, die vielen Computerzeitschriften beigelegt werden. Da der Autor den Vertrieb seiner Software nicht selbst übernimmt, hat er keine Möglichkeit, die Anwender seines Programms zu identifizieren, um eine Bezahlung nach Ablauf der Testzeit zu erhalten. Um der erfahrungsgemäß geringen Zahlungsmoral der Anwender vorzubeugen, ist Shareware häufig modifiziert. Meistens stehen nach Ablauf der Testzeit die Programmfunktionen nur eingeschränkt zur Verfügung, oder es lassen sich beispielsweise keine neuen Dateien mehr mit dem Produkt anlegen.

Software, die unter der Flagge „Shareware“ segelt, wird häufig von Privatleuten oder kleineren Firmen, die auf sich aufmerksam machen wollen, verwendet. Einige Programme, die Sie bestimmt kennen, haben ihre Karriere als Shareware begonnen, wie beispielsweise das Zeichenprogramm Paint Shop Pro, oder sind es teilweise heute noch, wie beispielsweise das Packprogramm Winzip. Diese meist kleinen Helferlein erfreuen sich nach wie vor großer Beliebtheit in den Unternehmen, umso wichtiger ist es auch hier, die Nutzungsbedingungen zu kennen und einzuhalten.

Freie Software, Free Software

Mehr als 20 Jahre gibt es jetzt schon Freie Software. Heute ist es durchaus üblich, auch in kommerziellen Umgebungen Freie Software wie beispielsweise das Betriebssystem Linux, den Internetbrowser Firefox, das E-Mail-Programm Thunderbird oder die Bürosuite Open Office einzusetzen. Das war aber nicht immer so. Erst in den letzten Jahren konnte sich Freie Software auch verstärkt in den Unternehmen etablieren, u. a. auch deshalb, weil viele große Firmen wie beispielsweise IBM für Freie Software Entwicklungsarbeit leisten.

Freie Software gibt Ihnen im Gegensatz zu proprietärer Software die Freiheit, sie für einen beliebigen Zweck auszuführen, ihre Funktionsweise zu studieren, sie Ihren eigenen Bedürfnissen anzupassen oder zu verbessern und diese Kopien der Software zu veröffentlichen oder weiterzugeben. Der Zugriff auf den Quelltext ist die Voraussetzung dafür, Software zu studie-

ren, anzupassen und zu verbessern. Mit der Beliebtheit Freier Software stieg auch die Zahl der Bezeichnungen. Die Free Software Foundation (FSF) empfiehlt im Deutschen die Verwendung des Terminus „Freie Software“, um diese entsprechend in andere Sprachen übersetzen zu können. Ein weiterer Begriff, der 1998 von der Open Source Initiative (OSI) vorgeschlagen wurde, um Freier Software zu größerer Akzeptanz in den Chefetagen zu verhelfen, ist „Open Source“. Die Idee war, sich auf die technischen Aspekte Freier Software zu konzentrieren und sie so im Unternehmensumfeld leichter verkaufen zu können. Schon nach kurzer Zeit konnte Open Source die ersten Erfolge verbuchen. Die Popularität von Linux – der Open-Source-Software schlechthin – bewog Firmen, wie beispielsweise IBM, Novell, Informix, Sun und viele weitere bekannte Soft- und Hardwarehersteller, Produkte für Linux zu entwickeln. Inzwischen ist Open Source ein anerkannter und oft benutzter Begriff, der für (fast immer) kostenlose, qualitativ hochwertige, frei verfügbare, modifizier- und weiter verbreitbare Software steht. Heute bedeuten die Begriffe Open Source und Freie Software das Gleiche.

Der Begriff „Freie Software“ umfasst im Kern die vier folgenden Freiheiten:

- Die Software darf eigenen Bedürfnissen angepasst werden.
- Die Software (Arbeitsweise) darf studiert werden.
- Die Software darf kostenlos kopiert und weiterverteilt werden.
- Die Software darf für jeden Zweck genutzt werden.



Hinweis:

Verwechseln Sie den Begriff „Freie Software“ nicht mit „Freeware“. Freeware ist zwar kostenlos erhältlich und frei verteil- und kopierbar, berechtigt Sie aber nicht, die Software eigenen Zwecken anzupassen oder sie zu verändern. Da bei Freeware kein offener Quelltext vorliegt, ist dies auch nicht möglich.

Einen zusammenfassenden Überblick über die vorgestellten Lizenzformen finden Sie in Tabelle 8.1. Zur besseren Übersicht wurden „Freeware“ und „Shareware“ als spezielle Untergruppe der proprietären Software dargestellt, da diese Lizenzformen keine Freie Software repräsentieren.

TABELLE 8.1 Übersicht über die gebräuchlichsten Lizenzformen⁴

	Kostenlos	Kopier- und weiter- verbreitbar	Unein- geschränkt nutzbar	Quelltext offen und modifizierbar	Unterliegt einer Lizenz
Freie Software	■	■	■	■	■
Open Source	■	■	■	■	■
Proprietäre Software	–	–	–	–	■
Freeware	■	■	–	–	■
Shareware	–	■	–	–	■

⁴ Tabelle aus [Gr09, Kap. 2.2.2].

Das Wissen, wann welche Lizenzbestimmungen bei welchem Softwareprodukt Anwendung finden, ist grundlegend für das Verständnis der im Unternehmen vorherrschenden bzw. einzusetzenden IT-Architektur.

Das Lizenzmodell⁵

Um beim Aufbau des Lizenzinventars die kaufmännische (erworbene) Software der technischen (installierten) korrekt zuordnen zu können, müssen Sie für jede einzelne Software das anzuwendende Lizenzmodell kennen und verstanden haben. Die Wahl des richtigen Modells kann Ihnen später erhebliche Kosten ersparen, die Wahl des falschen unnötige Kosten beschere. Die meisten Softwarehersteller tun jedoch alles, um die Nutzungsbestimmungen für ihr Produkt so auszuformulieren, dass der normale IT-Anwender seine liebe Mühe hat, dieses komplexe Geflecht zu verstehen.

Ein Lizenzmodell setzt sich unter anderem aus der Lizenzklasse, einem Lizenztyp und der Lizenzmetrik zusammen. Die Wahl des Lizenzmodells sollte sich deshalb an den individuellen Bedürfnissen und Gegebenheiten Ihres Unternehmens und des geplanten Software-Einsatzes orientieren (hierbei ist auch das Verständnis für die in Ihrem Unternehmen vorherrschende IT-Architektur sehr wichtig!). Die Kombinationsmöglichkeiten sind mittlerweile so vielfältig, dass sich viele Berater nur noch auf ein oder zwei Softwarehersteller spezialisiert haben, um ihre Kunden bei der Wahl des richtigen Lizenzmodells unterstützen zu können. Die häufigsten Spezialisierungen im Lizenzumfeld beziehen sich auf Microsoft-, Oracle- und SAP-Produkte.

Lizenzmodelle beeinflussen die rechtmäßige Softwarenutzung in Form folgender Faktoren:

- durch die Lizenzart (z. B. Einzellizenz, Mehrplatzlizenz);
- durch die Lizenzklasse (z. B. Vollversion, Upgrade Version);
- durch den Lizenztyp (z. B. pro Gerät, pro gedruckte Seite);
- durch die Lizenzmetrik, mit der man festlegt, wie gezählt wird (z. B. gilt die Lizenz für 5000 gedruckte Seiten pro Monat oder für 1000 zu verwaltende Systeme);
- durch die Lizenzbindungen bzw. Lizenzbeschränkungen (z. B. Einsatz auf einem Gerät mit maximal zwei CPU-Kernen oder auf einer bestimmten Hardwareumgebung);
- durch das Beschreiben von Weitergabeverboten (beispielsweise das einer OEM-Lizenz) sowie von Veräußerungs- und Vermietverboten;
- durch das Beschreiben bzw. Bestimmen von Laufzeiten der Softwarenutzung (begrenzt, unbegrenzt).



Tipp:

Überprüfen Sie in regelmäßigen Abständen, ob das ausgewählte Lizenzmodell noch Ihren Anforderungen und Gegebenheiten entspricht oder einer Anpassung bedarf.

⁵ Eine ausführlichere und umfassendere Beschreibung der Lizenzmodelle finden Sie in [Gr09].

■ 8.3 Der Software-Life-Cycle-Prozess und seine Bestandteile

In den meisten Unternehmen gibt es kaum noch einen Geschäftsablauf, der ohne die Unterstützung durch Computer auskommt. Damit die Computer funktionieren und den Geschäftsablauf steuern können, benötigt man Software. Aufgrund der Schnelligkeit der Entwicklungszyklen und der rasanten Weiterentwicklung der Hardware unterliegt Software einem festgelegten Lebenszyklus, „Software Life Cycle“ genannt, der mit der Beschaffung beginnt und mit der Entsorgung der Software endet.

Für das Betreiben eines funktionierenden Lizenzmanagements ist es eine ganz zentrale Voraussetzung, dass die Abläufe im Software-Life-Cycle-Prozess aufeinander abgestimmt sind. Dabei kristallisiert sich immer wieder das gleiche Problem heraus. In den meisten Unternehmen existieren zwar Prozessabläufe und Richtlinien, um auch noch die kleinste Büroklammer inventarisieren zu können – um es einmal etwas überspitzt zu formulieren – doch bei dem mittlerweile sehr kostbaren Wirtschaftsgut „Software“ sucht man solches oft vergeblich.

In Ansätzen gibt es Prozesse für die Beschaffung und Bestellung von Software, da hier der Einfachheit halber der schon existierende Beschaffungsprozess für Non-IT-Güter etwas umgewandelt mitbenutzt wird. Die Folgen sind bekannt: Es gibt keinen ausreichenden Überblick über die im Haus befindliche und genutzte Software, es herrschen meist König Chaos und Königin Intransparenz, sowie der Wirtschaftsminister Carlos Teuer. Ambitionen in Richtung Vereinheitlichung und Standardisierung von Software werden im Ansatz steckenbleiben, da beispielsweise keiner die Frage beantworten kann, wie viele unterschiedliche Grafiksoftware-Produkte im Unternehmen eingesetzt werden, und so Versuche, sich eventuell auf ein oder zwei Standardprodukte einigen zu können, bereits im Vorfeld scheitern.

Der Software-Life-Cycle-Prozess setzt sich aus sechs Hauptprozessen zusammen, wobei drei davon der Beschaffung – dem kaufmännischen Teil – und drei dem Betrieb – dem technischen Teil – zuzuordnen sind. In der Abbildung 8.2 sehen Sie die sechs Prozesse im Überblick.

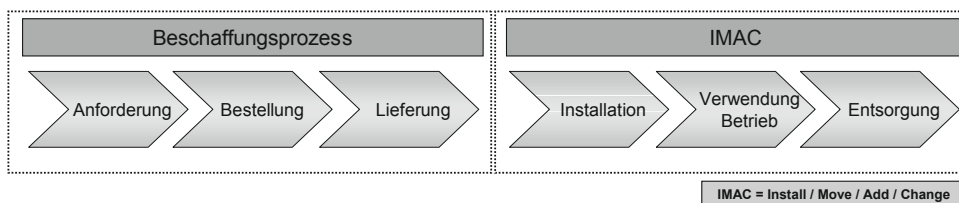


ABBILDUNG 8.2 Überblick der Software-Life-Cycle-Hauptprozesse, die sich in die beiden Bereiche „Beschaffungsprozess“ und „IMAC-Prozess“⁶ unterteilen

- Der **Beschaffungsprozess** setzt sich zusammen aus:
 - dem Anforderungsprozess;
 - dem Bestellprozess;
 - dem Lieferprozess.

⁶ IMAC = Install, Move, Add, Change

Die **IMAC-Prozesse** (technische Prozesse) bestehen aus:

- dem Installationsprozess;
- dem Verwendungs- und dem Betriebsprozess;
- dem Entsorgungsprozess.

Zu jedem dieser sechs Hauptprozesse gehören weitere Teilprozesse, wie Abbildung 8.3 exemplarisch zeigt (die Teilprozesse können je nach Unternehmenssituation variieren).

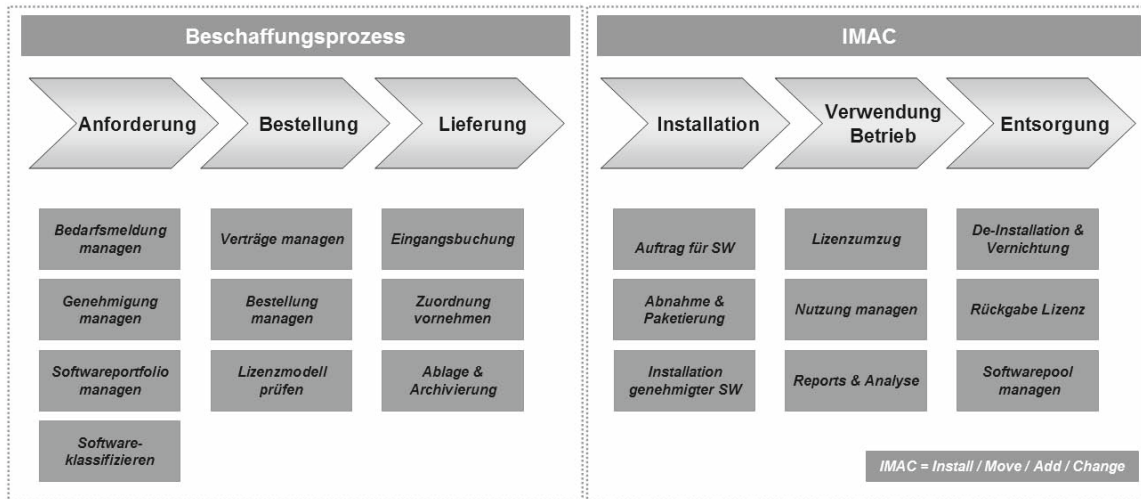


ABBILDUNG 8.3 Haupt- und Teilprozesse im Software-Life-Cycle-Prozess

Zum Beschaffungsprozess gehören das Verwalten und Optimieren von Verträgen wie Rahmenverträge, Einzelverträge, Bestellungen, Wartungsverträge für Software, aber auch für Hardware (beispielsweise Computer mit OEM-Lizenzen) sowie Services, Anforderungen, Lieferungen und natürlich auch das Verwalten und Optimieren der Verträge (Preis, Volumen, Lizenzmodelle, Lizenzmetriken) mit den Herstellern und Lieferanten. Sehr hilfreich können dabei Vertragsmanagementsysteme sowie andere Systeme sein, in denen die Beschaffungsvorgänge dokumentiert werden.

Meistens sind in einem Unternehmen aufgrund der Historie mehrere Systeme zu finden, die Daten meist über Schnittstellen austauschen und die benötigten Informationen vorhalten bzw. verwalten. Durch die gewachsenen Strukturen und Systeme werden die für den Ablauf erforderlichen Prozesse selten auf den Prüfstand gestellt, um eventuell Optimierungspotenzial ausfindig machen zu können.

Die technische Seite, quasi der Betrieb der beschafften Software (IMAC), reicht von der Installation (dazu gehört die Software-Identifikation, Software-Kennzeichnung, Zuordnung zu kaufmännischen Artikeln mit Materialnummern) über die Verwendung (der eigentliche Nutzungszeitraum der Software) mit den Zuordnungen zu Systemen, um die Compliance herstellen zu können (Abgleich kaufmännischen Daten mit technischen Daten), bis zur Verschrottung von Hardware und der damit einhergehenden De-Installation von Software. Abhängig von ihrer Unternehmensgröße ist es u. U. sinnvoll, sich von Zeit zu Zeit zu fragen, ob denn die momentan im Unternehmen „gelebten“ Prozesse noch effektiv und dem Unternehmensziel optimal angepasst sind.

Für ein korrektes Lizenzmanagement ist ein umfassender Überblick über alle jemals im Unternehmen beschafften Softwareprodukte unbedingt erforderlich. Dabei bietet sich ein pragmatisches Vorgehen an. Sie können nicht erwarten, bei einem Unternehmen mit Zehntausenden von Computern und Serversystemen und Hunderten im Einsatz befindlicher Softwareprodukte eine dauerhafte Compliance über alle Softwareprodukte zu erhalten. Hier müssen Sie sich zu Beginn der Aufgabenstellung „Erstellung einer Compliance“ einen Fahrplan zurechtlegen, um erst einmal beispielsweise die Top-20-Hersteller bzw. Lieferanten und deren im Einsatz befindliche Softwareprodukte zu überprüfen.

**Tipp:**

Wenn Sie planen, ein Lizenzmanagement-Tool einzusetzen und sich davon eine wirkungsvolle Unterstützung erhoffen, müssen Sie im Vorfeld die bestehenden Software-Life-Cycle-Prozesse einer Ist-Analyse unterziehen, um mögliches Optimierungspotenzial aufzeigen zu können. In einem zweiten Schritt sollte dann der Software-Life-Cycle-Prozess mit den heutigen Anforderungen im Unternehmen auf den Prüfstand gestellt werden. Denn das Lizenzmanagement-Tool sollte zu den Prozessen des Unternehmens passen und nicht das Unternehmen zu den (eventuell sehr starren) Prozessabläufen des Tools.

Viele Unternehmen haben die Anforderungs- und Beschaffungsprozesse für „Non-IT“-Güter recht gut im Griff. Schauen wir in die Softwareecke, sehen wir dort meist ein mehr oder minder großes Durcheinander. Der Grund: Früher wurde Software einfach mit dem Computer eingekauft, und keiner kümmert sich explizit darum, sie zu verwalten, geschweige denn, ein Lizenzmanagement einzurichten. Oft können auch die Mitarbeiter im Prinzip ihre Wünsche äußern, ohne dass auf die strategische Ausrichtung von Software im Unternehmen Rücksicht genommen werden muss. Hier sammeln sich dann sehr schnell die verschiedensten Softwareprodukte an, oft mit gleichen Funktionen. Ehe Sie zweimal blinzeln können, ist Ihr Unternehmen ein gewaltiger Software-Zoo. Aufwendige und komplexe Prozesse sowie gewachsene Einkaufsstrukturen, die das Thema Softwarebeschaffung eigentlich nur nebenbei als Aufgabe sehen, sind oft daran nicht ganz unschuldig.

Durch die Optimierung der Anforderungs- und Beschaffungsprozesse können Sie

- eine Erhöhung der Transparenz über Ihren Softwarebestand erreichen;
- die rechtliche Compliance gewährleisten;
- unter Umständen parallele Bestellungen vermeiden und damit doppelte Kosten verhindern sowie sicherstellen, dass die vereinbarten Einkaufskonditionen unternehmensweit angewendet und genutzt werden.



So erreichen Sie diese Ziele:

- Erstellen Sie sich ein Konzept, um die bestehenden Beschaffungswege zu vereinheitlichen, und legen Sie damit den Grundstein für eine einheitliche und zentrale Software- und Lizenzbeschaffung.
- Reduzieren Sie möglichst die bisherigen Beschaffungsprozesse auf ein notwendiges Minimum.
- Erstellen Sie eine einheitliche und unternehmensweit gültige Richtlinie für Ihre künftigen Beschaffungsprozesse.
- Legen Sie neue Rollen und Verantwortlichkeiten in Bezug auf die künftigen Beschaffungsprozesse fest.

Um diesen Dingen gezielter auf den Grund gehen zu können, empfehle ich Ihnen aber, alle Ihre Prozesse im Software-Life-Cycle auf den Prüfstand zu stellen und durch ein Benchmarking zu überprüfen, beispielsweise mit einer Reifegradanalyse (weitere Informationen siehe [Gr09]).

■ 8.4 Der Lizenzmanager und verwandte Rollen

Um das Lizenzmanagement betreiben und im Unternehmen umsetzen zu können, sind neue Rollen und Verantwortlichkeiten erforderlich, die häufig erst neu eingeführt und besetzt werden müssen.

Kein Schiff kommt ohne Kapitän und Steuermann aus, um nur die beiden wichtigsten Personen zu nennen. Um Lizenzmanagement zu etablieren und auch betreiben zu können, benötigen Sie mindestens die Rolle eines Kapitäns, der gleichzeitig Steuermann sein kann: einen Lizenzmanager (m/w).

Bei der Einführung eines Lizenzmanagements und im Betrieb desselben entstehen vielfältige neue Aufgaben und Verantwortlichkeiten. Dafür sollten Sie motivierte Mitarbeiter wählen, die eine gewisse Affinität zu IT-Themen haben – hier im Speziellen – zum Thema Hard- und Softwareasset-Verwaltung. In vielen Unternehmen werden sie diese Herausforderungen neben ihrem normalen Tagesgeschäft übernehmen müssen, denn nicht alle Unternehmen sind in der Lage und willens, sich eine eigene Abteilung für das Lizenzmanagement zu leisten. Ab einer bestimmten Unternehmensgröße ist aber genau das zu empfehlen.

Weil es schon immer Softwareprodukte unterschiedlicher Couleur für den Einsatzbereich Desktop (Client), Server und Hostbereich gab und auch deren Lizenz- und Nutzungsbedingungen teilweise stark voneinander unterscheiden, ist es sicherlich sinnvoll, jeweils speziell für diese (ich nenne sie „Objekttypen“) verantwortliche Lizenzmanager zu bestimmen. Denn jeder hat in seinem Bereich Softwareprodukte, die mit eigenen Nutzungsbedingungen für den jeweiligen Objekttyp ausgestattet sind und von der Komplexität her (ich nenne als Beispiel nur die IBM-Lizenzbestimmungen) teilweise so umfangreich sind, dass eine Spezialisierung pro Objekttyp auch in Hinsicht auf die zu verantwortende IT-Architektur zu empfehlen ist.

Die Rolle Lizenzmanager kann sich noch einmal je nach Erfordernis und Unternehmensgröße in die Rolle globaler und lokaler Lizenzmanager aufteilen. Die Verantwortung können Sie hier beliebig aufteilen und auch Ihre bisherigen Organisationsstrukturen darin abbilden.

Der Rolle Lizenzmanager stellt man für gewöhnlich (auch abhängig von der Größe des Unternehmens) noch die Rolle Lizenzadministrator und die Rolle Produktverantwortlicher zur Seite. Dieses Dreiergestirn verantwortet und betreibt in der Regel das Lizenzmanagement im Unternehmen. Bei besonderen Konstellationen (z. B. in internationalen Umgebungen) können durchaus noch weitere Rollen oder Rollenebenen hinzukommen.

Betrachten wir als Erstes die Rolle des Lizenzmanagers. Aus der Historie heraus wird die Rolle des Lizenzmanagers (LzM) häufig in den Einkauf bzw. in die Beschaffungsstellen integriert, da dieser Unternehmensbereich an vielen kaufmännischen Entscheidungen beteiligt ist.

Die Rolle Lizenzmanager

Der Lizenzmanager besitzt die strategische Verantwortung und hat folgende Aufgaben; er

- steuert und überwacht die Lizenzbeschaffung für alle Objekttypen (Client, Server, Host);
- unterstützt die Fachabteilungen bei der strategischen Softwarebedarfsplanung;
- formuliert Richtlinien, Maßnahmen und Kontrollmechanismen für den Umgang mit Lizenzen und agiert gemäß den Lizenzmodellen (z. B. Vermeidung von Peaks zum Stichtag der Lizenzzählung);
- begleitet Software-Audits (intern sowie extern) und stellt die hierfür benötigten Auskünfte und Bestandslisten bereit;
- verantwortet die Berichtserstellung zum Lizenzierungsstatus für das Management;
- plant und initiiert Maßnahmen zur Verbesserung der Lizenzmanagement-Prozesse;
- kontrolliert die nachhaltige Umsetzung des kontinuierlichen Verbesserungsprozesses aus den erforderlichen Lizenzmanagement-Maßnahmen;
- stellt Daten und Reports aus dem Lizenzmanagement-Tool für zukünftige Vertragsverhandlungen zur Verfügung;
- stellt Daten für die Bedarfsplanung der Fachbereiche/Geschäftsbereiche hinsichtlich der Plan- und Ist-Kosten zur Verfügung.

Dem Lizenzmanager können/sollten im Umfeld des Lizenzmanagements noch zwei weitere Rollen zur Seite gestellt werden: ein Lizenzadministrator und ein Produktverantwortlicher.

Die Rolle Lizenzadministrator

Der Lizenzadministrator besitzt die kaufmännische und technische Verantwortung. Er

- verantwortet Daten, Bestände und Merkmale seines Objekttyps sowohl aus technischer als auch kaufmännischer Sicht;
- führt Lizenzprüfungen durch und überwacht die Einhaltung der Nutzungsrechte;
- überprüft die ausreichende und korrekte Lizenzierung vor geplanten Softwareinstallationen und verwaltet die lokalen Software-Pools;
- verantwortet die Einleitung von Maßnahmen aus dem Compliance-Report gegen Über- und Unterlizenzierung;
- erstellt Berichte und setzt gestellte Reportinganforderungen um;

- löst Beschaffungen aus, gibt Lizenzen frei oder reserviert diese;
- verwaltet Lizenzscheine und Lizenzkeys, sofern diese lokal archiviert werden;
- steuert Lizenzen bei Veränderungen an seinen Systemen (Neuinstallation, Umzug, Verschrottung).

Die Rolle Produktverantwortlicher

Der Produktverantwortliche übernimmt die technische Verantwortung für seine Produkte entweder nur in seinem Fachbereich oder unternehmensweit, beispielsweise für alle SAP-, IBM- oder Microsoft-Produkte. Die Aufteilung ist auch hier jeweils abhängig von der konkreten Unternehmenssituation. Zu seinen Aufgaben kann Folgendes gehören: er

- erstellt Vorgaben für die Paketierung und Softwareverteilung;
- synchronisiert den Installationspaketnamen mit dem entsprechenden Softwareprodukt auf der kaufmännischen Seite (Zuordnung in einem Produktkatalog des Lizenzmanagement-Tools wie beispielsweise die SAP-Materialnummern mit der Installations-Materialnummer);
- steuert und kontrolliert die Wareneingänge in seinem Fachbereich;
- sammelt die Lizenzscheine, Lizenzkeys und Lizenzmedien und gibt sie an eine zentrale Archivierungsstelle weiter (physische Medien);
- gibt Informationen zur Verwaltung von Named-User-Lizenzen an das Lizenzmanagement weiter;
- überwacht die marktüblichen Lizenzmodelle auf Veränderungen bei seinen Produkten;
- berichtet an den Lizenzadministrator Neuerungen oder Änderungen seiner Produkte;
- arbeitet dem Lizenzmanagement bei einer strategischen Softwareplanung zu;
- steuert die Einteilung, Zuordnung und Klassifizierung der Softwareprodukte (z.B. eCI@ss-Kategorien).

Der Produktverantwortliche berichtet dabei an den Lizenzadministrator seines jeweiligen Objekttyps.

■ 8.5 Welche Daten sind für das Lizenzmanagement erforderlich?

Diese Frage ist nicht so einfach zu beantworten. Aufgrund der gestiegenen Komplexität sowohl im Bereich der Erfassung von technischen Daten (Inventory-Scan) als auch bei der Verwaltung der kaufmännischen Daten (umfangreiche, individuelle und komplexe Lizenz- und Nutzungsbedingungen der Hersteller) wachsen die Anforderungen an ein Lizenzmanagement stetig und sind noch dazu sehr dynamisch. Keine der mir derzeit bekannten Lizenzmanagement-Lösungen kann wirklich alle möglichen Konstellationen von Lizenzmetriken abbilden. Im Gegenteil, es kommt oft vor, dass nicht einmal der Softwarehersteller seine eigenen Lizenzmetriken (wie gezählt wird) versteht, wohl deshalb, weil sich der Vertrieb bzw. das Marketing, wo

bekanntlich am wenigsten Techniker anzutreffen sind, die Lizenzmodelle und Lizenzmetriken ausdenken. Kommen spezielle und individuelle Sondervereinbarungen, die beispielsweise eine sonst übliche Zählweise der Nutzungsbedingungen außer Kraft setzen, hinzu, können Sie erahnen, welche Artenvielfalt eine Lizenzmanagement-Lösung verwalten muss. Einige Tools können das sehr gut und sind auch für neue Aufgabenstellungen flexibel, andere scheitern schon daran.

Im Grunde klingt es eigentlich recht einfach: Das Lizenzmanagement hat die Aufgabe, die tatsächlich installierten Softwareprodukte (technisches Ist) mit den tatsächlich erworbenen (gekauften) Lizenzen (kaufmännisches Ist) abzugleichen und einen sogenannten Compliance-Report zu erstellen. In der Regel zeigt dieser Report – pro Softwareprodukt – entweder eine Überlizenzierung auf (Sie haben dann zu viel gekauft) oder eine Unterlizenzierung (mehr Softwareinstallationen als erworbene Lizenzen). Eigentlich kommt immer sowohl das eine wie das andere vor. In welchem Spielraum sich beide bewegen, hängt auch von der Qualität der bisherigen Software-Life-Cycle-Prozesse und der erhobenen und verarbeiteten Quelldaten ab.

Die technischen Daten

Das Lizenzmanagement-Tool muss in der Lage sein, über Schnittstellen technische und kaufmännische Daten aufzunehmen. Dies bedeutet eine Anbindung an Ihre bestehenden Inventory-Systeme (technischer Scan der Clients und Server) und eine Anbindung an Ihre kaufmännischen Systeme (mit Bestell-, Vertrags- und Artikeldaten). Eine Besonderheit ist bei der Erfassung der technischen Daten hervorzuheben. Das Lizenzmanagement kann nur namentlich identifizierte Softwarekomponenten aus dem technischen Datenbestand mit den kaufmännischen Bestands- und Bewegungsdaten abgleichen. Das bedeutet, entweder muss das Inventory-System bereits eine aus den eingesammelten Rohdaten übersetzte „lizenzrechtlich lesbare“ Softwareliste erstellen können, oder die Lizenzmanagement-Lösung muss dazu in der Lage sein (schon wieder eine Anforderung an das Tool). Die Systeme, entweder Scanner oder Lizenzmanagement-Tool, müssen nämlich für das Lizenzmanagement nicht verwendbare Daten, wie z.B. Patches, Hotfixe, Add Ons, Open-Source- oder Freeware-Produkte zumindest kennzeichnen können oder bestenfalls komplett ausfiltern. Eine weitere wichtige Aufgabe besteht darin, den gefundenen „*.exe-Dateien“ zu entnehmen, ob es sich beispielsweise um eine einzelne Installation von Microsoft Access oder um ein Access aus der Office-Professional-Suite handelt. Denn nur mit eindeutigen Installations-„Zahlen“ kann das Ergebnis gegen die kaufmännischen „Zahlen“ abgeglichen werden.

Beachten Sie, dass das Lizenzmanagement primär die Frage zu beantworten hat, ob das Unternehmen in Sachen Software rechtlich und gegenüber dem Hersteller in Compliance ist. Dabei sind nur die lizenzkostenpflichtigen Softwareprodukte und deren richtige Zählweise entsprechend den vereinbarten Nutzungsbedingungen von Bedeutung.

Die kaufmännischen Daten

Jetzt kommt der kaufmännische Part. Damit der Compliance-Report richtige Zahlen wiedergeben kann, muss die Lizenzmanagement-Lösung die Daten aus den Verträgen (die eingegangenen Nutzungs- und Lizenzbedingungen) korrekt anwenden können. Es muss also bekannt sein, ob ein 1:1 Abgleich möglich ist (eine technische Softwareinstallation repräsentiert eine kaufmännische Lizenz) oder ob noch andere Faktoren hineinspielen. Ich erinnere hier nur an das Zweitkopierrecht, bei dem ein Hauptbenutzer mit einem Desktop-PC noch das Recht

besitzt, auf einem tragbaren Computer (meist Laptop) eine zweite Kopie von Office zu installieren, ohne dass diese beim Zählen der Installationen mitgerechnet werden muss. Hier haben Sie bereits die nächste Komplexitätsstufe (und noch nicht die letzte!) bei der Auswertung der Daten.

Bei der Erfassung der kaufmännischen Daten wird es nicht ganz so komplex, weil die Aufgabe hier eigentlich nur darin besteht, die vereinbarten Nutzungsbedingungen (Zählweisen auch Lizenzmetrik genannt) und die entsprechenden erworbenen Lizenzrechte (gekaufte Mengen) abzubilden. Aber auch hier kann sich der Arbeitsaufwand schnell vervielfachen. Im Vorfeld sollten Sie also prüfen, ob die nachfolgend aufgeführten beispielhaften Punkte bei der Erfassung der kaufmännischen Lizenz- und Nutzungsdaten in Betracht zu ziehen sind.

Folgende Fragen sollten Sie sich zur Erfassung der Lizenz- und Nutzungsdaten stellen:

- Wie viele Verträge existieren jeweils von einem Lieferanten zu einem Produkt/Produktgruppe – pro Unternehmensstandort oder auch übergreifend?
- Fehlen eventuell Verträge aus anderen Unternehmensstandorten?
- Sind alle abgeschlossenen Verträge in einem zentralen Einkaufs- oder Vertragsmanagementsystem erfasst?
- Wie lässt sich eine Identifikation der zu jedem Softwarevertrag gehörenden Softwareprodukte gewährleisten?
- Existieren Softwareverträge und Einkaufsabschlüsse möglicherweise nur in Papierform? Muss deshalb Schrankware⁷ in erheblichem Umfang nacherfasst werden?
- Wie soll die Nacherfassung abgewickelt werden und durch wen?⁸
- Welcher Stichtag wäre für die Erstellung des Lizenzinventars festzulegen (beispielsweise der Windows 7 Rollout o. a.)?

Welche Problematiken könnten noch in Betracht kommen?

- Es können teilweise mehrere Einzelverträge zu einem Hersteller/Lieferanten mit ähnlichen Inhalten zu unterschiedlichen oder gleichen Konditionen existieren.
- Die Vertragsdetails sind nur wenigen Mitarbeitern bekannt.
- Das vorhandene Kopfwissen der Vertragsverantwortlichen ist nirgends erfasst.
- Ihr Einkaufs- oder Vertragsmanagementsystem ist nicht an allen Unternehmensstandorten verfügbar, d. h. es ist zu klären:
 - Wo werden Verträge und Einkaufsabschlüsse von den Standorten verwaltet, die keinen Zugriff auf das zentrale Einkaufs- bzw. Vertragsmanagementsystem haben?
 - Welcher Geltungsbereich wurde für die Verträge und Einkaufsabschlüsse definiert?
 - Welche Produkte von welchem Lieferanten?
 - Wer hat wo wie viel im jeweiligen lokalen Unternehmensstandort eingekauft?
 - Wenn es ein autonomes lokales Einkaufs- und Vertragsmanagementsystem gibt: Kann es, wie gewünscht, ausgewertet werden?
 - Haben Sie dafür genügend Ressourcen? Wer steuert sie, wer überwacht?

⁷ Als Schrankware werden Informationen zu Bestellungen und Verträgen bezeichnet, die noch nirgends elektronisch erfasst wurden, aber wichtig sind.

⁸ Hier ist ein besonderes Augenmerk auf die notwendige Historisierung zu legen (Abbildung von Upgrade Pfaden).

Die Aufzählung ist bei Weitem nicht vollständig, und es gibt eine Fülle weiterer möglicher Komplexitätstreiber, die je nach Unternehmenssituation entstehen können und betrachtet werden müssen.

Einen beispielhaften Auszug der notwendigen Informationen, die das Vertragsmanagement (meist in einem Lizenzmanagement-Tool mit integriert) abbilden sollte, präsentiert die folgende Aufzählung. (Auch wenn Sie bereits Vertragsdaten in einem Ihrer Systeme verwalten, werden Sie einige der unten aufgeführten Felder in Ihrem System nicht vorfinden. Bestenfalls sind diese für das kaufmännische Lizenzinventar wichtigen Informationen in einem an den Datensatz angehängten Dokument zu finden. Für das Lizenzmanagement ist es aber wichtig, genau diese Informationen elektronisch auswerten zu können.)

- Der Vertragskopf sollte bestehen aus:
 - Vertragsstatus (aktiv, inaktiv, in Bearbeitung)
 - Vertragsart (z. B. Software-Kauf)
 - Vertragsnummer
 - Vertragsname (Titel),
 - Vertragskategorie (Lizenzen, Wartung, Dienstleistung)
 - Vertragsnehmer
 - Vertragsgeber
 - Verantwortlicher Ansprechpartner Einkauf
 - Lieferant
 - Gültigkeitsbereich (z. B. > 50% Beteiligungsverhältnis) des Vertrages
 - Vertragslaufzeit (in Monaten)
 - Gültig ab, Gültig bis
 - Kündigungsfristen (Zeitraum z. B. 90 Tage)
 - Vertragssprache (z. B. Deutsch)
 - Anwendbares Recht
 - Gerichtsstand
- Der Teil für die Softwarelizenzinformationen sollte beinhalten:
 - Einsatz für welches Umfeld (Client, Server, Mainframe)
 - Einsatz zulässig auf Plattform (beispielsweise in Win-32- oder Win-64-Umgebungen sowohl Client als auch Server, Mac OS, Linux)
 - Name des Softwareproduktes
 - Version des Softwareproduktes
 - Einsetzbare Produktsprache für die Software
 - Produktgruppe (z. B. Datenbanksoftware, Datensicherung, Grafiksoftware), am besten eCl@ss verwenden⁹
 - Downgrade-fähig (darf für ein aktuelles Softwareprodukt z. B. Office 2007, auch ein älteres Softwareprodukt, z. B. Office 2003, eingesetzt werden?)

⁹ Weitere Informationen zur eCl@ss siehe im Internet unter www.eclass.de

- Lizenzklasse (Vollversion, Update)
- Lizenztyp (z. B. pro Gerät, pro User, pro Named User u. a.)
- Lizenzmetrik (z. B. gezählt wird pro CPU, pro Gerät u. a.)
- Wartungslaufzeit
- Wartung gültig ab, gültig bis
- Wartung Kündigungsfristen
- Nebenabreden
- Zusatzleistungen Vertragsgeber, Vertragsnehmer

Im nächsten Schritt müssen Sie dafür sorgen, dass die vorhandenen kaufmännischen Daten aus Ihren vorhandenen Systemen bzw. auch mögliche manuelle Daten und Informationen (Schränkware) korrekt im Lizenzmanagement-Tool erfasst werden. Nur so können Sie gewährleisten, dass die Zahlen aus dem zukünftigen Compliance-Report auch belastbar sind. Das Erfassen der notwendigen Informationen kann sich allerdings aus den unterschiedlichsten Gründen schwierig gestalten: Vielleicht gibt es in Ihrem System keine Sicht auf die Metadaten der Softwareverträge. Oder Bestandsdaten lassen sich nur schwer zusammenführen und konsolidieren, weil die Vertragsinformationen dezentral aufbewahrt und verwaltet werden. Und das sind nur zwei von vielen möglichen Hindernissen. Der nächste Abschnitt widmet sich deshalb der Erkennung und Bearbeitung möglicher Komplexitätstreiber.



Tipp:

Um nicht in einem Meer an Arbeit zu versinken, versuchen Sie am besten nicht, sofort alle Softwareprodukte und Verträge aufzunehmen. Das wäre in der ersten Phase überhaupt nicht zielführend. Legen Sie sich beispielsweise eine Top-10-Liste zurecht. Suchen Sie sich die 10 wichtigsten Verträge und/oder Produkte aus, und lassen Sie sich dabei von den Preis- und Stückzahlvolumen leiten. Sind die Top 10 abgearbeitet, können Sie sukzessive diese Liste erweitern, bis Sie irgendwann möglichst alle Softwareverträge und Produkte erfasst haben.

■ 8.6 Komplexitätstreiber im Lizenzmanagement

„Lizenzmanagement aufbauen und betreiben, unser Herr Meier ist da sehr kompetent, der macht das schon.“ So oder so ähnlich werden viele Mitarbeiter plötzlich vor eine Aufgabe gestellt, die für sie vollkommen neu und mit keinem ihnen bekannten Arbeitsstil oder Arbeitsmittel umsetzbar ist. Doch nicht nur die Mitarbeiter sehen sich einem für sie völlig neuen Thema gegenüber. Häufig unterschätzen auch die verantwortlichen Manager die Dimension des Themas, und erst recht rechnet niemand damit, dass es auch hier Komplexitätstreiber zu berücksichtigen gilt.

Aber was macht Lizenzmanagement so komplex?

Komplexitätstreiber gibt es in vier Kernbereichen zu beachten, und jeder Kernbereich hat wiederum weitere ihm zugeordnete Komplexitäten:

- Rollen
 - Komplexe Organisationsstrukturen
 - Organisatorische Hierarchien
 - Ressourcen
- Prozesse
 - vielfältige Beschaffungswege
 - Ablage der Lizenznachweise (Datenträger, Lizenzkeys)
 - Vielfältige Beschaffungssysteme, Vertragsmanagement, Software-Verteilung, CMDB u. a. m.
 - Asset-, Vertrags-, Beschaffungs-, Produktdaten
 - Komplexe und heterogene Datenstrukturen
 - Spezialbereiche (Testumgebungen)
- Verträge
 - Komplexe Lizenzbestimmungen (Unterschiede bei Client und Servern)
 - Versionswechsel einer Software (Update- und Downgradespezifika)
 - Komplexe und vielfältig abzubildende Lizenzmetriken
 - Abbildung der IT Architektur zu den erworbenen Nutzungsrechten
 - Geltungsrechte bei Wartung, Unterschiede bei Clients, Server
 - Vertragshierarchien (mehrere Verträge mit unterschiedlichen Bedingungen)
 - Wartungsverträge (unterschiedliche Laufzeiten, Vermischung von Lizenzen mit und ohne Wartung)
 - Abbildung der Vertragshistorie (Wechsel von Lizenzbedingungen und Lizenzmetriken)
- Schnittstellen
 - Vielfältige Systemlandschaften
 - Zu beachtende IT-Architekturen wie z.B. Client, Server, Terminal Server, Virtual Maschine-Umgebungen
 - Hohe Schnittstellenstrukturen zwischen unterschiedlichen Systemen
 - Vorherrschende Qualität der Daten (kann gut oder schlecht sein)

Damit Sie einigermaßen den Überblick behalten und auch eine Bewertung der identifizierten Komplexitätstreiber in den vier Kernbereichen durchführen können, sollten Sie diese jeweils pro Kernbereich in einem Steckbrief beschreiben. Damit können Sie in einer gewissen Weise Risikomanagement für das Lizenzmanagement-Projekt betreiben, indem Sie Prioritäten für die Aufarbeitung der Komplexitätstreiber vergeben.

Wie ein solcher Steckbrief aufgebaut werden sollte, veranschaulicht Ihnen das nachfolgende Beispiel in Tabelle 8.2.

Beispiel: Eine Abbildung von Vertragshistorien ist notwendig bzw. erforderlich.

TABELLE 8.2 Komplexitätstreiber – Steckbrief

Name des Treibers	Berücksichtigung der Vertragshistorie
Warum dies ein Treiber ist (kurze Begründung)	Verträge werden in unterschiedlichen Systemen gehalten, die Informationen für das Recherchieren von Basislizenzen sind teilweise nicht oder nur rudimentär erfasst. Es ist keine Trennung zwischen Softwareverträgen und Wartung erkennbar.
Grund/Ursache für den IST-Zustand	Verträge werden von unterschiedlichen Fachbereichen (Einkauf/Rechtsabteilung/Vertragsmanagement) in unterschiedlichen Systemen abgelegt. Wartungsverträge sind oft nicht identifizierbar.
Abhängigkeiten von welchen Stakeholdern	Hersteller/Lieferant Einkauf Vertragsowner Fachbereiche
Grad der Komplexität (Stufe 1–5)	Hohe Komplexität (Stufe > 3)
Priorität der Aufarbeitung (A1–C3)	A1

**Tipp:**

Wenn Sie sich aus den einzelnen erkannten Komplexitätstreibern z. B. eine Excel-Matrix erstellen, können Sie daraus auch für das Management und die beteiligten Projektmitglieder eine Übersicht erstellen, in der beispielsweise u. a. der kritische Pfad abbildbar ist.

■ 8.7 Der Einfluss der IT-Architektur auf das Lizenzmanagement

Früher war alles anders: Da gab es ein großes Rechenzentrum mit viel Hardware, die kaum geändert wurde, außer wenn einmal der Speicherplatz knapp wurde. Änderungen an der Konfiguration (z.B. CPU Erweiterung) gab es kaum. Somit war die bestehende IT-Architektur lange Zeit gar nicht bzw. nur selten irgendwelchen Änderungen unterworfen, weder in Hinblick auf die verwendete Hardware noch auf die betriebene Software.

Heute macht die Dynamik der IT-Entwicklungen selbst vor Rechenzentren nicht halt. Allein die rasante Verbreitung von Virtualisierungstechnologien macht eine permanente Anpassung der bestehenden IT-Architektur notwendig. Oft wird bei diesen Hardwareoptimierungen zum Zwecke der Betriebskostensenkung aber die jeweilige Architektur Einfluss auf die Lizenzierung der eingesetzten Software haben.

Noch komplexer wird das Ganze, wenn ein Provider für Sie die Server-Infrastruktur betreibt bzw. bereitstellt und Sie die Software beistellen. Denn dann müssen Sie ständig dafür Sorge tragen, dass mögliche Veränderungen an der Hardware (beispielsweise werden weitere CPUs im Server eingebaut, oder die VMware-Umgebung wird auf ein anderes physikalisches System verschoben) mit den Nutzungsbedingungen der darauf betriebenen Softwareprodukte im Einklang stehen.

Ein Beispiel dazu: Sie oder Ihr Provider betreiben einen Server, auf dem z. B. eine Datenbank von IBM im Einsatz ist (DB2). Das IBM-Lizenzmodell für die Nutzung einer Vollversion einer DB2-Datenbank wird nach der Lizenzmetrik PVU (Prozessor Value Unit) berechnet. IBM gibt hierfür bestimmte Bedingungen vor, nach dem sich dieser PVU-Faktor für bestimmte Hardware-Technologien bestimmt.¹⁰ So hat ein Server der Marke „Hewlett Packard Proliant ML 330 G6“ mit dem Prozessor Type „Intel Xenon“ gemäß der IBM-Liste einen PVU-Faktor von 50. Je nachdem, ob Sie nun einen DualCore oder QuadCore im Einsatz haben, wird dieser Wert mal zwei oder mal vier genommen. Damit ergibt sich, dass Sie für den Einsatz einer DB2-Datenbank auf einem dieser Server entweder 100 PVU oder 200 PVU „kaufen“ müssen. In diesem Fall müssen Sie also das komplette „Blech“ lizenzieren.

Jetzt könnte ja jemand auf die Idee kommen (das könnte auch Ihr Provider sein, da dieser ja ein erklärtes Interesse daran hat, Kosten zu sparen), auf diesem physikalischen Server eine VMware-Umgebung aufspielen zu lassen, um mehrere virtuelle Server und Datenbanken betreiben zu können. Jeder VMWare-Instanz wird nun nur noch jeweils ein Prozessor zugewiesen; damit werden also auch weniger PVU-„Punkte“ – lizenzrechtlich gesehen – verbraucht.

Ganz so einfach, wie es sich vielleicht technisch darstellt, lässt sich der mögliche Lizenzverbrauch aber leider nicht optimieren, denn es gibt auch hier wieder weitere Regeln¹¹ zu beachten, damit die von der IBM festgelegten Nutzungsbedingungen eingehalten werden. Dieser wichtige Aspekt wird aber von den beteiligten Personen sehr oft nicht wahrgenommen, und das Lizenzmanagement wird meistens erst recht nicht mit eingebunden. Oft verändert der Provider seine technischen Plattformen (Kostenoptimierung), ohne dass Sie als Kunde davon etwas mitbekommen. Sofern der Provider die Software stellt und Sie nur den Service in Anspruch nehmen, ist dagegen nichts einzuwenden. Sobald Sie aber für das Bereitstellen der Software verantwortlich zeichnen und auch das Lizenzmanagement dafür betreiben, müssen Sie über solche Veränderungen stets zeitnah informiert werden. Sonst steht Ihr Unternehmen im Fall eines Audits ziemlich schlecht da, und es wird unter Umständen sehr teuer. Da Vereinbarungen zu dieser Problematik in den Service-Verträgen oft fehlen, könnte es sein, dass Sie die Zeche ganz allein bezahlen müssen, denn aus der Sicht des Herstellers (z. B. IBM) sind Sie als Eigentümer der Software für die Einhaltung der vereinbarten Nutzungsbedingungen allein verantwortlich und voll haftbar.

Wenn Sie in dieses Thema tiefer einsteigen wollen oder müssen, schauen Sie sich für das Beispiel der anzuwendenden IBM-Nutzungsbedingungen am besten die in den Fußnoten aufgeführten Weblinks an. Mehr dazu finden Sie auch in [Gr12].

¹⁰ Siehe IBM-Webseite:

www01.ibm.com/software/lotus/passportadvantage/x86_server_processor_model_number_discovery_guide.html

¹¹ Siehe IBM-Webseite:

<http://www-01.ibm.com/software/lotus/passportadvantage/subcaplicensing.html> und

http://www-01.ibm.com/software/lotus/passportadvantage/pvu_licensing_for_customers.html

**Fazit:**

Wo auch immer Veränderungen an der IT-Architektur angedacht sind, sowohl im Client- (z. B. Citrix-Thema) als auch im Server-Umfeld (und hier ist es noch viel wichtiger), sollten Sie immer das Lizenzmanagement im Unternehmen mit einbeziehen bzw. die Personen, die das Thema Softwarebeschaffung zu verantworten haben. Geplante Optimierungen und Änderungen von Hardware- und Softwareumgebungen müssen Sie immer mit der korrekten Einhaltung der Nutzungsbedingungen abgleichen, sonst kann es für Ihr Unternehmen ein ungemütliches Erwachen im Falle eines Audits geben.

■ 8.8 Auswahl des Lizenzmanagement-Tools

Mal Hand aufs Herz, würden Sie ein fertiges Haus mit einem Keller und Nebengebäuden kaufen und erst nach dem Kauf überlegen, ob Sie überhaupt einen Keller oder die Nebengebäude benötigen? Ich denke nicht.

Aber genau das machen viele IT-Verantwortliche in ihrem Unternehmen, wenn es um die Frage geht, wer oder was das Lizenzmanagement am optimalsten unterstützen kann. Viele IT-Manager unterliegen leider noch zu oft dem Irrglauben, wenn sie ein Tool einkaufen und dieses implementiert haben, läuft alles von ganz alleine. Dabei ist beispielsweise ein im Vorfeld optimierter und funktionierender Software-Life-Cycle-Prozess eine wichtige Voraussetzung dafür, dass die zu implementierende Lizenzmanagement-Lösung auch später optimal funktioniert und den Lizenzmanager bei seinen Aufgaben unterstützen kann. Deshalb sollten Sie vor der Auswahl einer Lizenzmanagement-Lösung für Ihr Unternehmen die Anforderungen an diese Lösung genau kennen und beschreiben können. In einem ersten Schritt sollten – bei der Beachtung einiger Grundregeln – die angestrebten Ziele klar formuliert werden.

Beschreibung eines Ziels:

Ein Ziel wird am besten so formuliert, dass die anzustrebende Situation umfassend beschrieben wird, und zwar so, dass sie möglichst alle Beteiligten verstehen. Außerdem sollte eine Zielbeschreibung lösungsneutral erfolgen, um unabhängige und wertfreie Lösungsmöglichkeiten finden zu können. Natürlich spielen hierbei auch noch andere Faktoren, wie das verfügbare Budget, Ziele/Anforderungen anderer Beteiligter und vor allem die verfügbare Zeit, eine wichtige Rolle.

Stellen Sie sich dazu ergänzend diese Fragen:

- Was will man erreichen?
- Wie lässt es sich erreichen?
- Wie messe ich das Erreichte?

Sie sollten auch die beiden folgenden Kriterien beachten:

- Vollständigkeit: Alle Ziele sollten klar und vollständig beschrieben sein.

- Widerspruchsfreiheit: Formulieren Sie keine gegensätzlichen Ziele, denn diese können das Projekt in seiner geplanten Ausführung behindern.

Haben Sie die Zielformulierung erarbeitet und ist diese auch so vom Management verstanden und abgesegnet worden, können Sie sich mit dem nächsten Schritt beschäftigen.

Betrachtung der Ist-Situation:

Im Rahmen des geplanten Lizenzmanagement-Projekts betrachten Sie die bisherigen Ist-Prozesse und Vorgehensweisen für die Steuerung des Software-Life-Cycles-Prozess und bilden diese ab (Stichwort Reifegradanalyse):

- Optimieren Sie jetzt nach „Best Practise“-Erkenntnissen den „alten“ Software-Life-Cycle-Prozess mit den notwendigen Schnittstellen zu Ihren anderen Unternehmensprozessen.
- Beschreiben Sie dabei auch die neuen Verantwortlichkeiten und notwendigen Rollen.

Im nächsten Schritt werden daraus die Anforderungen an die Lizenzmanagement-Lösung aus der Sicht des Unternehmens möglichst genau formuliert und in ein Anforderungsdokument (Lastenheft) übertragen.

Achten Sie dabei unbedingt auf die folgenden Punkte:

- Die Anforderungen sind vollständig und verständlich beschrieben.
- Die Anforderungen sind dem derzeitigen Wissensstand angepasst, aktuell und korrekt.
- Die Anforderungen besitzen klare rechtliche Beschreibungen.
- Die Anforderungen sind konsistent, testbar und bewertbar.
- Die Anforderungen sind eindeutig, realisierbar und auch notwendig.

Mit der möglichst genauen Beschreibung der Anforderungen helfen Sie auch den Herstellern, die Ihre Ausschreibungsunterlagen erhalten und beantworten, ihre Chancen realistischer einzuschätzen, und Sie können diese im Rücklauf auch einfacher aus- und bewerten.



Hinweis:

Beschreiben Sie nur die unbedingt notwendigen und für die Funktionserfüllung erforderlichen Anforderungen im Lastenheft. Manches ist einfach nur „Schmuck am Nachthemd“, wie meine Oma zu sagen pflegte, wenn etwas überflüssig zu sein schien. Die Erfahrung zeigt, dass bis zu ca. 43% der geforderten Funktionen später in Wirklichkeit nicht benutzt werden!

Bevor Sie Ihre fertig beschriebenen Anforderungsunterlagen an die Hersteller schicken, wäre es sinnvoll, das Angebot an möglichen Lösungen auf dem Markt zu sondieren und im Vorfeld die am Markt verfügbaren Hersteller und Tools auf eine überschaubare Anzahl einzugrenzen (das Gesagte gilt nicht, wenn Sie der Ausschreibungspflicht von Gesetzes wegen unterliegen (Öffentlicher Auftraggeber) und dazu verpflichtet sind, eine Deutschland- oder sogar EU-weite Ausschreibung durchzuführen. *(Lesen Sie dazu bitte auch die Kapitel 13.2.1, Ausschreibung von Beschaffungsvorhaben, und 13.2.2, Voraussetzungen für die Ausschreibungspflicht, ab S. 676.)*

**Tipp:**

Versuchen Sie im Vorfeld ein realistisches Mengengerüst der zu verwaltenden Assets aufzustellen. Nur so können Sie vernünftig abschätzen, ob die angedachte Tool-Lösung auch zu Ihrem Bedarf passt. Natürlich sollte das System auch später ohne größere Anpassungen erweiterbar sein. Ein modular aufgebautes System wäre bereits ein guter Ansatz.

Sammeln Sie also möglichst schon vor dem Start der Ausschreibung Informationen über die verschiedenen auf dem Markt angebotenen Lösungen. Das spart Ihnen bei der späteren Ausschreibung eine Menge Zeit und Nerven. Haben Sie den Kreis schon etwas einschränken können, sollten Sie in einem zweiten Schritt mit den Herstellern in Kontakt treten, die eine für Ihr Unternehmen interessante Lösung anbieten. Bevor Sie mit den Herstellern tiefergehende Gespräche und Meetings anberaumen – was sehr zeitintensiv werden kann –, lassen Sie sich Kundenreferenzen nennen, die möglichst auch aus Ihrer Branche stammen sollten. So können Sie sich schon einmal einen ersten und vor allem ehrlichen Überblick verschaffen, ob die ins Auge gefasste Lösung halten kann, was Ihnen der Vertriebsmitarbeiter des Herstellers verspricht.

**Hinweis:**

Sie sollten eine Softwarelösung eines in diesem Bereich führenden Anbieters einsetzen. Durch eine Marktanalyse der in diesem Segment erhältlichen Tools können Sie eine Vorauswahl treffen. Im Rahmen dieser Analyse werden die bis dato bekannten Anforderungen auf Realisierbarkeit mit den angebotenen Produkten beleuchtet. Zusätzlich werden Technologie, Strategie und Professionalität der Tools untersucht. Auf Basis dieser Informationen versenden Sie die Ausschreibungsdokumente an verschiedene Hersteller bzw. Anbieter.

Haben Sie die beschriebenen Aktivitäten erfolgreich abgeschlossen, sollten Sie jetzt die Ausschreibungsunterlagen und einen Zeitplan für die geplante Ausschreibung erstellen, sofern nicht bereits geschehen.

**Tipp:**

Damit Sie es bei der Auswertung und Bewertung (Punktesystem) der Antworten etwas leichter haben, sollten Sie die Ausschreibungsunterlagen bereits so aufbauen, dass Sie mit einem Punktesystem für eine vergleichende Bewertung arbeiten können. Dabei sollte auch eine Unterscheidung in „Muss-Anforderungen“ (diese sind auf alle Fälle zu erfüllen) und sogenannte „Nice-to-Have-Anforderungen“ erfolgen. Wer schon nicht die Muss-Anforderungen erfüllt, wird so recht schnell aus der Bewertung rausfallen, und Sie ersparen sich die weitere Bearbeitung der Ausschreibungsunterlage dieses Herstellers.

1. Planen Sie dafür genügend Zeit ein, denn der Ablauf einer solchen Ausschreibung umfasst mehrere Schritte und zieht sich über mehrere Wochen hin, wie Abbildung 8.4. exemplarisch zeigt.

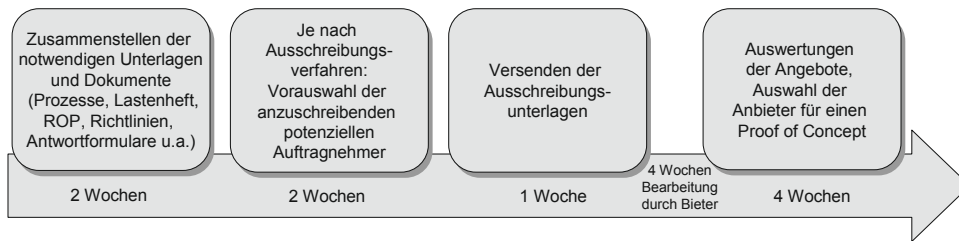


ABBILDUNG 8.4 Exemplarisches Zeitfenster eines Ausschreibungsverfahrens

2. Die Erfahrung lehrt, dass ein Zeitraum von mindestens drei Monaten bis zu einem Jahr durchaus als realistisch gelten kann (im Falle einer EU-Ausschreibung geht das schon in die Richtung von einem halben bis zu einem Jahr).
3. Die von den Herstellern retournierten Ausschreibungsunterlagen sollten jetzt zügig bearbeitet werden. Die Hersteller mit den drei höchsten Bewertungen können nun zu einem „Proof of Concept“ (PoC) eingeladen werden, bei dem jeder seine Lösung vor Ort in Ihrem Unternehmen präsentiert. Versuchen Sie, hierfür möglichst schon „echte“ Daten aus Ihrem Unternehmen zur Verfügung zu stellen. So können Sie bereits bei der Vorstellung der Lösung beurteilen, wie gut oder schlecht der Hersteller mit Ihren Daten „Out-of-the-Box“ arbeiten kann. Dies ist dann auch schon ein Hinweis darauf, ob man die angestrebte Lösung möglichst ohne größere Komplikationen in Ihrem Unternehmen implementieren kann.



Tipp:

Lassen Sie sich während des PoCs von den jeweiligen Herstellern Referenzkunden nennen, und sprechen Sie auch mit diesen. So finden Sie am schnellsten heraus, ob der Hersteller die dort ausgeführte Projektarbeit in dem zugesagten Budgetrahmen (Zeit und Geld) wenigstens einigermaßen eingehalten hat.

Wichtig ist auch, dass Sie sich noch einmal klären, ob der potenzielle Hersteller auch Erfahrung bei der Anbindung und Umsetzung von Geschäftsprozessen des Kunden in sein Tool vorweisen kann. Oft erlebe ich, dass außerhalb des Tools kaum Lizenzmanagement-Wissen bei den Beratern zu finden ist.

Nach Abschluss der Teststellungen und Vorführungen wird eine abschließende Bewertung durch das Lizenzmanagement-Projektteam und den Fachbereich, der das Tool später betreiben soll, durchgeführt. Oft liegen die ausgewählten Hersteller mit den erreichten Punkten sehr dicht nebeneinander. Wenn es keine weiteren technischen Ausschlussmöglichkeiten gibt, ist nun der Einkauf gefragt und sollte das beste Angebot verhandeln.

Mit der Auswahl einer Lizenzmanagement-Lösung ist es natürlich nicht getan, jetzt heißt es, die Anforderungen aus dem Lastenheft gemeinsam mit dem ausgewählten Anbieter umzusetzen und alle angrenzenden Geschäftsprozesse mit einzubinden.

■ 8.9 Einführung einer Lizenzmanagement-Lösung

Sie haben bislang einen sehr großen und wichtigen Meilenstein geschafft, das Werkzeug für die Unterstützung des Lizenzmanagements in Ihrem Unternehmen ist ausgewählt. Jetzt stehen Sie vor einer weiteren Herausforderung. Das Tool muss implementiert und in Betrieb genommen werden. Je nachdem, wie die Anforderungen definiert und beschrieben wurden und welche davon mehr oder weniger vollständig durch „Out-of-the-Box“-Funktionen des Tools umgesetzt werden können, kann diese Phase relativ kurz sein oder auch etwas länger dauern. Üblicherweise wird in Zusammenarbeit mit dem Hersteller ein Projekt- und Testplan für die anstehenden Aufgaben erstellt, in dem die Leistungen des Auftraggebers und Auftragnehmers festgehalten werden.



Hinweis:

Das Projekt wird zwangsläufig einige Änderungen im Unternehmensumfeld, in den Prozessen, Strukturen und Organisationseinheiten mit sich bringen. Diese Änderungen werden nicht von allen Beteiligten unbedingt als positiv empfunden. Versuchen Sie, diese Ängste zu identifizieren, und sprechen Sie rechtzeitig mit den Betroffenen über die zu erwartenden Veränderungen und deren Konsequenzen. Psychologisches Einfühlungsvermögen und die Information aller Beteiligten spielt eine wesentliche Rolle für die erfolgreiche Einführung der Lizenzmanagement-Lösung.

Für die Umsetzung der anstehenden organisatorischen und technischen Maßnahmen müssen sowohl der Auftraggeber als auch der Auftragnehmer bestimmte Voraussetzungen erfüllen. So sind beispielsweise verantwortliche Personen auf beiden Seiten zu benennen, das Projektorganigramm und der Projektplan sind zu erstellen, technische Voraussetzungen für die Installation des Tools auf Seiten des Auftraggebers zu schaffen, Test- und Vorproduktionsumgebungen zu erstellen, ein Backup-Szenario wird benötigt, und viele weitere wichtige Punkte sind zu beachten. Kapitel 16 in [Gr09] geht auf diese Punkte, die hier aus Platzgründen leider nicht eingehender behandelt werden können, ausführlicher ein. Für eine Planung und Meilensteinbestimmung, ist unter anderem ein Implementierungsplan ein unerlässliches Hilfsmittel. Abbildung 8.5 stellt einen beispielhaften Ablauf dar.

Wenn Sie die hier beschriebene Vorgehensweise anwenden, verringern Sie das Risiko, bei der Implementierung vom Weg abzukommen, und erzeugen damit für den Projektverlauf über die gesamte Laufzeit die notwendige Transparenz.



Tipp:

Die Erfahrung zeigt, dass sich immer irgendwo eine weitere kleine Baustelle ganz plötzlich und unerwartet auftut. Im Vorfeld kann einfach nicht an alles gedacht werden, dazu gibt es zu viele Faktoren und Größen, die sich gegenseitig beeinflussen. Implementieren Sie daher von Anfang an ein Risikomanagement, um auf diese unvorhergesehenen Ereignisse und Aufgaben entsprechend reagieren zu können.

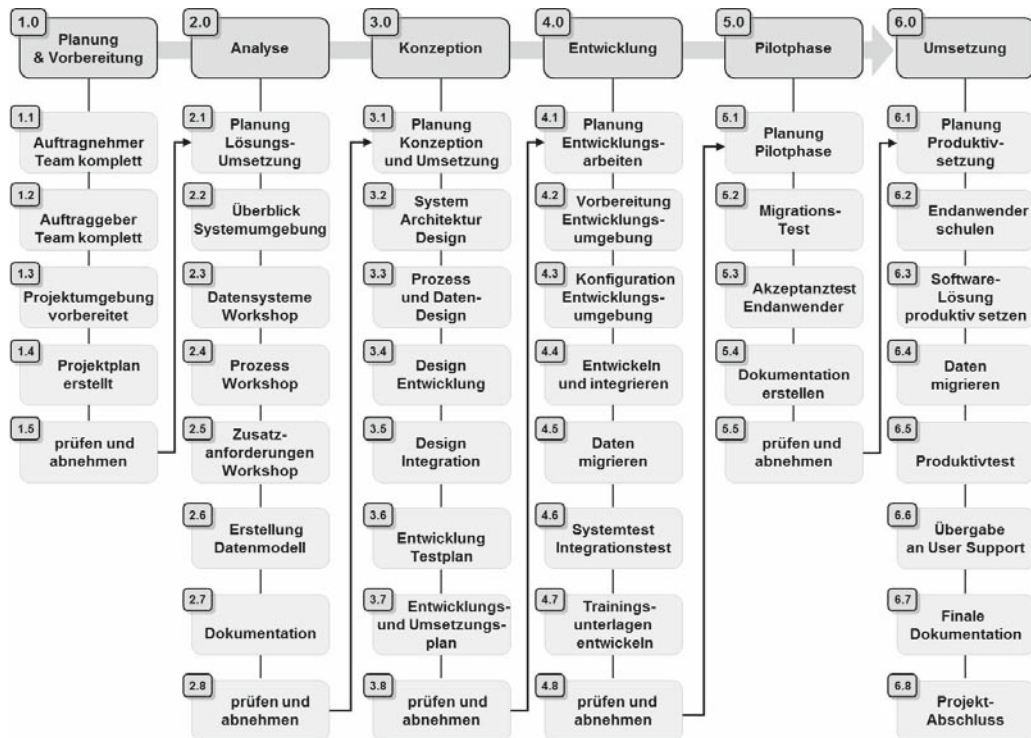


ABBILDUNG 8.5 Phasenablaufplan für eine Implementierung

Bei allen Aktivitäten, die mit den Funktionen des Tools unmittelbar oder mittelbar zusammenhängen, ist ein Testplan erforderlich, der unter anderem auch dafür sorgt, dass die gewünschten Ergebnisse während der Implementierung des Tools erreicht und bestätigt werden.

Nachdem die erforderlichen Tests erfolgreich waren, sollte der Produktiveinsatz des Tools anhand eines „Piloten“ geprüft werden. Hierbei wird die Produktivumgebung in einer Testumgebung nachgebildet, mit der Besonderheit, dass die Pilotumgebung Echtdaten aus der Produktivumgebung über die schon produktiven Schnittstellen erhält. Die Pilotumgebung wird außerdem oft auch als Schulungsumgebung für die Endanwender genutzt und muss damit zusätzlich unter Beweis stellen, dass alle gewünschten Prozesse und Funktionen ohne Probleme arbeiten.

Bevor Sie das Tool oder die Softwarelösung produktiv setzen, sollten alle Beteiligten ausreichend und ihrer zukünftigen Rolle entsprechend im Umgang mit der Software geschult worden sein. Bewährt hat sich auch, dass in den ersten zwei bis vier Wochen Mitarbeiter des Tool-Herstellers Unterstützung leisten. Geben Sie rechtzeitig eine vorher eingerichtete Hotline-Nummer und E-Mailbox bekannt, damit Ausfall und Problemmeldungen sofort an die richtige Stelle kommuniziert werden können. Haben Sie an alles gedacht, werden sich die Anrufe der Mitarbeiter in Grenzen halten, und die Akzeptanz für die Nutzung der Software wird gleich viel höher sein. Ist bei der Überführung in die Produktion alles gut verlaufen, können Sie und alle Beteiligten mit Recht stolz auf die in den letzten Wochen und Monaten geleistete Arbeit sein.

Jetzt bleibt nur noch, Ihnen zu wünschen, dass die am Anfang formulierten Ziele so weit erreicht wurden und Ihr System die gestellten Anforderungen auch erfüllt.

Das Kapitel konnte Ihnen aufgrund der begrenzten Seitenanzahl nur einen kleinen Ausschnitt des doch sehr umfangreichen und komplexen Themas „Lizenzmanagement“ beleuchten. Sollten Sie die Aufgabenstellung erhalten haben, ein Lizenzmanagement-Projekt aufzusetzen, empfehle ich Ihnen [Gr09] bzw. [Gr12].



Fazit:

Die Aufgabe, ein Lizenzmanagement in all seinen Facetten zu entwickeln, aufzubauen und letztendlich auch zu implementieren, ist selbst für gestandene IT-Fachleute eine große Herausforderung. Bedingt durch die wenigen Angebote auf dem Markt, sich in diesem Thema fachlich fundiert ausbilden zu lassen, hängt auch heute noch sehr viel von dem Wissen und den persönlichen Erfahrungen der verantwortlichen Mitarbeiter ab. Der Einsatz eines Werkzeugs ist dabei aber nur eine Möglichkeit, diesen Prozess zu unterstützen. Viel wichtiger sind die vielen unterschiedlichen Faktoren, die es zu beachten gilt, wenn ein Lizenzmanagement aktiv betrieben werden soll. Beispielsweise spielen das genaue Wissen und die Beachtung der bestehenden IT-Architektur eine große Rolle, damit die vereinbarten Nutzungsrechte lizenzkonform umgesetzt werden können.

Ebenfalls muss die Managementebene noch stärker als bisher in das Thema Lizenzmanagement eingebunden werden. Denn nur mit der Unterstützung des Managements kann der Lizenzmanager seine Rolle unternehmensweit ausüben und so die Einhaltung der gesetzlichen Vorgaben sowie die ordnungsgemäße Verwendung der durch die Softwarehersteller eingeräumten Nutzungsrechte sicherstellen.

Wenn Sie die Aufgabe erhalten haben, ein Lizenzmanagement im Unternehmen einzuführen, ist das Einholen von Informationen das erste Gebot der Stunde. Besuchen Sie dafür Seminare, Kongresse oder IT-Foren, die sich mit dem Lizenzmanagementthema beschäftigen. Hier können Sie sich fachlich austauschen und den einen oder anderen wertvollen Hinweis für Ihre Aufgabenstellung erhalten.

Denn letztendlich geht es darum, eine optimale, den funktionalen und natürlich auch wirtschaftlichen Verhältnissen in Ihrem Unternehmen angepasste Lösung zu finden. Wie groß dabei die Software-Lösung sein soll, hängt von mehreren Faktoren ab. Es muss aber nicht immer gleich eine umfangreiche Softwarelösung sein, um die gestellte Aufgabe erfüllen zu können.

■ 8.10 Literatur und weiteres Informationsmaterial

[Gr09] Groll, T.: 1x1 des Lizenzmanagements. Hanser; München 2009, 1. Auflage

[Gr12] Groll, T.: 1x1 des Lizenzmanagements. Hanser; München 2012, 2. Auflage

[Webseite] www.lmallLima.de im Menüabschnitt „Extras“, (Vorlagen für die Projektarbeit) und im Menüabschnitt „Seminare“, Termine und Seminarinhalte zum Thema „Lizenzmanagement in der Praxis“

Andreas Nehfort



Fragen, die in diesem Kapitel beantwortet werden:

- Warum ist Qualitätssicherung bzw. Qualitätsmanagement im IT-Bereich so wichtig?
- Wie funktioniert Qualitätsmanagement?
- Wie rechnen sich Qualitätsmanagement und Qualitätssicherung?
- Was Sie über die grundlegenden Unterschiede zwischen sequentieller und iterativer Entwicklung aus Qualitätsmanagementsicht wissen sollten!
- Wie Sie über unterschiedliche Blickwinkel Ihre Qualitätsziele verfolgen können:
 - Qualität des Produkts
 - Qualität des Projekts
 - Qualität der Prozesse.
- Welche Qualitätsmanagement-Standards können Sie bei der Qualitätsverbesserung unterstützen?

In diesem Buch „Handbuch IT-Management“ wird das Thema „Qualitätsmanagement“ aus einer grundlegenden (Management-)Sicht im IT-Umfeld betrachtet. Eine detailliertere Darstellung des Themas „Qualitätsmanagement und konkrete QS-Maßnahmen für IT-Projekte“ finden Sie in meinem Beitrag in [TIE10] (Kapitel 14).

■ 9.1 Begründungen und Ansätze für umfassende Qualitätsmanagement- Lösungen

9.1.1 Warum ist Qualitätssicherung bzw. Qualitätsmanagement im IT-Bereich so wichtig?

Qualität entsteht nicht von selbst!

Der Erfolg von Software-Projekten ist leider keine Selbstverständlichkeit, sondern eher die Ausnahme. Diese unerfreuliche Tatsache wird uns durch die Studien der Standish Group (Chaos Reports 1994 [STA01], 2000 [STA02], 2004 [STA03], 2006 [STA04] und 2008 [STA05] siehe Tabelle 9.1) drastisch vor Augen geführt.

TABELLE 9.1 Standish Group: Chaos Report

	Erfolgreiche Projekte	Projekte mit Abweichungen	Gescheiterte Projekte
1994	16%	53%	31%
2000	28%	49%	23%
2004	29%	53%	18%
2006	35%	46%	19%
2008	32%	44%	24%

Das Ergebnis ist wie folgt zu lesen (am Beispiel 1994): 1994 waren 16% der IT-Projekte erfolgreich, 53% der Projekte hatten (zum Teil erhebliche) Abweichungen und 31% der Projekte sind gescheitert. Der Anteil der „gescheiterten Projekte“ ist von 1994 bis 2004 deutlich rückläufig und 2006 etwa auf dem Niveau von 2004. Der Anstieg der gescheiterten Projekte im Report 2008 wird in Fachkreisen diskutiert und dürfte darauf zurückzuführen sein, dass in wirtschaftlich schwierigen Zeiten die Bereitschaft größer ist, ein wenig erfolgreiches Projekt zu stoppen. Für die Einteilung der Projekte werden von der Standish Group folgende Kriterien angewandt:

▪ *Erfolgreiche Projekte:*

Das Projekt wird termingerecht abgeschlossen, hält den Budgetrahmen ein und liefert alle Funktionen und Features, die zu Beginn spezifiziert worden sind (bei einer Toleranzbreite von 10%).

▪ *Projekte mit Abweichungen:*

Das Projekt wird abgeschlossen und das Projektergebnis eingesetzt; es gab jedoch Abweichungen hinsichtlich Terminen, Kosten und Funktionsumfang.

▪ *Gescheiterte Projekte:*

Das Projekt wird abgebrochen, ohne eine Software zu liefern, die vom Auftraggeber eingesetzt wird.

Laut Chaos Report hatten im Jahr 1994 die „Projekte mit Abweichungen“ eine durchschnittliche Kostenüberschreitung von 189% und einen durchschnittlichen Funktionsumfang von 61%, bezogen auf die ursprünglichen Vereinbarungen.

Im Jahr 2000 hatten diese „Projekte mit Abweichungen“ eine durchschnittliche Kostenüberschreitung von 45% und einen durchschnittlichen Funktionsumfang von 67%, bezogen auf die ursprünglichen Vereinbarungen.

Das ist von 1994 auf 2000 eine beachtliche Steigerung. Trotzdem lieferten laut Aussagen der Standish Group im Durchschnitt die Hälfte aller Projekte etwa 2/3 des vereinbarten Leistungsumfangs zu 150% der vereinbarten Kosten. Das ist wahrlich keine Erfolgsbilanz! Auch wenn diese Daten (die in den letzten Jahren in der IT-Community auch zunehmend kritisch hinterfragt werden) nicht 1:1 die Realität widerspiegeln, so haben sie doch eine eindeutige Botschaft: Die überwiegende Anzahl unserer IT-Projekte liefert ein deutlich schlechteres Preis-Leistungsverhältnis als in der Planung angesetzt. Das fordert nach Maßnahmen!

**Praxistipp:**

Qualitätssicherung und Qualitätsmanagement sind jene Maßnahmen, die unter den gegebenen Rahmenbedingungen die Wahrscheinlichkeit erhöhen, dass Ihre IT-Projekte – insbesondere die Software-Projekte – zu den erfolgreichen gehören!

Ausführlich können Sie sich über sämtliche Instrumente eines erfolgreichen IT-Projektmanagements in Kapitel 5 dieses Handbuchs informieren.

9.1.2 Wie funktioniert Qualitätsmanagement?

Taz Daughtrey, der Präsident der Amerikanischen Vereinigung für Software-Qualität, hat auf dem 3. Weltkongress für SW-Qualität (3WCSQ – München September 2005) Qualitätsmanagement wie folgt charakterisiert:

- Quality Management, that's the game with the rules, with the tools, and with the fools!*
- *the rules bring in effectiveness*
 - *the tools bring in efficiency*
 - *and with the fools it is impossible!*

Auf gut Deutsch:

- Die (richtigen) Regeln sorgen für die Wirksamkeit.
- Geeignete Werkzeuge erhöhen die Wirtschaftlichkeit.
- Doch wenn die Betroffenen nicht mitspielen, kannst du alles vergessen!

Anders gesagt: **Erfolg = Qualität x Akzeptanz**

In Anlehnung an Taz Daughtreys Spruch gibt es drei Hauptursachen, an denen Qualitätsmanagement scheitert:

- Die Maßnahmen sind nicht wirkungsvoll, d.h. sie verursachen Aufwand, ohne dass der entsprechende Nutzen (höhere Qualität) erreicht wird.
- Die Maßnahmen sind zu aufwändig, d. h. der Aufwand ist größer als der potenzielle Nutzen.
- Die Maßnahmen werden nicht akzeptiert.

9.1.3 Das Dilemma des Qualitätsmanagements

In der Praxis scheitert die Einführung von Qualitätssicherungs- oder Qualitätsmanagement-Maßnahmen oft an der Frage der Führungskräfte nach der Kosten/Nutzen-Relation: „Was bringen die Maßnahmen?“

- Die Frage nach den Kosten ist mit etwas Projektmanagement-Know-how und Erfahrung schnell einigermaßen vernünftig zu beantworten!
- Die Frage nach dem Nutzen lässt sich erst beantworten, wenn die Organisation ihre Kosten (= Verluste) kennt, die sich infolge von Qualitätsmängeln ergeben.

**Beachten Sie:**

Die wenigsten Organisationen können diese Kosten beziffern. Wenn man den Schaden nicht beziffern kann, lässt sich natürlich auch der potenzielle Nutzen der Qualitätssicherung nicht sauber kalkulieren.

Die gängigen Prozessreifegrad-Modelle wie CMMI oder SPICE (siehe Abschnitt 9.8.3) beantworten auch, warum das so ist: Um die Kosten (Verluste) durch Qualitätsmängel sauber messen zu können, braucht man Prozesse im Reifegrad zwei bis drei nach CMMI oder SPICE. Um auf Reifegrad zwei oder drei zu kommen, sind beträchtliche Investitionen ins Qualitätsmanagement erforderlich. Damit haben wir ein klassisches Henne-Ei-Problem!

Die Einführung von Qualitätsmanagement wird zur unternehmenspolitischen Entscheidung:

- Unternehmen, die daran glauben, werden in Qualitätsmanagement investieren – wenn sie es richtig machen, mit Erfolg!
- Unternehmen, die nicht daran glauben, scheitern am Henne-Ei-Problem:
 - Solange du mir nicht sagen kannst, was es bringt, will ich nicht in Qualitätsmanagement investieren!
 - Ohne Qualitätsmanagement sind die Kosten (Verluste) durch Qualitätsmängel nicht sauber quantifizierbar!

**Was lernen wir daraus?**

Wenn das Management nicht konsequent dahintersteht, sollte man die Finger davon lassen!

Der Chaos Report der Standish Group identifiziert das „Management Commitment“ als den wichtigsten Erfolgsfaktor für IT-Projekte – das gilt auch für die Einführung von Qualitätsmanagement!

■ 9.2 Grundlagen und Begriffe des IT-Qualitätsmanagements

In diesem Abschnitt erfahren Sie, auf welchen Grundlagen das moderne Qualitätsmanagement aufbaut.

Dabei erfolgt bewusst eine Orientierung an den Begriffen der ISO 9000. Damit soll dargelegt werden, dass uns eine konsequente Interpretation dazu anleiten kann, Qualitätsmanagement als Wettbewerbsfaktor einzusetzen. So sollen auch einige weit verbreitete Missverständnisse bezüglich Qualität und ihrer Kosten aufgeklärt werden.

Für einige Begriffe wird ergänzend auch auf die Definitionen der mittlerweile zurückgezogenen ISO 8402:1992 zurückgegriffen, weil diese dort verständlicher formuliert sind als die

neueren Definitionen der ISO 9000:2000 (für unsere Zwecke sind beide Definitionen inhaltlich ohnehin gleichbedeutend).

Im Folgenden also ein paar Qualitätsbegriffe und ihre Konsequenzen für die praktische Arbeit im IT-Qualitätsmanagement.

9.2.1 Qualität

Im alltäglichen Sprachgebrauch verstehen wir unter „sehr guter Qualität“ in der Regel möglichst hochwertige Produkte oder Dienstleistungen. „Besser“ wird oft mit leistungsfähiger, umfassender oder exklusiver assoziiert, was dazu führt, dass „bessere“ Produkte in der Regel auch teurer sind.

Für die Zwecke der Qualitätssicherung und des Qualitätsmanagements hat sich ein etwas anderes Qualitätsverständnis durchgesetzt, das sich an den Bedürfnissen der Kunden orientiert. Eine hilfreiche Definition ist die folgende:

Qualität ist der Grad, in dem der Benutzer das Gefühl hat, dass ein Produkt seine kombinierten Erwartungen erfüllt.

Das Schöne an dieser Definition ist, dass sie das Qualitätsverständnis der Kunden auf den Punkt bringt. Wenn man dieser Qualitätsdefinition gerecht wird, hat man wirklich zufriedene Kunden! Das Problem mit dieser Definition ist, dass sie einem nicht weiterhilft bei der Frage: Wie schaffe ich Qualität?

Qualität ist nach dieser Definition von zwei Faktoren abhängig, die man schwer in den Griff bekommt:

- die kombinierten Erwartungen;
- die Gefühle der Anwender.

Trotzdem: Wenn man sich erfolgreiche Produkte ansieht, kommt es genau auf diese beiden Faktoren an! Der Erfolg eines Auto-Modells oder einer Marke ist nicht in erster Linie von den Ergebnissen der ADAC-Pannenstatistik abhängig! Die Hersteller von Oberklasse-Fahrzeugen investieren beispielsweise beträchtliche Summen in das Sound-Design des Motors und – ganz wichtig – des Geräusches der ins Schloss fallenden Tür ..., um Qualität im Sinne der obigen Definition zu schaffen und die kombinierten Erwartungen ihrer zu Recht anspruchsvollen Kunden zu erfüllen.

Um Qualität schaffen zu können, muss man die „kombinierten Erwartungen“ in Anforderungen fassen.

Die gängigen **Qualitätsbegriffe in der Literatur** orientieren sich daher konsequent an den spezifischen Anforderungen der jeweiligen Kunden.

- **Qualität** (Definition nach ISO 8402:1992):
„Gesamtheit von Merkmalen und Merkmalswerten einer Einheit bezüglich ihrer Eignung, festgelegte und vorausgesetzte Erfordernisse zu erfüllen.“
- **Qualität** (Definition nach ISO 9000:2000):
„Grad, in dem ein Produkt oder eine Dienstleistung Anforderungen erfüllt.“
- **Anforderung** (Definition nach ISO 9000:2000):
„Erfordernis oder Erwartung, das oder die festgelegt, üblicherweise vorausgesetzt oder verpflichtend ist“.

Dieses Qualitätsverständnis führt P.B. Crosby in seinem Buch „Quality is free“ [CRO01] zur Formel:

Quality is conformance to requirements.

Diese Qualitätsdefinition hat einige Konsequenzen, die nachfolgend herausgestellt werden:

▪ **Qualität ist relativ:**

Sie ist abhängig von den jeweiligen Erfordernissen und Erwartungen (Anforderungen).

▪ **Qualität ist situativ:**

Die Erfordernisse und Erwartungen sind abhängig vom jeweiligen Einsatzgebiet.

▪ **Qualität ist subjektiv:**

Die Erfordernisse und Erwartungen sind abhängig von den handelnden Personen.

In der Praxis bedeutet das: Qualität basiert auf Vereinbarungen – Vereinbarungen über Anforderungen!

Der Satz „quality is conformance to requirements“ hat in der IT-Branche folgendes Missverständnis unterstützt:

- Der Kunde muss all seine Anforderungen explizit definieren.
- Wenn eine Funktion oder ein Leistungsmerkmal fehlt, das für den beabsichtigten Gebrauch wesentlich ist, vom Kunden jedoch nicht explizit spezifiziert wurde, ist der Kunde selber schuld – Qualitätsmangel ist das aber keiner!

Diese Sichtweise ist in der Praxis natürlich nicht vollständig haltbar. Qualität bedeutet vielmehr, die folgenden drei Kategorien von Anforderungen zu erfüllen:

- Anforderungen, die der Kunde festlegt;
- Anforderungen, die der Kunde üblicherweise voraussetzt (d.h. was er erwarten kann, auch wenn er es nicht explizit definiert ...)
- Anforderungen von verpflichtender Wirkung: gesetzliche Vorschriften, anwendungsspezifische Standards, ...

Walter Wintersteiger hat aus „quality is conformance to requirements“ abgeleitet:

Qualität bedeutet: Leistung : Anforderungen = 1

Genau Eins: nicht weniger, aber auch nicht mehr!



Praxistipp:

Für all jene, die Qualität schaffen wollen, sind – orientiert an der zuvor genannten Formel – folgende **Forderungen** zu erfüllen:

- Wir müssen die Anforderungen (Erfordernisse und Erwartungen) erkennen und verstehen.
- Wir müssen die Leistung erbringen können.

Und das mit einem vernünftigen Verhältnis von Leistung, Aufwand, Kosten und Terminen.

Die weiteren Kapitel des Abschnitts IT-Qualitätsmanagement geben einen Überblick, welche Maßnahmen uns dabei unterstützen.

9.2.2 Qualitätsverbesserung

Im alltäglichen Sprachgebrauch assoziieren wir mit „Qualitätsverbesserung“ in der Regel eine Veränderung hin zu höherwertigen Produkten oder Dienstleistungen. „Qualitativ besser“ bedeutet damit in der Regel auch aufwändiger und somit meist teurer.

Im Qualitätsmanagement hat auch der Begriff „Qualitätsverbesserung“ einen subtilen Bedeutungswandel mitgemacht:

- Qualitätsverbesserung (Definition nach ISO 9000:2000):
„Teil des Qualitätsmanagements, der auf die Erhöhung der Fähigkeit zur Erfüllung der Qualitätsanforderungen gerichtet ist.“
- Qualitätsverbesserung (Definition nach ISO 8402:1992):
Summe aller Maßnahmen zur **Erhöhung der Effektivität und Effizienz** von Tätigkeiten und Prozessen, um zusätzlichen Nutzen sowohl für die Organisation als auch für ihre Kunden zu erzielen.



Qualitätsverbesserung bedeutet demnach

- Erhöhung des Wirkungsgrades (Effektivität) und
 - Erhöhung der Wirtschaftlichkeit (Effizienz)
- unter Berücksichtigung der jeweiligen Anforderungen.

Die Qualität von Tätigkeiten und Prozessen wird also über ihre Wirksamkeit und Wirtschaftlichkeit definiert. „Qualitativ besser“ bedeutet in diesem Zusammenhang „wirksamer“ und „wirtschaftlicher“.



Qualitätssicherung wird im Wesentlichen als die Sicherung von Wirksamkeit und Wirtschaftlichkeit von Tätigkeiten und Prozessen verstanden.

Das ist weit entfernt von dem Bild, das sich in Teilen der Wirtschaft von Qualitätssicherung, Qualitätsmanagement und insbesondere von der ISO 9001 gebildet hat. Qualitätssicherung, QM-Systeme und die ISO 9001 sind in Verruf gekommen

- als Anleitung zum Dienst nach Vorschrift, also dem Befolgen von Arbeitsanweisungen;
- als Hort der Bürokratie und Zettelwirtschaft, also der Praxis umfassender Qualitätsaufzeichnungen;
- als Klotz am Bein, wenn es darauf ankommt, flexibel zu sein.

Der Zusammenhang zwischen Qualität und Wirtschaftlichkeit wird klarer, wenn man sich die folgende Definition der qualitätsbezogenen Kosten vor Augen führt:

Qualitätsbezogene Kosten (Definition nach ISO 8402:1992):

Kosten, die durch die Gewährung zufriedenstellender Qualität und durch das Schaffen von Vertrauen, dass die Qualitätsanforderungen erfüllt werden, entstehen, sowie Verluste infolge des Nichterreichens zufriedenstellender Qualität.



Die qualitätsbezogenen Kosten setzen sich demnach aus drei Faktoren zusammen:

- den Kosten für das Schaffen von Qualität;
- den Kosten für das Schaffen von Vertrauen in diese Qualität;
- den Verlusten durch Qualitätsmängel.

Erfolgreiches Qualitätsmanagement bedeutet also Reduzierung des Risikos von Qualitätsmängeln und damit Reduzierung der Verluste, die aus diesen Qualitätsmängeln resultieren. Erfolgreiches Qualitätsmanagement bedeutet aber auch, dafür zu sorgen, dass die Kosten aus Punkt 1 und 2 geringer sind als die Einsparungen aus Punkt 3.



Unter Berücksichtigung der Verluste durch Qualitätsmängel stimmt die Formel von P. B. Crosby „Quality is free“: Wenn ich bereit bin, eine Menge in Qualität zu investieren, sind meine Kosten für Qualitätsmanagement geringer als die (voraussichtlichen) Verluste durch Qualitätsmängel.

9.2.3 Qualitätsmanagement und Qualitätssicherung als Teil eines Managementsystems

Bis Mitte der 80er Jahre des letzten Jahrhunderts wurde Qualitätssicherung im Wesentlichen mit Qualitätskontrolle (= Prüfung am Endprodukt) gleichgesetzt. Seither hat sich das Verständnis von Qualitätssicherung deutlich gewandelt, hin zu:

Gleichbleibend hohe Qualität erreicht man nicht über die Prüfung am Endprodukt, sondern über die Beherrschung der Entwicklungs- bzw. Fertigungsprozesse.

Dieses Paradigma des prozessorientierten Qualitätsmanagements prägt alle modernen QM-Ansätze, wie ISO 9001, oder die Prozessreifegradmodelle CMMI und SPICE/ISO 15504.

Qualitätsmanagement ist Prozessmanagement!

Aktives Prozessmanagement macht uns unabhängig von der Befindlichkeit des Einzelnen! In den 70er und 80er Jahren des vorigen Jahrhunderts gab es für ein Auto, das besonders fehleranfällig war, den Begriff des „Montag-Autos“, weil montags – am ersten Arbeitstag nach dem Wochenende – die Fehleranfälligkeit der Arbeiter in der Fertigung höher war als an den anderen Arbeitstagen. Mit der Einführung des prozessorientierten Qualitätsmanagements ist das Montag-Auto ausgestorben.

So hat sich das Qualitätswesen schrittweise von der Qualitätsprüfung zur Qualitätssicherung und von der Qualitätssicherung zum Qualitätsmanagement weiterentwickelt.

Der Chaos Report der Standish Group identifiziert das „Management Commitment“ als den wichtigsten Erfolgsfaktor für den Projekterfolg. Folgerichtig wird **Qualitätsmanagement** heute als **Teil des Management-Systems** betrachtet.

Die aktuelle Sichtweise spiegelt sich in den folgenden Begriffsdefinitionen wider:

Qualitätsmanagement-System (Def. nach ISO 9000:2000):

„System für die Festlegung einer Qualitätspolitik und von Qualitätszielen sowie zur Erreichung dieser Ziele.“

Qualitätsmanagement basiert also auf einer Qualitätspolitik, die Teil der Unternehmenspolitik ist. Qualitätsziele sind die konkrete Ausprägung der Qualitätspolitik für das laufende Geschäftsjahr.

Qualitätsmanagement (Definition nach ISO 9000:2000):

„Gesamtheit der in einem QM-System verwendeten Prozesse.“

Qualitätsmanagement ist also die Summe jener Prozesse,

- mit denen wir einerseits die Qualitätspolitik und die Qualitätsziele festlegen (→ Lenkungsprozesse) und
- mit denen wir diese Qualitätsziele andererseits erreichen wollen (→ Leistungsprozesse und Supportprozesse).

Qualitätsmanagement wird damit zu einem wichtigen Teilaspekt des Prozessmanagements.

Qualitätssicherung (Definition nach ISO 9000:2000):

„Teil des Qualitätsmanagements, der auf die Schaffung von Vertrauen gerichtet ist, dass die zutreffenden Qualitätsforderungen erfüllt werden“

Qualitätssicherungsmaßnahmen sollen also das Vertrauen erhöhen, dass definierte Qualitätsanforderungen erreicht werden. Dies bedeutet: sie tragen nicht direkt zur Qualität oder zur Qualitätssteigerung bei, sondern reduzieren nur das Risiko, dass Qualitätsmängel nicht rechtzeitig entdeckt werden.



Alle Maßnahmen, die direkt der Qualitätsverbesserung dienen (Steigerung von Effektivität und Effizienz), sind Teil des Qualitätsmanagements, das über Qualitätssicherung hinausgeht; sie orientieren sich an der Qualitätspolitik und den Qualitätszielen der Organisation!

9.2.4 Konsequenzen für den Aufbau von Qualitätsmanagement-Systemen

Eine umfassende Ausrichtung an den zuvor skizzierten Definitionen und Interpretationen von Qualität und Qualitätsverbesserung sowie dem Ziel der Einrichtung eines leistungsfähigen Qualitätsmanagementsystems muss zur Konsequenz haben,

- dass wir Qualität an den Anforderungen (Erfordernissen und Erwartungen) unserer Kunden ausrichten;
- dass wir den Erfolg des Qualitätsmanagements an der Wirksamkeit und Wirtschaftlichkeit der Prozesse messen, und zwar Effektivität und Effizienz der Leistungsprozesse, aber auch Effektivität und Effizienz der Qualitätssicherungsprozesse;
- dass wir uns nicht damit begnügen, externe Forderungen zu erfüllen, sondern diese als Rahmenbedingungen verstehen, unter denen wir uns im Wettbewerb bewähren wollen.



Die Aufgaben des Qualitätsmanagements:

- Qualitätsplanung:
Qualitätspolitik und Qualitätsziele vorgeben!
 - Qualitätsverbesserung:
Effektivität und Effizienz steigern!
 - Qualitätssicherung: Mehr Vertrauen schaffen!
- Alles andere ist Ballast!

An dieser Vorgabe sollte sich jedes **Qualitätsmanagementsystem** messen lassen:

- Der erste Punkt ist Teil der Führungsaufgaben.
- Der zweite Punkt ist eine Kernaufgabe jeder Organisation.
- Der dritte Punkt ist eine Frage des Risikomanagements: Wie viel ist mir das Vertrauen wert, dass die zutreffenden Qualitätsforderungen erfüllt werden?
 - Wie viel Risiko bin ich bereit zu tragen?
 - Wie viel investiere ich in mehr Sicherheit?
 - Wie viel Sicherheit erreiche ich dadurch?

Ein gutes Qualitätsmanagementsystem ist wirksam und wirtschaftlich!



Praxistipp:

Sie werden nicht immer völlig ohne Ballast auskommen; wenn Sie beispielsweise nach ISO 9001 zertifiziert sind, benötigen Sie Aufzeichnungen, um im Audit zu belegen, dass Sie Ihre Prozesse befolgen; ein Teil dieser Aufzeichnungen dient sicherlich der Qualitätssicherung (→ Vertrauen schaffen), auf einen anderen Teil könnten Sie eigentlich verzichten. Dieser Teil ist „Ballast“, den Sie benötigen, um Ihr Zertifikat aufrechtzuerhalten. Der Mehraufwand sollte zum Nutzen des Zertifikats in einem vernünftigen Verhältnis stehen!

Auf den Punkt gebracht, kann man sagen:

Management muss sich rentieren!

Qualitätsmanagement auch!

Wenn ein Qualitätsmanagementsystem dieser Vorgabe nicht gerecht wird, hat es sein Ziel verfehlt!

Qualitätsmanagement basiert auf der Idee, vernünftige Regeln aufzustellen und diese konsequent zu befolgen. Damit schließt sich der Kreis zu dem Spruch von Taz Daughtry – Sie erinnern sich – „Quality Management, that’s the game with the rules, with the tools, and with the fools: the rules bring in effectiveness; the tools bring in efficiency; and with the fools it is impossible!“

- Wenn ein Qualitätsmanagementsystem mühsam und aufwändig ist, liegt es meist an der Form der Umsetzung → den Tools.
- Wenn ein Qualitätsmanagementsystem nicht wirkt,
 - liegt es entweder an den Regeln, die Sie sich auferlegt haben, oder

- an der fehlenden Akzeptanz, die wiederum stark von der Sinnhaftigkeit der Regeln und der Qualität der Implementierung (den Tools) abhängig ist.
- Denn Narren haben wir in unseren Organisationen nicht so viele, dass es unmöglich wäre ...

Erfolg = Qualität x Akzeptanz



Praxistipp:

Ein gutes Qualitätsmanagementsystem ist wirksam und wirtschaftlich! Qualitätsmanagement- oder Qualitätssicherungsmaßnahmen, die nicht wirksam und wirtschaftlich sind, sind nicht gut! Wenn Sie diese Maxime beachten, brauchen Sie sich um die Akzeptanz Ihres Qualitätsmanagementsystems in der Regel keine Sorgen zu machen.

■ 9.3 Sequenzielle versus iterative Entwicklungsmodelle: Risiko-Strategie

In diesem Kapitel sollen die beiden vorherrschenden Entwicklungsmodelle im IT-Bereich aus Sicht der Qualitätssicherung verglichen werden.

Die *sequenzielle* Entwicklung:

- Wasserfall-Modell
- V-Modell
- Diverse Spielformen einer inkrementellen Implementierung, die auf einem sequenziellen Ansatz aufbauen, bei dem die Anforderungen relativ früh spezifiziert werden.

Die *iterative* Entwicklung:

- RUP – Rational Unified Process;
- MSF – Microsoft Solution Framework;
- Agile Software-Entwicklung, wie z.B.:
 - XP – eXtreme Programming als erster radikaler Ansatz in Richtung Agilität;
 - Scrum als heute prominentester Vertreter der Agilen Software-Entwicklung.

Die Frage, unter denen beide Modelle miteinander verglichen werden sollen, lautet: Welches Modell reduziert in welcher Situation das Risiko, entscheidende Fehler zu machen? Dazu sollen die beiden fundamentalen Risiken der Software-Entwicklung betrachtet werden:

- Das Risiko, das falsche Produkt zu entwickeln, d. h. fachliche Fehler zu machen.
- Das Risiko, das Produkt falsch zu entwickeln, d. h. technische Fehler zu machen.

Eine Publikation zu diesem Thema finden Sie unter [NEH01]; dieses Paper steht auch in der Download-Section von www.nehfort.at zum freien Download bereit.

9.3.1 Sequenzielle Entwicklung: das V-Modell

Die sequenzielle Entwicklung ist seit Mitte der 70er Jahre das vorherrschende Entwicklungsmodell. Sie umfasst folgende Schritte:

- Anforderungsanalyse
- Design
- Implementierung
- Test
- Abnahme

Sie basiert auf der Überlegung, einen Entwicklungsschritt abzuschließen, bevor der nächste begonnen wird. Ein Schritt nach dem anderen, dazwischen qualitätsgesicherte Ergebnisse.

Die Überlegung dahinter ist grundvernünftig: Wenn meine Arbeit auf den vollständigen Ergebnissen des vorhergehenden Entwicklungsschritts aufbaut, dann ist die Gefahr am geringsten, Fehler zu begehen. Dies gilt insbesondere für die Anforderungen.

9.3.1.1 Die Risikostrategie der sequenziellen Entwicklung

Die Risikostrategie der sequenziellen Entwicklung:

Eine frühe Fixierung der Anforderungen verhindert Fehler in der Entwicklung!

Das Leitmotiv der sequenziellen Entwicklung:

Die Entwicklung basiert auf vollständigen Anforderungen!



Die Risikostrategie der sequenziellen Entwicklung:

Wenn wir die Anforderungen früh fixieren, dann minimieren wir das Risiko, in der Entwicklung etwas falsch zu machen, und haben gute Voraussetzungen für ein Fixpreis-Angebot.

Diese Strategie ist erfolgreich, wenn es gelingt, in einer frühen Phase **die richtigen Anforderungen** zu definieren und diese über die Projektdauer **stabil** zu halten. Dies illustriert Abbildung 9.1.

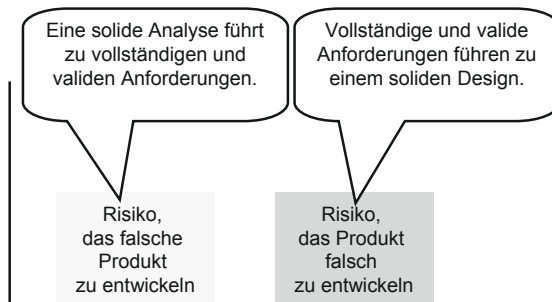


ABBILDUNG 9.1

Die ideale Risiko-Charakteristik der sequenziellen Entwicklung

Für den Fall, dass es nicht gelingt, die richtigen Anforderungen früh zu fixieren, haben wir einen Ausweg gefunden:

Wenn wir den Kunden zwingen, die Anforderungen früh zu fixieren, trägt er das volle Risiko, wenn die Anforderungen falsch oder unvollständig sind!

Das hat den Kunden zwar nicht gefallen, wir konnten jedoch jahrelang überzeugend argumentieren, dass wir so vorgehen müssen: Ohne stabile Anforderungen keine stabile Lösung. Die Reaktion unserer Kunden:

- Fixpreis-Projekte und Abnahmetests bei der Lieferung;
- Wenn das Ergebnis nicht brauchbar war, hatte man als Kunde über die noch ausstehenden Zahlungen ein überzeugendes Argument in der Hand, sich aus dem Dilemma zu befreien ...

9.3.1.2 Die Konsequenzen der sequenziellen Entwicklung

Mit der sequenziellen Entwicklung minimieren wir zwar das Risiko **technischer Fehler**. Gleichzeitig maximieren wir aber das Risiko **fachlicher Fehler!**

- Das Risiko falscher Anforderungen trägt der Kunde!
- Das Risiko, Anforderungen falsch zu verstehen, tragen wir. Doch damit lässt sich leben!

Wenn es uns tatsächlich gelingt, in dieser frühen Phase die Anforderungen stabil zu definieren, dann ist der sequenzielle Entwicklungsprozess höchst effektiv und effizient!

Wie die Studien der Standish Group belegen (siehe Abschnitt 9.1.1), ist das nicht allzu oft gelungen; die Risikostrategie der sequenziellen Entwicklung in der breiten Anwendung ist nicht sehr erfolgreich gewesen.

Einer der Gründe liegt in der Innovationskraft der IT-Branche und der Dynamik, die dadurch ausgelöst wird.

9.3.1.3 Das sequenzielle Dilemma

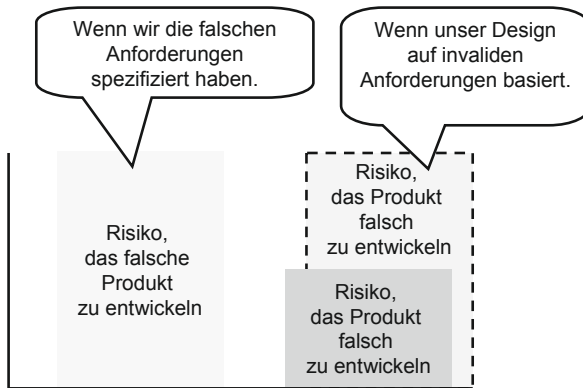
Der sequenzielle Entwicklungsprozess basiert auf der frühen Fixierung der Anforderungen und stößt damit auf folgendes Problem:

Je innovativer eine IT-Lösung sein soll, desto weniger wissen wir zu Beginn über die erforderlichen Eigenschaften des Systems!

Der sequenzielle Entwicklungsprozess basiert auf stabilen Anforderungen; das limitiert unsere Flexibilität und führt uns in der Praxis oft zu folgendem Problem:

Je dynamischer sich ein Geschäftszweig entwickelt, desto rascher ändern sich die Anforderungen an die zugehörige IT-Unterstützung!

Dieses Dilemma der sequenziellen Entwicklung führt in der Praxis oft zu der Risiko-Charakteristik, wie sie in Abbildung 9.2 (nächste Seite) dargelegt wird.

**ABBILDUNG 9.2**

Die resultierende Risiko-Charakteristik der sequenziellen Entwicklung

**Beachten Sie:**

Wir sehen erst am Ende der Entwicklung, ob das Produkt etwas taugt: das heißt, wir investieren viel Zeit und Geld ohne verlässliches Feedback! Damit gehen wir ein beträchtliches Risiko ein!

In dieser unangenehmen Situation haben viele Kunden und Lieferanten gemeinsam einen scheinbaren Ausweg gefunden. In einer stillschweigenden Allianz haben sie entschieden: Wenn wir die Anforderungen ohnehin nicht so genau kennen, müssen auch die Spezifikationen nicht so genau sein: Das reduziert den Termindruck, denn ordentliche Spezifikationen kosten Zeit und Geld. Es hat aber noch einen anderen verlockenden Vorteil:

Wenn wir nicht so genau spezifizieren, haben beide Partner das Gefühl, jeweils ihr eigenes fachliches Risiko zu reduzieren!

Ist die Spezifikation nicht so genau, kann man uns bei Fehlern nicht so leicht festnageln; wir gewinnen dadurch an Verhandlungsspielraum. Diese Defensivstrategie hat schon so manches Projekt umgebracht. Natürlich nennt das niemand „ungenau Spezifikation“; wir nennen es Erfahrung, Kompetenz, Vertrauen – oder schlicht und einfach Termindruck.

9.3.2 Iterative Entwicklung

Die iterative Entwicklung ist als Reaktion auf das sequenzielle Dilemma entstanden. Sie hat ihre Ursprünge in den Ideen von Grady Booch aus den frühen 80er Jahren, die Booch wie folgt auf den Punkt brachte [BOO01]:

„Analyze a little, design a little, code a little, test a little!“

Sie basiert auf der Überlegung,

- dass uns falsche oder instabile Anforderungen nicht weiterhelfen und
- dass wir aus Erfahrungen lernen – mehr und schneller lernen als durch theoretische Analysen.

Ziel ist daher, sich nicht allzu lange mit der Analyse und Definition (ohnehin unzuverlässiger) Anforderungen zu befassen, sondern auf der Basis eines Teils der Anforderungen möglichst rasch einen Teil des Systems zu realisieren, um damit Erfahrungen und Sicherheit für die nächsten Schritte (die nächste Iteration) zu gewinnen.

Die iterative Entwicklung basiert auf der Überlegung, einen Teil des Systems zu entwickeln, bevor die Anforderungen weiter verfeinert und vervollständigt werden:

- Iteration1: Anforderungen → Umsetzung → Feedback;
- Iteration2: Anforderungen → Umsetzung → Feedback;
- Iteration3: Anforderungen → Umsetzung → Feedback;
- usw.

Auch hier geschieht ein Entwicklungsschritt nach dem anderen, auch hier mit qualitätsgesicherten Ergebnissen: Das Ergebnis jeder Iteration führt zu einer Bestätigung oder Korrektur der bisherigen Vorgaben. Die neuen Erkenntnisse unterstützen die weitere Entwicklung.



Praxistipp:

Wenn wir die Anforderungen zu Beginn nicht so gut kennen, ist die Gefahr einer Fehlentwicklung am geringsten, wenn wir mit einem kleinen Teil beginnen und die weiteren Entscheidungen auf später verschieben.

9.3.2.1 Die Risikostrategie der iterativen Entwicklung

Die Risikostrategie der iterativen Entwicklung:

Eine schrittweise Entwicklung der Anforderungen verhindert die Entwicklung einer falschen Lösung!

Das Leitmotiv der iterativen Entwicklung:

Die Entwicklung basiert auf einer flexiblen und robusten Architektur!



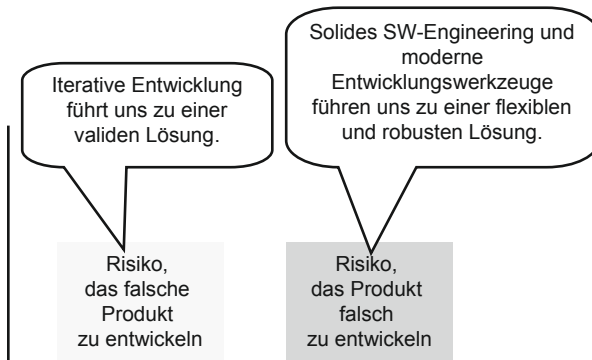
Die Risikostrategie der iterativen Entwicklung:

Wenn wir die Anforderungen nicht so genau kennen oder diese sich rasch ändern können, minimieren wir das Risiko,

- wenn wir Entscheidungen möglichst spät treffen!
- wenn wir ein rasches Feedback ermöglichen!
- wenn wir für einen raschen „Return on Investment“ sorgen!

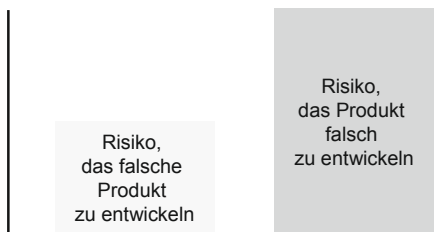
Das damit verbundene technische Risiko können wir eher eingehen als das fachliche Risiko der sequenziellen Entwicklung!

Diese Strategie ist erfolgreich, wenn es gelingt, die Architektur des Systems so flexibel und robust zu halten, dass wir bei späteren Entscheidungen nicht alles wegwerfen und neu beginnen müssen. Dies verdeutlicht Abbildung 9.3 (nächste Seite).

**ABBILDUNG 9.3**

Die ideale Risiko-Charakteristik der iterativen Entwicklung

Wenn wir mit der Entwicklung beginnen, obwohl viele Anforderungen noch nicht definiert sind, kennen wir beim Design einen Großteil der Anforderungen noch nicht. Das erhöht naturgemäß das Risiko von Designentscheidungen, die sich später als Fehlentscheidungen herausstellen, und führt uns zu der initialen Risiko-Charakteristik der iterativen Entwicklung, wie sie in Abbildung 9.4 illustriert wird.

**ABBILDUNG 9.4**

Die initiale Risiko-Charakteristik der iterativen Entwicklung

Das Risiko falscher oder unzureichender Design-Entscheidungen hat sich in den letzten 20 Jahren durch den technischen Fortschritt unserer Software-Entwicklungsumgebungen und der IT-Infrastruktur deutlich reduziert. Es ist heute wesentlich leichter möglich, Teile eines Software-Systems auszutauschen oder zu verändern, ohne damit automatisch größere Änderungen in allen anderen Teilbereichen des Systems auszulösen.

Darüber hinaus wurde für die iterative Entwicklung eine eigene Technik entwickelt, das Design-Risiko über die Laufzeit der Entwicklung zu minimieren: Refactoring (dafür findet man auch in der deutschen Fachliteratur keine deutsche Übersetzung).

Refactoring bedeutet, das Design am Ende jeder Iteration zu überarbeiten, um es möglichst klar, sauber und einfach zu halten:

- Redundanter Code wird entfernt → Lokalität.
- Nicht genutzte Funktionalität wird entfernt.
- Das Design wird punktuell überarbeitet, um für die nächsten Iterationen ein aufgeräumtes und übersichtliches System zu hinterlassen.

Refactoring verhindert, dass das Design durch die kurzen Iterationszyklen rasch „altert“ und damit unübersichtlich und schwerfällig bezüglich Änderungen wird. Ohne Refactoring läuft man in der iterativen Entwicklung Gefahr, sehr bald mit den typischen Wartungsproblemen älterer SW-Systeme konfrontiert zu werden.

9.3.2.2 Die Konsequenzen der iterativen Entwicklung

Mit der iterativen Entwicklung minimieren wir zwar das Risiko **fachlicher Fehler**. Gleichzeitig maximieren wir aber das Risiko **technischer Fehler**!

Doch dieses Risiko ist weitaus geringer als in den 80er Jahren des letzten Jahrhunderts, wenn wir die Vorteile der aktuellen Entwicklungssysteme nutzen und Refactoring konsequent einsetzen.

Die iterative Entwicklung hat noch einige weitere Konsequenzen:

- Wir benötigen während der gesamten Projektlaufzeit einen intensiven Kontakt zu unserem Kunden (für Feedback und neue Vorgaben). Das verändert die Form der Zusammenarbeit.
- Wir müssen viel öfter Entscheidungen treffen (am Beginn und Ende jeder Iteration) und daher öfter planen (die nächste Iteration).
- Wir brauchen eine Vision, die unserer Entwicklung eine klare Richtung gibt. Diese Vision beschreibt den Geschäftszweck der Anwendung (seinen erwarteten Nutzen) und seine wesentlichen Eigenschaften aus Kundensicht. Diese Vision ersetzt in den frühen Iterationen die noch fehlenden Anforderungen. Die Entwickler müssen sich daher viel stärker mit den Zielen und Visionen der Auftraggeber beschäftigen als in der traditionellen Software-Entwicklung.
- Der Wert der typischen Zwischenergebnisse der Software-Entwicklung, wie Anforderungs- oder Designdokumente, ist geringer als in der sequenziellen Entwicklung. Dies hat zur Konsequenz, dass auch der Nutzen traditioneller Qualitätssicherungsmaßnahmen (Review von Dokumenten) sinkt.
- Dafür gewinnen die Einhaltung von Programmier-Richtlinien und ein sauberer Code stark an Bedeutung für das Projektteam → Disziplin in der Programmierung.
- Testen wird zu einem Lenkungsprozess zwischen den Iterationen, die Automatisierung von Tests wird zu einer zentralen Qualitätssicherungsmaßnahme.

Über jeden dieser Aspekte könnte man ein ganzes Kapitel schreiben, doch würde das den Rahmen dieser Publikation sprengen.

Eine wesentliche praktische Konsequenz ist sicherlich, dass die Kernaktivitäten der Software-Entwicklung – Design, Programmierung und Testen – wieder an Bedeutung gewonnen haben.

Damit kommen wir bei einer erfolgreichen Implementierung des iterativen Ansatzes zu der in Abbildung 9.5 dargestellten Risiko-Charakteristik.

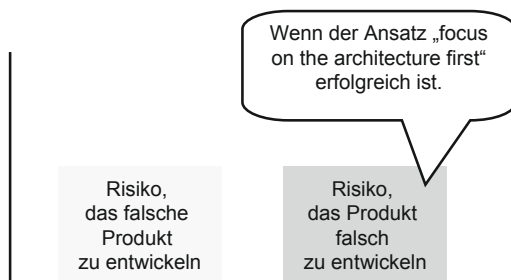


ABBILDUNG 9.5

Die resultierende Risiko-Charakteristik der iterativen Entwicklung, wenn der Ansatz „focus on the architecture first“ erfolgreich ist!

Die konsequenteste Interpretation der iterativen Entwicklung findet man in den **agilen Software-Entwicklungsmethoden**, wie eXtreme Programming, Scrum oder Feature Driven Development.

Die Grundkonzepte der agilen Software-Entwicklung sind in Abschnitt 9.6.4 „Prozessqualität in den agilen Prozessen“ erläutert.

9.3.3 Schlussfolgerungen zum Vorgehensmodell in der Software-Entwicklung unter Qualitätsaspekten

9.3.3.1 Das richtige Vorgehensmodell für das richtige Projekt

Die Wahl eines Vorgehensmodells ist eine sensible Entscheidung, bei der man die Projekt-Rahmenbedingungen berücksichtigen sollte:

- Die sequenzielle Software-Entwicklung ist der optimale Ansatz für Software-Projekte, in denen stabile Anforderungen oder besondere Rahmenbedingungen (z.B. sicherheitskritische Systeme oder integrierte Echtzeitsysteme) für ein strikt geplantes (vorhersehbares) Vorgehen sprechen.
- Die iterative Entwicklung ist der optimale Ansatz für Softwareprojekte, in denen es so viele Unsicherheiten gibt, dass die Anforderungen zu Beginn nicht stabil definiert werden können. Wenn in einer solchen Situation die Anforderungen schrittweise erarbeitet und umgesetzt werden, bestehen gute Chancen, über diesen adaptiven Ansatz zu einer brauchbaren Lösung zu gelangen.

9.3.3.2 Kriterien zur Auswahl des Vorgehensmodells

Die meisten Projekte können nicht so klar klassifiziert werden wie in den oben genannten Szenarien. Die folgenden Fragen sollen eine Orientierungshilfe für die Wahl des passenden Software-Entwicklungsansatzes geben:



Wird das Projekt öffentlich ausgeschrieben?

- Ja → Iterative Entwicklung kann in jenen Bereichen helfen, wo die Ausschreibung mangels Detailliertheit große Interpretationsspielräume lässt.
- Nein → Ein iterativer Prozess kann für das gesamte Projekt in Erwägung gezogen werden!

Haben Sie einen internen Kunden?

- Ja → Der iterative Ansatz kann die Lücke zwischen Theorie und Praxis schließen, die Sie in der Vergangenheit möglicherweise hatten.
- Nein → Der iterative Ansatz erfordert eine intensive Kooperation des externen Kunden – können Sie diese sicherstellen?

Sind Sie sicher, dass der Kunde genau weiß, was er braucht?

- Ja → Ein starker Indikator für den sequenziellen Ansatz.
- Nein → Der iterative Ansatz könnte helfen, das Problem in den Griff zu bekommen.

Sind Sie von der Kompetenz des Projektteams im Anwendungsgebiet überzeugt?

- Ja → Der sequenzielle Ansatz hat gute Erfolgsaussichten, wenn der Kunde weiß, was er will.
- Nein → Der iterative Ansatz könnte Ihr Problem entschärfen.

Sind Sie sicher, dass Ihr Kunde für das Projekt kompetente Leute abstellt, von denen Sie ein qualifiziertes Feedback erhalten?

- Ja → Gute Voraussetzung für einen iterativen Software-Entwicklungsansatz.
- Nein → Präzise Anforderungen am Anfang könnten Ihr Problem entschärfen.

Sind die Mitglieder des Software-Entwicklungsteams an den Visionen des Kunden interessiert?

- Ja → Gute Voraussetzung für jeden Software-Entwicklungsansatz.
- Nein → Präzise Anforderungen am Anfang könnten Ihr Problem entschärfen.

Wie groß ist Ihr Projekt/System?

- Sehr großes System und langfristige Projekte → Ein iterativer Ansatz kann die Komplexität reduzieren und Ihr Projekt beschleunigen. Das könnte Ihnen helfen, essenzielle Aspekte Ihres Systems in Betrieb zu nehmen (→ „return on investment“), bevor eine Veränderung in den Rahmenbedingungen Ihr Projekt möglicherweise kippt.
- Kleine Projekte → Ein iterativer/agiler Ansatz könnte dabei helfen, den Dokumentations- und Verwaltungsaufwand zu reduzieren, der in der Vergangenheit Probleme bereitet hat. Das könnte Ihr Projekt beschleunigen, ohne Ihre Risiken zu erhöhen.

Neben diesen allgemeinen Fragen können Sie in Ihren eigenen Softwareprojekten eine Menge Indikatoren finden. Sie müssen nur ein Auge auf die kritischen Situationen werfen:

- In welchen Situationen ist Ihr Team erfolgreich?
- In welchen Situationen haben Sie Probleme?

Welche Risikostrategie könnte Ihre Erfolgschancen verbessern?

- Die sequenzielle Entwicklung, oder
- die iterative Entwicklung?



Praxistipp:

Treffen Sie eine klare Entscheidung, denken Sie an die Implikationen und gehen Sie diesen Weg konsequent!

Bei Halbheiten laufen Sie Gefahr, die Risiken beider Seiten auf sich zu nehmen, ohne von den Vorteilen eines der beiden Ansätze konsequent zu profitieren!

■ 9.4 Qualität von Produkten

9.4.1 Brauchbarkeit und Wartbarkeit

Die Qualität eines Produkts – so auch von IT-Produkten wie Software – lässt sich mit zwei übergeordneten Qualitätsmerkmalen beschreiben:

- Brauchbarkeit und
- Wartbarkeit

„**Brauchbarkeit**“ beschreibt die Qualität des im Einsatz befindlichen Produkts aus der Sicht des Anwenders. Sie umfasst die Eignung des Produkts für einen bestimmten Anwendungszweck und damit alle Qualitätsmerkmale, die sich im Produkteinsatz äußern, wie beispielsweise Funktionalität (Angemessenheit und Korrektheit), Zuverlässigkeit und Fehlertoleranz, Verständlichkeit und Bedienbarkeit oder Zeitverhalten und Verbrauchsverhalten.

„**Wartbarkeit**“ beschreibt die Qualität des Produkts aus der Sicht der Entwickler oder des IT-Betriebs. Sie umfasst die Eignung des Produkts, es in einer bestimmten Systemumgebung einzusetzen (→ Installierbarkeit, Übertragbarkeit) und es zu verändern und anzupassen (Fehlerbehebung oder Weiterentwicklung → Verständlichkeit, Änderungsfreundlichkeit, Testbarkeit, Stabilität).

Eine detaillierte Gliederung der Qualitätsmerkmale finden Sie in Abschnitt 9.6.2 ISO/IEC 9126 Part 1–4: Information Technology – Product Quality.

Die **Brauchbarkeit** entscheidet über die Akzeptanz des Produkts bei den Kunden; schwere Mängel in der Brauchbarkeit müssen rasch behoben werden, damit das Produkt seinen Zweck erfüllen kann.

Die **Wartbarkeit** entscheidet über die wirtschaftliche Einsatzdauer eines Produkts. Kaum ein Software-Produkt bleibt über längere Zeit unverändert im Einsatz. Fehler sind zu beheben, geänderte Einsatzbedingungen und neue Anforderungen erfordern funktionale Änderungen und Erweiterungen, damit die Software über längere Zeit brauchbar bleibt.



Praxistipp:

Die Anforderungen an die Brauchbarkeit haben in der Realisierung einen starken Anwalt: den Kunden. Sie werden mehr oder weniger klar definiert und bei der Übergabe eingefordert. Allfällige Mängel fallen in der Regel rasch auf: beim Systemtest, bei der Abnahme oder spätestens im Betrieb; ihre Behebung ist in den meisten Fällen ein Muss!

Was ist mit der Wartbarkeit? Wer stellt hier Anforderungen? Wer definiert sie und prüft ihre Erfüllung? In vielen Projekten sieht es bei der Beantwortung dieser Fragen nicht gut aus! Tom DeMarco stellte diesbezüglich schon vor mehr als 15 Jahren das Theorem der Kostenwanderung auf und meinte:

*„Kosten tendieren zur Wanderung von Posten, die gut beobachtet werden,
zu Posten, die weniger gut beobachtet werden.“*

Das am weitesten verbreitete Phänomen der Kostenwanderung ist die Wanderung der Kosten vom Projekt in die Wartung.

In der klassischen sequenziellen Entwicklung beträgt das Verhältnis von Entwicklungs- zu Wartungskosten an den Gesamtkosten über den gesamten Lebenszyklus etwa 30% zu 70% (Abbildung 9.6)!

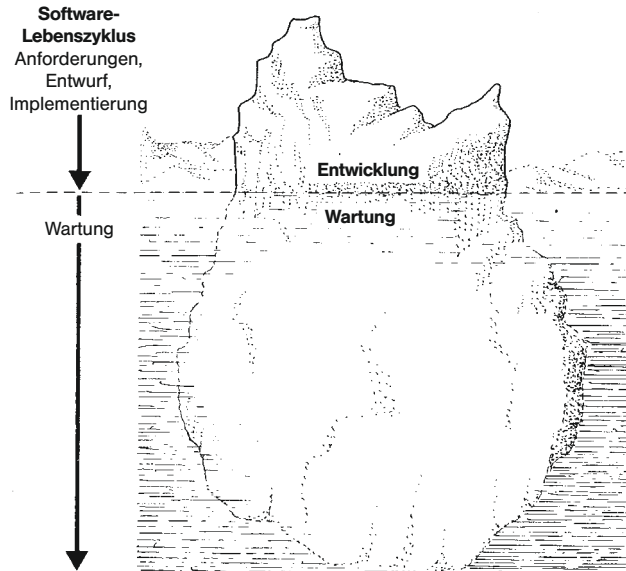


ABBILDUNG 9.6

Der Eisberg: Entwicklung und Wartung

Mängel in der Wartbarkeit gehen also ins Geld! Hier kann die Qualitätssicherung ansetzen! Anforderungen an die Wartbarkeit erhöhen möglicherweise die Projektkosten, amortisieren sich aber auf längere Sicht. Dies setzt voraus, dass das Management über die Betrachtungseinheit „Projekt“ hinausblickt und im Projekt Investitionen einfordert oder ermöglicht, die über den Projektabschluss hinaus wirken. In diesem Punkt steht uns der Projektgedanke als einmalige zeitlich abgeschlossene Aufgabe mit definiertem Termin- und Kostenrahmen eindeutig im Wege, wenn wir Qualitätsmaßnahmen einführen wollen!

Qualität bedeutet:

1. Wir müssen die Anforderungen (Erfordernisse und Erwartungen) erkennen und verstehen!
2. Wir müssen die Leistung erbringen können!

Diesen beiden Aspekten sind die zwei folgenden Abschnitte gewidmet:

- Qualität der Anforderungen
- Qualität der Lösung

9.4.2 Qualität der Anforderungen

Quality is conformance to requirements.

Qualität bedeutet: Leistung : Anforderungen = 1.

Ohne präzise Kenntnis der Anforderungen wird Qualität zum Lotteriespiel. Wie kommen wir zu diesen Anforderungen? Das müssen Sie wissen:

- Das Wichtigste ist sicherlich, den Zweck der Anwendung zu verstehen.
 - Wofür will der Kunde ein neues System?
 - Was bezweckt er damit?
 - Warum ist er bereit zu investieren?
 - Was sind seine Erfolgskriterien für unser Projekt?
- Daraus lässt sich ableiten, welche Funktionen und Eigenschaften für diese Lösung essenziell sind! Damit haben wir den Kern der Anforderungen gefunden, den wir nun schrittweise um folgende Anforderungen ergänzen:
 - Weitere nötige oder erwünschte Funktionen.
 - Weitere nicht funktionale Anforderungen, die wir z. B. anhand der Qualitätsmerkmale der ISO 9126 strukturieren können.
- Vorgaben bezüglich der technischen Lösung (Required Restrictions), wie z. B.: Vorgabe des Betriebssystems, der zugrunde liegenden Datenbank oder technischer Schnittstellen.



Was brauchen wir für gute Anforderungen?

- Das Erste, was wir brauchen, sind die richtigen Ansprechpartner – im Fachjargon Requirements-Provider genannt.
- Das Zweite sind die richtigen Software-Ingenieure, die diese Anforderungen analysieren, sauber formulieren und dokumentieren.
- Das Dritte ist ein passendes Vorgehen zur Ermittlung der Anforderungen.
- Das vierte Element ist die Qualitätssicherung der Anforderungen.

9.4.2.1 Ansprechpartner – Requirements Provider

Unsere Ansprechpartner für die Anforderungsentwicklung sollten über folgende Voraussetzungen verfügen:

- Erfahrung und Sachverstand im Anwendungsgebiet;
- Interesse und Verständnis für das Lösungskonzept;
- Kenntnisse der einschlägigen Vorschriften: sie führen uns zu den Anforderungen, die verpflichtend sind, weil von dritter Seite vorgeschrieben;
- technische Kompetenz, um technische Vorgaben festzulegen, die bei der Realisierung zu befolgen sind und den Lieferanten bei der Gestaltung der Lösung einschränken;
- technisches Verständnis, um die Abbildung der User Requirements auf System Requirements nachvollziehen zu können;
- ausreichende Entscheidungskompetenz, um tragfähige Vereinbarungen abschließen zu

können; Sie erinnern sich: *Qualität basiert auf Vereinbarungen – Vereinbarungen über Anforderungen!*

**Praxistipp:**

Es ist leicht einsichtig, dass wir für diese Anforderungen nicht einen, sondern eine Reihe von Ansprechpartnern benötigen; darüber hinaus ist von entscheidender Bedeutung, bei der Anforderungsanalyse alle relevanten Interessenspartner ins Boot zu holen.

9.4.2.2 Anforderungsentwickler

Anforderungsentwickler sollten folgende Voraussetzungen erfüllen:

- Interesse und Verständnis für das Anwendungsgebiet;
- Verständnis der technischen Möglichkeiten;
- die Fähigkeit, User Requirements in System Requirements zu übertragen;
- die Fähigkeit zu strukturieren;
- Genauigkeit und sprachliche Präzision;
- kommunikative Fähigkeiten;
- ein klares Rollenverständnis: Der Kunde trifft fachliche Entscheidungen – der Lieferant trifft technische Entscheidungen. Der Anforderungsentwickler ist diesbezüglich Lieferant!
- die Fähigkeit, Vereinbarungen auszuhandeln.

Ein guter Anforderungsentwickler für Kundenanforderungen und Systemanforderungen muss also weder im Anwendungsgebiet noch als Software-Entwickler ein Experte sein; viel wichtiger sind seine Fähigkeiten als Vermittler zwischen den beiden Welten.

9.4.2.3 Anforderungsentwicklung: das Vorgehen

Wie gelangen wir zu den Anforderungen an ein IT-Produkt? Typischerweise in einem mehrstufigen Prozess:

- Definition der Kundenanforderungen (User Requirements);
- Definition der Systemanforderungen (sie definieren das zu entwickelnde oder zu liefernde System);
- Definition der Anforderungen an die Komponenten des Systems, die von den Systemanforderungen und der Architektur abgeleitet werden.

Wenn wir die Anforderungen so unterteilen, wird sofort klar, dass Letztere nicht unabhängig vom Konzept der Lösung sein können, sondern Schritt für Schritt parallel zur Konkretisierung der Lösung erarbeitet und verfeinert werden.

Der von der Lösung völlig unabhängige Anforderungsprozess ist also Fiktion! Das Prinzip, Produkt-Anforderungen unabhängig von der Implementierung zu definieren, gilt jedoch weiterhin. Allerdings nur auf der jeweils betrachteten Abstraktionsebene. Die Design-Entscheidungen auf einer Ebene sind die Anforderungen für die nächste.

Das Design der Geschäftsprozesse entscheidet über einen Teil der Kundenanforderungen an die IT-Lösung. Das Design des IT-Systems (Systemarchitektur) entscheidet über einen Teil der

Systemanforderungen. Die Aufteilung der Funktionalität auf die Komponenten des Systems (eine Design-Entscheidung) entscheidet über einen Teil der Anforderungen an diese Komponenten. Von der Logik her ein strikter Top-down-Prozess, der in der Praxis nicht so stringent gelebt wird, da die einzelnen Entscheidungen meist nicht so strikt Top-down gefällt werden. Damit bleibt die Idee, dass Produkt-Anforderungen den Anbieter beim Design der Lösung nicht unnötig einschränken sollen, erhalten. Nötige Einschränkungen sind als Realisierungsvorgaben und damit als Anforderungen zu betrachten.

9.4.2.4 Qualitätssicherung der Anforderungen

Ohne Qualitätssicherung bekommen wir keine brauchbaren Anforderungen!

Die Qualitätssicherung der Anforderungen beginnt bei der Auswahl der richtigen Ansprechpartner für die Analyse und endet bei der qualifizierten Prüfung und Bestätigung der Anforderungen.

Im traditionellen (sequenziellen) Entwicklungsprozess erfolgt die Prüfung und Bestätigung der Anforderungen in der Regel über Reviews (siehe Abschnitt 9.7) und die Freigabe der Anforderungsdokumente. Zur Unterstützung können bei Bedarf Prototypen oder bei Standard-SW-Lösungen Demo-Installationen dienen.

Der entsprechende **Qualitätssicherungszyklus** sieht etwa wie folgt aus:

- Anforderungen entwickeln;
- Anforderungen dokumentieren;
- Anforderungsdokumente prüfen → Review;
- Anforderungsdokumente bei Bedarf überarbeiten und neuerlich prüfen;
- Anforderungen (= Anforderungsdokumente) freigeben.

Im iterativen Software-Entwicklungsprozess verschiebt sich der Schwerpunkt der Qualitätssicherung der Anforderungen schnell von den Reviews der Anforderungsdokumente zum Test der Ergebnisse der laufenden Iteration.

Der Qualitätssicherungszyklus sieht dabei etwa wie folgt aus:

- Anforderungen für die laufende Iteration entwickeln und dokumentieren (die Dokumentation fällt dabei wesentlich knapper aus als im sequenziellen Prozess);
- Anforderungen gegen die Vision prüfen: Geht die Entwicklung in die richtige Richtung?
- Anforderungen in der Iteration rasch umsetzen;
- die Software der laufenden Iteration testen;
- aus den Erkenntnissen des Tests werden einerseits die Anforderungen geprüft und bestätigt bzw. korrigiert und andererseits die Anforderungen für die nächste Iteration entwickelt.

In beiden Fällen wird der oft als Deming-Cycle bezeichnete Qualitätssicherungszyklus eingehalten:

Planen – umsetzen – prüfen – verbessern!



Anforderungen ohne Qualitätssicherung umzusetzen, ist Zeitverschwendung! Wer etwas effizient realisieren will, muss dafür sorgen, dass er es beim ersten Mal möglichst richtig macht! Dafür brauchen wir qualitätsgesicherte Anforderungen!

9.4.3 Qualität der Lösung

Dem Capability Maturity-Modell – CMMI [CMMI] entstammt eine wichtige Botschaft:

Gute Lösungen basieren auf Alternativen!

Good design is based on alternatives!

Gute Lösungen basieren aber auch auf nachvollziehbaren Kriterien zur Bewertung der Alternativen. Das wichtigste Kriterium ist die Erfüllung der Anforderungen (unter der Annahme, dass wir die richtigen Anforderungen definiert haben). Nun ist die Erfüllung der Anforderungen in der Regel keine einfache Ja/Nein-Entscheidung. Verschiedene Lösungen

- können die Anforderungen mehr oder weniger gut erfüllen;
- sind schnell umsetzbar oder brauchen etwas länger;
- verursachen unterschiedlich hohe Aufwände oder Kosten;
- sind mit unterschiedlichen Risiken verbunden.



Beachten Sie:

Ohne Alternativen bewusst zu betrachten, kommen wir zu irgendeiner Lösung, die unsere Anforderungen irgendwie erfüllt. Mögliche Alternativen, die verworfen wurden, sind nicht nachvollziehbar, da die Entscheidungen implizit getroffen wurden.

Ohne Kriterien zur Bewertung der Alternativen ist es schwer zu beurteilen, welche Lösung unter den gegebenen Umständen zu bevorzugen ist. Mögliche Alternativen sind zwar bekannt, aber es ist nicht nachvollziehbar, ob die getroffene Entscheidung eine gute Entscheidung ist.

Es sind jedoch nicht alle Kriterien, die wir betrachten sollten, „Anforderungen“; viele Eigenschaften abseits der eigentlichen Anforderungen sind wünschenswert („nice to have“), andere sind störend oder hinderlich.

Ein **qualifizierter Entscheidungsprozess** schafft hier Transparenz:

- Ziele
- Alternativen
- Bewertungskriterien, mit denen sich Zielerreichung messen lässt
- Bewertung der Alternativen
- Reihung der Alternativen
- Auswahl der bevorzugten Alternative und Begründung der Entscheidung.

Dabei orientieren sich unsere Bewertungskriterien an der angestrebten **Qualität der Lösung**. Im Folgenden soll das Thema „Qualität der Lösung“ unter diesen Aspekten betrachtet werden:

- *Externe Qualitätsmerkmale:*
Jene Qualitätsmerkmale, die sich von außen beobachten lassen, z. B. durch den Anwender oder den Tester im Abnahmetest.
- *Interne Qualitätsmerkmale:*
Jene Qualitätsmerkmale, die sich bei einem Blick ins Innere des Systems beobachten lassen.
- *„Quality-in-Use“:*
Die Sicht des Anwenders auf die Qualität des Systems in einem bestimmten Anwendungskontext.

Dieses Konzept stammt aus der „ISO/IEC 9126: Information Technology – Product Quality“, die in Abschnitt 9.7.2 kurz vorgestellt wird.

9.4.3.1 Qualität der Lösung – äußere Qualität

Für die Betrachtung hier möchte ich die externen Qualitätsmerkmale und die „Quality-in-Use“ gemeinsam unter dem Begriff „äußere Qualität“ zusammenfassen.

Die äußere Qualität entscheidet in der Regel über die **Brauchbarkeit** des Produkts; schwere Mängel in der Brauchbarkeit müssen rasch behoben werden, damit das Produkt seinen Zweck erfüllen kann.

Die Kriterien für die Brauchbarkeit sind mit dem Auftraggeber zu klären; entweder bereits in der Spezifikationsphase oder schrittweise im Zuge der Realisierung, wenn diese Kriterien im Zuge der Bewertung von Alternativen benötigt werden.

Alle Fehler, die man hier begeht, fallen einem spätestens bei der Abnahme auf den Kopf. Der häufigste Fehler: Implizite Annahmen durch die Entwickler ersetzen fehlende explizite Vorgaben oder Vereinbarungen; diese stellen sich später oft als unzutreffend heraus!



Praxistipp:

Ob bzw. wie gut die Kriterien für die Brauchbarkeit unserer Lösung erreicht werden, ist bei jedem Entwicklungsschritt (Design, Implementierung, Test) zu prüfen. Wichtige Entscheidungen (hinsichtlich der Auswahl der bevorzugten Lösung aus verschiedenen Varianten) sollten später nachvollziehbar sein.

9.4.3.2 Qualität der Lösung – innere Qualität

Die innere Qualität beeinflusst in der Regel zwei Faktoren:

- Sie entscheidet oft darüber, wie gut eine Anforderung erfüllt wird und ist damit oft ein Schlüssel zur **Kundenzufriedenheit**.
- Sie entscheidet in der Regel über die **Wartbarkeit** und damit über die wirtschaftliche Einsatzdauer eines Produkts.

Für die inneren Qualitätsmerkmale bekommen Sie in der Regel keine Vorgaben von Ihren Kunden. Diese müssen Sie also selber festlegen, d.h. schrittweise mit dem Fortschreiten der Entwicklung erarbeiten (Architektur, Detailed Design, Implementierung).

Alle hier begangenen Fehler fallen einem spätestens bei der Wartung auf den Kopf:

- Die Durchführung von Änderungen (z.B. Bug-Fixes) wird kompliziert und ist selbst fehleranfällig.
- Die Weiterentwicklung des Produkts zur Realisierung neuer Leistungsmerkmale wird aufwändiger als gedacht, manche Features lassen sich gar nicht realisieren oder können nur unzureichend unterstützt werden.

Der häufigste Fehler: Es werden keine Anforderungen an die innere Qualität definiert; man verlässt sich auf die Professionalität und die Qualitätsansprüche der Entwickler. Das Ergebnis ist in der Regel eine undefinierte, manchmal von Modul zu Modul völlig unterschiedliche innere Qualität. Das kann in beide Richtungen ausschlagen:

- in eine völlig unzureichende innere Qualität;
- in eine übertrieben hohe innere Qualität.

In der Praxis führt der übliche Termindruck eher zu einer (wie sich meist erst später herausstellt) völlig unzureichenden inneren Qualität; es gibt jedoch auch Fälle, in denen der Qualitätsanspruch einzelner Projektmitarbeiter zu so genannten Goldrand-Lösungen führt, die das Projekt unnötig verteuern oder verzögern.

Ob bzw. wie gut die Kriterien für die innere Qualität von unserer Lösung erreicht werden, ist bei jedem Entwicklungsschritt (Design, Implementierung, Test) zu prüfen.

Welche Kriterien für die innere Qualität anzusetzen sind, ist von zwei Faktoren abhängig:

- von den externen Anforderungen;
- von der Technik der Implementierung und der gewählten Entwicklungsumgebung.

Wichtige Entscheidungen hinsichtlich der Auswahl der bevorzugten Lösung aus verschiedenen Varianten sollten später nachvollziehbar sein.

■ 9.5 Qualität des Projekts

IT-Projektmanagement wird in diesem Handbuch ausführlicher in Kapitel 5 behandelt. An dieser Stelle soll nur kurz dargelegt werden, welche Punkte aus Sicht der Qualitätssicherung besonders zu beachten sind, und zwar

- bei der Planung von Projekten;
- bei der Projektleitung (Projekt-Controlling).

9.5.1 Qualität in der Projektplanung

Die folgende Checkliste kann Ihnen dabei helfen, die qualitätskritischen Punkte in der Projektplanung zu identifizieren:



1. Motiv und Ziele klären

- Warum wird das Projekt gemacht?
- Was sind aus Sicht des Auftraggebers die wichtigsten Erfolgsfaktoren?
- Woran wird der Auftraggeber den Erfolg messen?
Wenn Sie darauf keine konkrete Antwort erhalten, haben Sie einen wichtigen Risikofaktor identifiziert!
- Welche Produkteigenschaften sind essenziell?

2. Termin und Kostenrahmen klären

- Zieltermin und Budget
- Was hat im Falle von Zielkonflikten Priorität:
 - die volle Erfüllung der Produktanforderungen?
 - der Zieltermin?
 - die Einhaltung des Budgetrahmens?

3. Auftraggeber- und Auftragnehmerbeziehung klären

- Identifikation der Entscheidungsträger auf beiden Seiten
- Identifikation sonstiger Interessenspartner („Stakeholder“)
- Vereinbarung der Zuständigkeiten
- Vereinbarung der Berichtswege
- Vereinbarung der Eskalationsprozeduren

4. Projektumfeldanalyse

- Welche Chancen und Risiken ergeben sich aus dem Projektumfeld?

5. Planung

- Planung der Ergebnisse (des Lieferumfangs)
- Planung des Vorgehens
- Planung des Ressourceneinsatzes und der Termine
- Plausibilitätsprüfung: Passen Aufgaben und Termin- bzw. Kostenrahmen zusammen?
Wenn nein: Prioritäten setzen lassen nach dem folgenden Prinzip:
 - Der Kunde trifft geschäftliche Entscheidungen,
 - der Lieferant trifft technische Entscheidungen!

6. Aktives Risikomanagement betreiben

- Risiken identifizieren und analysieren
- Schadensausmaß und Eintrittswahrscheinlichkeit abschätzen
- Vorbeugende Maßnahmen planen, die entweder
 - die Eintrittswahrscheinlichkeit oder
 - den möglichen Schaden reduzieren.
- Abhilfemaßnahmen planen für den Fall, dass der Schaden eintritt.

9.5.1.1 Termindruck als Qualitätskiller

Zu knappe Planung und der daraus entstehende Termin- und Kostendruck sind die wirkungsvollsten Qualitätskiller! Jeder Projektplan, der nur die Aufwände für jene Aktivitäten berücksichtigt, die zum Planungszeitpunkt bekannt sind, ist zwangsläufig zu knapp bemessen. Er plant auf Basis eines Best-Case-Szenarios, das in der Praxis so gut wie nie eintritt.

Ein Projektplan mit Augenmaß enthält Planposten für Aufwände, die wir zwar heute noch nicht genau kennen, mit größter Wahrscheinlichkeit aber leisten müssen:

- für Mehraufwände, die nötig werden, wenn aus einem Risiko ein Schadensfall geworden ist. Zu erwarten, dass keines der Risiken schlagend wird, wäre naiv!
- für Mehraufwände, die sich aus der Änderung von Anforderungen ergeben:
 - Aufwände für das Change-Management;
 - Aufwände zur Realisierung heute noch unbekannter Anforderungen, die nötig sind, um das Produkt brauchbar zu machen.

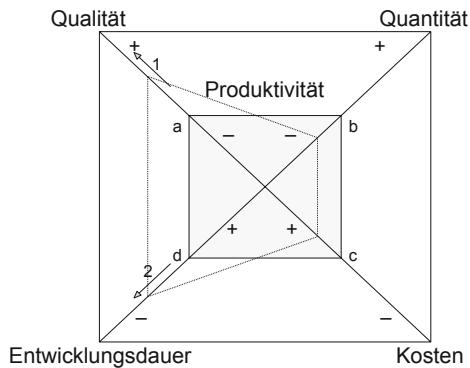
Diese Aufwände haben wir in jedem Fall – so sicher wie das Amen im Gebet! Unabhängig davon, ob oder wie diese Mehraufwände vertraglich abgegolten werden, sollten wir sie in der Planung berücksichtigen – weil sonst jedes kleine Problem unseren schönen Best-Case-Plan über den Haufen wirft. Diese Planposten sind also keinesfalls als „Polster“ für Unvorhergesehenes zu betrachten, sie sind vorhersehbar, aber noch nicht im Detail bekannt! Diese Planposten eignen sich daher auch nicht als disponierbare Verhandlungsmasse!

9.5.1.2 Planung mit dem Bruchfaktor

Im Aufwandsschätzverfahren CoCoMo II [BOE01] werden die Aufwände für vorhersehbare, aber noch nicht im Detail bekannte Aufgaben als Bruchfaktor bezeichnet und mit einem gewissen Prozentsatz in der Planung berücksichtigt. Wie in der Fertigung: Wenn 100 Stück geliefert werden sollen, werden 102 Stück produziert (oder 107 Stück, je nach Qualität des Fertigungsprozesses); der Rest ist als möglicher Ausschuss (Bruch) kalkuliert. Wenn Sie den Bruch nicht mitplanen, werden Sie den Auftrag nicht voll erfüllen können. Der Bruchfaktor in gut geführten IT-Projekten beträgt nach meinen Erfahrungen typischerweise zwischen 10% und 20%. In dieser Betrachtung sind Mehraufwände aus allfälligen Schätzfehlern noch gar nicht berücksichtigt.

9.5.1.3 Das Teufelsquadrat

Den Zusammenhang zwischen Planung und Qualität zeigt Abbildung 9.7 (nächste Seite) sehr anschaulich. Im Teufelsquadrat hat Harry M. Sneed [SNE01] die drei bekannten Planungsgrößen – Projektumfang (Quantität), Termine und Kosten – um die Qualität als vierte Einflussgröße ergänzt.

**ABBILDUNG 9.7**

Das Teufelsquadrat von Harry M. Sneed [SNE01]

Die **vier Zielgrößen** bewegen sich auf den Diagonalen des Quadrats; je weiter außen der Punkt liegt, desto besser ist das Ergebnis:

- „Mehr“ Quantität und Qualität führen zu einem besseren Ergebnis (daher steht das „Plus“ außen und das „Minus“ innen);
- kürzere Entwicklungsdauer und geringere Kosten führen zu einem besseren Ergebnis (daher steht das „Minus“ außen und das „Plus“ innen).

Interpretation des Teufelsquadrats

Wenn man einen der vier Parameter verändert, ändert sich zwangsläufig mindestens einer der drei anderen Parameter. In einer vereinfachten Darstellung könnte man die Länge der Linie, die die vier Punkte verbindet (den Umfang des Vierecks), als konstant ansehen:

- Mehr Quantität bei gleich bleibender Dauer und gleich bleibenden Kosten geht zwangsläufig zu Lasten der Qualität.
- Mehr Quantität bei gleich bleibendem Qualitätsanspruch führt zwangsläufig zu höheren Kosten und/oder zu einer längeren Entwicklungsdauer.
- Die vereinbarte Quantität zu den vereinbarten Kosten, jedoch zu einem früheren Liefertermin (Entwicklungsdauer) geht zwangsläufig zu Lasten der Qualität.
- Auch entstehende „Mehraufwände“, die aus Schätz- und Planungsfehlern resultieren, schlagen auf die Qualität durch, wenn es nicht gelingt, Termin- und Kostenvorgaben anzupassen.
- usw. ...

Das Teuflische an diesem Quadrat ist der Umstand, dass die Qualität in der Regel die am schlechtesten definierte Zielgröße ist. Daher werden die Auswirkungen von Veränderungen in den drei anderen Plangrößen auf die Qualität leicht übersehen.



Praxistipp:

Qualität in der Projektplanung bedeutet:

- gezielt darauf zu achten, dass die Qualität der Ergebnisse nicht schon durch eine unrealistische Planung unter Druck gerät;
- im laufenden Projekt gezielt darauf zu achten, dass die Auswirkungen von Änderungen der Plangrößen auf die Qualität angesprochen und berücksichtigt werden.

9.5.2 Qualität in der Projektlenkung

Die folgende Checkliste kann Sie darin unterstützen, die qualitätskritischen Punkte in der Projektlenkung zu identifizieren:



1. Fortschrittskontrolle

- Erreichen wir die Etappenziele? Arbeiten wir schnell genug?
 - Meilenstein Trendanalyse
 - Individuelle Verfolgung wichtiger Arbeitspakete
 - Den Project Flow beobachten/messen!

2. Ein Blick auf die Produktqualität

- Erfüllen die Zwischenergebnisse ihren Zweck?

3. Change Management

- Das Änderungsvolumen beobachten/messen:
Anzahl/Prozentsatz der Change Requests
- Wird das Änderungsvolumen zu hoch, sollte der Projektleiter lenkend eingreifen!

4. Das Risikomanagement weiterführen

- Bekannte Risiken periodisch beobachten:
 - Greifen die Vorbeugemaßnahmen?
 - Hat sich die Eintrittswahrscheinlichkeit geändert?
- Neue Risiken identifizieren und managen

5. Ein Blick auf die Qualitätssicherung

- Wie wirkungsvoll sind unsere QS-Maßnahmen?
(Reviews, ...)
- Beobachtung der Qualität durch Qualitäts- und Fehlermetriken
- Bei Bedarf lenkend eingreifen!



Praxistipp:

Der Projektleiter kann in der Regel die Qualität der Ergebnisse nicht selber produzieren, seine Aufgabe ist es jedoch, Rahmenbedingungen zu schaffen, die Qualität ermöglichen und fördern!

■ 9.6 Qualität der Prozesse

Gleichbleibend hohe Qualität erreicht man nicht über die Prüfung am Endprodukt, sondern über die Beherrschung der Entwicklungs- bzw. Fertigungsprozesse.

So lautet **das Paradigma des modernen Qualitätswesens**. Prozessqualität ist also der Schlüssel zur Qualität der Ergebnisse. Prozessqualität bedeutet, wie in Abschnitt 9.2.2 erläutert, Wirksamkeit und Wirtschaftlichkeit der Prozesse.

Das moderne Prozessmanagement unterstützt uns auf dem **Weg zur Prozessqualität** im Wesentlichen mit folgenden **Ansätzen**:

- Prozessmodellierung
- Referenz-Prozessmodelle (Best-Practice-Modelle)
- Prozessreifegrad-Modelle
- das Konzept der agilen Prozesse

9.6.1 Prozessmodellierung

Die Prozessmodellierung ist ein sehr sauberer Weg, Prozesse zu definieren. Je deterministischer ein Prozess abläuft, desto leichter lässt er sich modellieren und desto größer ist der Nutzen des Modells. Vom einfachen Ablaufdiagramm bis hin zur Prozesssimulation zum Vergleich verschiedener Prozessvarianten mit diversen Lastprofilen lässt sich mit modernen Prozessmodellierungswerkzeugen viel machen.

Nun sind die meisten IT-Prozesse nicht sehr deterministisch, sie eignen sich daher in der Regel schlecht für eine Modellierung. Realitätsnahe Modelle werden unglaublich komplex und unübersichtlich, einfach gehaltene Prinzipialabläufe können die wesentlichen Aufgaben beschreiben, geben aber kaum Hilfestellung für die Entscheidungen im Prozessablauf.



Beachten Sie:

Die meisten erfolgreichen IT-Prozessmodelle beschränken sich darauf, die wichtigen Aktivitäten zu beschreiben, und verzichten auf eine Darstellung der Ablaufsteuerung.

9.6.2 Referenz-Prozessmodelle

Referenz-Prozessmodelle decken in der Regel ein bestimmtes Anwendungsgebiet ab. Sie definieren typischerweise:

- eine einheitliche Begriffswelt für dieses Anwendungsgebiet;
- eine Reihe von Prozessgruppen und Prozessen.

Jeder Prozess wird durch folgende Elemente beschrieben:

- den Zweck
- die wichtigsten Inputs
- eine Reihe von Aktivitäten/Basispraktiken (die oft als Best Practices nach dem Stand der Technik zu interpretieren sind)
- die wichtigsten Ergebnisse
- die wichtigsten Rollen.

Referenz-Prozessmodelle definieren Anforderungen an die Prozesse für ihr Anwendungsgebiet im Sinne einer Best-Practice-Sammlung und können daher als Beispiel gebender Input für die Gestaltung der eigenen Prozesse genutzt werden. Darüber hinaus sind Referenz-Prozessmodelle vielfach die Grundlage für Zertifizierungen zum Nachweis der eigenen Kompetenz.

Im Folgenden ein grafischer Überblick über die relevanten Referenzmodelle und Regularien in der IT, d. h. für Software-Entwicklung und IT-Betrieb:

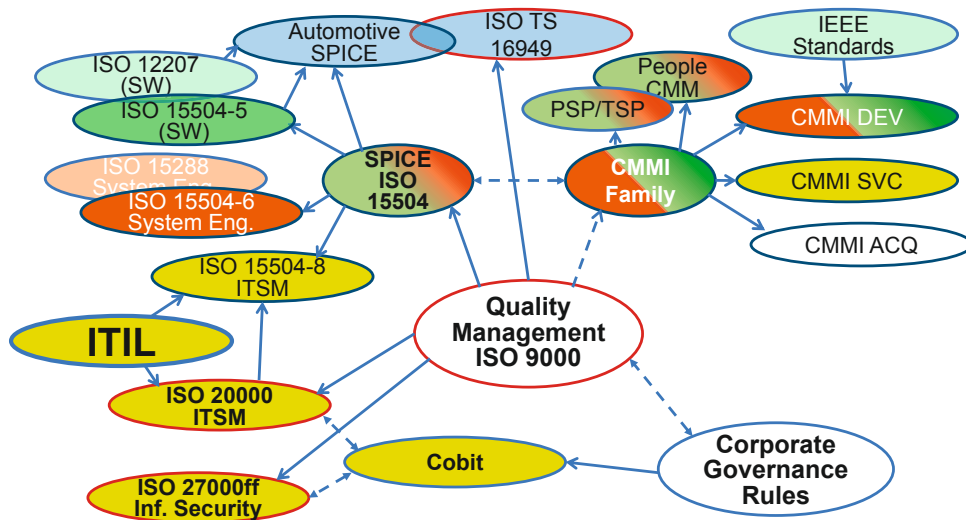


ABBILDUNG 9.8 Die Normenlandschaft in der IT: Relevante Regularien für Software Entwicklung und IT-Betrieb

Die angeführten Standards sind ein kleiner Ausschnitt dessen, was von den Standardisierungsgremien angeboten wird – ich habe versucht, mich auf die wesentlichen Themenbereiche zu fokussieren.

Die Entwicklung von Referenzprozessmodellen hat in den letzten Jahren an Bedeutung gewonnen. Die ISO hat dem mit einem eigenen Standard für die Beschreibung von Referenzprozessen Rechnung getragen:

ISO/IEC TR 24774 Systems and software engineering – Life cycle management – Guidelines for process description

Eine Reihe relevanter Referenzprozessmodelle finden Sie in Kapitel 9.8 Relevante Qualitätsmanagement-Standards.

9.6.3 Prozessreifegrad-Modelle

Die Prozessreifegrad-Modelle ergänzen Referenz-Prozessmodelle um das Konzept der Prozessreife. Die Idee dahinter ist, dass man einen Prozess auf verschiedenen Anspruchsniveaus (Capability Levels/Fähigkeitsstufen/Reife) implementieren und leben kann.

Die Prozessreifegrad-Modelle wurden von Watts Humphry mit dem SW-CMM-Modell (Capability Maturity Model) Ende der 80er Jahre begründet. Die folgende Liste zeigt die Entwicklung der Reifegrad-Modelle als Zeitreihe:

▪ SW-CMM – das Konzept	1988
▪ SW-CMM V1.0	1990
▪ Bootstrap	1992
▪ SW-CMM V1.1	1993
▪ SE-CMM V1.1 (SE ... System Engineering)	1995
▪ ISO/TR 15504/SPICE	1998
▪ CMMI V1.1	2001
▪ ISO 15504/SPICE	2003–2006
▪ CMMI V1.2	2006
▪ Automotive SPICE	Seit 2006 (jährliche Updates)
▪ ISO 15504-6 SPICE for Systems Engineering	2008
▪ ISO 15504-7 Assessment of Organisational Maturity	2008

In dieser mehr als 20-jährigen Entwicklung haben sich bis heute zwei Gruppen an Prozessreifegrad-Modellen etabliert:

- **CMMI** (Capability Maturity Model Integrated): Modell des Software Engineering Instituts der Carnegie Mellon University (USA);
- **ISO IEC 15504**, auch **SPICE** genannt: **S**oftware **P**rocess **I**mprovement and **C**apability **D**etermination (mit seinen Derivaten, wie z.B. Automotive SPICE oder TestSPICE)

Beide Modelle definieren sechs Fähigkeitsstufen von null bis fünf (siehe Abbildung 9.9):

- Capability Level 0: Incomplete Process
- Capability Level 1: Performed Process
- Capability Level 2: Managed Process
- Capability Level 3: Established (= Standard) Process
- Capability Level 4: Predictable (= Quantitatively Managed) Process
- Capability Level 5: Optimizing Process

Anmerkung: Mit CMM-V1.3 (Dezember 2010) werden im CMMI Modell die Capability Level 4 und 5 gestrichen!

Die Fähigkeitsstufen (Capability Levels) sind aufeinander aufbauend definiert. Die Erreichung eines Capability Levels setzt voraus, dass sowohl die Kriterien der jeweiligen Stufe als auch die Kriterien aller darunter liegenden Stufen ab Stufe 1 erfüllt werden.

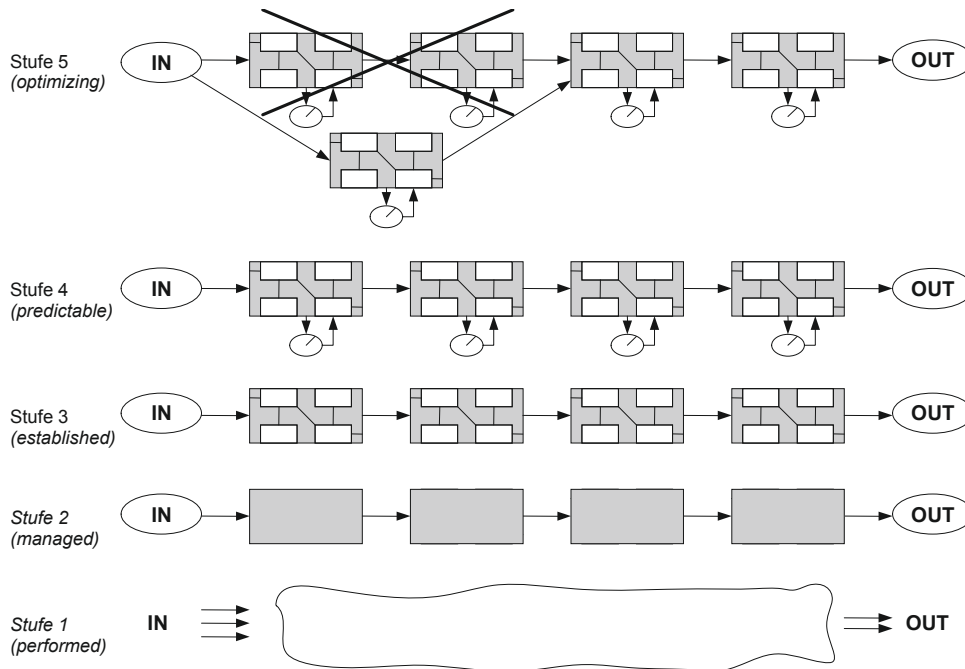


ABBILDUNG 9.9 Prozessreifegrade/Fähigkeitsstufen (aus [PAU01])

9.6.3.1 Capability Level 0: Incomplete Process

Der Prozess ist nicht implementiert oder verfehlt seinen Zweck:

- Die Ergebnisse sind unvollständig oder fehlerhaft.
- Erhebliche Termin- und/oder Kostenüberschreitungen.

Der Prozess erfüllt die Basisanforderungen nicht!

9.6.3.2 Capability Level 1: Performed Process

Der Prozess ist implementiert und erfüllt im Großen und Ganzen seinen Zweck:

- Brauchbare Ergebnisse
- Einigermaßen vernünftige Kosten-Nutzen-Relation

Der Erfolg ist in hohem Maße abhängig von

- den handelnden Personen: Qualifikation und aktuelle Verfassung;
- den Rahmenbedingungen.

Charakteristik des Prozesses:

- Gute Ergebnisse bei günstigen Rahmenbedingungen!
- Probleme bei ungünstigen Rahmenbedingungen!

9.6.3.3 Capability Level 2: Managed Process

Die Beteiligten haben den Prozess im Griff – auch unter schwierigen Bedingungen:

- Der Prozess wird in jedem Projekt individuell geplant und beschrieben;
- es gibt Ziele für die Prozessdurchführung;
- er wird beobachtet, gelenkt und überwacht;
- die Befolgung des Plans wird überprüft.

Ein Prozess auf Level 2 stützt sich im Wesentlichen auf die Techniken des Projektmanagements und auf inhaltliche Vorgaben für die Ergebnisse.

9.6.3.4 Capability Level 3: Defined Standard Process

Die Organisation hat auf Basis der Erfahrungen mit „Managed Processes“ (Capability Level 2) Standardprozesse definiert, die organisationsweit gelten. Jede Prozessinstanz wird von diesen Standardprozessen abgeleitet. Die Beteiligten können die Erfahrungen der anderen systematisch nutzen:

- Man weiß, was sich bewährt hat → Standard Prozess;
- man weiß, was unter welchen Bedingungen funktioniert → Tailoring Guidelines;
- jetzt ergeben Prozessmessungen einen Sinn: man vergleicht Äpfel mit Äpfeln und nicht mit Birnen!

Capability Level 3 erfordert ein sehr hohes Prozessverständnis, denn:

- Gute Standards werden gerne eingesetzt!
- Weniger gute Standards verletzen die Gebote der Prozessqualität – Wirksamkeit und Wirtschaftlichkeit – und werden daher von den Betroffenen nicht wirklich angenommen; Zwangsverpflichtung schadet in der Regel dem Ergebnis! Hier gilt ganz besonders der Satz:
Erfolg = Qualität x Akzeptanz

9.6.3.5 Capability Level 4: Quantitatively Managed Process

Die Prozessmessungen an den Standardprozessen liefern statistische Erkenntnisse über die Prozessleistung. Damit kann die Prozesslenkung auf die Basis von Zahlen, Daten und Fakten gestellt werden.

- Prozessziele werden über Kennzahlen vorgegeben.
- Die Zielerreichung wird anhand von Kennzahlen gemessen und beurteilt.

9.6.3.6 Capability Level 5: Optimizing Process

Auf diesem Level unterstützt ein systematischer Regelkreis die Prozessverbesserung:

- Prozessmessungen dokumentieren Fehler und Schwächen.
- Quantitative Analysen decken diese Fehler auf.
- Ursachen für diese Fehler werden **systematisch** untersucht und **systematisch** eliminiert!
- Die Prozesse werden **systematisch** verbessert!
- Der Erfolg ist an den (verbesserten) Kennzahlen abzulesen.

9.6.4 Prozessqualität in agilen Prozessen

Das sequenzielle Dilemma (siehe Abschnitt 9.3.1) und die in Abschnitt 9.3.2 angeführten Konsequenzen der iterativen Entwicklung haben Ende der 90er Jahre zur Entwicklung der sogenannten agilen Software-Entwicklungsmethoden geführt.

Ausgangspunkt für die Entwicklung der agilen Prozesse ist die Beobachtung, dass in vielen Software-Entwicklungsprojekten ein plangetriebenes Vorgehen, wie es auf Capability Level 2 gefordert wird, oder gar die Anwendung definierter Standardprozesse (Capability Level 3) die Grundforderungen der Prozessqualität nicht erfüllt: Wirksamkeit und Wirtschaftlichkeit.

In unübersichtlichen Situationen mit sich rasch ändernden Vorgaben und Rahmenbedingungen führt ein plangetriebenes Vorgehen zu einer Menge Aufwand (planen, umplanen, Pläne anpassen, ...), ohne dass dadurch eine entsprechende Sicherheit geschaffen werden kann. Es fehlen stabile Plandaten, auf denen man aufbauen kann.

Agilität versteht sich daher als Anti-These zu den definierten Standardprozessen, wie sie von CMMI [CMMI] und SPICE [ISO15504] ab Reifegradstufe 3 gefordert werden.

Die These der agilen Prozesse lautet: In einer unübersichtlichen Situation mit sich rasch ändernden Vorgaben und Rahmenbedingungen helfen einem intelligenten Menschen **einfache Regeln** mehr als **komplexe Prozessbeschreibungen** oder Pläne.

Das **traditionelle Prozessmanagement** basiert im Wesentlichen auf folgenden Säulen:

- Prozesslenkung durch Prozessbeschreibung und Planung;
- Sicherstellung der Prozessbefolgung durch QS-Maßnahmen (unabhängige Kontrolle von außen).

Agiles Prozessmanagement funktioniert grundlegend anders:

- Prozesslenkung durch einfache Regeln;
- Sicherstellung der Prozessbefolgung durch Disziplin (ein Kulturfaktor) und Selbstkontrolle im Team (Vier-Augen-Prinzip).

Das funktioniert in erster Linie gut in kleinen, überschaubaren Teams und Organisationen. Also genau dort, wo der traditionelle Prozessmanagement-Ansatz am schwierigsten umzusetzen ist.

Die Interpretation der einfachen Regeln führt in unterschiedlichen Situationen zu unterschiedlichen Vorgehensweisen. Das macht den agilen Ansatz so mächtig, erfordert aber Vertrauen in die handelnden Personen.

Große Teams und Großunternehmen tun sich mit dem agilen Ansatz grundsätzlich schwerer. Dafür ist der agile Ansatz ursprünglich auch gar nicht gedacht. Im Gegensatz zu den meisten Referenzmodellen erhebt der agile Ansatz keinen Anspruch auf Allgemeingültigkeit. Das agile Gedankengut ist jedoch in jedem Fall eine Bereicherung, weil es dafür sorgt, dass der Sach- und Hausverstand wieder mehr Gewicht bekommt.

Die **Grundideen der agilen Software-Entwicklung** wurden 2001 von den Gründern der Agile Alliance in folgendem Manifest zusammengefasst:

Manifesto for Agile Software Development:

„We are uncovering better ways of developing software by doing it and helping others do it. Through this work we have come to value:

- Individuals and interactions over processes and tools*
- Working software over comprehensive documentation*

- *Customer collaboration over contract negotiation*
- *Responding to change over following a plan*

That is, while there is value in the items on the right, we value the items on the left more.“

Agile Alliance: <http://www.agilemanifesto.org/>

Das **Agile Manifest** wird durch eine Reihe von Erläuterungen und die folgenden 12 **Prinzipien** ergänzt (vgl. <http://www.agilemanifesto.org/principles.html>).



Principles behind the „Agile Manifesto“:

- Our highest priority is to satisfy the customer through early and continuous delivery of valuable software.
- Welcome changing requirements, even late in development. Agile processes harness change for the costumer's competitive advantage.
- Deliver working software frequently, from a couple of weeks to a couple of months, with a preference to the shorter timescale.
- Business people and developers must work together daily throughout the project.
- Build projects around motivated individuals. Give them the environment and support they need, and trust them to get the job done.
- The most efficient and effective method of conveying information to and within a development team is face-to-face conversation.
- Working software is the primary measure of progress.
- Agile processes promote sustainable development. The sponsors, developers, and users should be able to maintain a constant pace indefinitely.
- Continuous attention to technical excellence and good design enhances agility.
- Simplicity – the art of maximizing the amount of work not done – is essential.
- The best architectures, requirements, and designs emerge from self-organizing teams.
- At regular intervals, the team reflects on how to become more effective, then tunes and adjusts its behavior accordingly.

Quelle: <http://www.agilemanifesto.org/principles.html>

Eine ausführliche Erläuterung des agilen Ansatzes würde den Rahmen dieser Publikation sprengen. Einen guten Überblick verschafft [HRS01], als weiterführende Literatur seien [GER01] und [HRR01] empfohlen. Ebenfalls sehr empfehlenswert sind die Bücher von Kent Beck und Martin Fowler über eXtreme Programming ([BEC01] und [BEC02]).



Praxistipp:

Die wichtigste Botschaft der agilen Software Entwicklungsmethoden ist sicherlich, dass es weniger darauf ankommt, ob Ihr Prozess Best Practice repräsentiert, sondern vielmehr darauf, dass Ihr Prozess in der konkreten Situation funktioniert. Agilität forciert Lösungen, die ein lokales Optimum für Ihr konkretes Projekt schaffen sollen; diese können daher von Fall zu Fall sehr unterschiedlich aussehen!

■ 9.7 Qualitätssicherung

Traditionell unterscheidet man in der Qualitätssicherung:

- Konstruktive Qualitätsmaßnahmen
- Analytische Qualitätsmaßnahmen

Ergänzend können organisatorische Qualitätsmaßnahmen betrachtet werden.

9.7.1 Organisatorische Qualitätsmaßnahmen

Organisatorische Qualitätsmaßnahmen sind alle Maßnahmen im Projekt- und Prozessmanagement, die dazu beitragen, die Erfolgsaussichten des Projekts zu erhöhen.

Alle Maßnahmen zur Erhöhung der Wirksamkeit und Wirtschaftlichkeit der (Projekt-)Arbeit, wie sie in den Abschnitten 9.3 bis 9.6 im Überblick beschrieben sind, fallen unter die organisatorischen Qualitätsmaßnahmen.



Beachten Sie:

Im Bereich der Organisation liegt eigentlich der größte Hebel, um die Qualität im IT-Bereich nachhaltig zu sichern oder zu verbessern.

9.7.2 Konstruktive Qualitätsmaßnahmen

Unter den konstruktiven Qualitätsmaßnahmen versteht man:

- Maßnahmen zur Eliminierung von Fehlerursachen;
- Maßnahmen, die das Produkt **a priori** besser oder sicherer machen.

Im Folgenden einige anschauliche **Beispiele konstruktiver Qualitätssicherung**:

- Asymmetrische Stecker: damit wird verhindert, dass Steckverbindungen irrtümlich verkehrt herum zusammengesteckt werden.
- In der Datenbankentwicklung: Der Primärschlüssel darf kein Datenbankfeld sein, das Nutzdaten enthält, die für den Anwender in der Benutzeroberfläche aufscheinen. Damit können Änderungen der fachlichen Anforderungen nicht auf den DB-Index durchschlagen.
- In der Programmierung sind Coding-Standards die bekannteste konstruktive Qualitätsmaßnahme.
- In einem Wiener Konferenzzentrum wurde eine drahtlose Simultan-Dolmetschanlage mit Infrarot-Übertragung realisiert. Das hat gegenüber einer Funk-Übertragung einige Nachteile; für diese Anwendung hat es jedoch den entscheidenden Vorteil der Abhörsicherheit von außen (ohne Sichtverbindung keine Datenübertragung!).

Wie diese Beispiele zeigen, sind konstruktive Qualitätsmaßnahmen von der jeweiligen Realisierungstechnik abhängig. Sie werden im Rahmen des Designs definiert und im Zuge der Implementierung umgesetzt.

Aus Sicht der Qualitätssicherung ist darauf zu achten,

- dass sich im Design sinnvolle konstruktive Qualitätsmaßnahmen in den Kriterien zur Bewertung der alternativen Lösungsansätze niederschlagen (vgl. Abschnitt 9.4.3, „good design is based on alternatives“);
- dass die im Design festgelegten konstruktiven Qualitätsmaßnahmen auch wirklich konsequent umgesetzt werden.

9.7.3 Analytische Qualitätsmaßnahmen

Unter analytischen Qualitätsmaßnahmen versteht man alle **Maßnahmen zur Analyse/Prüfung von (Entwicklungs-)Ergebnissen**:

- Prüfen von Zwischenergebnissen der Entwicklung (Reviews von Dokumenten und Source-Code);
- Prüfen der lauffähigen Software (Testen).

9.7.3.1 Reviews

Reviews sind eine wesentliche Maßnahme der Qualitätssicherung, um Teilergebnisse eines Projekts zu überprüfen. Bei einem Review wird ein Entwicklungsergebnis (Dokument) von einigen ausreichend qualifizierten Personen einer kritischen Durchsicht unterzogen.

Eine kurze Beschreibung der gängigen Review-Verfahren finden Sie in Abschnitt 9.7.4.

9.7.3.2 Testen

Die eigentliche Durchführung der Tests wird in der Literatur oft nicht als Qualitätssicherungs-, sondern als Entwicklungsaufgabe gesehen. Frei nach dem Motto: Ohne Testen keine vernünftig laufende Software.

Der qualitätssichernde Aspekt im Rahmen des Testens ist das **Testmanagement**, d.h. die Planung, Vorbereitung und Lenkung von Tests; z. B. durch die Vorgaben von definierten Kriterien für die Testabdeckung, die Testdauer oder für den Testabbruch.

Erst durch solche Maßnahmen erreichen wir mit dem Testen die gewünschte qualitätssichernde Wirkung: „Schaffung von Vertrauen, dass die zutreffenden Qualitätsforderungen erfüllt werden.“

9.7.3.3 Die Wirtschaftlichkeit der analytischen Qualitätsmaßnahmen

Analytische Qualitätssicherung kostet Zeit und damit Geld. Sobald ein Projekt unter Druck gerät, ist es verlockend, an dieser Stelle zu sparen und analytische QS-Maßnahmen zu kürzen oder ganz zu streichen:

- Kurzfristig können relevante Kapazitäten für jene Aufgaben freigemacht werden, mit denen man im Rückstand ist;
- kurzfristig fällt das Ausbleiben der Reviews und Tests meist nicht groß auf.

Längerfristig schaut die Geschichte anders aus:

Wenn man etwas effizient erledigen will, muss man es beim ersten Mal richtig machen!

Wenn eine Organisation Arbeiten beim ersten Mal richtig machen will, muss sie dafür sorgen, dass sie das auch kann!

Mit fehlerhaften Zwischenergebnissen als Arbeitsgrundlage wird das wohl kaum gelingen!

Fehlerkosten steigen exponentiell mit der Dauer, die der Fehler unentdeckt in der Entwicklung mitgeschleppt wird (siehe Abbildung 9.10)!

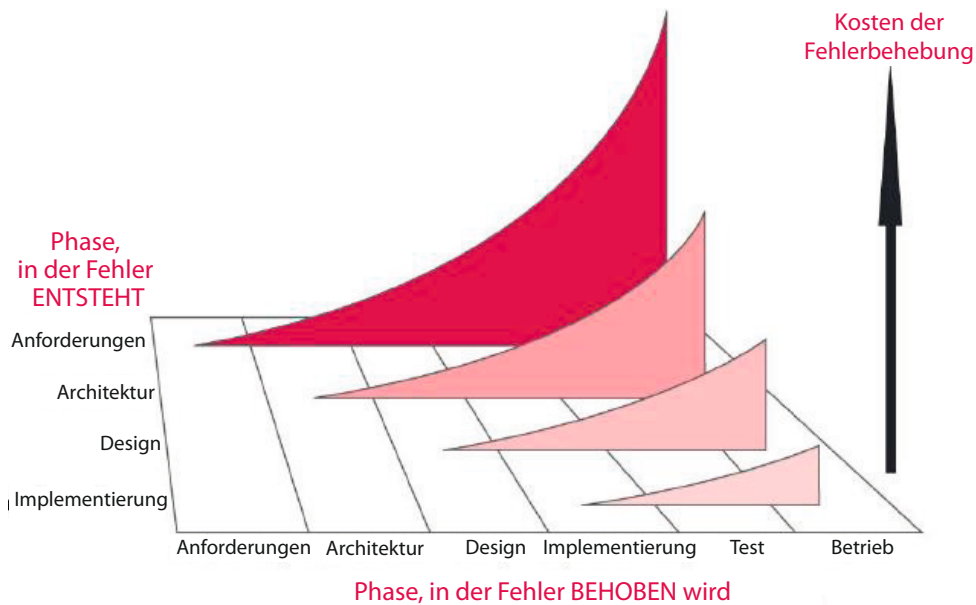


ABBILDUNG 9.10 Steigerung der Fehlerkosten abhängig von ihrer Entdeckung
(Quelle: Steve McConnell, Windows Tech Journal)

Spät gefundene Fehler kommen folglich teuer zu stehen, wie auch die folgenden Zahlen in Tabelle 9.2 zeigen [PRES01]!

TABELLE 9.2 Relative Fehlerkosten

Phase der Fehlerentdeckung	Kostenfaktor
Spezifikation	1
Design	3–6
Implementierung	10
Unit- bzw. Integrationstest	15–40
Systemtest	30–70
Betrieb	40–1000

Die Daten der Tabelle können wie folgt interpretiert werden:

- Finden wir einen Spezifikationsfehler noch vor Freigabe der Spezifikation (d.h. im Rahmen des Reviews der Spezifikation), kostet die Behebung des Fehlers z.B. eine Personenstunde.
- Finden wir den Fehler erst im Zuge des Designs, kostet die Fehlerbehebung bereits zwischen 3 und 6 Personenstunden.
- In der Implementierung steigt der Aufwand für die Fehlerbehebung auf etwa 10 Personenstunden.
- Finden wir den Fehler beim Unit- oder Integrationstest, liegen wir mit den Fehlerkosten bereits im Bereich von etwa 2 Tagen bis zu einer Personenwoche.
- Finden wir den Fehler erst beim Systemtest, liegen wir mit den Fehlerkosten bereits im Bereich von ein bis zwei Personenwochen.
- Wird der Fehler erst im Betrieb gefunden, sind die Fehlerkosten nach oben offen (abhängig von der Größe der installierten Basis und dem Schaden, den der Fehler beim Kunden anrichtet).



Eine möglichst frühe Fehlerbehebung ist also die wirtschaftlichste Form der Fehlerbehebung. Mit den Einsparungen durch eine frühe Fehlerbehebung müssen wir die Aufwände für die Qualitätssicherung finanzieren.

Um die Wirksamkeit und Wirtschaftlichkeit von QS-Maßnahmen beurteilen zu können, empfiehlt es sich, einige Daten zu erheben:

- Je Review/Test:
 - Aufwände für Reviews und Test
 - Anzahl der gefundenen Fehler, klassifiziert nach dem Fehlertyp (z.B. Blocking, Major, Minor, Typos)
- Je gefundenen Fehler:
 - Wo ist der Fehler entstanden (damit kann der Abstand zwischen Entstehung und Entdeckung gemessen werden)?
 - Aufwand für die Fehlerbehebung

9.7.4 Reviews

Reviews sind eine wesentliche Maßnahme der Qualitätssicherung, um Teilergebnisse eines Projekts zu überprüfen. Bei einem Review wird ein Entwicklungsergebnis (Dokument) von einigen ausreichend qualifizierten Personen einer kritischen Durchsicht unterzogen. Durch Reviews sollen

- Probleme oder Fehler frühzeitig erkannt,
- eventuell fehlende Punkte gefunden,
- Unklarheiten in der Beschreibung aufgezeigt und
- die Einhaltung von vorgegebenen Methoden und Standards überprüft werden.

Im Rahmen des Reviews sollen Probleme aufgezeigt, aber nicht sofort gelöst werden.

Reviews dienen der konstruktiven Kritik am Review-Objekt (Dokument) und nicht der Mitarbeiter-Beurteilung!

9.7.4.1 Formen des Reviews

Man unterscheidet zwei wesentliche Grundformen von Reviews:

- Schriftliche Reviews:
 - Kommentar-Review und
 - Einspruchsverfahren.
- Mündliche Reviews:
 - Formlose Reviews nach dem Vier-Augen-Prinzip: Cross-Review, Walk Through
 - Sitzungsreviews mit Moderator
 - Inspektionen: stark formalisierte Sitzungsreviews mit genauer Rollenverteilung

9.7.4.2 Planung von Reviews

Die Planung von Reviews erfolgt im Rahmen der QS-Planung in mehreren Stufen:

- Festlegen der QS/Review-Strategie: Welche Ergebnisse/Ergebnistypen sollen durch welche Art von QS-Maßnahme gesichert werden?
- Planung der „großen“ Reviews für die wichtigsten Ergebnisdokumente: Reviewform, Teilnehmerkreis, Termin, ...

Vorgabe von Richtlinien/Spielregeln für alle anderen Ergebnistypen, die durch Reviews qualitätsgesichert werden sollen, im QS-Plan aber nicht einzeln geplant werden.

9.7.4.3 Ablauf schriftlicher Reviews

Schriftliche Reviews müssen geplant werden, d. h.

- dem Autor ist der Teilnehmerkreis bekannt;
- die Reviewpartner wissen, dass sie an diesem Review teilnehmen werden.

Ablauf:

- Der Autor versendet das Review-Objekt an die Reviewpartner mit der Bitte um Stellungnahme. Dabei ist es wichtig, einen vernünftigen Zeitraum für die Stellungnahme anzusetzen.
- Die Review-Partner tragen ihre Kommentare und Bemerkungen in das Dokument (oder ein entsprechendes Formular) ein und senden das so ergänzte Dokument innerhalb der gesetzten Frist an den Verfasser zurück (in MS-Word eignet sich dafür die Funktion „Einfügen Kommentar“).
- Der Verfasser überarbeitet das Dokument aufgrund der ihm überbrachten Bemerkungen und Anregungen. Eventuelle Unklarheiten klärt er mit dem entsprechenden Review-Partner telefonisch oder in einem persönlichen Gespräch.
- Er dokumentiert das Ergebnis des Reviews in einem Review-Protokoll.
- Er sendet das Review-Objekt und Review-Protokoll an alle Teilnehmer.

- Erfolgen daraufhin innerhalb einer festgelegten (kurzen) Einspruchsfrist keine wesentlichen Einsprüche, so gilt das Dokument als angenommen und wird freigegeben.
- Bei wesentlichen Einsprüchen, die nicht zwischen Autor und Review-Partner geklärt werden können, wird die Entscheidung an den Fach-Vorgesetzten (Projektleiter, Entwicklungsleiter) delegiert.

Der hier beschriebene klassische Ablauf schriftlicher Reviews wird sich naturgemäß etwas ändern, wenn man die Review-Durchführung mit (typischerweise WEB-basierten) SW-Tools unterstützt, in denen das Review in Form eines Diskussionsforums organisiert ist.

Je nach Größe und Bedeutung des Dokuments können ein oder mehrere Review-Zyklen erfolgen.

Für große Dokumente, an deren Erstellung viele Personen beteiligt sind (z. B. Pflichtenheft), ist es oft zweckmäßig, vor einem Sitzungsreview ein schriftliches Review durchzuführen.

9.7.4.4 Kommentar-Review

Bei einem Kommentar-Review wird von jedem Review-Partner eine fristgerechte Stellungnahme erwartet. Bleibt diese aus, kann sie vom Verfasser des Dokuments eingemahnt werden.

Die einfachste Form des Kommentar-Reviews ist die Durchsicht eines Entwicklungsdokuments durch den fachlich Verantwortlichen (Projektleiter, Entwicklungsleiter). Dieser gibt das Dokument mit seinen Anmerkungen an den Verfasser zur Überarbeitung zurück oder er gibt das Dokument durch seine Gegenzeichnung frei.

9.7.4.5 Einspruchsverfahren

Bei einem Einspruchsverfahren wird nicht von jedem Review-Partner eine Stellungnahme erwartet. Bleibt die fristgerechte Stellungnahme aus, so gilt dies als vorbehaltlose Zustimmung.

Einspruchsverfahren werden immer dann angewandt, wenn ein Review-Partner zu keiner Stellungnahme verpflichtet werden kann (z. B. weil er der Auftraggeber oder der Ansprechpartner einer anderen am Projekt beteiligten Firma ist).

Bei einem Einspruchsverfahren ist es besonders wichtig, geeignete Review-Partner auszuwählen. Nur von organisatorisch und fachlich Zuständigen ist eine kompetente Stellungnahme zu erwarten, aus diesem Personenkreis darf niemand übergangen werden.

Von ungeeigneten Review-Partnern erhält man meist wenig ergiebige oder überhaupt keine Stellungnahmen, aber später Protest, wenn das fertige Ergebnis vorliegt.

9.7.4.6 Ablauf mündlicher Reviews

Mündliche Reviews finden im Rahmen einer Besprechung statt. Je nach Art und Umfang des zu prüfenden Dokuments können mündliche Reviews gut vorbereitet und im größeren Rahmen oder eher spontan und formlos und nur mit ein oder zwei Review-Partnern durchgeführt werden.

Mündliche Reviews, die entsprechend vorbereitet werden, nennt man Sitzungsreviews, für formlose Reviews gibt es unterschiedliche Bezeichnungen, wie z. B. Cross-Review oder Walk-Through.

9.7.4.7 Sitzungs-Review

Sitzungs-Reviews müssen geplant werden, d. h.

- Autor und Moderator müssen wissen, dass ein Sitzungsreview durchzuführen ist;
- die Reviewpartner sind bekannt und wissen, dass sie an diesem Review teilnehmen werden.

Ablauf:

- In einem Vorbereitungsgespräch erläutert der Verfasser den Review-Partnern das im zu prüfenden Dokument beschriebene Objekt (Modul, Programm) und übergibt ihnen die notwendigen Unterlagen. Dieses Vorbereitungsgespräch soll möglichst kurz gehalten werden. Es kann bei einfacheren Dokumenten entfallen.
- Während des Vorbereitungszeitraums arbeiten sich die Review-Partner in das Dokument ein und versuchen es zu verstehen. Offensichtliche gröbere Fehler werden dem Verfasser sofort mitgeteilt, sonstige Mängel, Anmerkungen oder Fragen werden notiert, um sie in der Review-Sitzung zu besprechen.
- In der Review-Sitzung erklärt der Verfasser das Review-Objekt im Detail. Die Review-Partner unterbrechen, wenn sie glauben, einen Fehler entdeckt zu haben, oder etwas nicht verstehen. Sie lassen sich dann, wenn möglich, durch den Verfasser von der Richtigkeit überzeugen. Dabei ist es wichtig, dass die Review-Partner wesentlichen Fragen hartnäckig nachgehen.
- Die Leitung der Review-Sitzung sollte nach Möglichkeit von einem unabhängigen Moderator übernommen werden, der die Methoden der Gesprächsführung beherrscht. Aufgabe des Moderators ist es, alle der Fehlerfindung dienenden Diskussionsbeiträge zu fördern, aber die Behandlung von Nebensächlichkeiten und Problemlösungs-Diskussionen zu verhindern. Das Gespräch sollte auf einem sachlichen und freundlichen Niveau geführt werden.
- Die Ergebnisse des Reviews werden vom Moderator oder einem Protokollführer in einem Review-Protokoll festgehalten.

Review-Sitzungen mit nicht vorbereiteten Teilnehmern sind in der Regel unproduktiv und daher Zeitverschwendung. In so einem Fall ist es oft das Beste, die Review-Sitzung zu verschieben oder auf die Teilnahme der unvorbereiteten Review-Partner zu verzichten. Die Entscheidung darüber obliegt dem Moderator.

Das Dokument gilt als angenommen, wenn in den wesentlichen Kritikpunkten ein Konsens zwischen dem Verfasser und den Review-Partnern erzielt wurde. Bei Nichteinigung ist vom Moderator die Klärung der offenen Probleme an den fachlich Zuständigen (Projektleiter, Entwicklungsleiter) zu delegieren.

9.7.4.8 Formlose mündliche Reviews

Formlose Reviews stellen den gezielten Einsatz des Vier-Augen-Prinzips dar: Vier Augen sehen mehr als zwei.

Die Entscheidung, welche Kritikpunkte und Anregungen zu einer Überarbeitung des Dokuments führen, liegt bei formlosen Reviews beim Verfasser.

Trotz der eher formlosen Durchführung sollte auch hier ein einfaches Review-Protokoll angefertigt werden (z. B. als Prüfvermerk beim Check-in des reviewten Dokuments oder Source-Codes). Formlose Reviews bedürfen keiner großen Planung:

- In der QS-Planung wird festgelegt, welche Ergebnistypen formlos reviewed werden sollen und nach welchen Kriterien der Autor Review-Partner finden soll (z.B. wechselseitiges Review von Detail-Entwürfen durch die Entwickler).
- Das eigentliche Review wird vom Autor oder vom Projektleiter kurzfristig initiiert.

Cross-Review

Als Cross-Review bezeichnet man mündliche Reviews mit einer kurzen Vorbereitung durch den Review-Partner und einem formlosen Review-Meeting.

Ablauf:

- Der Autor übergibt oder versendet das Review-Objekt an den Review-Partner mit der Bitte um kritische Prüfung.
- In einer formlosen Review-Sitzung bespricht man all jene Punkte, die dem Autor oder dem Review-Partner diskussionswürdig erscheinen:
 - Punkte, in denen sich der Autor durch eine zweite Meinung absichern will.
 - Punkte, die der Review-Partner kritisch angemerkt hat.

Walk Through

Als Walk Through bezeichnet man formlose Reviews, bei denen der Autor dem Review-Partner (oder den Review-Partnern) das Review-Objekt erläutert.

Ablauf:

- In einer formlosen Review-Sitzung stellt der Autor sein Arbeitsergebnis vor und führt durch das Review-Objekt; er kann dabei seine Überlegungen bei der Erarbeitung einfließen lassen, um so die aus seiner Sicht kritischen Entscheidungen zu hinterfragen.
- Die Review-Partner unterbrechen, wenn sie glauben, einen Fehler entdeckt zu haben, oder etwas nicht verstehen. Sie lassen sich dann, wenn möglich, durch den Verfasser von der Richtigkeit überzeugen. Dabei ist es wichtig, dass die Review-Partner wesentlichen Fragen hartnäckig nachgehen und sich bei weniger wichtigen Punkten auf keine Glaubensdiskussionen mit dem Autor einlassen.

Eine detailliertere Darstellung der Qualitätssicherung in IT-Projekten (heruntergebrochen auf konkrete QS-Maßnahmen für die verschiedenen Aufgabenbereiche eines IT-Projekts) finden Sie in [TIE10] in Kapitel 14.

■ 9.8 Relevante Qualitätsmanagement-Standards

9.8.1 Die Normenreihe ISO 9000ff

Die Normenreihe ISO 9000 ist die weltweit am weitesten verbreitete Qualitätsnorm; sie besteht aus folgenden Normen:

- ISO 9000:2005 Qualitätsmanagementsysteme Grundlagen und Begriffe
- ISO 9001:2008 Qualitätsmanagementsysteme Anforderungen
- ISO 9004:2009 Leiten und Lenken für den nachhaltigen Erfolg einer Organisation
Ein Qualitätsmanagementansatz

Für IT-Organisationen gibt es ergänzend die

- ISO 90003:2004 Software engineering
Guidelines for the application of ISO 9001:2000 to computer software

Unternehmen, die ein Qualitätsmanagementsystem betreiben, können sich durch eine akkreditierte Zertifizierungsgesellschaft bestätigen lassen, dass ihr QM-System die Forderungen der ISO 9001 erfüllt.

Welche Philosophie steht hinter der ISO 9001?

1. Qualitätssicherung ist eine Führungsaufgabe:
Die Qualitätspolitik muss von allen verstanden werden! Das QM-System muss wirksam sein!
2. Vorbeugen ist besser als heilen:
Qualitätssicherung = Beherrschung des Prozesses.
3. Wenn dennoch Fehler auftreten:
Analyse der Ursachen und Verbesserung des Prozesses.

In der Praxis der Umsetzung tritt diese Philosophie leider oft in den Hintergrund. In vielen Unternehmen ist das QM-System nach ISO 9001 zu einem „Papiertiger“ degeneriert, der sein Eigenleben entwickelt hat, das weit an den Qualitätsbedürfnissen der Betroffenen vorbeiläuft. Wenn man diese Philosophie jedoch ernst nimmt und sich an den folgenden 8 Prinzipien der ISO 9000 orientiert, ist die ISO 9000-Serie ein wirkungsvolles Instrument des Qualitätsmanagements!

Die 8 Prinzipien der ISO 9001 (zitiert aus der ISO 9000:2005):

- a) Kundenorientierung:
Organisationen hängen von ihren Kunden ab und sollten daher gegenwärtige und zukünftige Erfordernisse der Kunden verstehen, deren Anforderungen erfüllen und danach streben, deren Erwartungen zu übertreffen.
- b) Führung:
Führungskräfte schaffen die Übereinstimmung von Zweck und Ausrichtung der Organisation. Sie sollten das interne Umfeld schaffen und erhalten, in dem sich Personen voll und ganz für die Erreichung der Ziele der Organisation einsetzen können.
- c) Einbeziehung der Personen:
Auf allen Ebenen machen Personen das Wesen einer Organisation aus, und ihre vollständige Einbeziehung ermöglicht, ihre Fähigkeiten zum Nutzen der Organisation einzusetzen.
- d) Prozessorientierter Ansatz:
Ein erwünschtes Ergebnis lässt sich effizienter erreichen, wenn Tätigkeiten und dazugehörige Ressourcen als Prozess geleitet und gelenkt werden.
- e) Systemorientierter Managementansatz:
Erkennen, Verstehen, Leiten und Lenken von miteinander in Wechselbeziehung stehenden Prozessen als System tragen zur Wirksamkeit und Effizienz der Organisation beim Erreichen ihrer Ziele bei.

- f) Ständige Verbesserung:
Die ständige Verbesserung der Gesamtleistung der Organisation stellt ein permanentes Ziel der Organisation dar.
- g) Sachbezogener Ansatz zur Entscheidungsfindung:
Wirksame Entscheidungen beruhen auf der Analyse von Daten und Informationen.
- h) Lieferantenbeziehungen zum gegenseitigen Nutzen:
Eine Organisation und ihre Lieferanten sind voneinander abhängig. Beziehungen zum gegenseitigen Nutzen erhöhen die Wertschöpfungsfähigkeit beider Seiten.



Im Folgenden eine Zusammenfassung, was Qualitätsmanagement nach ISO 9001 bedeutet:

Die Anforderungen der ISO 9001 in der Praxis:

- Wir müssen unsere Qualitätspolitik festlegen und dokumentieren.
- Wir müssen daraus Qualitätsziele ableiten, die unsere Unternehmensziele unterstützen.
- Wir müssen sicherstellen, dass unsere Politik (unsere Strategie) verstanden und beachtet wird, und die Erreichung der Qualitätsziele messen.
- Wir müssen Verantwortung und Befugnisse unserer Mitarbeiter festlegen.
- Wir müssen für die Qualifikation und Ausbildung unserer Mitarbeiter sorgen.
- Wir müssen QS-Pläne erstellen und deren Anwendung sicherstellen.
- Wir müssen die Wirksamkeit unseres QM-Systems sicherstellen.
- Wir müssen lesbare Qualitätsaufzeichnungen führen und aufbewahren.
- Wir müssen unsere Lieferverträge überprüfen und unsere Lieferanten katalogisieren und bewerten.
- Wir müssen unsere QM-Fachkräfte selbstständig entscheiden lassen.

9.8.2 Standards für Software-Produktqualität

9.8.2.1 ISO/IEC 9126 Part 1–4: Information Technology – Product Quality

Die ISO 9126 ist der anerkannte Standard für die Gliederung von (nicht funktionalen) Software-Qualitätsmerkmalen. Die ISO 9126 besteht aus 4 Teilen:

- ISO/IEC 9126-1:2001 Software engineering – Product quality – Part 1: Quality model
- ISO/IEC TR 9126-2:2003 Software engineering – Product quality – Part 2: External metrics
- ISO/IEC TR 9126-3:2003 Software engineering – Product quality – Part 3: Internal metrics
- ISO/IEC TR 9126-4:2004 Software engineering – Product quality – Part 4: Quality in use metrics

Teil 1 definiert die Qualitätsmerkmale, die Teile 2 bis 4 definieren Metriken, wie man diese Qualitätsmerkmale messen kann. In Teil 1 werden **drei Gruppen von Qualitätsmerkmalen** unterschieden:

- *Externe Qualitätsmerkmale*: von außen erkennbar, z. B. durch den Anwender oder den Tester im Abnahmetest.
- *Interne Qualitätsmerkmale*: mit einem Blick ins Systeminnere erkennbar.
- „*Quality in Use*“: Anwendersicht auf die Qualität des Systems in einem bestimmten Anwendungskontext.



Anmerkung:

Die Normungsgremien der ISO arbeiten derzeit an einer Zusammenführung der Normen für Software-Qualitätsmerkmale (ISO 9126) und für Software-Bewertung (ISO 14598) in der neuen Normenreihe ISO 25000ff. unter dem Namen „Software Engineering – Software Product Quality Requirements and Evaluation (SQuaRE)“.

Den Zusammenhang zwischen interner und externer Qualität sowie der Quality-in-use beschreibt die ISO 25000 wie folgt (siehe auch Abbildung 9.11):

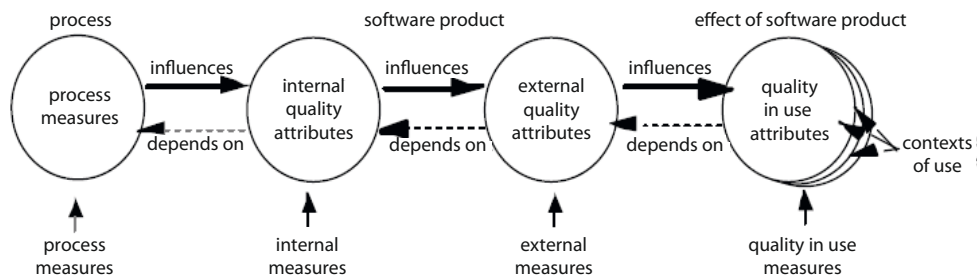


ABBILDUNG 9.11 Die Qualitätsattribute nach ISO 9126 bzw. ISO 25000ff

- Die Prozessqualität (in der SW-Entwicklung) beeinflusst die interne Qualität.
- Die interne Qualität beeinflusst die externe Qualität.
- Die externe Qualität beeinflusst die Quality in Use.

Die Unterscheidung zwischen externen Qualitätsmerkmalen und Quality in Use kommt immer dann zum Tragen, wenn eine (Standard-)Lösung in verschiedenen Anwendungskontexten zum Einsatz kommt. Trotz identischer externer Qualitätsmerkmale kann die „Quality in Use“ für verschiedene Anwendungen oder Anwender sehr unterschiedlich sein.

Für die externen und internen Qualitätsmerkmale gibt es folgende Kategorien:

- Functionality – Funktionalität
- Reliability – Zuverlässigkeit
- Usability – Benutzbarkeit
- Efficiency – Effizienz
- Maintainability – Änderbarkeit
- Portability – Übertragbarkeit

Für jede dieser Kategorien sind drei bis fünf Qualitätsmerkmale definiert, die Sie Abbildung 9.12 entnehmen können.

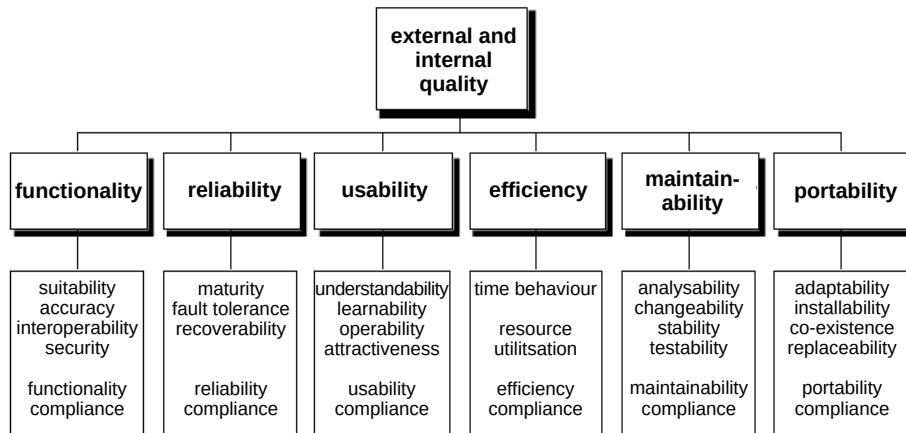


ABBILDUNG 9.12 Externe und interne Qualitätsmerkmale nach ISO 9126 bzw. ISO 25000ff

Die Quality-in-Use wird über folgende Qualitätsmerkmale definiert:

- Effectiveness – Wirksamkeit
- Productivity – Produktivität
- Safety – Sicherheit
- Satisfaction – die Fähigkeit, den Anwender zufrieden zu stellen

Die Idee hinter diesem Qualitätsmodell lässt sich so beschreiben:

- Aus den Bedürfnissen der Anwender werden die Anforderungen an die Quality in Use abgeleitet, gegen diese Anforderungen muss sich die Anwendung im Einsatz bewähren.
- Aus den Quality-in-Use-Anforderungen werden die Anforderungen an die externen Qualitätsmerkmale abgeleitet; gegen die externen Qualitätsmerkmale wird das Produkt validiert, um zu bestätigen, dass es für den beabsichtigten Gebrauch geeignet ist.
- Aus den externen Qualitätsanforderungen werden die Anforderungen an die internen Qualitätsmerkmale abgeleitet; gegen die internen Qualitätsmerkmale wird das Produkt verifiziert, um zu bestätigen, dass es der Spezifikation entspricht.

Dies ist eine saubere Methode, um uns zu den drei gängigsten **Typen von Anforderungsspezifikationen** zu führen:

- User Requirements Specifications
- System Requirements Specifications
- Software-/Subsystem Requirements Specifications

Die Teile 2 bis 4 der ISO 9126 definieren Metriken zur Messung dieser Qualitätsmerkmale. Diese Metriken geben auch gute Hinweise darauf, wie man die Anforderungen an diese Qualitätsmerkmale so spezifiziert, dass sie im Test überprüft werden können.

Der zugehörige Bewertungsprozess ist in der ISO/IEC 14598 – Software Product Evaluation – definiert (Abbildung 9.13).

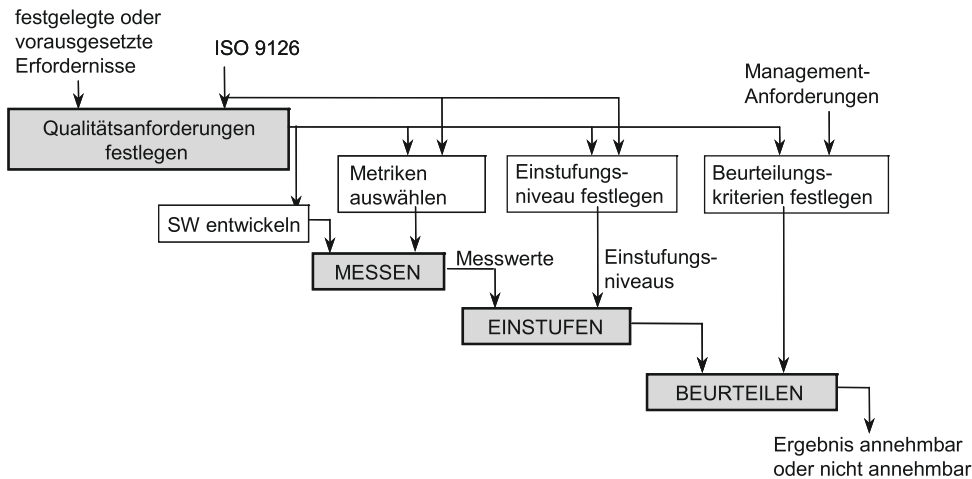


ABBILDUNG 9.13 Software-Bewertungsprozess nach ISO 14598

9.8.2.2 Die ISO 25000-Serie – SQuaRE

Die Normungsgremien der ISO arbeiten derzeit an einer Zusammenführung der Normen für Software-Qualitätsmerkmale (ISO 9126) und für Software-Bewertung (ISO 14598) in der neuen Normenreihe ISO 25000ff unter dem Namen „Software Engineering – Software Product Quality Requirements and Evaluation (SQuaRE)“.

Bisher erschienen sind (Stand Januar 2009):

- **ISO/IEC 25000:2005**
Software Engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Guide to SQuaRE (available in English only)
- **ISO/IEC 25001:2007**
Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Planning and management (available in English only)
- **ISO/IEC 25010:2011**
Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models
- **ISO/IEC 25012:2008**
Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Data quality model
- **ISO/IEC 25020:2007**
Software Engineering – Software quality requirements and evaluation (SQuaRE) – Quality measurement – Measurement reference model and guide (available in English only)
- **ISO/IEC TR 25021:2007**
Software engineering – SQuaRE – Quality measure elements
- **ISO/IEC 25030:2007**
Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Quality requirements (available in English only)

- **ISO/IEC TR 25040:2011**
Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Evaluation process
- **ISO/IEC TR 25045:2010**
Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Evaluation module for recoverability
- **ISO/IEC 25051:2006 Ed. 1** Current stage 60.60 JTC 1/SC 7
Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Requirements for quality of Commercial Off-The-Shelf (COTS) software product and instructions for testing (available in English only)
- **ISO/IEC TR 25060:2011**
Systems and software engineering – Systems and software product Quality Requirements and Evaluation (SQuaRE) – Common Industry Format (CIF) for usability: General framework for usability-related information

Weitere ISO-Standards mit Nummern von 25002 bis 250xx werden schrittweise folgen und schließlich die Standards ISO/IEC 9126 Teil 1–4 und ISO/IEC 14598 Teil 1–6 ablösen.

9.8.3 Prozessreifegrad-Modelle (CMMI & SPICE/ISO15504)

9.8.3.1 CMMI – Capability Maturity Model Integration

„Capability Maturity Model Integration“ ist sicherlich das am häufigsten beachtete Prozessreifegrad-Modell für Software und System Engineering.

CMMI wurde im Auftrag der amerikanischen Regierungsbehörden am Software Engineering Institute der Carnegie Mellon University entwickelt und umfasst mittlerweile drei Modelle (Model Constellations):

- CMMI for Development, Version 1.3 (ist das bekannteste Modell)
- CMMI for Acquisition, Version 1.3
- CMMI for Services, Version 1.3

Die CMMI-Referenzdokumente sind unter folgender Web-Adresse frei verfügbar:

→ <http://www.sei.cmu.edu/cmmi/tools/cmmiv1-3/index.cfm>.

CMMI ist von seiner Entstehungsgeschichte her ein Modell für Großprojekte, die zwischen großen Organisationen abgewickelt werden. Wichtige Sponsoren sind die amerikanische Rüstungs-, Luft- und Raumfahrtindustrie sowie ihre öffentlichen Auftraggeber. Dementsprechend legt das Modell einen besonderen Wert auf penible Planung, die Befolgung der definierten Prozesse und die Überprüfung, ob die definierten Prozesse befolgt werden.

Diese Anforderungen sind im Kontext der angesprochenen Großprojekte durchaus vernünftig. Manche von ihnen sind allerdings für kleinere und mittlere Organisationen und Projekte einerseits schwer erfüllbar und andererseits nur beschränkt hilfreich.

Kern des CMMI-Modells ist das in Abbildung 9.14 dargestellte Prozessreifegrad-Modell (mit CMMI-Version 1.3 wurden die bisher bekannten Capability Levels 4 und 5 abgeschafft).

Defined

Predefined processes are tailored for specific use, resources are managed..

Level 3 Defined

GP 3.1 Establish a Defined Process
GP 3.2 Collect Process related Experience

Level 2 Managed

GP 2.1 Establish an Organizational Policy
GP 2.2 Plan the Process
GP 2.3 Provide Resources
GP 2.4 Assign Responsibility
GP 2.5 Train People
GP 2.6 Manage Configurations
GP 2.7 Identify and Involve Relevant Stakeholders
GP 2.8 Monitor and Control the Process
GP 2.9 Objectively Evaluate Adherence
GP 2.10 Review Status with Higher-Level Management

Managed

Process and results are managed, responsibilities identified.

Level 1 Performed

GP 1.1 Perform Specific Practices

Performed

Processes are intuitively performed, input and output work products are available

Level 0 Incomplete

Incomplete Performance and results are incomplete, chaotic processes

ABBILDUNG 9.14 Das CMMI-Prozessreifegrad-Modell

Die Anforderungen von Capability Level 2 sind in einigen Punkten wesentlich rigider als in der ISO 15504/SPICE (vgl. Abbildung 9.16 auf Seite 457).

Das CMMI-Modell unterscheidet zwischen der Capability eines einzelnen Prozesses und der Maturity der Organisation. Jedem Maturity Level (Target Profile) sind eine Reihe von Prozessgebieten (process areas) zugeordnet. Diese Zuordnung – im CMMI-Modell „Equivalent Staging“ genannt – stellt Abbildung 9.15 dar.

Name	Abbr.	ML	CL1	CL2	CL3
Configuration Management	CM	2	Target Profile 2		
Measurement and Analysis	MA	2			
Project Monitoring and Control	PMC	2			
Project Planning	PP	2			
Process and Product Quality Assurance	PPQA	2			
Requirements Management	REQM	2			
Supplier Agreement Management	SAM	2			
Decision Analysis and Resolution	DAR	3	Target Profile 3		
Integrated Project Management	IPM	3			
Organizational Process Definition	OPD	3			
Organizational Process Focus	OPF	3			
Organizational Training	OT	3			
Product Integration	PI	3			
Requirements Development	RD	3			
Risk Management	RSKM	3			
Technical Solution	TS	3			
Validation	VAL	3			
Verification	VER	3			
Organizational Process Performance	OPP	4	Target Profile 4		
Quantitative Project Management	QPM	4			
Causal Analysis and Resolution	CAR	5	Target Profile 5		
Organizational Performance Management	OPM	5			

ABBILDUNG 9.15 Equivalent Staging – der Zusammenhang zwischen Process Capability und Organisational Maturity

- Die Fläche von Target Profile 2 zeigt, welche Process Areas Capability Level 2 erreichen müssen, damit die Organisation Maturity Level 2 erreicht.
- Die Fläche von Target Profile 3 zeigt, welche Process Areas Capability Level 3 erreichen müssen, damit die Organisation Maturity Level 3 erreicht.
- Die Fläche von Target Profile 4 zeigt, welche Process Areas Capability Level 3 zusätzlich erreichen müssen, damit die Organisation Maturity Level 4 erreicht.
- Die Fläche von Target Profile 5 zeigt, welche Process Areas Capability Level 3 zusätzlich erreichen müssen, damit die Organisation Maturity Level 5 erreicht.

Was dabei auffällt:

- Für Maturity Level 2 werden nur Management- und Supportprozesse betrachtet.
- Erst für Maturity Level 3 werden die Engineering-Prozesse betrachtet.

Dafür gibt es eine plausible Erklärung: Die Engineering-Prozesse sind die natürliche Kernkompetenz einer Entwicklungsorganisation.



Erste wesentliche Verbesserungen sind daher dort zu holen, wo eine Organisation nicht ihre Kernkompetenzen hat: beim Management – und bei den Supportprozessen. Erst wenn man diese Basistechniken im Griff hat, ist es sinnvoll, sich der Regelung der Engineering-Prozesse zuzuwenden.

Weiterführende Literatur zu CMMI:

- Kneuper, R.: CMMI. Verbesserung von Softwareprozessen mit Capability Maturity Model Integration (CMMI-DEV); 3. überarb. u. erw. Auflage, dpunkt.verlag, 2007 [KNE01]
- Ahern, D., Clouse, A., Turner, R.: CMMI Distilled: A Practical Introduction to Integrated Process Improvement. 2. Aufl., Addison-Wesley, Boston 2003 [ACT01]

9.8.3.2 ISO/IEC 15504 Part 1–7: Information Technology – Process Assessment

Die ISO 15504 ist trotz des Status als ISO-Standard im Wesentlichen als europäisches Gegenstück zum amerikanischen CMMI-Standard zu betrachten.

ISO/IEC 15504 Information technology – Process assessment – Part 1–7 → www.iso.ch

- ISO/IEC 15504-1:2004: Information technology – Process assessment – Part 1: Concepts and vocabulary
- ISO/IEC 15504-2:2003: Information technology – Process assessment – Part 2: Performing an assessment
- ISO/IEC 15504-3:2004: Information technology – Process assessment – Part 3: Guidance on performing an assessment
- ISO/IEC 15504-4:2004: Information technology – Process assessment – Part 4: Guidance on use for process improvement and process capability determination
- ISO/IEC 15504-5:2006 Information technology – Process assessment – Part 5: An exemplar Process Assessment Model
- ISO/IEC 15504-6:2008 Information technology – Process assessment – Part 6: An exemplar system life cycle Process Assessment Model

- ISO/IEC 15504-7:2008 Information technology – Process assessment – Part 7: Assessment of Organizational Maturity)

Weitere Teile der ISO/IEC 15504 sind in Arbeit oder in Planung (Stand Mai 2011):

- ISO/IEC TR 15504-8 Information technology – Process assessment – Part 8: An exemplar Process Assessment Model for service management
- ISO/IEC TR 15504-9 Information technology – Software process assessment – Part 9: Capability Target Profiles
- ISO/IEC TR 15504-10 Information technology – Process assessment – Part 10: Safety extension

Kern der ISO 15504 ist das in Abbildung 9.16 dargestellte Prozessreifegrad-Modell.

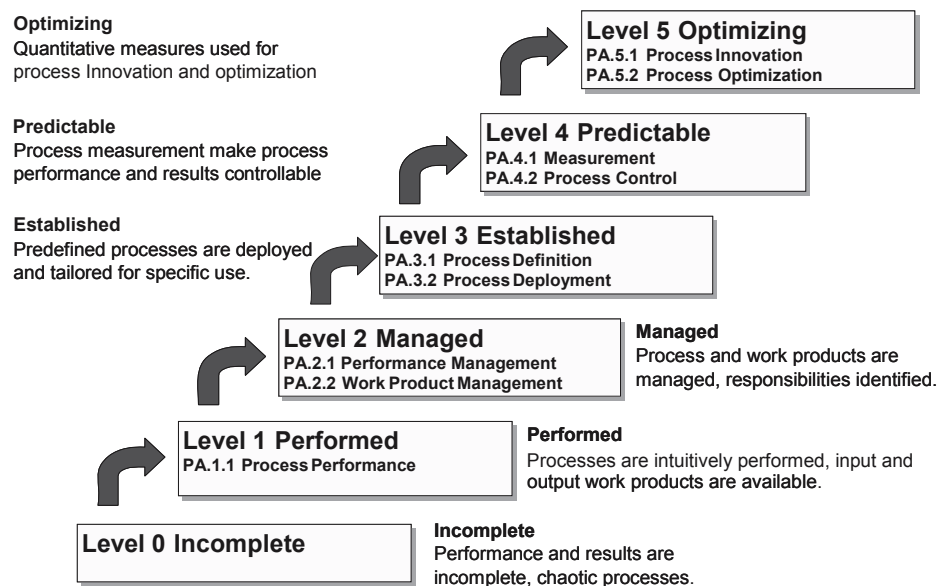


ABBILDUNG 9.16 Das Prozessreifegrad-Modell der ISO 15504

Die ISO 15504 hat sich vom Assessment Standard für die Bewertung von Software-Entwicklungsprozessen zum universellen ISO-Standard für Process Assessments in der IT weiterentwickelt. Die Idee dahinter betrifft die Möglichkeit, für verschiedene Anwendungsgebiete verschiedene Prozess-Referenz- und Assessmentmodelle zu schaffen.

Neben den beiden Assessmentmodellen für Software- und Systemsengineering (Teil 5 und 6 der ISO 15504) gibt es eine Reihe weiterer SPICE-konformer Referenz- und Assessmentmodelle:

- Automotive SPICE: Assessmentmodell für die Bewertung der Software-Entwicklungsprozesse für Automobil-Lieferanten (→ Steuergeräte im Auto)
- Mit der ISO 20000-4:2010 und der in Arbeit befindlichen ISO 15504-8 wird die Möglichkeit geschaffen, IT Servicemanagement nach ISO 20000-1 SPICE-konform zu assessieren.
- TestSPICE ist ein Referenz- und Assessmentmodell für Testprozesse und die Prozesse von Test-Service Providern; TestSPICE wurde im Dezember 2010 von intacs (→ www.intacs.info) validiert.

Für die weitere Entwicklung der ISO Standards zum Thema Prozess Referenz- und Assessmentmodelle hat die ISO die Nummernstrecke von 33000–33100 reserviert.

9.8.4 Referenz-Prozessmodelle in der IT

Es gibt zwei Klassen von Referenz-Prozessmodellen:

- *Offizielle Standards:*
definieren Anforderungen an die Prozesse im Sinne einer Best-Practice-Sammlung und sind vielfach die Grundlage für Zertifizierungen.
- *Best-Practice-Modell der Software-Industrie:*
bieten ein Beispielmmodell, das aus Sicht des jeweiligen Herstellers Best Practice repräsentiert. Die Best-Practice-Modelle der Software-Industrie sind in der Regel als Unterstützung der Software-Entwicklungsumgebungen des jeweiligen Herstellers konzipiert.

9.8.4.1 Referenz-Prozessmodelle für die Software-Entwicklung

- ISO IEC 12207: Information technology – Software life cycle processes (ist die Basis für das Assessmentmodell der ISO 15504-5)
- Das Prozessmodell von CMMI (process areas & specific practices)
- Das „Exemplar Assessment Model“ (process dimension) der ISO/IEC 15504 -5
- RUP – Rational Unified Process – das Prozessmodell von IBM-Rational rund um die Rational Software-Entwicklungstools
- MSF – Microsoft Solution Framework Process – das Software-Entwicklungsmodell von Microsoft
- In der agilen Software-Entwicklung fungieren die Regeln von XP oder Scrum als quasi Referenzmodelle für die agile Software-Entwicklung.

9.8.4.2 Referenz-Prozessmodelle für IT Service Management

ITIL – IT Infrastructure Library – das britische Best-Practice-Modell für IT Service Management gewinnt auch in Mitteleuropa zunehmend an Bedeutung (ITIL ist in Kapitel 4 genauer beschrieben; siehe auch www.itil.co.uk). Die ISO 20000 ist der ISO-Standard für IT Service Management; sie verbindet das Konzept eines Management-Systems nach ISO 9001 mit den ITIL Best Practices für IT Service Management.

- ISO/IEC 20000-1:2011 Information technology – Service management – Part 1: Service management System requirements
- ISO/IEC 20000-2:2005 Information technology – Service management – Part 2: Code of practice
- ISO/IEC TR 20000-3:2009: Information technology – Service management – Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1
- ISO/IEC TR 20000-4:2010: Information technology – Service management – Part 4: Process reference model

- ISO/IEC TR 20000-5:2010: Information technology – Service management – Part 5: Exemplar implementation plan for ISO/IEC 20000-1
- Cobit ist ein internationaler Standard zur Erreichung der „IT Governance“ und wird von der ISACA – Information Systems Audit and Control Association – herausgegeben (www.isaca.org).

Unter IT-Governance versteht man die konsequente Ausrichtung der IT als (interner bzw. externer) Dienstleister zur Erreichung der Unternehmensziele (vgl. ausführlich Kapitel 10 in diesem Handbuch). Auf der Homepage von ISACA (www.isaca.org) wird Cobit wie folgt charakterisiert:

„COBIT has been developed as a generally applicable and accepted standard for good Information Technology (IT), security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners.“

„COBIT is increasingly internationally accepted as good practice for control over information, IT and related risks.“

Cobit befasst sich also sowohl mit Praktiken des IT Service Managements als auch mit Praktiken des IT Security Managements. Während ITIL das IT Service & Security Management eher aus Sicht des IT-Dienstleisters betrachtet (Innensicht), wird bei Cobit viel stärker der Blickwinkel des Auftraggebers oder Kunden (Außensicht) eingenommen → Framework of High Level Control Objectives. Cobit gilt daher auch als anerkannter Standard für das IT-Controlling. Die Cobit Mission lautet:

„To research, develop, publicise and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers, IT professionals and assurance professionals.“ (www.isaca.org)

Cobit hat insbesondere mit den Anforderungen an das interne Controlling Börsen-notierter Gesellschaften nach dem **Sarbanes Oxley Act (SOX)** stark an Bedeutung gewonnen. Cobit gilt als Standard zur Erfüllung der SOX-Kriterien in der IT.

9.8.4.3 Referenz-Prozessmodelle für Information Security Management

- Das deutsche Grundschutzhandbuch
- Das IT-Sicherheitshandbuch des Bundes (Österreich)
- **ISO/IEC 27001:2005**: Information technology – Security techniques – Information security management systems – Requirements
- **ISO/IEC 27002:2005**: Information technology – Security techniques – Code of practice for information security management
- **ISO/IEC 27003:2010**: Information technology – Security techniques – Information security management system implementation guidance
- **ISO/IEC 27004:2009**: Information technology – Security techniques – Information security management – Measurement
- **ISO/IEC 27005:2008**: Information technology – Security techniques – Information security risk management
- **ISO/IEC 27006:2008**: Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems



Das Wichtigste – zusammengefasst

- Management muss sich rentieren – Qualitätsmanagement auch!
- Wenn man sich die wahren Kosten von Qualitätsmängeln vor Augen führt, sollte das kein Problem sein ... ☺.
- Wenn man sich mit diesen Kosten nicht auseinandersetzt, dann sind Qualitätsmanagement- und Qualitätssicherungs-Maßnahmen immer zu teuer ... ☹.
- Achten Sie auf die Wirksamkeit Ihrer Qualitätsmanagement- und Qualitätssicherungs-Maßnahmen!
- Verankern Sie das Qualitätsmanagement in Ihrer IT-Strategie (→ siehe auch Kapitel 2)
- Die Qualität eines (Software-)Produkts steht und fällt mit der Qualität der Anforderungen! Beginnen Sie mit der Qualitätssicherung bei den Anforderungen!
- Die Qualität eines Produkts oder einer Dienstleistung hängt signifikant von der Qualität der zugrunde liegenden Prozesse ab, welche angewendet werden, um das Produkt zu entwickeln, herzustellen und zu warten.
Nutzen Sie die verfügbaren Best-Practice Modelle, um Ihre Prozesse weiterzuentwickeln.
- Prozessreifegradmodelle sind State-of-the-Art im Prozessmanagement!
- Orientieren Sie sich am Konzept der Prozessreife und etablieren Sie Ihre Kernprozesse zumindest als „managed process“ auf Capability Level 2!
- Nutzen Sie (SPICE) Assessments als Treiber Ihres kontinuierlichen Verbesserungsprozesses!
- Die agile SW-Entwicklung ist eine wesentliche Bereicherung des Vorgehens in der Entwicklung, aber sie ist kein Allheilmittel für Ihre Probleme!
Prüfen Sie den Einsatz agiler Methoden und nutzen Sie deren spezifischen Stärken!
- Und last but not least: Erfolg ist Qualität x Akzeptanz!
Qualitätsmanagement braucht die Akzeptanz der Betroffenen! In wenigen Bereichen wird einem das so deutlich vor Augen geführt, wie im Qualitätsmanagement und in der Qualitätssicherung.
- Wenn es Ihnen nicht gelingt, die Betroffenen ins Boot zu holen, werden die Maßnahmen verpuffen – egal wie gut sie sind ...

■ 9.9 Literatur

- [AGM01] *Agile Alliance*: Manifesto for Agile Software Development <http://www.agilemanifesto.org/>
- [BEC01] *Beck K., Fowler M.*: Extreme Programming: Das Manifest. Addison Wesley 2001
- [BEC02] *Beck K., Fowler M.*: Extreme Programming planen. Addison Wesley 2001
- [BOE01] *Boehm, B. W., et al.*: Software Cost Estimation with Cocomo II. Prentice-Hall 2000
- [BOO01] *Booch, G.*: Software Engineering With ADA. 1983
- [CKS01] *Chrissis M. B., Konrad M., Shrum S.*: CMMI. Guidelines for Process Integration and Product Improvement. SEI Series in Software Engineering, Addison Wesley, Boston, 2003
- [CRO01] *Crosby, P. B.*: Quality is free. McGraw-Hill. New York 1979
- [DEMLI] *DeMarco, T., Lister, T.*: Wien wartet auf dich. Der Faktor Mensch im EDV-Management. Hanser, München 1991
- [GER01] *Gernert, C.*: Agiles Projektmanagement. Risikogesteuerte Softwareentwicklung. Hanser, München, Wien 2003
- [HRS01] *Hruschka, P., Rupp, C., Starke, G.*: Agility kompakt. Tipps für erfolgreiche Systementwicklung. Spektrum Akademischer Verlag 2004
- [HRR01] *Hruschka, P., Rupp, C.*: Agile Softwareentwicklung für Embedded Real-Time Systems mit der UML. Hanser, München 2002
- [KNE01] *Kneuper R.*: CMMI. Verbesserung von Softwareprozessen mit Capability Maturity Model Integration (CMMI-DEV), 3. überarb. u. erw. Auflage; dpunkt.Verlag, 2007
- [NEH01] *Nehfort, A.*: Shifting the Risk. 3rd World Congress for Software Quality; Proceedings Volume II; ISOI 2005
- [PRES01] *Pressmann R. S.*: Software Engineering: A practitioner's approach; 5th edition McGrawhill 2001
- [RUPP01] *Rupp, C.*: Requirements-Engineering und -Management. Hanser, München 2000
- [PAU01] *Paulk M. C., et al.*: The Capability Maturity Model, Addison Wesley, 1995
- [SNE01] *Sneed, H. M.*: Software Management. R. Müller, Köln 1987
- [STA01] *Chaos Report 1994: The Standish Group International Inc.* 1994; <http://www1.standishgroup.com>
- [STA02] *Chaos Report 2000: The Standish Group International Inc.* 2000
- [STA03] *Chaos Demographics and Project Resolution, excerpt from 3rd Quarter 2004: The Standish Group International Inc.* 2004
- [STA04] *Chaos Report 2006: The Standish Group International Inc.* 2006
- [STA05] *Chaos Report 2008: The Standish Group International Inc.* 2008
- [TIE10] *Tiemeyer E. (Herausgeber)*: Handbuch IT-Projektmanagement: Vorgehensmodelle, Management-instrumente, Good-Practices; Hanser, München 2010. Hier besonders: Kap. „14. Qualitätsmanagement für IT-Projekte“ von A. Nehfort

Robert Bergmann, Ernst Tiemeyer

*Im Leben gibt es keine Lösungen.
Es gibt nur Kräfte, die in Bewegung sind:
Man muss sie erzeugen – und die Lösungen werden folgen.
Antoine de Saint-Exupéry*



Fragen, die in diesem Kapitel beantwortet werden:

- Warum wird eine zentrale Steuerung von IT-Aktivitäten auf Unternehmensebene immer wichtiger?
- Inwiefern leistet der IT-Governance-Ansatz einen unmittelbaren Beitrag zum Unternehmenserfolg?
- Welche Zielsetzungen lassen sich mit der Einführung von Strukturen und Verfahren der zentralen IT-Governance im Unternehmen realisieren?
- Welche aktuellen Herausforderungen ergeben sich für die IT-Welt, und wie kann eine Positionierung von IT-Governance im Unternehmen vorgenommen werden?
- Welche Kernaufgaben zentraler IT-Steuerung werden unterschieden?
- Welchen Beitrag können eine unternehmensweite IT-Strategieentwicklung, das Aufsetzen eines Enterprise Architecture Management sowie ein ganzheitliches Anforderungsmanagement für die Umsetzung von IT-Governance leisten?
- Welche Bedeutung kommt einem ausgereiften IT-Investitionsmanagement im Rahmen von IT-Governance zu?
- Wie können Verfahren und Prozesse der IT-Governance erfolgreich in Unternehmen implementiert werden?

Als Antwort auf die vielfältigen technologischen und organisatorischen Herausforderungen im IT-Bereich haben sich in den letzten Jahren Verfahren, Strukturen und Instrumente der „IT-Governance“ etabliert; um zu kennzeichnen, dass die Organisation, Steuerung und Kontrolle des IT-Einsatzes in einem Unternehmen zentral durch Personen erfolgen sollte, die in der Unternehmensführung verankert sind. Hauptstoßrichtung dieses Ansatzes ist die konsequente Ausrichtung der IT-Prozesse, IT-Architekturen und IT-Projekte bzw. IT-Investitionen an der Unternehmensstrategie und die sich daraus ergebenden Geschäftsfelder und Geschäftsprozesse.

Eine zentrale These dieses Beitrags geht dahin, dass die Zusammenarbeit von „Strategen“ bzw. Planern und „Umsetzern“ auf der Tagesgeschäftsebene unverzichtbar ist. Das Ziel dieses

strategischen Business-IT-Alignments besteht in der Realisierung einer erfolgreichen Zusammenarbeit in Form bewusst eingerichteter unternehmensweiter „Plattformen“.

Die damit verbundene Steuerung (engl. „Governance“) durch eine zentrale Institution wird als dringend notwendig erachtet. Wesentliche Gründe können sein:

- Hoher Wert der IT-Assets. Die zunehmende Durchdringung des Unternehmens mit IT-Produkten sowie die hohe Komplexität der IT-Lösungen hatten zur Folge, dass der Wert der IT-Investitionen und somit der Wert des gesamten IT-Bestandes eines Unternehmens im Vergleich zum Gesamtwert des Unternehmens immer wichtiger geworden ist.
- IT ist ein wesentlicher Erfolgsfaktor für den reibungslosen Ablauf und die konsequente Verbesserung der unterstützten Geschäftsprozesse.
- Strategieorientierung ist unverzichtbar. Ohne eine strategische Ausrichtung der IT und die Orientierung an strategischen Zielsetzungen ist eine nachhaltige Entscheidungsfindung auch für den IT-Bereich nicht mehr zu bewerkstelligen.
- Risikoanalysen und Risikobewertungen für die IT-Architekturen und IT-Prozesse erfordern ein durchdachtes Risikomanagement mit klaren Verantwortlichkeiten. IT-Produkte verfügen über eine hohe Komplexität, die damit aber auch einem hohen Ausfallrisiko unterliegen. Auch die IT-Prozesse – insbesondere die Serviceprozesse – spielen in vielen Unternehmen eine immer wichtigere und auch kritische Rolle. Gezieltes IT-Risikomanagement ist deshalb ständig weiterzuentwickeln.

Funktioniert die IT und ist sie Basis für ausreichend Flexibilität am Markt, oder hat man sich zwar gute, aber teure IT-Produkte und inflexible IT-Prozesse geschaffen? Mit einer Momentaufnahme lässt sich diese Frage nur unzureichend beantworten. Wichtig ist vielmehr, sich mit den Strukturen und Prozessen, insbesondere den Planungs-, Koordinations- und Entscheidungsprozessen für Veränderungen im Unternehmen zu beschäftigen.

Dieses Kapitel soll Ihnen als Orientierung und Entscheidungshilfe für die vielfältigen Aspekte der IT-Governance dienen.

■ 10.1 Merkmale und Bedeutung von IT-Governance

Um die konstituierenden Merkmale von IT-Governance herauszukristallisieren, gilt es vorab zu verdeutlichen: Die im Rahmen von IT-Governance zu betrachtenden Standards und Vorgaben werden typischerweise aus der **Corporate Governance** des Unternehmens abgeleitet. Unter Corporate Governance werden allgemein alle selbstgesetzten und extern vorgegebenen (ethischen) Werte, Grundsätze, Verfahren und Maßnahmen für eine gute und verantwortungsvolle Unternehmensführung zusammengefasst, die sowohl für die Mitarbeiterinnen und Mitarbeiter als auch für die Unternehmensführung selbst gelten.

Die aus der Corporate Governance abgeleiteten strategischen Ziele der IT werden im Rahmen der IT-Governance strukturiert verfolgt. IT-Governance leistet damit einen wesentlichen und

heute unverzichtbaren Beitrag, um IT-Lösungen im Sinne der ganzheitlichen Betrachtung des Unternehmens zu entwickeln, auszuwählen und zu implementieren.

Die Gründe für einen verstärkten Wunsch nach zentraler IT-Steuerung sind vielfältig. Im Wesentlichen sollten durch entsprechende Verfahren und Instrumente die Negativfolgen vermieden werden, die sich bei unzureichend ausgeprägter IT-Governance ergeben. Dies veranschaulicht Tabelle 10.1.

TABELLE 10.1 Effektiver IT-Einsatz im Gesamtunternehmen – Situationsanalysen und mögliche Folgen

Situationen/Situationsanalysen	Typische Folgen für die IT-Welt
Vorhandene dezentrale Organisationsstrukturen sind durch Eigenverantwortlichkeit in der Führung, Ergebnisverantwortung und marktkonforme Leistungsbeziehungen gekennzeichnet. Bei einer unzureichend ausgeprägten oder nicht vorhandenen Corporate Governance sind nur wenige grundlegende Sachverhalte geregelt, was ein hohes „Eigenleben“ der dezentralen Einheiten zur Folge hat.	▪ Vielzahl unterschiedlicher IT-(Teil-)Architekturen (Plattformen und Technologien, Applikationen) ▪ Leistungserbringung wird nicht ausreichend gesteuert (unterschiedliche Anforderungen trotz gleicher Prozesse) ▪ unzureichende Skaleneffekte für die IT-Beschaffung (Vendor-Management und strategisches Sourcing finden nicht statt) ▪ zahlreiche redundante IT-Lösungen ▪ mangelnde Portfolio- und Projektsteuerung

10.1.1 Zielsetzungen und Rahmenbedingungen für eine erfolgreiche IT-Governance

Um unternehmensweit eine wirtschaftliche, hocheffiziente IT zu gewährleisten, sind eine Konsolidierung der IT-Architekturen, eine Harmonisierung der Anforderungen der Fachbereiche an die IT sowie eine zentrale Projektsteuerung (Multiprojektmanagement für IT-Projekte) unverzichtbar. Dies lässt sich mithilfe klarer IT-Governance-Strukturen und -Prozesse gewährleisten. Einen ersten konkreten Zugang zum Begriff „IT-Governance“ kann die folgende Definition geben:



Definition

IT-Governance besteht aus Führung, Organisationsstrukturen und Prozessen, die sicherstellen, dass die IT die Unternehmensstrategie und -ziele unterstützt. („Leadership and organizational structures and processes that ensure that the organisation's IT sustains and extends the organization's strategy and objectives“) [ITGI08].

IT-Governance ist somit ein Instrumentarium bzw. ein vereinbartes System, durch das die IT innerhalb eines Unternehmens gelenkt und kontrolliert wird. Mittels einer klaren IT-Governance-Struktur können die Rechte und Pflichten unter verschiedenen Akteuren im Unternehmen (etwa dem Vorstand bzw. Aufsichtsrat, Unternehmens- und IT-Management sowie den

Mitarbeiterinnen und Mitarbeitern der Fachbereiche) vereinbart und angewandt werden. Dazu gibt es beispielsweise entsprechende Regeln und Verfahren für die Entscheidungsfindung im IT-Bereich. IT-Governance stellt auf diese Weise sowohl Strukturen, mit deren Hilfe IT-Ziele definiert werden können, als auch Mittel zum Erreichen dieser Ziele und zur Überwachung der Performance bereit.

IT-Governance schafft und erfordert letztlich eine Struktur von Beziehungen und Prozessen, um via IT-Alignment die Geschäftsprozesse so zu steuern, dass sich die Geschäftsziele optimal erreichen lassen. Den entsprechenden Wertzuwachs erzielt man durch das Ausbalancieren von Risiko und Ertrag der IT-Lösungen und ihrer Prozesse (vgl. [G006] S. 6). Dieses Ausbalancieren ist Aufgabe der Führungskraft sowie von Gremien (Strategisches Projekt- oder besser Projektinvestitionssteuergremium). Ziel ist ein Optimum der Zielerreichung (im Sinne einer Balanced Scorecard).

Durch das Etablieren von IT-Governance soll eine möglichst hohe Transparenz im Unternehmen über die IT-Lösungen geschaffen werden, wobei gleichzeitig eine Konsolidierung und Harmonisierung der IT-Landschaft angestrebt wird, ohne jedoch die Fachbereiche zu bevormunden. Konkret bedeutet dies, dass alle Fachbereiche (inkl. der IT selbst) bei der Planung von Veränderungen alle Prozesse und Schnittstellen sowie Anforderungen an Daten für alle plausiblen Handlungsalternativen zugrunde legen. Auf dieser Basis liegen den Verantwortlichen alle Informationen für eine effektive Beauftragung der IT und die spätere Steuerung ihrer Geschäftsprozesse und somit der erfolgskritischen Vorgänge vor. Der IT-Dienstleister wird dadurch effektiv an Geschäftsprozessen ausgerichtet und durch die zentrale IT-Steuerung sowie Steuergremien im Sinne des Geschäfts geleitet.



Eine gut organisierte IT-Governance umfasst somit Strukturen, Prozesse und Ressourcen, die mit der Unternehmensstrategie und deren Zielen verknüpft sind. Im Rahmen dieser Art der Zusammenarbeit ist eine sich immer stärker selbst organisierende Organisation, die primär an Prozessen statt an Organisationsstrukturen ausgerichtet ist, die Vision. IT-Governance befähigt Organisationen, sämtliche Geschäftsprozesse dezentral zu verantworten, aber zentral sicherzustellen, dass alle am gleichen Strang in die gleiche Richtung ziehen.

Worin bestehen die primären **Zielsetzungen der Etablierung von IT-Governance**? Die Prinzipien der IT-Governance sollen sicherstellen, dass die Umsetzung der IT-Strategie im Sinne der Verantwortungsträger – also der Unternehmensführung – erfolgt. Insbesondere können folgende Anforderungen und Zielsetzungen formuliert werden:

- IT-Governance soll die Sicherheit (Integrität, Verfügbarkeit, Vertraulichkeit) und Verlässlichkeit (Einhaltung externer Anforderungen) der Informationen bzw. der IT-Systeme gewährleisten.
- Es soll ein effizienter Einsatz der IT-Ressourcen bei gleichzeitiger Ausrichtung der IT auf die Unternehmensziele hergestellt werden (IT-Strategie als integraler Bestandteil der Business-Strategie eines Unternehmens).
- Durch die Schaffung von Transparenz (etwa die strategische und betriebswirtschaftliche Bewertung von IT-Projekten unter Berücksichtigung von Aspekten des Risikomanagements) soll auch ein Beitrag zur Kostensenkung im Bereich der IT geleistet werden.

- Durch klare, revisionssichere Strukturierung der IT-Organisation, Prozesse und Projekte nach allgemeinen Standards (z. B. ITIL, SPICE) wird ein Beitrag zu einer optimalen IT-Organisation geschaffen.
- Es kann die Erfüllung gesetzlicher Vorgaben (z. B. Ableitung von Sicherheitsanforderungen aus der IT-Risikoanalyse) gewährleistet werden. Dabei sind im Rahmen der Organisation zweckmäßige und funktionsbezogene Planungs- und Kontrollsysteme einzurichten und weiterzuentwickeln.

Tabelle 10.2 zeigt eine Zusammenstellung wesentlicher Zielsetzungen der Einführung von IT-Governance und gibt Hinweise zur Umsetzung.

TABELLE 10.2 Wichtige Ziele bei Einführung von IT-Governance

Zielsetzungen	Begründung/Implementierungshinweise
Ganzheitliche Ausrichtung der IT auf Unternehmenslösungen	Geschäfts- und IT-Strategie müssen so in Übereinstimmung gebracht werden, dass die Gesamtstrategie der Organisation die Ausgestaltung der IT-Strategie ganzheitlich – und wechselseitig – bedingen kann („Strategic Alignment“). Darunter verstehen wir Transferleistungen einer operativen „Plattform“ von Anforderungsmanagern bzw. -koordinatoren, die sowohl die Ist-Prozesse genau kennt als auch jeweils auf Bereichsebene strategische Veränderungen plant.
Unternehmensweite Standardisierung und Verfügbarkeit der IT erhöhen	Die Einführung von unternehmensweiten, standardbasierenden Hard- und Softwarelösungen ermöglicht eine erhöhte Verfügbarkeit und erleichtert die Flexibilität und Adaptionsfähigkeit der IT-Systeme.
Wirtschaftlichkeit der IT für das Gesamtunternehmen gewährleisten	Mittels Konsolidierung der unternehmensweiten IT-Landschaften können die mitunter explodierenden Kosten für IT-Wartung bzw. Pflege gesenkt werden.
Optimiertes Innovations- und Investitionsmanagement	Nutzengenerierung mit Fokus auf die Optimierung der Ausgaben und Bewertung des Nutzens der IT. Unterstützung des Unternehmens bei der Erreichung der Geschäftsziele, verantwortungsvoller und nachhaltiger Einsatz der IT-Ressourcen (Management von Ressourcen, Optimierung von Wissen und IT-Infrastruktur)
IT-Landschaft insgesamt vereinheitlichen bzw. vereinfachen	Konsolidierte Hardware-Systeme (Server, Storage, Netze etc.), Daten (Datenbanken) und Applikationen können eine Verbesserung der betrieblichen Effizienz gewährleisten sowie eine erhöhte Verfügbarkeit des Gesamtsystems sicherstellen. Der Verwaltungsaufwand wird reduziert, die Supportkosten werden gesenkt.
IT-Risiken minimieren und erfolgreich meistern	Risikomanagement, das sich auf den Schutz des IT-Assets bezieht, unter Berücksichtigung von Disaster Recovery (Wiederanlauf nach Katastrophen) und Fortführung der Unternehmensprozesse im Krisenfall.

**Hinweis:**

Beim Aufbau von Strukturen und Prozessen einer IT-Governance ist zu beachten, dass sie von einer Vielzahl bisweilen auch konkurrierender interner und externer Faktoren beeinflusst wird und es keinen allgemeingültigen Standard für die IT-Governance gibt. In ihrer Ausprägung ist sie – notwendigerweise – so verschieden, wie es die Ausrichtung und Ziele von Unternehmen sind. Zudem wird durch IT-Governance kein statischer (Ideal-)Zustand erzeugt, sondern ein **zyklischer Prozess** initiiert, der die verschiedenen Governance-Ziele mit den Einflüssen auf die IT in ein (dynamisches) Gleichgewicht zu bringen versucht. IT-Governance lässt sich daher mit Best-Practice-Ansätzen (vgl. [Biexx07]) nicht erreichen. Zu beachten ist, dass sich damit vor allem auch der „Umgang mit IT“ in einer Organisation mit einer Einführung grundlegend verändert (vgl. [WeRo04]).

10.1.2 IT-Governance-Prozesse und Corporate Governance

Grundsätzlich wird mit der Einführung von IT-Governance eine Vielzahl von Entscheidungen auf den Prüfstand gestellt:

- Wie sieht der Entscheidungsfindungsprozess in der IT aus, und wie sind die Verantwortlichkeiten verteilt?
- Wie wird die IT-Nachfrage mit den vorhandenen Ressourcen, und wie werden operative mit strategischen Prioritäten ausbalanciert?
- Wer ist für die Ausrichtung und Leitung der IT und der Geschäftsbereiche verantwortlich? Wer untersucht und empfiehlt neue Technologien? Wer trifft Investitionsentscheidungen?
- Wie behalten Führungskräfte die Übersicht und Kontrolle über die Organisation – mit klar definierten Verantwortlichkeiten und geeigneten Anreizsystemen?
- In welchem Unternehmenskontext steht die IT, und wie werden IT-Governance-Designs aktualisiert, angepasst und abgestimmt?

Bei der Einführung einer *zentralen IT-Steuerung* muss Wert auf eine ganzheitliche Sichtweise gelegt werden, weil Know-how und Führung zentrale Merkmale effektiver Strukturen (Prozesse) darstellen. Betrachtet man die Kunden- und Finanzsicht als weitere Grundpfeiler dieses Ansatzes im Unternehmen, ist der Schritt zu einer Balanced Scorecard eigentlich schon vollzogen.

Unternehmens-Governance legt Methoden (Standards) und Verantwortung (z. B. Leitsätze) in der Organisation fest, um Gesetze einzuhalten (basierend auf OECD-Principles of Corporate Governance, um beispielsweise Rechte von Anteilseignern, die Rolle von Stakeholdern oder Verfügbarkeit und Transparenz von Informationen zu regeln), Ziele etc. zu erreichen, d. h. Unternehmensressourcen verantwortungsvoll einzusetzen. Dabei wird zwischen einer sog. Enterprise- und Corporate-Governance unterschieden (vgl. [Jo07], S. 36ff.).

IT-Governance soll Chancen und Risiken der IT durch die IT aktiv managen. Bislang war die IT oft getrieben von Fachbereichsinitiativen und reagierte mehr, statt zu agieren. Durch aktives Management, gesteuert durch IT-Governance, ist die IT in der Lage, das Erreichen der

Unternehmensziele nachhaltig zu unterstützen und erlangt so wachsende Bedeutung. IT-Governance stellt somit einen wesentlichen Bestandteil einer gesamtheitlichen Unternehmensführung dar (vgl. [Jo07], S. 32f.).

Abbildung 10.1 zeigt einen Bezugsrahmen, der die Einordnung der verschiedenen Ansprüche an eine Governance-Struktur im Zusammenhang verdeutlichen soll. Während „die Corporate Governance (...) das Unbehagen der Aktionäre, den Umgang mit den von ihnen bereitgestellten Finanzmitteln (...) abbauen soll, so geht es bei der IT-Governance (...) um das Adressieren des Unbehagens beim Top-Management, wenn es um Kosten und Nutzen des Einsatzes von Informationstechnologie im Unternehmen geht“ ([RüSG06], S. 4).

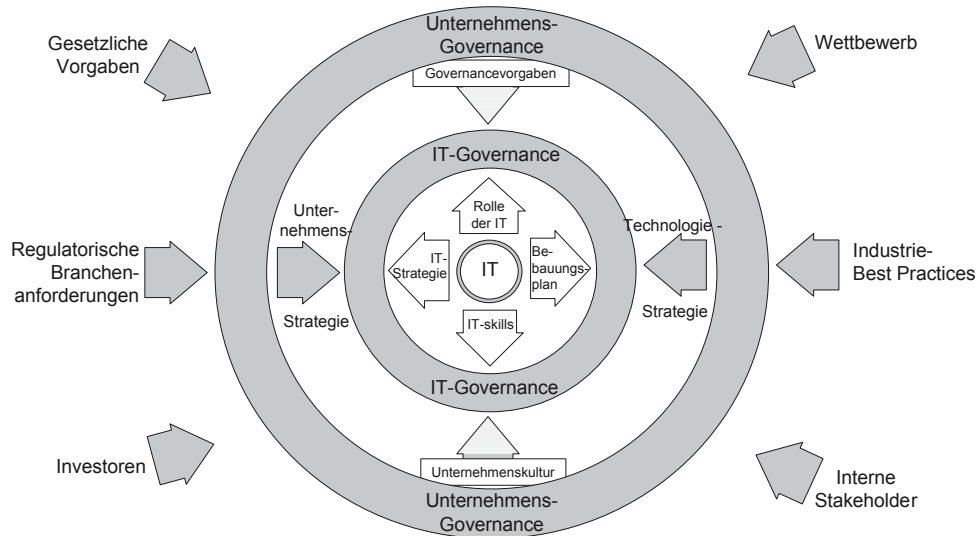


ABBILDUNG 10.1 Bezugsrahmen für IT-Governance (nach [RüSG06], S. 5)

IT-Governance fungiert oft als Bindeglied zwischen Corporate Governance und IT-Dienstleister. Die Definition von klaren Prozessen und Verantwortlichkeiten ist eine Grundvoraussetzung, um IT-Entscheidungen effizient zu treffen und durchsetzen zu können. Hierbei geht es vor allem um die Steuerung und Zuteilung von IT-Ressourcen und um die Methoden und Kriterien zur Priorisierung von IT-Investitionsentscheidungen. Bewährt hat sich der Einsatz von Portfoliomanagementmethoden, mit denen sich IT-Initiativen (Projekte) hinsichtlich ihrer strategischen und operativen Bedeutung sowie in Hinblick auf Finanzierung und Projektrisiken bewerten lassen. Im Einzelnen gilt es dabei zu beachten:

- Maßgebliches Kriterium zur Bewertung von IT-Initiativen ist die Wertschöpfung.
- Langfristige und kurzfristige Perspektive müssen abgewogen sowie die Verbindlichkeit von Initiativen berücksichtigt werden, die sich aus gesetzgeberischen Anforderungen ergeben.
- IT und Fachbereich priorisieren gemeinsam Aktivitäten für IT-Lösungen.
- Ein effektives Instrumentarium zur Leistungsmessung und -überprüfung muss installiert werden.

**Beachten Sie:**

Neben den Prozessen der IT-Governance, die sich primär mit den IT-Anforderungen und der Priorisierung von IT-Initiativen beschäftigen, sind auch die nachgelagerten Prozesse für die IT-Governance zu definieren, die sich mit der Umsetzung der Projekte befassen und sicherstellen, dass die geplanten Projektergebnisse tatsächlich erreicht und umgesetzt werden. Dabei spielen stets Bereichs- und Unternehmensziele eine entscheidende Rolle.

■ 10.2 Kern-Aufgabenbereiche zentraler IT-Steuerung

IT-Governance gilt derzeit als wichtiger Ansatzpunkt, wenn es um eine zukunftsorientierte Konzeptentwicklung und Organisation der IT im Unternehmen geht. Wichtig ist eine übergreifende IT-Steuerung aus Unternehmenssicht. IT-Governance ist für ein Unternehmen von so großer Bedeutung, dass die Planung, Organisation, Steuerung und Kontrolle der IT auf der Ebene der Unternehmensführung erfolgen muss (quasi unabhängig von der Leitung des eigentlichen IT-Bereichs, etwa der IT-Abteilung bzw. des IT-Dienstleisters).

Grundlegendes Merkmal für die Positionierung von IT-Governance ist die Orientierung an der Unternehmensstrategie. Dies gilt sowohl für die Formulierung der IT-Strategie, für Festlegungen zur IT-Organisation und für Vereinbarungen zu den IT-Prozessen. Da IT eine Querschnittsfunktion mit grundlegenden strategischen Nutzenpotenzialen darstellt, ist auf die Zusammenarbeit der strategischen und der operativen Ebenen großer Wert zu legen. Eine zentrale Verzahnung dieser zwei Perspektiven über die Anforderungsebene, die durch eine IT-Steuerung koordiniert wird, schafft es, die theoretisch vielfältig beschriebenen Ansätze praktisch umzusetzen.

Abbildung 10.2 gibt einen Überblick über die Herausforderungen und die sich daraus ableitenden Kern-Aufgabenfelder zentraler IT-Governance.

Ein Ziel der zentralen IT-Steuerung ist es, die funktionale Bedarfsermittlung der Fachbereiche weitestgehend von frühzeitigen Fokussierungen auf bestimmte Lösungen zu trennen. Auch oder gerade vor dem Hintergrund von Diskussionen zu Themen wie SOA halten wir dies für eine notwendige Prämisse. Erhält die IT funktionale, prozessbezogene Anforderungen, sollte sie die Entscheidung und damit Verantwortung für die spezifische Lösung haben.

Somit wird eine verbesserte Wertschöpfung im Konzern durch klare Trennung von Fachbereichs-Bedarf und IT-Bedarf möglich. Mittel- bis langfristig muss die IT den geschäftsbezogen-fachlichen Bedarf aus den Fachabteilungen weitestgehend von den in die immer komplexer werdende IT-Landschaft einzufügenden Lösungen trennen. Niemand unterstreicht dies mit dem Hinweis, dass ein Großteil der Potenziale (und somit auch Risiken) im „Housekeeping“, also dem Handhaben der vorhandenen IT-Landschaft, stecken [NI05, S. 60], welches ca. 80% der IT-Kosten beinhaltet.

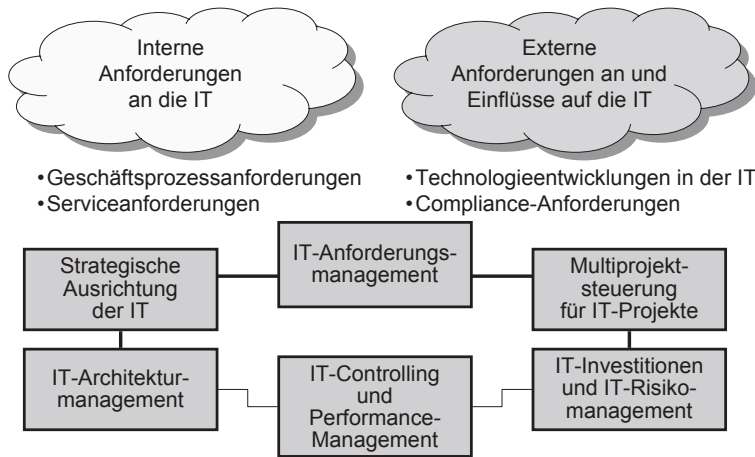


ABBILDUNG 10.2
Aufgabenbereiche einer zentralen IT-Steuerung

Wertbeiträge durch Investitionen: Flankierend ist es ebenso wichtig, die betriebswirtschaftlichen Anforderungen an IT-Lösungen bzw. IT-Projekte frühzeitig zu einer bewertbaren Basis auszuarbeiten. Der Nutzen nicht nur für einen einzelnen Bereich, sondern der vernetzte Unternehmens- oder Konzernnutzen müssen in den Vordergrund gerückt werden. Regeln und Vereinbarungen (Top down) sind hier erforderlich. Außerdem das enge Zusammenspiel mit Konzerncontrolling und Unternehmensentwicklung.

Insgesamt ist festzustellen, dass die IT ein zentraler Baustein zukünftiger Unternehmensentwicklungen ist. Wichtig für die IT-Governance sind Durchsetzungs- und Veränderungsmechanismen im Bereich Führung und Kommunikation. Ein Zusammenspiel mit der Personalabteilung stellt hier ein die Planung begleitendes proaktives Agieren sicher.



Konsequenzen:

Bestand bislang oftmals die Rolle der IT-Abteilung bzw. eines IT-Dienstleisters darin, „lediglich“ technische Komponenten und eine Infrastruktur zur Verfügung zu stellen, so wird die IT zunehmend als aktiver Partner für diverse andere Bestandteile im Unternehmensgefüge gesehen, etwa:

- als Unterstützung/Berater für Fachabteilungen (sog. Business-IT-Alignment);
- als zentraler Anlaufpunkt für Mitarbeiter und Kunden bei technischen Fragen und Problemen;
- als Geschäftspartner für externe und interne Lieferanten, Outsourcing-Firmen oder für externe Consultants.

Aus diesem neuen Rollenverständnis als Partner für unterschiedlichste Stakeholder ergibt sich, dass an die IT-Organisation verschiedenste neue Anforderungen gestellt werden. Neben den „klassischen“ Anforderungen an die IT bzw. die IT-Systeme (wie Benutzerfreundlichkeit, Performance, Sicherheit, Funktionalität und Support) werden Aspekte wie die folgenden immer wichtiger:

- Know-how-Transfer zwischen den Abteilungen;

- wirtschaftliche Bereitstellung von IT-Produkten (Hardware, Applikationen);
- qualitativ hochwertige IT-Services;
- konsequente Unterstützung der Geschäftsprozesse.

Damit trotz wachsender Kostensenkungsbestrebungen und sog. Industrialisierung der IT die Innovationsfähigkeit der IT auf einem hohen Niveau bleibt, ist es Aufgabe der IT-Governance, hierauf ein Augenmerk zu legen.

10.2.1 Ganzheitliche IT-Strategieentwicklung

IT-Governance-Verantwortliche sind in jedem Fall gefordert, in regelmäßigen Abständen eine aussagekräftige ganzheitliche IT-Strategie zu formulieren und dabei zukunftsweisende Entscheidungen für die Ausrichtung der unternehmensweiten IT-Architekturen sowie Empfehlungen hinsichtlich durchzuführender IT-Projekte zu treffen. Dabei kommt es heute vor allem darauf an, kosten- und wertorientiert zu denken, gleichzeitig aber auch technologisch up to date zu bleiben und den zunehmenden Anforderungen der Anwender bzw. Endbenutzer gerecht zu werden.

Für die Formulierung und Ausgestaltung der IT-Strategie sind ausgehend vom Ist-Zustand der IT im Unternehmen, den Anforderungen des Unternehmens an die IT sowie den organisatorischen und technischen Möglichkeiten auf dem Gebiet der Informations- und Kommunikations-Technologien verschiedene Festlegungen zu treffen:

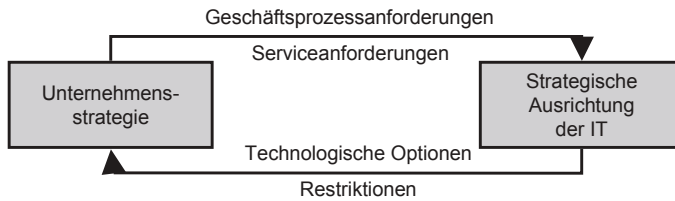
- Formulierung der Vision, der Mission, der Zielsetzungen und Wege, wie die IT in Zukunft in einem Unternehmen genutzt werden soll;
- Eckpunkte für anzustrebende unternehmensweite Soll-IT-Architekturen sowie
- die Bereitschaft, für entsprechende Projekte organisatorische Veränderungen zu schaffen.

Im Ergebnis sollte ein Konzept bzw. Vorgehensmodell existieren, das

- die Erarbeitung einer an den Unternehmenszielen ausgerichteten IT-Strategie ermöglicht (IT-Governance folgt Corporate Governance),
- eine darauf aufbauende technische Architektur und Infrastruktur kreiert sowie
- die Darstellung und Vermarktung des daraus resultierenden Werts für die Kunden des IT-Bereichs realisiert.

Darüber hinaus sind aus der IT-Strategie die Qualitätsziele für das jeweilige Jahr abzuleiten.

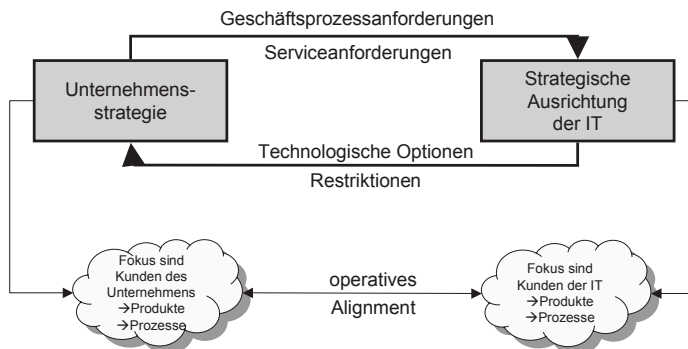
Die Herausforderung des „Strategic Alignment“ bzw. der Ausrichtung der IT-Strategie an der Geschäftsstrategie ist die ganzheitliche Verzahnung beider Strategien (siehe Abbildung 10.3). Schafft man es, die Unternehmensziele durch geeignete IT-Aktivitäten bzw. IT-Produkte zu unterstützen, ist eine effektive Basis für eine nachhaltige Unternehmensentwicklung geschaffen.

**ABBILDUNG 10.3**

Strategische Ausrichtung der IT und Beachtung der Unternehmensstrategie

Diese Verzahnung [vgl. HE07] *muss* auf einer Ebene der Zusammenarbeit im operativen und im strategischen Bereich geschehen, da so die Grenzen der Aufbauorganisation schon im Planungsstadium überwunden werden können. Geschäftsbereichsstrategien müssen auf Kunden-Produkte und Kunden-Prozesse abstellen und auf zukünftige Transaktionsarten zwischen Kunden und Unternehmen. Darauf aufsetzend, moderiert die zentrale IT-Steuerung im Rahmen der skizzierten Anforderungskoordinatorenrunde die Generierung neuer Ideen.

Parallel wird unter Mitwirkung der IT die bestehende Unternehmensstrategie weiterentwickelt. Insgesamt erfolgt eine Verzahnung durch Verbesserung des gegenseitigen Verständnisses und der gemeinsamen Grundlagenarbeit für die mindestens jährlichen Planungsunden. Ein Aspekt ist dabei auch das sprachliche Zusammenwachsen sowie das Generieren einer „Konzernbrille“, da heute teilweise immer noch von Alleingängen bzw. Abteilungsegoismen berichtet wird. Erst wenn diese Verzahnung erreicht ist, kann eine IT-Strategie richtig *effektiv* sein. Eine solche Entwicklung in der Organisation kann ausschließlich die **Führungsarbeit** der Unternehmensleitung sicherstellen, welche mit der erfolgreichen Steuerung solch kritischer Prozesse auch entscheidend die Kultur des Unternehmens prägt. Der scheinbare Widerspruch zwischen den Thesen Chandlers und Mintzbergs wird durch effektive Führung überwunden, denn grundsätzlich haben beide Recht: Harvardprofessor Alfred Chandler mit seiner 1962 veröffentlichten, auf empirischen Studien basierenden Theorie, dass die Organisationsstruktur auf die Umsetzung der Strategie ausgerichtet sein muss und von der Strategie gesteuert wird und Henry Mintzberg, der den Erfolg einer Organisation wesentlich auf die Unternehmenskultur bezieht. Geeignete Koordinationsmechanismen zwischen freier Abstimmung und direkter Anweisung schaffen eine Kultur des „pulling together“, um die Zentrifugalkräfte des Tagesgeschäfts (z. B. Interessen Einzelner setzen sich durch, Erfolge werden nur den Führungskräften zugeschrieben, nicht nachvollziehbare Machtausübung) zu minimieren und das Unternehmen auf der Ebene gelebter Werte ständig zusammenzuhalten (vgl. [Mi89], S. 95ff). Abbildung 10.4 veranschaulicht diese Zusammenarbeit auf operativer und strategischer Ebene.

**ABBILDUNG 10.4**

Perspektiven für die Umsetzung des strategischen Alignments

Direkte Auswirkungen hat das gesamte Vorgehen auch auf die Prioritäten bei der Auswahl geplanter IT-Projektvorhaben im Rahmen des Multiprojektmanagements und somit auf IT-Produkte und IT-Serviceprozesse.

Abbildung 10.5 zeigt ein Beispiel für die Inhalte des Strategiepapiers (= IT-Master-Plan).

Inhalte von unternehmensweiten IT-Strategiefestlegungen (Beispielgliederung eines IT-Master-Plans)	
1 Management-Summary	7 Beschreibung der Teilstrategien – Soll-Konzept und Entscheidungen
2 Ziele und Rahmenbedingungen	7.1 Organisatorische Positionierung der IT
3 Positionierung der IT im Gesamt-Unternehmen (Wertbeitrag, etc.)	7.2 Strategisches Anforderungsmanagement (Vorgehen, Instrumente)
4 Umfeldanalyse	7.3 IT-Servicestrategie
4.1 Interne Aspekte (Geschäftsmodelle)	7.4 IT-Personalstrategie
4.2 Externe Aspekte (Wettbewerbsanalysen)	7.5 IT-Sourcing-Konzept
4.3 Technologie Aspekte (Trendanalysen)	7.6 Richtlinien für IT-Projekte (Vorgehen, Instrumente)
5 Ist-Analyse und IT-Diagnose	7.7 Konzept für das IT-Qualitätsmanagement und die Qualitätssicherung
5.1 Methodisches Herangehen und Ergebnisse	7.8 IT-Risikopolitik und Compliance-Strategie
5.1.1 Situationsanalyse	8 Empfehlungen und Richtlinien zu den IT-Architekturen (IT-Architekturkonzept)
5.1.2 SWOT-Analyse	8.1 Technologiearchitektur
5.2 IT-Diagnose und Beurteilungen	8.3 Applikationsarchitektur
5.2.1 Fachliche Beurteilung	8.3 Fachliche Architekturen (Fachkonzepte)
5.2.2 Technische Beurteilung	8.4 Organisation (Prozesse, Strukturen etc.)
5.2.3 Organisatorische und wirtschaftliche Beurteilung	8.5 Sicherheitsarchitektur (Richtlinien für IT-Security)
6 Grundsätze und Standards für die IT (IT-Prinzipien)	9 Vorhabens-Planung und Investitionsmanagement
6.1 Zulässige Basissysteme in der IT	9.1 Value-Management
6.2 Richtlinien zur IT-Nutzung im Unternehmen (unternehmensweite Vorgaben)	9.2 Unternehmensweite Wirtschaftlichkeitsbewertung
	9.3 Projekt-Portfolio und Projekt-Budgetierung

ABBILDUNG 10.5 IT-Strategie und IT-Master-Plan (Gliederungsvorschlag für Dokument)

10.2.2 IT-Anforderungsmanagement

Die Wünsche der Anwender an die IT können sich auf unterschiedliche Bereiche (Produkte, Dienste) beziehen. Dies können sein:

- Software-Anforderungen (Applikationen, Anwendungen)
- Anforderung an die Ausstattung mit IT-Systemen (Arbeitsplatzsystem, Vernetzung, Speicher- und Serverleistungen)
- Möglichkeiten der Implementierungsunterstützung (Schulung etc.)
- Erbringen von Serviceleistungen bzw. Anforderungen an die IT-Prozesse (Support bei Ausfällen, Fehlern etc.)

Ein professionalisiertes bzw. in das Tagesgeschäft integriertes IT-Anforderungsmanagement leistet für ein Unternehmen einen wesentlichen Beitrag zu optimierten IT-Lösungen, die den Anforderungen der Anwender (Fachbereiche, Endbenutzer) in besonderer Weise unter Beachtung von Wirtschaftlichkeitsaspekten Rechnung tragen. Der Grundgedanke war ganz einfach: Jahr für Jahr steht die IT unter dem Druck, viele Projekte gleichzeitig zu realisieren, die regelmäßig Kapazitäts- und auch Budgetgrenzen sprengen. Schnell war deshalb klar, dass ein

optimierter Input (Summe aller IT-Anforderungen der Fachbereiche) insbesondere im Zusammenspiel mit einer Multiprojektsteuerung auch zu einer Entlastung der IT während der Projektphasen und auch später bei der Wartung der Systeme führen müsste.

Wichtig ist in jedem Fall eine klare Kundenorientierung für das Handeln im IT-Bereich, also eine Sichtweise auf die Fachabteilung als sog. internen Kunden. Damit verbunden ist die Notwendigkeit einer umfassenden Serviceorientierung, etwa auch durch

- die Bereitstellung von IT-Produkt- und Leistungskatalogen,
- die Vereinbarung von Service Level Agreements sowie
- die Einrichtung eines leistungsfähigen Service-Desks.

Im Sinne einer verstärkten Kundenorientierung muss sich das Management bzw. die IT-Governance nicht nur Gedanken darüber machen, wie das Unternehmen seine Aufgaben möglichst gut erledigt. Im Mittelpunkt müssen – gerade aufgrund der großen Bedeutung, die der IT für den Unternehmenserfolg heute zukommt – auch die Klärung und Verfolgung der folgenden Fragenkreise stehen:

- Wie lässt sich die Kundenzufriedenheit bezüglich der IT-Produkte und der IT-Leistungen steigern?
- Wie etabliert man erfolgreich neue bzw. implementierte IT-Produkte und Leistungen im Unternehmen?
- Was sind die wesentlichen Erfolgsfaktoren für die IT-Lösungen des Unternehmens?

Prinzipiell steigt der Wertbeitrag der IT umso mehr, je besser sich Letztere um ihre Kunden im Unternehmen kümmert (eine auch durch die Erfahrung vielfach bestätigte These).

Für das Finden und sachgerechte Beurteilen der Kundenwünsche ist es besonders wichtig, den Zweck zu verstehen, mit dem der Kunde eine Anforderung formuliert:

- Wofür will der Kunde ein neues System?
- Was bezweckt er damit?
- Warum ist er bereit zu investieren?
- Was sind seine Erfolgskriterien für unser Projekt?

Daraus lässt sich ableiten, welche Funktionen und Eigenschaften für die gewünschte Lösung essenziell sind. Damit ist letztlich der Kern der Anforderungen gefunden, der nun schrittweise um funktionale Anforderungen ergänzt wird. Ergänzend sind weitere nicht funktionale Anforderungen, die sich beispielsweise bei Softwareanforderungen anhand der Qualitätsmerkmale der ISO 9126 strukturieren können, zu erarbeiten. Vorgaben bezüglich der technischen Lösung (Required Restrictions), wie z.B.: Vorgabe des Betriebssystems, der zugrunde liegenden Datenbank oder technischer Schnittstellen runden die Anforderungen vor allem auch vor dem Hintergrund der zu erbringenden Integrationsleistung der IT ab.

Zum Aufbau eines Anforderungsmanagements ist festzuhalten:

- Anforderungsmanagement wird als eine Managementaufgabe für die effiziente und fehlerarme (störungsfreie) Entwicklung und Bereitstellung komplexer IT-Systeme bzw. IT-Lösungen verstanden.
- Anforderungsmanagement ist vor allem dort von Bedeutung, wo komplexe IT-Produkte bzw. IT-Systeme konzipiert werden und sehr arbeitsteilig an deren Entwicklung, Integration und Implementierung gearbeitet wird.

- Die Planung von Änderungen, die zu Anforderungen führen, soll von Anforderungskoodinatoren in *regelmäßiger* Abstimmung mit entsprechenden KollegInnen aus dem Konzern diskutiert werden als Basis für koordinierte Geschäftsprozessoptimierung. Dabei steht die Entwicklung eines gemeinsamen Konzerngedankens im Sinne eines kognitiven Alignments auf der Basis gemeinsamer Werte und Visionen im Vordergrund (vgl. [KEMA08], S. 30).

Grundsätzlich ist neben der Rollendefinition eines Anforderungskoodinators (oft auch als Anforderungsmanager bezeichnet) auch auf eine systematische Zusammenarbeit der Anforderungskoodinatoren untereinander großen Wert zu legen. Erst diese operative Plattform von Anforderungskoodinatoren im Unternehmen stellt sicher, dass die Einzelplanungen koordiniert bzw. aus Konzernsicht optimiert sind.

Durch die Einführung und Umsetzung von Verfahren und Methoden des IT-Anforderungsmanagements wie

- Positionierung (Scoping),
- Anforderungserhebung,
- Anforderungsanalyse,
- Anforderungsspezifikation,
- Anforderungsmodellierung,
- Anforderungsreviews

werden in den Unternehmen ein positives Ergebnis und ein positiver Abschluss eines IT-Projektes bzw. eines Auftrages gewährleistet.



Schlussfolgerungen und Konsequenzen:

- Durch eine zentrale IT-Steuerung kann eine Gruppe von Anforderungskoodinatoren gesteuert werden, um eine Vergleichbarkeit bei der Bewertung von Anforderungen zu erreichen.
- Durch diese fachbereichsübergreifende neutrale Steuerung sind Synergieeffekte (Wertbeiträge) erzielbar.
- In Verbindung mit der Multiprojektsteuerung lassen sich Ressourcenengpässe vermeiden und eine übergreifende Einsatzsteuerung realisieren.
- Durch ein fachbereichsübergreifendes IT-Anforderungsmanagement lässt sich eine stärkere ganzheitliche Entwicklung von IT-Strategien erreichen.

IT-Anforderungen zu spezifizieren und zu managen, ist eine Herausforderung, der sich jede Organisation stellen muss. Erst wenn diese Prozesse optimiert sind, wird es möglich, dass die Fachabteilungen mit den ausgelieferten bzw. implementierten IT-Lösungen und Leistungen zufrieden sind und dass der IT-Bereich qualitativ hochwertige Produkte und leistungsfähige IT-Services bereitstellen kann.

Erfahrungen der Praxis zeigen, dass das Aufstellen von Anforderungen allein nicht ausreicht, sondern für die erfolgreiche Realisierung eines IT-Produktes oder IT-Systems ein umfassender Prozess des ganzheitlichen Anforderungsmanagements notwendig ist. Anforderungsmanagement kann dabei als eine Managementaufgabe für die effiziente und fehlerarme (störungsfreie) Entwicklung und Bereitstellung komplexer IT-Systeme bzw. IT-Lösungen gesehen

werden. Anforderungen und ihre Spezifikation können zu unterschiedlichen Anlässen und zu unterschiedlichen Zeitpunkten (Phasen) im Rahmen von IT-Projekten zu dokumentieren und zu prüfen sein:

- Anforderungsdefinition anlässlich der Festlegung einer Projektskizze (des Projekt-Steckbriefes)
- Anforderungsdefinition in Verbindung mit einem Projekt-Antrag: Fein-Spezifikation
- Festlegung der Anforderungsspezifikation im Rahmen eines Lastenheftes
- Anpassung der Anforderungen aufgrund geänderter Gegebenheiten im Projektverlauf (Claim-Management); vor allem nötig bei Ansätzen des Agilen Projektmanagements.

In allen Fällen können die folgenden Grundprozesse (mehr oder weniger gründlich) durchlaufen werden: Anforderungen erheben und erfassen, Anforderungen bewerten, Anforderungen validieren.

Wie gelangen wir zu den Anforderungen an ein IT-Produkt? Nehmen wir etwa eine Anwendungslösung als Beispiel. Typischerweise wird die Anforderungsdefinition in einem mehrstufigen Prozess realisiert:

- Definition der Kundenanforderungen (User Requirements);
- Definition der Systemanforderungen (sie definieren das zu entwickelnde oder zu liefernde System);
- Definition der Anforderungen an die Komponenten des Systems, die von den Systemanforderungen und der Architektur abgeleitet werden.

Wenn wir die Anforderungen so unterteilen, wird sofort klar, dass Letztere nicht unabhängig vom Konzept der Lösung sein können, sondern Schritt für Schritt parallel zur Konkretisierung der Lösung erarbeitet und verfeinert werden.

10.2.3 IT-Architekturmanagement und Enterprise Architecture Management

Optimales Architekturmanagement – so die generelle Annahme – liefert durch die Definition von Rahmenbedingungen und Standards für den IT-Einsatz die Grundlage für eine effektive IT-gestützte Bewältigung der komplexen Anforderungen der Fachabteilungen und Endbenutzer sowie für die Beherrschung der komplexen IT-Systeme.

Eine Steuerung und Kontrolle der installierten IT-Architekturen sowie eine damit in Verbindung stehende Entscheidungsfindung ist natürlich nicht gerade einfach:

- So wurden in der Vergangenheit mitunter komplexe IT-Systeme aufgebaut und Applikationen entwickelt, die anschließend im Betrieb und Support einen unangemessenen Wartungs- und Betreuungsaufwand erfordern.
- IT-Infrastrukturen und IT-Applikationen sind organisch gewachsen. Über Jahre hinweg ist so eine IT-Anwendungslandschaft basierend auf sehr unterschiedlichen Technologien, Entwicklungsparadigmen und Werkzeugen entstanden. Diese gilt es durch eine zentrale IT-Governance „in den Griff“ zu bekommen.
- Implementierte IT-Systeme weisen umfassende Funktionalitäten auf und unterliegen raschen Entwicklungszyklen. Im Ergebnis existieren komplexe IT-Anwendungen auf unter-

schiedlichen Technologieplattformen. Diese müssen transparent und beherrschbar gemacht werden; etwa durch einen Tooleinsatz zur Darstellung der Applikations-Landschaft.

- Hinzu kommt, dass mitunter Redundanzen auftreten: in der Datenarchitektur, den Schnittstellen, der Funktionsabdeckung der Anwendungen und bei der Ausstattung mit Technologieplattformen.

Insgesamt kann festgestellt werden, dass die IT-Infrastruktur- und die Anwendungslandschaft in der Unternehmenspraxis komplex sind. Hier gilt es sowohl aus strategischer als auch operativer Sicht im IT-Architekturmanagement anzusetzen. Ziel muss es sein, durch Dokumentation Transparenz zu schaffen und anhand verschiedener Sichten und Detaillierungen, die auf die Interessengruppen im Unternehmen ausgerichtet sind (vgl. [NI05], S. 21f), die Planbarkeit und Steuerbarkeit der komplexen IT-Landschaft zu erreichen. Entscheidend für den Erfolg ist dabei die Qualität des Dialogs der Geschäftsbereiche mit dem IT-Bereich. Zu viele technische Details schrecken die Fachbereiche ab, und zu wenige führen zu keinem sinnvollen Ergebnis. Natürlich sind die erforderlichen Informationen zur Beschreibung heutiger und zukünftiger Geschäftsprozesse inkl. aller Schnittstellen und Anforderungen an die wirklich notwendigen Daten in den Unternehmen vorhanden – nur fehlen in der Regel Strukturen, Vorgaben und die Organisation, um eine unternehmensweite Planung von Geschäftsprozessen, Produkten, Dienstleistungen und der unterstützenden IT unter einen Hut zu bringen. Governance im Unternehmen hat dies zum Ziel und erreicht damit auch, dass *bessere* Entscheidungen über Produkte, Prozesse und Anwendungen getroffen werden.

Aufgrund der Ist-Situation können sich für die IT-Verantwortlichen unter Umständen Problemfelder ergeben, wie:

- **Fehlender Überblick aufgrund der hohen Komplexität der IT-Landschaft:** Es ist aufgrund der über Jahre gewachsenen IT-Systeme vielfach nicht ohne Weiteres nachvollziehbar, wie das Zusammenspiel zwischen den Geschäftsprozessen bzw. Arbeitsabläufen und der eingesetzten Soft- und Hardware im Detail erfolgt. Analysen der IT-Landschaft in Bezug auf Redundanzen, Strukturprobleme oder Optimierungsmöglichkeiten sind nur schwerlich möglich. Hilfreich wäre zumindest eine grafische Darstellung der IT-Landschaft als Kommunikationsmittel.
- **Erhöhte Risiken und fehlende Steuerbarkeit der IT-Infrastruktur:** Diverse Infrastruktur-Technologien sind oft so miteinander vernetzt, dass sehr unterschiedliche Systeme in unterschiedlicher Weise verkoppelt sind. Fällt ein Teilsystem aus, hat dies ggf. gravierende Folgen für weitere Systeme.
- **Risiken für eine sichere Software-Bereitstellung:** Softwareentwicklung und -beschaffung sind mangels eines umfassenden Überblicks über die IT-Architektur ebenfalls nur schwer steuerbar. Es existieren große Anwendungslandschaften, innerhalb deren zahlreiche Anwendungen untereinander und mit externen Systemen Informationen bzw. Daten austauschen müssen. Im Laufe der Zeit sind diese Anwendungslandschaften allerdings oft hochkomplex und unflexibel geworden. Infolgedessen ergeben sich erhöhte Risiken für die Bereitstellung, Integration und den Betrieb von leistungsfähigen IT-Systemen und IT-Anwendungen.

Wie sehen die wesentlichen Rahmenbedingungen und Zielsetzungen bei Einführung eines systematischen IT-Architekturmanagements aus? Welche Merkmale bei der Implementierung moderner Architekturen Beachtung finden sollten, zeigt Tabelle 10.3.

TABELLE 10.3 Eckpunkte für Architekturmanagement

Merkmale	Begründung/Implementationshinweise
Standardisierung	Die Einführung von standardbasierenden Hard- und Softwarelösungen ermöglicht eine erhöhte Verfügbarkeit und erleichtert die Flexibilität und Adaptionfähigkeit der IT-Systeme.
Modularität & Integration	Durch eine modulare, integrierte Systemarchitektur lassen sich Skalierbarkeit, Effizienz und Ressourcenauslastung von IT-Systemen wesentlich verbessern.
Erhöhte Wirtschaftlichkeit der IT	Bei der Architekturentscheidung müssen zunehmend betriebswirtschaftliche Betrachtungen (ROI, TCO) in den Vordergrund treten. So lassen sich durch eine Konsolidierung der IT-Landschaften insbes. auch auf Ebene der genutzten Funktionalitäten die explodierenden Kosten für IT-Wartung bzw. Pflege in den Griff bekommen.
Vereinfachung bzw. Vereinheitlichung der IT-Landschaft	Konsolidierte Hardware-Systeme (Server, Storage, Netze etc.), Daten (Datenbanken) und Applikationen können eine Verbesserung der betrieblichen Effizienz gewährleisten sowie eine erhöhte Verfügbarkeit des Gesamtsystems sicherstellen. Der Verwaltungsaufwand wird reduziert, die Supportkosten werden gesenkt.
Verbesserte Flexibilität in der Anwendungsrealisierung	Immer schneller sich verändernde wirtschaftliche Rahmenbedingungen erfordern eine höhere Flexibilität und schnellere Reaktionsfähigkeit (Time to Market) bei der Realisierung von IT-Anwendungen. Nur so lassen sich entscheidende Wettbewerbsvorteile erzielen.
Ganzheitliche IT-Strategieorientierung	Geschäfts- und IT-Strategie müssen so in Übereinstimmung gebracht werden, dass die Gesamtstrategie der Organisation die Ausgestaltung der IT-Strategie ganzheitlich – und wechselseitig – bedingen kann („Strategic Alignment“).

Kernprozesse im IT-Management sind die Beherrschung der installierten IT-Architekturen sowie eine sach- und zeitgerechte Entwicklung, Auswahl und Umsetzung von IT-Architekturen. Nur durch professionelle Architekturarbeit kann heutzutage die Grundlage für eine schnelle, IT-gestützte Bewältigung der immer komplexeren Anforderungen der Organisation und der dortigen Fachabteilungen und Endbenutzer gewährleistet werden. Das nachhaltige erfolgreiche Bestehen einer Organisation hängt mitunter vom Einsatz dieses Instruments zur Planung und Steuerung der Geschäftsprozesse und IT-Systeme ab.

Eine Kernforderung muss die effiziente Umsetzung einer effektiven Geschäftsprozessplanung und damit maßgeblicher Veränderungen im Unternehmen sein. Ob dies gelingt, wird größtenteils von den IT-Architekturen und deren Leistungsfähigkeit bestimmt. Aufgabe des Architekturmanagements ist es, die Kerngeschäfts- und Querschnittsprozesse wirksam zu unterstützen und dabei die Flexibilität und Effizienz zu wahren.

Das IT-Management muss die vorhandene IT-Architektur „beherrschen“ und ein tragfähiges Gesamtbild der IT-Entwicklung als Orientierungsrahmen bieten: die Zielarchitektur von Infrastruktur und Anwendungslandschaft. Dazu sind Gestaltungsprinzipien und Systemscheidungen zu formulieren, wie auch „strategische“ Technologien und Produkte definiert und kommuniziert werden sollten. Für das Strategic Alignment gilt es, Soll-Szenarien der verschiedenen *Architektursichten* sowie die sich daraus ergebenden IT-Projekte im Sinne einer „Roadmap“ für die weitere IT-Entwicklung zu erstellen. Um einen „Turmbau zu Babel“ zu vermeiden, sind konkrete Vorgaben und Standards für die Erarbeitung der Szenarien festzulegen.

Im Rahmen des IT-Architekturmanagements gilt es zu entscheiden, wie eine standardisierte Entwicklung, Integration, Installation und Wartung (Modifikation) von IT-Systemen (IT-Architekturen) mithilfe von IT-Strategien erfolgen kann. Wichtig ist es festzuhalten, in welchen Prozessen IT-Architekten mit welcher Unterstützung an die Arbeit gehen können. Dazu gehören folgende Aufgabenbereiche:

- Methodische Planung der Unternehmensarchitektur, eingebettet in den strategischen IT-Planungsprozess
- Konzeption und Entwicklung der Facharchitektur
- Entwurf eines Bebauungsplans der Anwendungslandschaft (Applikationsarchitektur)
- Effiziente und bedarfsgerechte Entwicklung der IT-Infrastruktur
- Risikomanagement für technologieintensive Projekte, präventive Planung und Review von Softwarearchitekturen

Zu den Merkmalen und Handlungsebenen des IT-Architekturmanagements gehören:

- Mit der Erhebung und Beschreibung der IT-Architekturen (Technologiearchitektur, Anwendungsarchitektur, Datenarchitektur und Geschäftsarchitektur) lassen sich die vorhandenen Anwendungs- und Systemwelten strukturieren und der Ist-Zustand verdeutlichen.
- Durch die Definition von Soll-IT-Architekturen werden Rahmenbedingungen für eine flexible Anpassung der Informationstechnologien an veränderte Marktanforderungen geschaffen.

Die hier beschriebenen Architektursichten sind ganzheitlich konzipiert und beschreiben eine Unternehmensarchitektur, die sich im nahezu allgegenwärtigen IT-Umfeld abbildet. Dort resultierende Unternehmens- bzw. effektive IT-Architekturen stellen eine gemeinsame Entscheidungsbasis für den IT-Bereich, die Fachbereiche und das Management dar und fördern so einen Entscheidungsprozess unter Berücksichtigung vielfältiger Sichtweisen. Durch ein permanentes Controlling kann hier eine wesentliche Hilfe geleistet werden

Wichtige Eckpunkte des Architekturmanagements sind: kontinuierliche Entwicklung und Pflege der Architektur, situationsabhängige Durchsetzung der Architektur sowie Institutionalisierung des Architekturmanagements zur „Beherrschung“ der IT-Landschaften.



Wichtig:

IT-Architekturmanagement definiert die erforderlichen Prozesse und Strukturen, um aus den strategischen Zielsetzungen des Unternehmens adäquate Fach-, Software- und Systemarchitekturen ableiten zu können, die optimal aufeinander abgestimmt sind und einen reibungslosen bzw. sicheren IT-Betrieb gewährleisten.

Um zu überschaubaren und nachhaltigen IT-Architekturen zu kommen, wird eine IT-Architektur für Unternehmen häufig durch die folgenden Grundbausteine bzw. Sichten beschrieben:

- Technologie-Architektur (IT-Infrastrukturen, die nach dem sog. IT-Infrastructure-Layer dargestellt werden können);
- Anwendungsarchitektur (Applikations-Architekturen, die sich typischerweise als Business-Layer bzw. Knowledge-Layer im Schichtenmodell abbilden lassen);
- Geschäftsarchitektur (fachliche Architekturen);
- Prozess- und Organisations-Architektur.

Diese Bereiche geben den Rahmen für viele wesentliche Umsetzungsmöglichkeiten in der Praxis und auch für strategische Diskussionen vor.

Von besonderer Relevanz ist die ganzheitliche Betrachtung auf Unternehmensebene und die Entwicklung von Architekturen im Großen sowie die Berücksichtigung der Wechselwirkungen zwischen den Bausteinen der Architekturen.

IT-Architekturen bewerten: Für Planungen und Entscheidungen ist es unverzichtbar, eine Bewertung der vorhandenen Architekturen vorzunehmen. Dazu stehen verschiedene Instrumente und Verfahren zur Auswahl (siehe Abbildung 10.6).

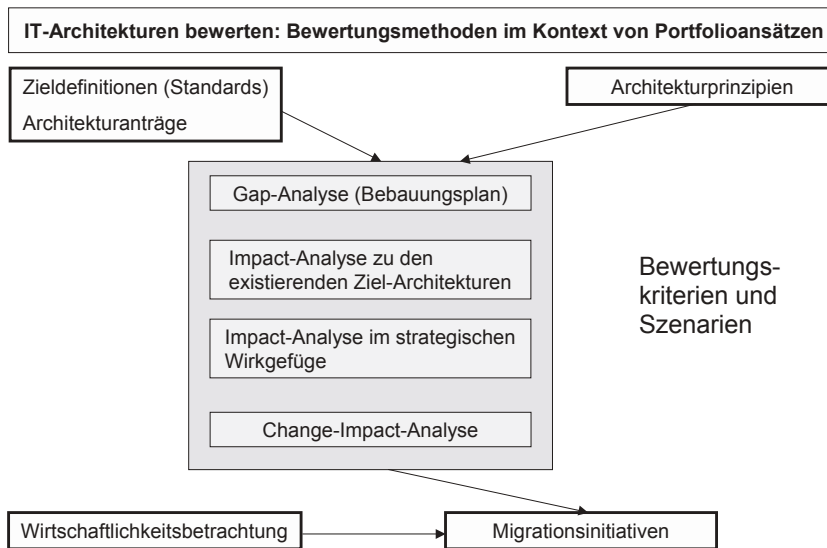


ABBILDUNG 10.6 Bewertung von IT-Architekturen (modifiziert nach IBM)

IT-Architekturen planen und steuern: Vorhandene IT-Architekturen bedürfen in jedem Fall zunächst einer permanenten Steuerung (inkl. eines damit verbundenen Performance Managements). Die Schwierigkeit besteht mitunter darin, die komplexe IT-Landschaft so zu managen, dass einerseits die IT-Unterstützung für die Geschäftsprozesse jederzeit in der vereinbarten Qualität erbracht wird, andererseits aber auch genügend Sicherheit und Flexibilität für künftige Veränderungen an Teilsystemen entsteht.

IT-Architekturen können in der Regel nicht „auf der grünen Wiese“ geplant werden. In der Realität beherrschen gewachsene Systeme mit unterschiedlichen Lebenszyklen die IT-Landschaft von Organisationen. So ist ein komplexes Geflecht von Beziehungen und Abhängigkeiten entstanden. Dieses Geflecht muss handhabbar, skalierbar, steuerbar und stringent gestaltet sein und entsprechende Mechanismen zur Verfügung stellen, um die Anforderungen aus dem Tagesgeschäft erfüllen zu können.

Im Rahmen des IT-Architekturmanagements sind Entscheidungen darüber zu treffen, wie eine standardisierte Entwicklung, Integration, Installation und Wartung (Modifikation) von IT-Systemen (IT-Architekturen) aufgrund von vereinbarten Vorgaben erfolgen kann. Es ist wichtig, festzuhalten, in welchen Prozessen IT-Architekten mit welcher Unterstützung ihre Arbeit aufnehmen können. Dazu gehören folgende Aufgabenbereiche:

- effiziente und bedarfsgerechte Entwicklung und Betreuung der IT-Infrastruktur
- Risikomanagement für Technologie-intensive Projekte, präventive Planung und Review von Softwarearchitekturen
- methodische Planung der Unternehmensarchitektur, eingebettet in den strategischen IT-Planungsprozess
- Konzeption und Entwicklung der Facharchitektur
- Entwurf eines Bebauungsplans der Anwendungslandschaft

Die Umsetzung der Konzepte des Architekturmanagements verändert in vielen Organisationen die Art und Weise, wie die Planung, Entwicklung und Einführung von Informationssystemen in der IT eines Unternehmens durchgeführt wird. So müssen Rollen und Abläufe verändert werden, um die Architekturen erfolgreich planen und einführen zu können.

Abbildung 10.7 zeigt, wie die Aktivitäten bei der IT-Bebauungsplanung miteinander zusammenhängen.

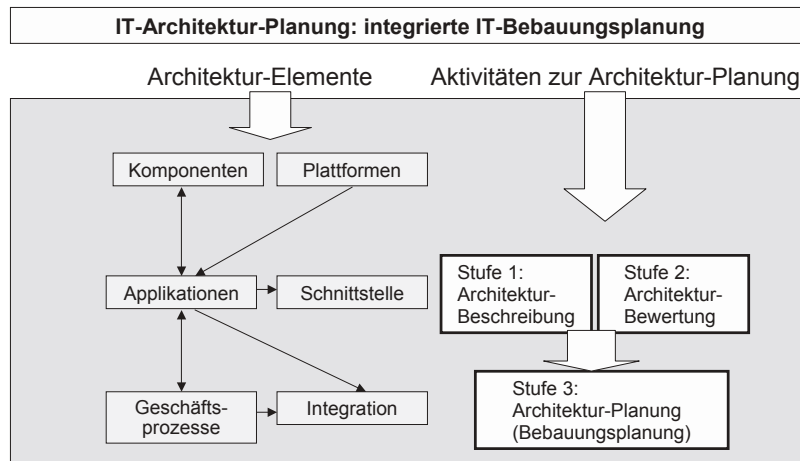


ABBILDUNG 10.7 Vorgehen und Elemente für einen IT-Bebauungsplanung

10.2.4 Multiprojektsteuerung für IT-Projekte

IT-Verantwortliche müssen in der Regel mehrere IT-Projekte gleichzeitig managen. Diese Projekte können einen sehr unterschiedlichen Charakter (seien es Software-Entwicklungsprojekte, IT-Infrastrukturprojekte oder strategische IT-Projekte) sowie eine unterschiedliche Relevanz für das Unternehmen haben. Dies gilt es bei Auswahlentscheidungen, aber auch bei der Durchführung zu berücksichtigen. Mit Methoden und Instrumenten des Projekt-Portfoliomanagements lassen sich die vielfältigen Aufgaben zur Bewertung, Qualifizierung und kontrollierten Steuerung sämtlicher IT-Projekte ganzheitlich erfolgreich realisieren, von der Anforderungsanalyse und Priorisierung bis hin zur Realisierung und Produktivsetzung der jeweiligen IT-Projekte.

Eine erfolgreiche Umsetzung der genehmigten IT-Projekte setzt in jedem Fall eine entsprechende Multiprojektmanagement-Organisation voraus. Die IT-Projekte sollten sich durch eine

relativ hohe Komplexität und einen nicht unerheblichen Innovationsgehalt der Aufgabenstellung auszeichnen. Dabei sind Mitarbeiter aus unterschiedlichen Abteilungen und Kulturen einzubeziehen sowie externe Mitarbeiter in die Projektarbeit zu integrieren. Hinzu kommen bereits während der Projektlaufzeit diverse Änderungen an den zuvor festgelegten Projektzielen und Kunden-Anforderungen.

Optimal ergänzt wird die systematische Erarbeitung von Anforderungen durch eine Multiprojektsteuerung, die das effektive Nutzen der Unternehmensressourcen zum Ziel hat.

**Definition:**

Multiprojektsteuerung oder Multiprojektmanagement ist das Management mehrerer „paralleler“ Projekte, die über begrenzte Ressourcen oder über Sachergebnisse miteinander verbunden sind. Daraus ergeben sich folgende Aufgaben:

- Erhebung der Anforderungen zu IT-Vorhaben
- Aufdecken von Abhängigkeiten (Redundanzen, Synergien)
- Priorisierung (Bewertung)/laufende Anpassung
- Kapazitäten-/Ressourcensteuerung
- Terminsteuerung

Bei der Einführung eines Multiprojektmanagements müssen klare Governance-Regeln geschaffen werden. Dies bezieht sich vor allem auf den Ablauf und die Rollenverteilung. Die folgenden fünf Phasen geben dem Instrument der IT-Projektinvestitionssteuerung einen Rahmen:

- Klären des Nutzens der geplanten Maßnahme
- Bewerten der Maßnahme
- Entscheiden, wann in welchem Rahmen realisiert wird
- Umsetzung der Maßnahme
- Nachbetrachtung nach Inbetriebnahme

Weil größere Projekte oder Projektalternativen zur Erarbeitung der Chancen und Risiken teilweise schon erhebliche Ressourcen benötigen, sind zwei Entscheidungsphasen erforderlich: die Freigabe einer Voruntersuchung und die Freigabe der Umsetzung im Rahmen des IT-Portfolios.

Diese Phasen werden von Ansprechpartnern und Richtlinien unterstützt. In der Entscheidungsphase ist ein Herzstück das Steuergremium IT-Projekte, wobei als IT-Projekt auch Maßnahmen ab einem Gesamtaufwand von etwa 50 TEUR betrachtet werden sollten, sobald die IT direkt oder indirekt betroffen ist. Kriterien für das Vorliegen eines IT-Projektes sind die Nutzung von IT-Ressourcen sowie der Bezug zu Geschäftsprozessveränderungen. Damit konzentriert sich eine zentrale IT-Steuerung auf strategisch induzierte Veränderungen. Durch die Betrachtung auch kleinerer Vorhaben entsteht neben der Transparenz zu entstehenden Aufwendungen bzw. Investitionen auch eine Kultur der Offenheit, da keine „Salamitaktik“ bspw. eine bewertbare Anforderungsspezifikation umgehen kann. Optimal wäre es, wenn anfordernde Abteilungen einen Business Case erarbeiten, der die Bewertungskriterien des Unternehmens, die natürlich vorher definiert und festgelegt werden müssen, adressiert.



Ergebnisse der Multiprojektsteuerung:

Ziel des Managements von zeitlich und inhaltlich um dieselben IT-Ressourcen konkurrierenden Anforderungen von Fachbereichen ist es, einen Konsens auf Ebene der verantwortlichen Entscheidungsträger zu erzielen. Ein zurückgestelltes Projekt bedeutet dann, dass der Nutzen anderer Maßnahmen im zu beplanenden Zeitraum größer war, oder es kann auch heißen, dass ein anderer Manager seine Hausaufgaben besser gemacht hat.

Damit ist ein nicht unwichtiger Aspekt eines solchen offenen, diskursiven Vorgehens angesprochen, welches hohe Transparenz auf Entscheidungsebene bedeutet. Gut vorbereitete Maßnahmen, welche die Nutzenpotenziale klar erkennen lassen, wirken für die Priorisierung wie ein plausibler Businessplan bei einem kreditvergebenden Banker. Aufgabe der zentralen IT-Steuerung ist es hier, die Argumente (mit jeweils gleicher Subjektivität) zu bewerten und ein Projektportfolio für das IT-Investitions-Gremium zu erstellen.

Doch damit sind noch nicht alle Vorteile benannt. Jede Anwendung kann unterschieden werden in Basisfunktionalitäten und besonders ausgeprägte bzw. solche, mit denen sich Anbieter von der Konkurrenz unterscheiden können; auch Fachbereiche haben aufgrund ihrer Geschäftsprozesse oft solche besonderen Ausprägungen vor Augen. Kontrollt man nun die Kosten und Deckungsbeiträge aus den hinter den Anforderungen liegenden Geschäftsprozessen, handelt es sich bei den zuletzt genannten Funktionalitäten der gewünschten Anwendung um eher beeinflussbare Kosten. Hier gibt es also Potenzial für Einsparungen oder Wettbewerbsvorteile.

10.2.5 IT-Risikomanagement

Projekte, Prozesse und Produkte (IT-Infrastrukturen, Software) im IT-Bereich unterliegen – das steht außer Zweifel – immer einem gewissen Risiko. Eine Vielzahl von Einflussfaktoren kann dazu führen, dass das Erreichen der angestrebten Ziele gefährdet oder gar erhebliche negative Folgewirkungen denkbar sind (etwa aus Fehlern oder Verzögerungen in der Ausführung der IT-Prozesse oder der IT-Projekte).

Für die Handhabung von IT-Risiken wurden inzwischen einige brauchbare Lösungsansätze entwickelt, die erhebliche Potenziale zur Zukunftssicherung eröffnen. Entsprechende Konzepte gilt es im Rahmen von IT-Governance mit Unterstützung geeigneter Akteure für das IT-Risikomanagement zu entwickeln und umzusetzen.

Die Bedeutung des Risikomanagements wurde im IT-Bereich lange nicht erkannt. Mittlerweile bekommt IT-Risikomanagement aber einen immer höheren Stellenwert. So machen zahlreiche Beispiele deutlich, welche IT-Risiken mit Negativfolgen zu beachten sind. Zur Vermeidung gravierender Schäden wird es für Unternehmen – unabhängig von der Unternehmensgröße – zu einer unverzichtbaren Aufgabe, zu untersuchen, welche möglichen Risiken bzw. Schwierigkeiten im IT-Bereich auftreten können und welche Folgen damit verbunden sind.

In jedem Fall müssen sich die Verantwortlichen für IT-Governance vergegenwärtigen,

- welche IT-Risiken bei den IT-Produkten, IT-Prozessen und IT-Projekten es zu beachten gilt;
- welche Aktivitäten für das IT-Risikomanagement üblich sind;

- wie eine Einordnung dieser Aktivitäten aus operativer und strategischer Sicht möglich ist;
- welche Zielgruppen sich für das IT-Risikomanagement unterscheiden lassen.

Zunächst ist eine genauere Einordnung der Herausforderungen und Aufgaben zum IT-Risikomanagement für die jeweilige Organisation vorzunehmen. Mit einem IT-Risiko wird gemeinhin die Möglichkeit bezeichnet, dass es bei IT-Projekten und IT-Produkten bzw. IT-Prozessen zu Problemen mit negativen Auswirkungen kommt. Ein solches Risiko setzt sich zusammen aus

- den möglichen Problemen/Ereignissen,
- der Wahrscheinlichkeit ihres Auftretens,
- der Tragweite (Auswirkungen) beim Auftreten der Probleme sowie
- den erforderlichen Aufwänden, um das Risiko zu mindern.

Soll ein Risikomanagement-System für den IT-Bereich neu aufgesetzt oder verbessert werden, gilt es also, zunächst eine strategische Positionierung vorzunehmen. Im Zuge einer Konzeptentwicklung werden dabei die Abläufe und Werkzeuge des Risiko-Managements bestimmt. Dazu sind vier Schritte erforderlich. Diese müssen permanent durchlaufen werden, da neue Risiken hinzukommen oder bestehende sich ändern können:

- **Risiko-Identifikation:** Es sind die IT-Risiken zu identifizieren. Dies geschieht etwa durch Meldungen der beteiligten und betroffenen Personen eines IT-Prozesses.
- **Risiko-Analyse:** Die identifizierten Risiken müssen anschließend hinsichtlich der Erreichung der Zielsetzungen einer genauen Analyse unterzogen werden.
- **Risiko-Bewertung:** In diesem Fall schätzt der Risikomelder, mit welcher Wahrscheinlichkeit das Risiko eintritt. Dann wird ermittelt, welches Ausmaß das Risiko in Bezug auf Funktion, Zeit und Ressourcen voraussichtlich hat. Die Risikokennzahl ergibt sich aus der Kombination von Eintrittswahrscheinlichkeit und Risikoausmaß. Je größer die Kennzahl, desto größer die Wahrscheinlichkeit des Eintritts bzw. des Schadensausmaßes.
- **Maßnahmen zur Risikobehandlung:** Es gilt, Maßnahmen einzuleiten, die den Risiken entgegenwirken. Bei Prozessen zählt dazu beispielsweise die Anpassung von Zielen, Plänen oder Ressourcen. Ist dieses Potenzial ausgeschöpft, können Risiken auch auf Dritte verlagert werden, etwa durch Outsourcing oder die Vereinbarung von Schadensersatz bei Nichterfüllung von Dienstleistungen durch Dritte.

Ähnlich einem effektiven Controlling-Ansatz, bei dem es zu einem Dialog zwischen Entscheider und Controller kommen muss, ist auch die Identifikation von Risiken im IT-Bereich, wenn diese nicht nur die rein technische Infrastruktursicht (bspw. Business Continuity) beinhalten soll, stark von einer inhaltlichen Transparenz abhängig. Weiß der IT-Verantwortliche, wo die strategische Reise des Unternehmens hingehen soll und kennt er darüber hinaus auch konkrete Details wie strategische Kunden, Produkte und Prozesse, dann kann er in diesen Kontexten die Risiken darstellen und bewerten – hier sind natürlich die Produkte und Prozesse aus END-Kundensicht gemeint.

Sinn und Zweck eines effektiven, durch die IT-Governance gesteuerten Risikomanagements ist also nicht nur die Identifizierung von Risiken, sondern vielmehr die Ermittlung von Maßnahmen, um diese Risiken von vornherein zu vermeiden bzw. um die zu erwartenden Schäden für die Unternehmung und ihre Kunden möglichst gering zu halten. Dies beinhaltet neben der Identifizierung und Bewertung der Risiken auch die Planung und konsequente Umsetzung von

Risikomaßnahmen mit dem Ziel, den IT-Bereich in optimierter Form erfolgreich zu einer hohen Ergebnisqualität zu führen (siehe Abbildung 10.8).

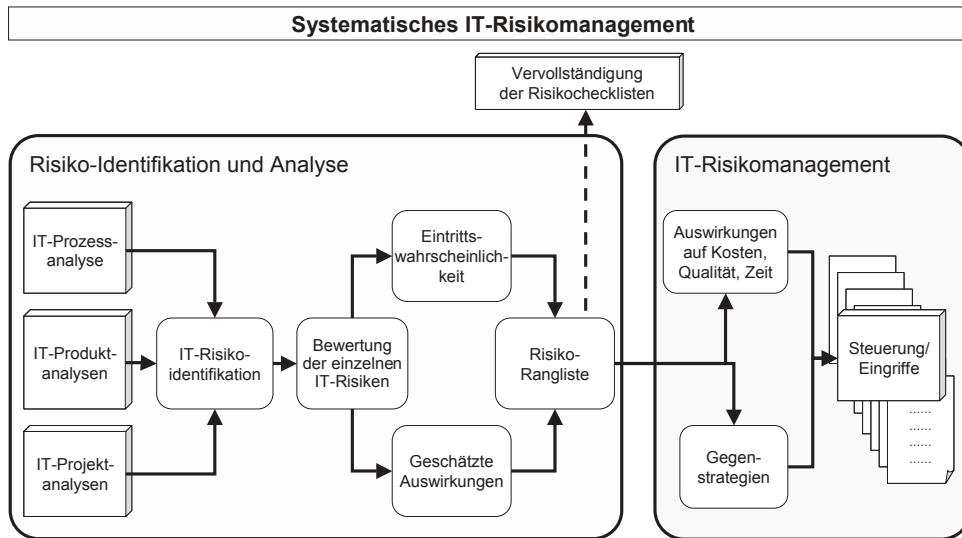


ABBILDUNG 10.8 Von der Identifikation von IT-Risiken zum IT-Risikomanagement

Analog einer Investitionsplanung lassen sich Risiken in der Regel nur vergleichend bewerten, d. h., es müssen Alternativen gefunden und dargestellt werden. Hierfür eignet sich ebenfalls das Architekturmanagement, da es in der Lage ist, die Komplexität der vorhandenen Systeme und Sichtweisen darzustellen.

IT-Risikomanagement ist grundsätzlich in allen Unternehmen zu etablieren; bei Unternehmen, die besonders von ihrer IT abhängig sind, ist es sogar eine wesentliche Compliance-Aufgabe (vgl. [FrGl07], S. 53f.). Damit stellt es eine zentrale Aufgabe der IT-Governance dar, die beispielsweise auf standardisierten IT-Prozessen aufbauend diese zu definierten und dokumentierten IT-Dienstleistungen bündelt, welche einer ständigen Qualitätskontrolle zu unterziehen sind.

10.2.6 Compliance Management

Vorgaben verschiedener Art – seien es Gesetze, Richtlinien oder Verwaltungsvorschriften – haben auch für das IT-Management in den letzten Jahren eine immer höhere Bedeutung erlangt. Dafür hat sich mittlerweile der Begriff IT-Compliance eingebürgert.

Im Rahmen eines Compliance Managements ist es wesentlich, dass in der IT-Organisation geeignete Maßnahmen definiert und umgesetzt werden, die sicherstellen, dass die vorliegenden IT-Prozesse und die entwickelten IT-Lösungen so gestaltet sind, dass sie den gesetzlichen Anforderungen sowie sonstigen internen und externen Vorgaben entsprechen.

Mögliche Maßnahmen können im organisatorischen, personellen und technischen Umfeld angesiedelt sein. Ein gesetzeskonformes (Compliance-gerechtes) Verhalten soll dabei sowohl

für Handlungen des Unternehmens insgesamt als auch für Handlungen der einzelnen Mitarbeiterinnen und Mitarbeiter sichergestellt werden. Hauptziel dieser Maßnahmen ist, bereits im Vorfeld durch entsprechende Regelungen Gesetzesverstöße zu verhindern.

IT-Compliance-relevant sind primär **Gesetze** (z.B. BDSG, KonTraG), Verwaltungsvorschriften (z.B. GDPdU) sowie **Richtlinien, Standards** und Referenzmodelle (z.B. COBIT, ITIL sowie BSI-Standards und -Grundschutzkataloge), die einen Bezug zur IT aufweisen.

Hinweis: Zum Compliance-Management vergleiche ausführlich Kapitel 13 „IT-Compliance“ in diesem Handbuch.

10.2.7 IT-Investitionsmanagement und Value-Management

Die Planung, Durchführung und Bewertung von IT-Investitionen sind Aufgaben, die immer von mehreren Stellen und Personen im Unternehmen erledigt werden. Ausgehend von den Grundsätzen der IT-Governance ist es wichtig, dafür ein klares Verfahrenskonzept zu entwickeln und einzuführen.

Oberste Zielsetzung ist es, dass die IT einen Beitrag zur Optimierung der Geschäftsprozesse leistet, egal ob es sich um betriebliche Kernprozesse oder Managementprozesse handelt. Dies ist gerade bei Investitionsentscheidungen zu berücksichtigen. Die IT-Investitionen können unterschiedlichen Zwecken dienen. Aus strategischer Sicht unterscheidet man beispielsweise die folgenden drei Arten von IT-Investitionen:

1. *Investitionen zur Sicherung der Betriebs- und Lieferfähigkeit:*

IT-Investitionen zur Sicherung der Betriebs- und Lieferfähigkeit stellen ein absolutes Muss zur Aufrechterhaltung des laufenden Betriebs dar. Der größte Teil aller IT-Investitionen – 70 Prozent und mehr – dient in der Praxis lediglich der Sicherung der Betriebstätigkeit.

2. *Investitionen zur Verbesserung der Leistungsfähigkeit:*

IT-Investitionen zur Verbesserung der Leistungsfähigkeit sollen die Wirtschaftlichkeit des Betriebes erhöhen, indem sich größere Transaktionsvolumina dann mit weniger Aufwand abwickeln und Dienstleistungen effizienter erbringen lassen.

3. *Investitionen zur Verbesserung der Wettbewerbsfähigkeit:*

IT-Investitionen zur Verbesserung der Wettbewerbsfähigkeit können etwa durch eine Differenzierung der Produkte und Dienstleistungen mittels IT ermöglicht werden. Diese Differenzierung resultiert weniger aus der bloßen Implementierung einer bestimmten Technologie oder eines bestimmten IT-Systems als vielmehr aus einem richtigen strategischen Einsatz der IT.

Tabelle 10.4 zeigt, welche Stellen oder Gruppen in welchen IT-Governance-Prozessen für Aufgaben bezüglich der IT-Investitionen zuständig sind.

TABELLE 10.4 IT-Governance-Aufgaben und Verantwortliche für IT-Investitionen
(analog IT-Governance Institute; ITGI 3, S.67)

IT-Governance-Prozess	Stelle/Gruppe	Herausforderungen/Aufgaben
Strategic IT-Alignment	Technology Council	▪ Technologie-Richtlinien zur Verfügung stellen ▪ Relevanz von neuen Entwicklungen der IT aus Sicht des Kerngeschäfts der Organisation analysieren und Empfehlungen geben
	IT Architecture Review Board	Architektur-Richtlinien entwickeln und die Einhaltung sicherstellen
Value Delivery (Wert-Management)	Top Management	IT-Investitionen müssen ein ausgewogenes Kosten-/Nutzenverhältnis aufweisen (akzeptable Budgets) und eine Risikoprüfung inkludieren.
	CFO	IT Budget und IT Investitionspläne sind nachhaltig und realistisch; darüber hinaus sind sie in den übergeordneten Finanzplan integriert.
	Linien-Management	▪ Neue IT Services identifizieren und Beschaffung unterstützen ▪ Operativen Nutzen von IT-Investitionen feststellen und kommunizieren
	IT Steering Committee (Steuerremium für IT-Projekte)	▪ Identifikation und Berücksichtigung aller relevanten Kosten sicherstellen ▪ Kosten-/Nutzenanalyse durchführen
	Technology Council	Technologieauswahl unterstützen (in Abstimmung mit den definierten Standards)
	IT Architecture Review Board	Anwendung der Architektur-Richtlinien kontrollen und performen
IT Resource Management	Top Management	Ein ausgewogenes Maß an IT-Investitionen für Erhalt bzw. Wachstum des Unternehmens bereitstellen
	IT Strategy Committee	Eine allgemeine Richtung für Sourcing und den Einsatz von IT-Ressourcen (z. B. strategische Allianzen) vorgeben
	CIO	▪ IT Infrastruktur bereitstellen, die die Erstellung und Kommunikation von Information zu optimalen Kosten unterstützt ▪ Standardisierung von Architektur und Technologie entwickeln und gewährleisten
Risk Management	IT Strategy Committee	Risikواسpekte von IT-Investitionen berücksichtigen
Performance Management	CEO	Performance, Kontrollen und Risiken der IT und der wesentlichen Investitionen evaluieren
	Technology Council	Einhaltung von Technologiestandards und Vorgaben verifizieren
	IT Architecture Review Board	Einhaltung von Architekturstandards und Vorgaben verifizieren

Die IT leistet einen wesentlichen und unverzichtbaren Beitrag zur Bewältigung der Herausforderungen des Informationszeitalters. Sie stellt die Summe der technischen und organisatorischen Mittel (Hardware, Software, Services) zur Unterstützung der Geschäfts- und Führungsprozesse sowie der verschiedenen informationellen Prozesse (der Beschaffung, Verarbeitung, Speicherung, Übertragung und Bereitstellung von Informationen) dar.

Auch in der Literatur wird die IT mittlerweile nicht mehr nur als Kostenfaktor und Dienstleister, sondern zum Beispiel als „Value Center“ oder Werttreiber gesehen, der durch seine Orientierung am langfristigen Erfolg ein Unternehmen auch zu besseren und neuen Leistungen befähigen und sich durch seine Marktorientierung sogar als „Profit Center“ profilieren kann. Im Grunde wird also – in der Theorie wie in der Praxis – die IT zunehmend als eine Art Unternehmen im Unternehmen betrachtet, das Kundenbedürfnisse befriedigen, profitabel im Markt agieren, kostenbewusst arbeiten und zukunftsfähig handeln muss.

Die Möglichkeiten und Chancen der IT, den Erfolg zu beeinflussen, liegen unter anderem in der Kostensenkung. Die positive Beeinflussung der Erlössituation ist sicherlich auch durch eine Steigerung der Erlöse möglich, leichter und prozentual gewichtiger aber durch Kostensenkung erreichbar. Eine effiziente betriebliche IT kann Bestandskosten und Gemeinkosten nachhaltig senken. Wichtig ist es aber auch, den anfallenden Kosten den Wertzuwachs gegenüberzustellen, der sich durch die Anwendung von Informations- und Kommunikationstechnologien realisieren lässt.

Möchte man den Beitrag eines Informationssystems zur Wertschöpfung eines Unternehmens genauer untersuchen, gilt es zunächst, bestimmte Wertkategorien abzugrenzen und herauszuarbeiten. Folgende Wertkategorien, die durch die Nutzung moderner IT-Lösungen realisierbar sind, können unterschieden werden:

1. **Return on Investment.** In diese Kategorie fällt der enge Nutzenbegriff der traditionellen Kosten/Nutzen-Analyse und Investitionsrechnung.
2. **Strategische Unterstützung.** Investitionen werden vielfach durchgeführt, um strategische Zielsetzungen des Unternehmens zu unterstützen. Lautet ein strategisches Ziel „Kundennähe“, so wird dieses Ziel durch den Einsatz von Informationstechnologie für direkte Kundenkommunikation gefördert.
3. **Wettbewerbsvorteil.** In diese Kategorie fallen die Schaffung neuer Marktstrukturen, verbesserte Positionierung der Produkte oder die Schaffung neuer Geschäftsmöglichkeiten. Ein Beispiel ist das Angebot von Dienstleistungen, wie dies verschiedene Fluggesellschaften in Form von Buchungssystemen tun, deren Kerngeschäft in einem anderen Bereich liegt.
4. **Management-Information.** Dieser Faktor umfasst Informationen über die Kernaktivitäten des Unternehmens, über kritische Erfolgsfaktoren. Liefert ein Management-Informationssystem derartige Informationen, ist dies zu berücksichtigen.
5. **Reaktion auf Wettbewerb.** Vielfach fordert der Markt bestimmte Maßnahmen vom Unternehmen, so etwa die Einführung bestimmter technischer Systeme. Die Forderung kann von Kundenseite kommen oder durch Aktivitäten der Mitbewerber diktiert werden.
6. **Strategische IT-Architekturen.** Es gibt Systeme und Systemlösungen, die zwar nicht unmittelbar Erträge und Wirtschaftlichkeitsvorteile bedeuten. Diese IT-Architekturen können jedoch aus strategischer Sicht unverzichtbar sein und ein Zukunftspotenzial darstellen. Insofern kann man sie als besonders zu berücksichtigende Werte ausweisen.



Gerade in den nächsten Jahren werden sich zahlreiche Unternehmen mit der Ressource-Information stärker als bisher auseinanderzusetzen haben, was auch eine aktive Mitwirkung von Fach- und Führungskräften einschließt. Informationssysteme werden zur strategischen Waffe erfolgreicher Unternehmensführung, das Management wird zum Gestalter und Nutzer solcher Systeme.

■ 10.3 Zentrale IT-Governance einführen

10.3.1 Die Ansätze

Die Implementierung von IT-Governance ist nicht mit klassischen CRM- oder ERP-Projekten vergleichbar, aber gewisse Projektelemente sind ähnlich: etwa die dedizierten Teams, welche die Maßnahmen und ihre Koinzidenz mit den Business-Strategien ständig überprüfen.

Ein integraler Bestandteil von IT-Governance ist die Etablierung von Rahmenbedingungen zur Ermöglichung der kontinuierlichen Verbesserung des Konzeptes. Exemplarisch einige Beispiele für derartige Rahmenbedingungen:

- Gegeben ist eine klare, marktoffene Auftragnehmer-/Auftraggeber-Beziehung zwischen den Fachbereichen und der IT.
- IT-Ausgaben und -Aufwendungen (inkl. Budgetierungen für den IT-Bereich) werden zentral gesteuert.
- Projektentscheide erfolgen auf Basis eines einheitlichen, verpflichtenden Business-Case-Formats (Kosten-, Nutzen- und Risikobetrachtung) mit anschließendem Nutzeninkasso (Prüfung und Kontrolle des Business Case).
- Transparenz über das IT-Projektportfolio des Unternehmens (Einzelprojektcontrolling durch die Auftraggeber, Existenz einer übergreifenden IT-Controlling-Instanz für das Multi-projektmanagement).

Ohne praktische Erfahrung in den Bereichen der Projektorganisation, -abwicklung sowie dem Wissen um die eigene Wertschöpfungskette und der einzuführenden Methodologie ist ein solches Projekt kaum zum bewältigen. Wichtig ist die Berücksichtigung der Erfolgsfaktoren für IT-Governance, die Tabelle 10.5 aufführt.

TABELLE 10.5 Hauptgründe und Erfolgsfaktoren für IT-Governance

Erfolgsfaktor	Hinweise
Transparenz für alle Fachbereiche schaffen	▪ schafft Vertrauen in die IT ▪ verbessert die Zusammenarbeit von IT und Fachbereich ▪ motiviert die Betroffenen
General-Management über die Bedeutung von IT-Governance informieren	▪ ermöglicht die Bestärkung und Veränderung von Verhaltensweisen des General Managements zu IT-Managementfragen ▪ Management als Sponsor ist unverzichtbar
Governance-Regeln an das Unternehmen anpassen	▪ nicht einfach Standards anderer Unternehmen als Regeln übernehmen, sondern Governance-Regeln mit Stakeholdern und Betroffenen vereinbaren ▪ General Management einbinden
Governance-Regeln konzentrieren	▪ auf wenige strategische IT-Ziele konzentrieren ▪ klare Verhaltensweisen (Prozessbeschreibungen und Verfahrensregeln) dokumentieren ▪ überschaubares Kennzahlensystem ▪ klare Regelung von Ausnahmen

IT stellt im Unternehmen ein verbindendes Element dar, dessen Integrationsbestreben aufgrund bereichsindividueller Zielsetzungen kein primäres Ziel der einzelnen Bereichsverantwortlichen darstellt. Um mit diesen divergierenden Einstellungen umzugehen und eine geschlossene Strategie zu entwickeln, sollten Führungskräfte und Vorstände eine starke IT-Steuerungsstruktur in ihren Unternehmen einführen. Viele müssen ihre Einstellung überdenken, dass IT-Steuerung nicht ihre eigene Verantwortung ist. Sie müssen damit beginnen, proaktiv zu führen, um sicherzustellen, dass ihre Organisationen die vielen Vorteile nutzen, die sich aus einer Optimierung von IT-Chancen ergeben, und sich gleichzeitig vor Risiken zu schützen.



Beachten Sie:

Um die möglichen Vorteile eines Governance-Konzeptes zu nutzen, muss die Einführung mit großer Sorgfalt und Disziplin erfolgen. Die konsequente Analyse des Ist-Zustandes der eigenen unternehmerischen Prozesse sowie der vorhandenen IT-Infrastruktur inklusive der dafür oder dadurch erbrachten Dienstleistungen sind Grundvoraussetzungen für die erfolgreiche Einführung.

IT Governance liegt in der Verantwortung des Vorstands sowie des Managements und ist ein wesentlicher Bestandteil der Unternehmensführung.

Primäres Ziel des Einsatzes von IT-Systemen ist es, Informationen zur richtigen Zeit, im richtigen Umfang, in angemessener Qualität und Form am richtigen Ort zur Verfügung zu stellen. Ziel des IT-Managements ist es, das dafür erforderliche IT-System angemessen und wirtschaftlich bereitzustellen und zu betreiben.

10.3.2 Vorgehen

Neben den inhaltlichen Schritten muss sich die zentrale IT-Steuerung zunächst als Organisationseinheit im Unternehmen formieren, ihre Rolle definieren und anschließend die skizzierten Handlungsfelder in Angriff nehmen.

Letztendlich laufen sämtliche Planungen und Abstimmungen auf konkrete Maßnahmen hinaus, die in der Regel als IT-Projekte bzw. IT-Vorhaben gesteuert, umgesetzt und überwacht werden. Wesentlich ist, dass die für den Unternehmenserfolg maßgeblich verantwortlichen Geschäftsbereiche die IT als ihr Mittel zur Zielerreichung sehen müssen, gleichzeitig aber die Wechselwirkungen innerhalb der IT-Landschaft auf Konzernebene berücksichtigen lernen. Damit hat IT-Steuerung auch mit Entscheidungsrechten sowie Verantwortungsrahmen zu tun und will einen anderen *Umgang mit der IT* erreichen (vgl. [WeRo04]). Da dies sehr theoretisch klingt, ist es ein plausibles Vorgehen, sich auf die Planungsphase zu konzentrieren und auf drei wesentliche logische Schritte zu fokussieren (siehe Abbildung 10.9):

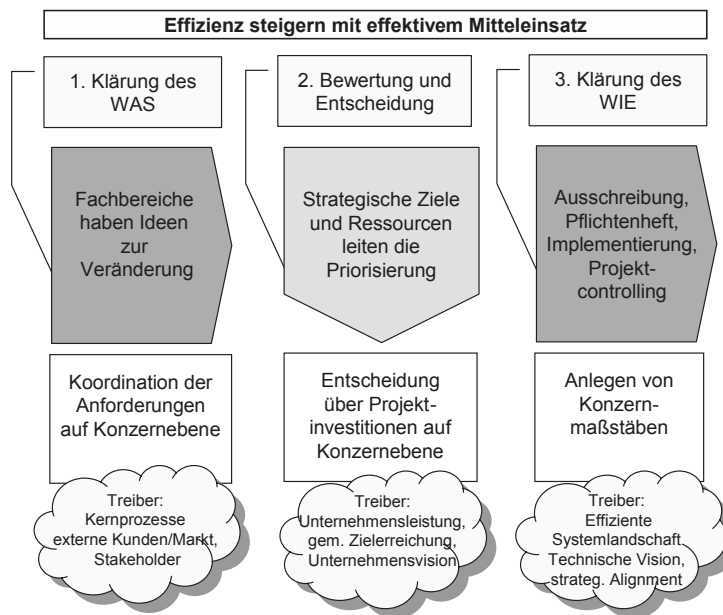


ABBILDUNG 10.9
Planung der Geschäftsbereiche als Grundlage eines effektiven IT-Governance-Handelns

- Klärung des WAS oder rein funktionaler Zielsetzungen – hier kann durchaus eine Technologie die gewünschten Funktionalitäten erst ermöglichen;
- Klärung der Bewertungskriterien und Entscheidung vor dem Hintergrund strategischer Zielsetzungen und begrenzter Ressourcen im Unternehmen;
- Klärung des WIE oder der Realisierung innerhalb der IST-IT-Architektur im Sinne einer optimierten Planungsalternative.

Problematisch bezüglich der Umsetzung von IT-Governance-Regeln und Prinzipien ist ein in der Praxis oftmals formulierter Zeitdruck: die Geschäftsbereiche wollen neue Ideen in der Regel unmittelbar angehen. Der Einstieg in das Thema IT-Governance in der beschriebenen Form kann deshalb für viele Organisationen nicht konzentriert (quasi als Big Bang) erfolgen,

sondern muss Schritt für Schritt umgesetzt und parallel zum Tagesgeschäft durchgeführt werden. Das bedeutet auch, dass der Erfolg – wie bei strategischen Maßnahmen ohne Krisensituationen – erst mit der Zeit an Konturen gewinnt. In eine ganzheitliche Architekturplanung mit allen wesentlichen Geschäftsbereichen müssen alle Beteiligten gemeinsam hineinwachsen. Wichtig ist deshalb ein Grundkonsens im Unternehmen zu der strategischen Maßnahme „IT-Governance“, um den Ansatz nachhaltig zu implementieren.

Unter *WAS* versteht man im Wesentlichen die funktionalen Anforderungen aus den Unternehmensprozessen, die im Rahmen von übergeordneten Zielen und Vorgaben sowie begrenzten Ressourcen einmal optimiert werden müssen (die richtigen Dinge tun). Aufgrund eines permanenten technologischen Wandels ist insbesondere bei der Entscheidung zum *WIE* der technischen Umsetzung auf einen systemischen Ansatz zu achten, der den hohen Ansprüchen an Integration und somit Beherrschbarkeit sowie Flexibilität nachkommt. Dabei muss es der IT gelingen, die wesentlichen Geschäftsprozesse und damit die wesentlichen Aktivitäten, um unsere Kunden am Markt zufrieden zu stellen, aktiv zu unterstützen. Der IT kommen hier als Berater *und* Dienstleister im Unternehmen zwei wichtige Rollen zu, die eine wohldosierte IT-Governance unterstützen und steuern soll.

IT-Governance kümmert sich aus Gesamtunternehmenssicht

- einerseits um die Steuerung der IT-Investitionen und deren Abstimmung mit der Unternehmensstrategie (liefert insofern über die Anforderungen auf Basis der Geschäftsprozesse den essenziellen Input zum Change Management) sowie
- andererseits um die Performance der IT selbst. Der laufende IT-Betrieb ist dabei ebenfalls als Fachbereich zu sehen, der ständiger Innovation unterliegt, die erkannt und integriert werden muss.

Das Thema „IT-Governance“ gewinnt seit einigen Jahren aufgrund des Stellenwerts von IT für viele Geschäftsprozesse zusehends an Bedeutung. Die These, wonach IT-Steuerung bzw. IT-Governance bei immer mehr IT innerhalb der Geschäftsprozesse vieler Unternehmen ebenfalls zunimmt, soll dieser Beitrag nicht nur begründen, sondern konkrete Ansätze liefern, um dem ebenfalls wachsenden IT-Integrationsproblem aus Sicht der unternehmerischen Investition zu begegnen. Einen Überblick vom Geschäftsmodell bis zur konkreten Anforderung des Fachbereichs an die IT verschafft Abbildung 10.10.

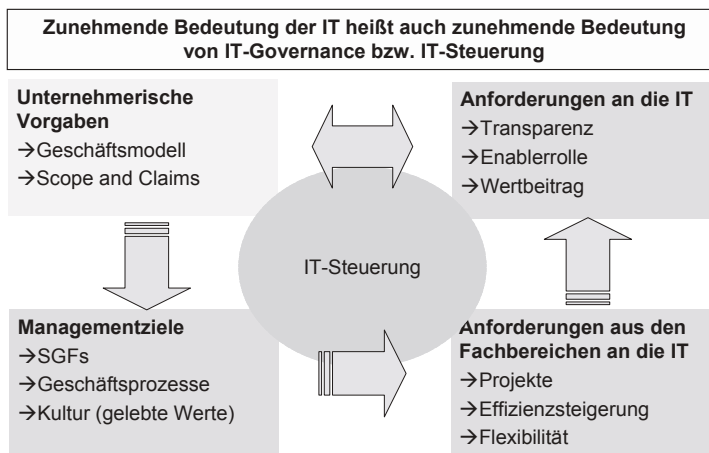


ABBILDUNG 10.10
Spannungsfeld der
IT-Steuerung

■ 10.4 Performance Management für IT-Governance

Neben der Definition von IT-Governance-Prozessen und -Strukturen ist auch die Einführung geeigneter Messgrößen von großer Bedeutung. Nur so kann sichergestellt werden, dass die angestrebten Ziele durch die IT-Governance ebenfalls erreichbar sind. Die Kontrolle der IT-Governance wird durch die Definition von Kennzahlen, so genannter Key Performance Indicators (KPIs), formalisiert. Mit ihrer Hilfe überprüft man, inwieweit die in der IT-Strategie festgelegten strategischen und operativen Ziele erreicht werden. Für die Definition von KPIs lassen sich einige Grundregeln festlegen:

- Die KPIs müssen eindeutig messbar und durch die verantwortlichen Strukturen, Prozesse und Personen beeinflussbar sein.
- Die Kontrollmechanismen müssen bekannt und allgemein akzeptiert sein.
- Die KPIs sollten nicht nur auf quantitative finanzielle Messgrößen beschränkt sein, sondern auch qualitative Kriterien und andere Bewertungsperspektiven in Betracht ziehen (vgl. Balanced Scorecard).
- Der Aufwand bei der Ermittlung von KPIs sollte immer in angemessener Relation zum Nutzen stehen.
- Eine Verbindung von KPIs mit Leistungsanreizen (z. B. Prämien) erhöht die Motivation zur Erreichung der Zielwerte.

Als Basis für einen IT-Governance Framework kann COBIT (Control Objectives for Information and related Technology) herangezogen werden, denn es deckt praktisch alle IT-Aktivitäten ab. Dabei handelt es sich um ein umfassendes Referenzmodell für IT-Governance, das eine Menge von Kontrollzielen für die Informatikprozesse definiert, die für die Auditierung von IT-Systemen verwendet werden können (vgl. hierzu ausführlich ITSM Library: IT-Governance, Das Taschenbuch basierend auf COBIT). Hier wird vor allem die Brücke von der rückwärts gerichteten Sicht der Prüfung zu der nach vorne gerichteten Gestaltung Service-orientierter Geschäftsprozesse geschlagen (zu COBIT siehe ausführlich auch Abschnitt 4.2.1).

COBIT unterstützt den Aufbau eines internen Kontroll- und Steuerungssystems im Sinne der IT-Governance durch:

- die Verbindung mit den Geschäftsanforderungen ([externe] Kundensicht);
- die Einbindung IT-bezogener Aktivitäten in ein allgemein akzeptiertes Prozessmodell;
- die Identifikation wesentlicher zu steuernder IT-Ressourcen;
- die Definition zu berücksichtigender Kontrollziele.

Der COBIT-Würfel hat sich als zweckmäßiger Ausgangspunkt für ein Assessment bewährt. Er erlaubt Aussagen zu den wesentlichen Dimensionen Steuerung (Control), Ressourcen und Prozessen.

Im Einzelnen ist festzuhalten: Der COBIT-Framework

- ist 1996 in der ersten Version entstanden und wird vom ISACA (Information Systems Audit and Control Association) herausgegeben;
- liegt aktuell in der Version 4.1 vor (die Ausgabe Version 5 hat 2011 als Veröffentlichungstermin), herausgegeben von der ISACA und dem IT Governance Institute (ITGI);

- stellt mittlerweile einen international anerkannten Standard für IT-Governance sowie für IT-Controlling (aus Außensicht) dar;
- unterscheidet vier Domänen (Planung & Organisation, Akquisition & Implementierung, Betrieb & Unterstützung, Monitoring & Evaluierung);
- identifiziert innerhalb dieser Domänen 34 kritische Prozesse;
- orientiert sich an Prozesszielen, sog. „High Level Control Objectives“ (318 Kontrollziele werden unterschieden).

Für jeden der 34 COBIT-Prozesse ist Folgendes festgelegt:

- Prozessbeschreibung
- Prozessziel (High-Level Control Objective)
- wesentliche Aktivitäten
- wesentliche Messgrößen
- 318 Kontrollziele
- Managementrichtlinien
- Reifegradmodell, das – angelehnt an CMMI (Capability Maturity Model Initiative) – die jeweiligen typischen Ausprägungen des Prozesses in sechs Reifegradstufen (0 bis 5) beschreibt.

COBIT ist sehr umfassend und deckt wie kein anderes Framework die Prozesse und Aktivitäten in der IT ab. Es eignet sich daher insbesondere zur Umsetzung einer IT-Governance, d. h. die optimale Unterordnung und den Einsatz der IT zur Unterstützung der Geschäftsanforderungen. Einen Überblick über das COBIT-Framework mit den vier wesentlichen Domänen sowie den 34 Prozessen sehen Sie in Abbildung 10.11.

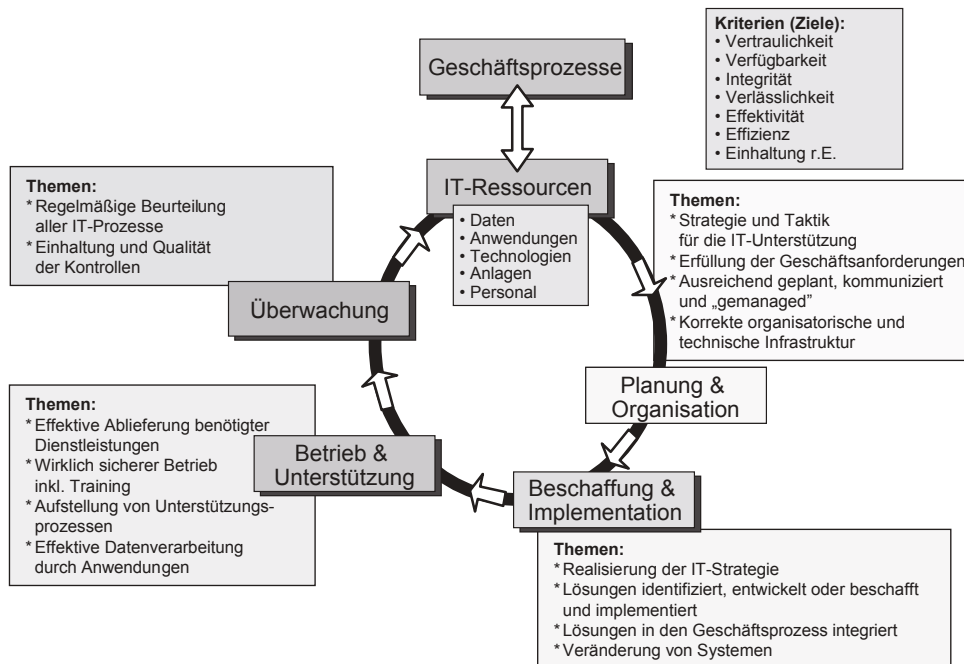


ABBILDUNG 10.11 COBIT-Framework im Überblick

Über Zieldefinitionen bzw. sog. „Critical Success Factors“ (CSF) und korrespondierende Messgrößen zur Zielerreichung – „Key Performance Indicators“ (KPI) – und andere Kennzahlen wird im Rahmen von IT-Governance-Konzepten dem Bedarf des Managements nach Kontrolle und Messbarkeit der IT Rechnung getragen. Pro CSF kann es mehrere KPIs geben; dabei geht es um finanzielle und nicht-finanzielle Ziele gleichermaßen. Beispielsweise können mittels KPIs ITIL-Prozesse innerhalb der IT-Serviceerbringung über das gesamte Prozessmodell hinweg überwacht und gesteuert werden. Auf diese Weise ist es möglich, die IT-Umgebung mit den von COBIT identifizierten IT-Prozessen zu vergleichen und sie zu beurteilen (vgl. www.isaca.org/cobit.htm).

Die Zielsetzungen, welche sich aus Maßnahmen (CSF) und jeweils korrespondierenden Messgrößen (KPI) im Rahmen geplanter Budgets ergeben, sollten jeweils die normative, strategische und operative Dimension betrachten, um in alle Unternehmensbereiche hinein kommunizierbar zu sein (vgl. [BiWi07]). Im Fokus stehen dabei nicht die Kosten, sondern die Zusammenhänge zwischen Zielen, Kosten und Ergebnissen – die **Performance**. Abschließend sei an dieser Stelle darauf hingewiesen, dass nicht genutzte Performance-Messungen und die insofern nicht stattgefundene Lernkurve auf diesem Gebiet bei der Beurteilung, ob bspw. „Outsourcing“ oder „Offshoring“ die besseren Alternativen sind, oft zu Fehlentscheidungen führen können. Eine konsequent durchgeführte und „gelebte“ IT-Governance kann helfen, Entscheidungen dieser Tragweite besser zu beurteilen und letztendlich das Potenzial des eigenen Unternehmens besser zu nutzen.

Im Prozessmodell von COBIT werden unterschiedliche Funktionen betrachtet. Hierzu werden in einem RACI-Chart folgende, überwiegend IT-bezogenen Funktionen einander gegenübergestellt:

- Chief Executive Officer (CEO)
- Chief Financial Officer (CFO)
- Business Executive
- Chief Information Officer (CIO)
- Geschäftsprozesseigner
- Leitung Betrieb
- Chief Architect
- Leitung Entwicklung
- Leitung Administration
- Projektbüro
- sowie Verantwortliche für Compliance, Audit, Risk und Security.

■ 10.5 Fazit

Unter Beachtung der in den vorhergehenden Abschnitten skizzierten Handlungsfelder dient die in Abbildung 10.12 dargestellte **Roadmap** als Orientierung, wenn eine ganzheitliche und umfassende Einführung von IT-Governance-Strukturen und -Prozessen im Unternehmen angestrebt wird.

Im Einzelnen sind in Abbildung 10.12 verschiedene Handlungsfelder skizziert, die sich mittels geeigneter Prozessbeschreibungen optimiert umsetzen lassen. Allerdings stehen diese Prozesse nicht isoliert da, sondern sind miteinander verknüpft und bedürfen einer Verankerung in geeigneten organisatorischen Strukturen.

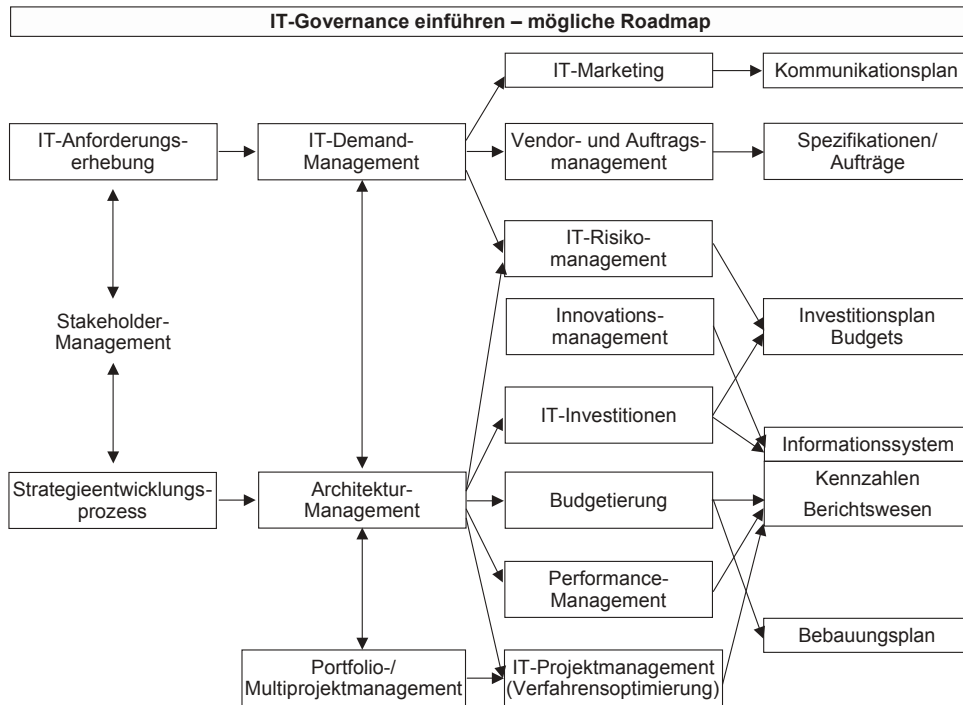


ABBILDUNG 10.12 Teilbereiche und Teilaktivitäten zur Einführung von IT-Governance-Strukturen

Bezüglich der Verankerung der Prozesse in der Unternehmensorganisation ist zunächst einmal eine Zuweisung von Rollen und Verantwortlichkeiten zu bestimmten Personen notwendig. Außerdem sind Entscheidungsgremien einzurichten, welche die notwendigen Entscheidungen treffen und deren Umsetzung im Sinne der Governance-Zielsetzungen sicherstellen.

Diese Gremien können sowohl auf der Angebots- als auch auf der Nachfrageseite aktiv werden und dazu Entscheidungen vorbereiten, treffen und umsetzen. So sind bezüglich der Angebotsseite Entscheidungen und Gremien notwendig, die sich mit der Überwachung externer IT-Dienstleister und der operativen Bereitstellung von IT-Produkten befassen. Entscheidungsgremien, die im strategischen Umfeld aktiv sind, müssen Überlegungen zur generellen Ausrichtung der IT-Organisation, zu Beschaffungsstrategien und IT-Investitionen großen Umfangs „anstellen“ und dazu entsprechende Aktivitäten anstoßen. Bezüglich der Nachfrageseite sind Gremien bzw. Rollen nötig (etwa IT-Koordinatoren), die auf der operativen Ebene die Anforderungen bzw. Wünsche der Fachbereiche bündeln bzw. harmonisieren, kleinere Investitionsentscheidungen treffen sowie Change Requests behandeln und „abwickeln“.

Welche Erwartungen werden an eine professionelle Governance gestellt? Der Nutzen, den eine gezielte und umfassende zentrale IT-Steuerung für die Praxis bietet, ist vielfältig, wie Abbildung 10.13 (nächste Seite) verdeutlicht.

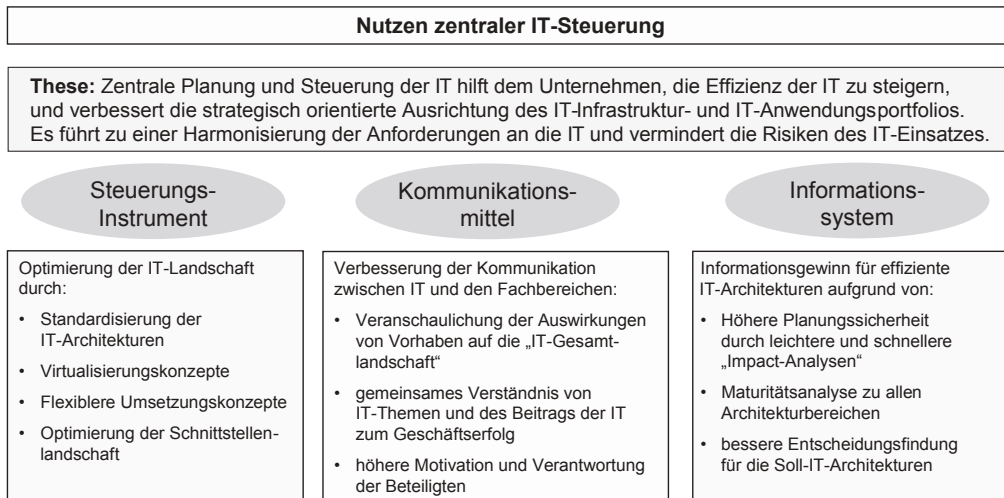


ABBILDUNG 10.13 Wesentliche Vorteile durch Einführung zentraler IT-Governance

Als Fazit kann festgehalten werden: In der Realität sind alle Unternehmen in immer stärkerem Ausmaß von einer funktionierenden IT abhängig. Sie ist der integrale Bestandteil vieler Geschäftsprozesse. Deswegen ist gerade für die Schnittstelle zwischen IT und Geschäft eine effektive Governance essenziell. Fehlt sie, kann dies in den meisten Unternehmen gravierende Folgen haben: Die Reihe der missglückten IT-Projekte setzt sich fort, und die gesamte Wertschöpfung sowie der nachhaltige Bestand eines Unternehmens leiden.



Das Wichtigste – zusammengefasst

- **Beachten Sie, dass eine zentrale Planung und Steuerung der IT-Aktivitäten für viele Organisationen eine immer höhere Bedeutung und Notwendigkeit erlangt!**

Business-IT-Alignment, zunehmende Risikosituationen sowie Compliance-Anforderungen machen die Zentralisierung von Steuerungsfunktionen für die Unternehmens-IT unverzichtbar.

- **Die Corporate Governance ist der wesentliche Treiber für die IT-Governance!**

IT-Governance und die dabei zu betrachtenden Standards und Vorgaben werden typischerweise aus der Corporate Governance des Unternehmens abgeleitet.

- **Stellen Sie sicher, dass durch die Anwendung der Prinzipien der IT-Governance eine Umsetzung der IT-Strategie im Sinne der Verantwortungsträger – also der Unternehmensführung – erfolgt!**

Das bedeutet, dass die IT-Strategie als möglichst integraler Bestandteil der Business-Strategie eines Unternehmens gesehen und entsprechend daraus abgeleitet werden sollte. Letztlich sollen damit die Chancen und Risiken der IT für das Unternehmen aktiv gemanaged werden.

▪ **Arbeiten Sie auf der Grundlage von zentral definierten Kernaufgabenfeldern für die IT-Governance!**

Ausgehend von einer unternehmensweiten IT-Strategieentwicklung sowie einem gezielten Anforderungsmanagement sind die Enterprise Architekturen zu planen und zu entwickeln sowie Maßnahmen der Risikosteuerung zu implementieren!

▪ **Ein unternehmensweites Anforderungs- und Architekturmanagement schafft wesentliche Voraussetzungen für einheitliche IT-Lösungen, die eine hohe Akzeptanz bei den Kunden gewährleisten sowie eine nachhaltige Unternehmenssicherung ermöglichen.**

▪ **Nutzen Sie als Unternehmensleitung die Chance, in Zeiten komplexer und wichtiger werdender IT-Systeme für Ihre Organisation effektive Strukturen zu schaffen, die auch die Kultur Ihres Unternehmens durch die neue Qualität der Zusammenarbeit positiv verändern werden.**

▪ **Ausgehend von den Grundsätzen der IT-Governance ist es wichtig, dass die Planung, Durchführung und Bewertung von IT-Investitionen nach einem klaren Verfahrenskonzept erfolgt.**

Auf diese Weise kann sichergestellt werden, dass ein sachgerechter und effizienter Einsatz der für IT-Zwecke zur Verfügung stehenden Mittel erfolgt.

▪ **COBIT (Control Objectives for Information and related Technology) kann als das herausragende Framework für IT-Governance vielfach nutzbringend herangezogen werden!**

Es deckt wie kein anderes Framework die Prozesse und Aktivitäten der IT ab, die für eine unternehmensweite IT-Steuerung wesentlich sind.

10.6 Literatur

- [BiWi07] *Bienert, P., Faulhaber, B.:* IT-Governance – Strategische Führung und Kontrolle von Informationssystemen als Teil der New Corporate Governance. Forte Advisors AG, 2007
- [BrWi07] *Brenner, W.; Witte, C.:* Erfolgsrezepte für CIOs. Was gute Informationsmanager ausmacht. Hanser, München 2007
- [Br05] *Brugger, R.:* Der IT Business Case. Springer, Berlin 2005
- [Bu05] *Buchta, D.; Eul, M.; Schulte-Croonenberg, H.:* Strategisches IT-Management. Wert steigern, Leistung steuern, Kosten senken. Gabler, Wiesbaden 2005
- [FrGl07] *Fröhlich, M., Glasner, K.:* IT Governance – Leitfaden für eine praxisgerechte Implementierung. Gabler, 2007
- [Ge02] *Gernert, Chr.; Ahrend, N.:* IT-Management: System statt Chaos. Ein praxisorientiertes Vorgehensmodell. Oldenbourg, München 2002
- [Go06] *Goltzsche, Wolfgang:* COBIT kompakt und verständlich. 2006
- [He07] *Hess, T.:* Vorlesungsskript Neue Medien II – SS 2007.
http://www.wim.bwl.uni-muenchen.de/lehrveranstaltungen/neuemedien2/ss07/vl1_2f.pdf am 23.12.08

- [ITGI08] ITGI 2, 2008. About IT Governance [online]. Verfügbar unter:
http://www.itgi.org/template_ITGI.cfm?Section=About_IT_Governance1&Template=/ContentManagement/HTMLDisplay.cfm&ContentID=19657 [Zugriff am 21.06.2008]
- [ISTM05] ITSM Pocket Library: IT Governance. Das Taschenbuch basierend auf COBIT. Van Haren Publishing, 2005
- [Jo07] *Joisten, C.*: IT Governance A new concept or an innovative development of Information Management. VDM Verlag Dr. Müller, 2007
- [Ke07] *Keller, W.*: IT-Unternehmensarchitektur – Von der Geschäftsstrategie zur optimalen IT-Unterstützung. dpunkt.verlag, 2007
- [KeMa08] *Keller, W., Masak, D.*: Was jeder CIO über IT-Alignment wissen sollte. IM Information management & Consulting, 23. Jahrgang 1/2008
- [Mi89] *Mintzberg, H.*: Mintzberg on Management. Inside our strange world of organizations. Free Press, 1989
- [Ni05] *Niemann, K.*: Von der Unternehmensarchitektur zur IT Governance – Bausteine für ein wirksames IT-Management. Vieweg, 2005
- [RüSG06] *Rüter, A., Schröder, J., Göldner, A.*: IT-Governance in der Praxis, Springer, 2006
- [Ti05a] *Tiemeyer, E.*: IT-Servicemanagement kompakt. Elsevier, Spektrum Akademischer Verlag, Heidelberg 2005
- [Ti05b] *Tiemeyer, E.*: IT-Controlling kompakt. Elsevier, Spektrum Akademischer Verlag, Heidelberg 2005
- [Ti07] *Tiemeyer, E.*: IT-Strategien entwickeln – IT-Architekturen planen. Rauscher Verlag, Haag i. OB 2007
- [WeRo04] *Weill, P., Ross, W.*: IT Governance How top performers manage IT decision rights for superior results, Harvard Business Scholl Press, 2004

Klaus Schmidt



Fragen, die in diesem Kapitel beantwortet werden:

- Inwiefern gewinnt das IT-Security-Management zunehmend an Bedeutung, und welche Herausforderungen stellen sich für das IT-Management?
- Wie lässt sich die Sicherheitsrelevanz der IT-Systeme bestimmen, und wie kann IT-Security als Erfolgsfaktor für das Unternehmen genutzt werden?
- Mit welchen Kriterien kann man die IT-Sicherheit bestimmen?
- Mit welchen Anforderungen wird ein hochwertiges IT-Security-Management konfrontiert, und wie stellt man deren Erfüllung fest?
- Welche Möglichkeiten gibt es zur Gestaltung der Sicherheitsorganisation?
- Welche Rollen sind bei der Implementierung von IT-Security-Management und den damit verbundenen Prozessen zu etablieren?
- Wie kann die Sicherheitssituation einer IT-Organisation reportet werden?
- Wie baut man eine Security Policy zweckmäßig auf, und welche Inhalte sollten im Rahmen entsprechend unterstützender Dokumente geführt werden?
- Welche gesetzlichen Vorgaben sind im Zusammenhang mit der IT-Sicherheit zu beachten?

Ein wichtiger Punkt innerhalb des IT-Managements ist die Gewährleistung eines sicheren IT-Betriebs. IT-Manager und ggf. vorhandene Security-Manager müssen Wege finden, das Management der IT-Security zu planen, zu organisieren und zu steuern. Das Kapitel „IT-Security-Management“ soll deshalb nicht nur Merkmale und Herausforderungen des Managements der IT-Security beschreiben, sondern auch Hilfestellungen bieten, diese Wege zu finden, geeignete Maßnahmen und Vorkehrungen zu treffen und dabei bewährte Instrumente und Techniken zu nutzen.

■ 11.1 Ausgangssituation und Bedeutung von IT-Security-Management

11.1.1 Problemlage

Es sind vielerlei Probleme, denen sich ein Unternehmen im IT-Bereich gegenüberstellt, wenn die Geschäftsprozesse konsequent IT-gestützt realisiert werden. Unter anderem sind dies:

- *Steigende Fehlermöglichkeiten und Fehleranfälligkeit*

IT-Systeme, Komponenten und Dienste werden immer umfangreicher und komplexer. Allein ein modernes ERP-System durchschaubar zu halten und zu managen, erfordert einen enormen Aufwand.

Immer neue Dienste, Features und Möglichkeiten erhöhen die Anfälligkeit für Fehler und Angriffe. Zudem werden die Release-Zyklen aufgrund gestiegener „time-to-market“-Anforderungen immer kürzer. Für detaillierte Produkttests bleibt keine Zeit, lieber arbeitet man reaktiv mit Patches.

- *Steigende Dynamik und Abhängigkeiten*

Die Abhängigkeit der Geschäftsprozesse von der IT nimmt immer mehr zu. Auch die Abhängigkeit zwischen den einzelnen Systemen, Komponenten und Diensten steigt stetig. Die Veränderungsgeschwindigkeit nimmt ebenfalls zu. Oft können da Kontroll- und Dokumentationsmechanismen nicht mithalten.

- *Zunehmende Öffnung nach außen*

Während früher die EDV-Systeme eines Unternehmens abgeschottet waren, verfügen moderne IT-Systeme über eine Vielzahl von Verbindungen zu anderen IT-Systemen, sowohl unternehmensintern als auch in globalen Netzwerken.

- *Erhöhtes Missbrauchspotenzial*

Betrüger, Hacker, Saboteure etc. stellen sich nur eine Frage: „Wie kann ich die Merkmale und das Verhalten eines IT-Systems für meine Zwecke missbrauchen?“ Bei umfangreichen und komplexen Architekturen mit ständigen Änderungen und neu implementierten Anwendungen und Diensten fällt ein Missbrauch natürlich leichter.

Angesichts solcher Probleme steigt mit der IT-Durchdringung des Unternehmens und der damit steigenden Bedeutung der IT insbesondere auch die Bedeutung der IT-Sicherheit.

11.1.1.1 Vielzahl von IT-Bedrohungen

Ständig suchen Hacker, Betrüger, Saboteure und andere Angreifer nach neuen Wegen, um IT-Systeme für ihre Zwecke zu missbrauchen. Ebenso regelmäßig tauchen neue Viren und Würmer auf, gefälschte E-Mails, Spionageprogramme (Trojaner) usw. Die weiter oben beschriebene größere Verwundbarkeit kommt den Angreifern da sehr gelegen.

Oft ist aber gar kein Angreifer nötig. Inkompatibilitäten, Leichtsinn, technische Schwächen und eine oft nicht mehr vollständig beherrschbare Komplexität erzeugen eine Vielzahl von Störungsmöglichkeiten sowohl auf der Ebene eines einzelnen IT-Systems als auch auf der der Gesamtarchitektur.

Tatsächlich sind die Unternehmen tagtäglich mit sicherheitsrelevanten Ereignissen und Schadensfällen konfrontiert. Die Bedrohungen sind hierbei vielfältig (siehe dazu Abschnitt „Entstehung von Risiken“ in Kapitel 12).

11.1.1.2 Kleiner Fehler – große Wirkung

Ein weiterer Punkt kommt hinzu: In einem komplexen System kann ein winziger Fehler gravierende Auswirkungen haben. Gerade beim Einsatz von Software in steuernden Systemen (z. B. zur Produktions-, Prozess- oder Ablaufsteuerung) haben viele Unternehmen diese Tatsache bereits schmerzlich erfahren müssen. Dazu ein *Beispiel* aus der europäischen Raumfahrt:

Im Programm des Trägheits-Navigationssystems der Ariane-5-Rakete wurde der vom Geschwindigkeitssensor gemeldete Wert für die Horizontalgeschwindigkeit der Rakete in eine Ganzzahl umgewandelt und einer Variablen zugeordnet:

```
horizontal_veloc_bias := integer(horizontal_veloc_sensor);
```

Beim Jungfernflug meldete der Sensor 37 Sekunden nach der Zündung einen Geschwindigkeitswert von 32768,311 – 16-Bit signed Integer reicht jedoch nur bis 32767 – das Programm versagte, die Rakete wurde gesprengt. Schaden: **1,6 Mrd. DM**.

Angesichts solcher Schadensfälle (von denen es eine Menge gibt) wird deutlich, wie wichtig die Sicherheit der IT für das Unternehmen bzw. Produkte des Unternehmens sein kann. Eine kleine Sicherheitslücke, ein kleiner Fehler – und schon kann ein unter Umständen existenzieller Schaden für das Unternehmen entstehen.

IT-Security ist zudem viel weniger greifbar als andere Sicherheitsbereiche. In der physischen Sicherheit ist ein Loch im Zaun oder ein offenes Fenster klar ersichtlich. Eine nicht abgefangene Eingaberoutine, die zu einem Pufferüberlauf und schließlich zum Programmabsturz führt, oder ein falsch gesetzter break-Befehl (Ursache für einen neunstündigen Ausfall des kompletten AT&T-Telefonnetzes in den USA im Januar 1990 – Schaden: 75 Mio. USD) – so etwas zu finden, ist viel schwieriger. Das Gefahrenpotenzial der Zuweisung im obigen Beispiel hat trotz strenger Qualitätskontrollen und Softwareprüfungen niemand bemerkt.

11.1.2 Ermittlung der Sicherheitsrelevanz

Die IT-Sicherheitsrelevanz betrachtet, wie schlimm es ist, wenn ein IT-System versagt bzw. zum Versagen gebracht wird, ein falsches Ergebnis liefert bzw. manipuliert wird oder Daten Unberechtigten zugänglich macht. Sie hängt von mehreren Faktoren ab:

- *Wo wird das IT-System eingesetzt?*

Es ist leicht nachvollziehbar, dass es schlimmer ist, wenn ein Rechner zum Stellen von Signalen und Weichen der Deutschen Bahn versagt, als wenn die Webseite einer Betriebskantine nicht aufgerufen werden kann. In der Praxis werden daher Schadenskategorien definiert (siehe dazu Abschnitt 12.4.5 „Risikofeststellung“ in Kapitel 12). Die Schadenskategorien werden u. a. genutzt, um Schutzbedarfsklassen zu definieren. Mit diesen Klassen wird festgelegt, wie wichtig der Aspekt Sicherheit für das jeweils betrachtete IT-Objekt (z. B. ein Server oder ein LAN-Switch) ist und wie gut daher der Schutz ausgeprägt sein muss.

- *Wie lange hält die Funktionsstörung an?*

Je länger ein IT-System ausfällt bzw. falsche Ergebnisse produziert, desto schlimmer ist in der Regel der resultierende Schaden.

- *Wie gut kann die Situation vor der Funktionsstörung wiederhergestellt werden?*
Dabei unterscheidet man zum einen die Machbarkeit (von „vollständig möglich“ bis „unmöglich“) und, falls die Machbarkeit nicht unmöglich ist, zum anderen die Schwierigkeit (von „einfach“ bis „extrem schwierig“).
- *Wie vertraulich sind die vom System gespeicherten oder verarbeiteten Informationen?*
In jedem Unternehmen gibt es Informationen, die gegen unberechtigte Kenntnisnahme geschützt werden müssen. Erfährt beispielsweise ein Konkurrent bei einer Ausschreibung meine Angebotskonditionen, kann er mich unterbieten. Daher wird in vielen Unternehmen bei Informationen angegeben, wie vertraulich sie zu behandeln sind. Oft finden sich folgende Vertraulichkeitsstufen:
 - *Streng vertraulich*
Die Informationen dürfen nur einzelnen, genau definierten Personen zugänglich gemacht werden.
 - *Vertraulich*
Die Informationen dürfen nur einem bestimmten Verteilerkreis zugänglich gemacht werden.
 - *Intern*
Die Informationen dürfen nur Personen des eigenen Unternehmens zugänglich gemacht werden.
 - *Öffentlich*
Die Informationen dürfen jedermann zugänglich gemacht werden.



Praxistipp:

Zur Ermittlung und Dokumentation der IT-Nutzung hat es sich als sinnvoll erwiesen, nicht von der IT auszugehen, sondern bei den Geschäftsprozessen zu beginnen und dort zu ermitteln, in welchen Prozessschritten welche IT-Anwendungen durch wen in welcher Weise genutzt werden. In einem zweiten Schritt kann man die zugrunde liegenden Applikationen bzw. die tragende IT-Infrastruktur (Server, Netzwerke usw.) ermitteln.

Die genannten Punkte verdeutlichen, dass ein wichtiger Teil des Managements der IT-Security darin besteht, folgende Fragen klären:

1. Wie stellt sich die IT-Situation dar?

Die IST-Situation der IT-Architektur muss vollständig und korrekt erkannt sein. So müssen Informationen dazu vorliegen, welche IT-Komponenten mit welchen anderen Komponenten wie zusammenarbeiten bzw. in Verbindung stehen. Alle Abhängigkeiten von IT-Komponenten untereinander müssen bekannt sein; es darf keine versteckten Abhängigkeiten geben. Dazu werden bestehende Dokumentationen gesichtet und die tatsächliche Situation durch Begehungen, Interviews, Tests o. Ä. erhoben. Hilfreich sind auch toolgestützte Beschreibungen (grafisch oder in Datenbanken) zu den IT-Komponenten (vgl. hierzu auch das Kapitel 3 „IT-Architekturen planen und managen“).

2. Auf welche Weise werden IT-Komponenten genutzt?

Es muss bekannt sein, in welchem Kontext die IT-Komponenten eingesetzt und wo (in wel-

chen Prozessen), durch wen und wie welche IT-Komponenten verwendet werden. Mit der Geschäftseinflussanalyse (Business-Impact-Analyse) steht hierfür eine Methodik zur Verfügung, die Kapitel 12 („IT-Risikomanagement“) näher beschreibt.

3. Welche Folgen hätten verschiedene Funktionsstörungen?

Es muss zumindest grob eingeschätzt werden, welche Auswirkungen sich ergeben, wenn eine bestimmte IT-Komponente ausfällt, falsche Ergebnisse liefert oder Daten Unberechtigten zugänglich macht.

11.1.3 IT-Security-Management als Erfolgsfaktor

IT-Security kann nicht an erfolgsorientierten Bereichen (z. B. Marketing) gemessen werden. Ein Unternehmen verkauft nicht unmittelbar mehr Produkte dadurch, dass es in IT-Security investiert. Doch genau wie ein Fußballtrainer keine Mannschaft mit ausschließlich 11 Stürmern aufstellt, sondern sein eigenes Tor durch eine gute Verteidigung schützt, ist die sichere Informationsverarbeitung in Unternehmen in vielen Fällen unerlässlich, um den Geschäftserfolg zu ermöglichen. Stabilität und Sicherheit sind somit zwei wichtige Erfolgsfaktoren für das Unternehmen, wie Abbildung 11.1 zeigt.

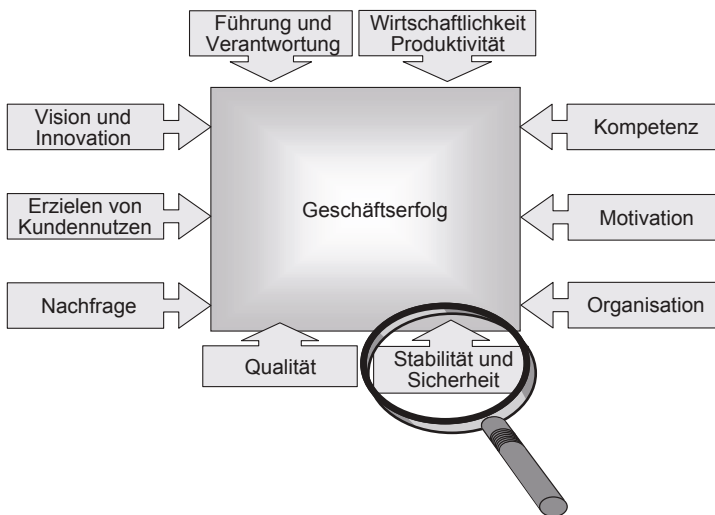


ABBILDUNG 11.1
Einige Erfolgsfaktoren
für ein Unternehmen

Das IT-Security-Management dient dabei mehreren Zwecken:

- **Schadensabwendung**

Primäres Ziel der IT-Security ist es, durch vorbeugende Maßnahmen Schadensereignisse in der Informationstechnik zu verhindern und das eigene Unternehmen, aber auch Kunden und Geschäftspartner vor Beeinträchtigungen und Verlusten zu schützen.

- **Schadensbegrenzung**

Nicht immer lassen sich Schadensereignisse verhindern. Für den Fall, dass es trotz aller Anstrengung zu einem IT-Ernstfall kommt, sorgen Konzepte wie Business Continuity oder Disaster Recovery dafür, dass der Schaden so gut es geht begrenzt wird.

- *IT-Security als Qualitätsmerkmal*

Mit diesem Punkt wird die geschäftliche Bedeutung der IT-Security zum Ausdruck gebracht. Die sichere Informationsverarbeitung kann für Kunden des Unternehmens ein wichtiges Qualitätsmerkmal darstellen, zu denken ist beispielsweise an das Online-Banking eines Geldinstituts.

- *IT-Security als Wettbewerbs- und Imagevorteil*

Die Existenz eines durchdachten IT-Security-Managements kann bei sonst vergleichbaren Leistungen einen Beitrag dazu liefern, dass das eigene Unternehmen gegenüber Wettbewerbern in einem besseren Licht erscheint. Es ist ein Zeichen von Professionalität und Seriosität.

11.1.4 Rechtlicher Rahmen für die IT-Security

Solange die Informationsverarbeitung eines Unternehmens eine interne Funktion ohne Außenwirkung darstellt, ist das Unternehmen frei in der Entscheidung, ob und inwieweit es sich um die IT-Security kümmern möchte. Für den Gesetzgeber gilt hier der Grundsatz der unternehmerischen Freiheit. Danach sollte der Staat nicht bestimmen wollen, wie ein Unternehmen zu arbeiten hat.

Doch diese Freiheit findet dort ihre Grenzen, wo ein Schutzinteresse von Dritten besteht. Stellt ein Kunde einem Unternehmen persönliche Informationen zur Verfügung, muss er sich darauf verlassen können, dass mit diesen Informationen verantwortungsvoll umgegangen wird. Investiert ein Kleinanleger Geld in eine Unternehmensaktie, muss er davon ausgehen können, dass sich das Unternehmen zumindest um existenzgefährdende Risiken kümmert.

Die einzelnen Staaten haben deshalb unterschiedliche Richtlinien und Vorgaben für eine verantwortungsvolle Unternehmensführung entwickelt, die oft aus konkreten Anlässen heraus (schuldhaftes Unternehmenszusammenbrüche, Bilanzskandale o. Ä.) formuliert wurden. Für diese Richtlinien hat sich der Begriff *Corporate Governance* eingebürgert (vgl. hierzu auch Kapitel 10 „IT-Governance“).¹

11.1.4.1 KonTraG (Deutschland)

Einige Fälle von überraschenden und schuldhaften Unternehmenszusammenbrüchen erschütterten im letzten Jahrzehnt die Wirtschaft in Deutschland und Europa. Die Vorstände hatten existenzbedrohende Risiken leichtfertig ignoriert, und die Aktionäre, die keinen Einblick in und keinen Einfluss auf die Arbeit des Vorstandes hatten, verloren ihr eingesetztes Kapital.

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) soll die Anteilseigner eines Unternehmens vor solchen Missständen schützen. Es ist ein Artikelgesetz², von dem eine Vielzahl von Wirtschaftsgesetzen betroffen sind (z. B. Aktiengesetz, Handelsgesetzbuch, GmbH-Gesetz oder die Wirtschaftsprüferordnung). Die wichtigste Forderung besteht in der Verpflichtung des Vorstands, ein Früherkennungssystem für bestandsgefährdende Risiken einzurichten:

¹ Der Begriff lässt sich im Unternehmen auf die verschiedenen Funktionsbereiche herunterbrechen. Bezogen auf die IT findet sich daher der Begriff *IT-Governance*.

² d. h. ein Gesetz, das andere Gesetze erweitert, ergänzt oder ändert.



§91 Abs. 2 AktG:

Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.

In der Praxis bedeutet diese Forderung, dass ein Risikomanagementsystem (RM-System) aufgebaut werden muss, das insbesondere bestandsgefährdende Risiken betrachtet (siehe hierzu Kapitel 12 „IT-Risikomanagement“).

Für die Existenz, Aktualität, Funktion und Kontrolle dieses Systems ist der Vorstand verantwortlich. Die Verantwortung kann nicht delegiert werden, die Umsetzung dagegen schon. Dies ist auch notwendig, weil der Vorstand in der Regel nicht über das erforderliche operative Wissen verfügt.

Das Gesetz definiert keine operativen Maßnahmen, jedoch wird im Zuge der Prüfung durch den Wirtschaftsprüfer kontrolliert, ob ein solches System eingerichtet wurde und ob es den Anforderungen genügt, die an ein solches System zu stellen sind. Folgende Punkte sind dabei wichtig:

1. *Nachweis der Existenz*

Es ist nachzuweisen, dass ein solches System im Unternehmen existiert. Der Vorstand ist verpflichtet, Informationen über den Aufbau des Systems zu geben und zu zeigen, dass das System geeignet ist, um die im Gesetz definierten Anforderungen zu erfüllen. Von der Eignung ist auszugehen, wenn:

- risikobehaftete Entwicklungen identifiziert, klassifiziert, bewertet und überwacht werden;
- auf der Grundlage der Risikobestimmung bei bestandsgefährdenden Risiken risikokontrollierende oder risikomindernde Maßnahmen ergriffen werden.

2. *Nachweis der Umsetzung*

Das System muss im Unternehmen verankert sein und darf nicht nur auf dem Papier existieren. Es müssen Verantwortlichkeiten und Aufgaben an Personen vergeben sein, die von diesen auch wahrgenommen werden.

3. *Nachweis der Nachvollziehbarkeit*

Die Aktionen und Informationen im System müssen so organisiert und abgelegt werden, dass sich die Funktion des Systems nachvollziehen lässt.

4. *Nachweis der Globalität*

Das System darf nicht auf einzelne Bereiche im Unternehmen beschränkt werden, sondern muss unternehmensweit Geltung besitzen. Die betroffenen Mitarbeiter müssen Kenntnis von der Existenz und Funktion des Systems haben.

Alle Forderungen von KonTraG können auf die IT heruntergebrochen werden. In diesem Fall werden nur Informationsrisiken betrachtet und ein IT-Risikomanagementsystem installiert.

Das KonTraG wurde in der Vergangenheit wenig ernst genommen. Ein Grund dafür ist, dass es bislang noch keine spektakulären Anklagen und Urteile gab. Das wird sich in den nächsten Jahren wohl ändern, denn auf europäischer Ebene bereitet man die stärkere Einforderung der nationalen Bestimmungen vor.

11.1.4.2 Sarbanes Oxley Act und COSO (USA)

Aufgrund einiger Bilanzskandale (z. B. Enron) sah sich auch die US-Regierung veranlasst, die gesetzlichen Bestimmungen für die Bilanzierung börsennotierter Unternehmen zu verschärfen. Insbesondere sollte die Korrektheit der in der Bilanz dargestellten Zahlen sichergestellt werden.

Der resultierende Gesetzesentwurf wurde nach den beiden maßgeblich beteiligten Personen, dem Senator Paul Sarbanes und dem Kongressabgeordneten Mike Oxley, benannt und erhielt die Bezeichnung „Sarbanes Oxley Act“ (kurz SOX oder SOA).

Das Gesetz gilt für alle an der New Yorker Börse notierten Unternehmen (also auch für deutsche Unternehmen, die dort gelistet sind). Die wichtigen Vorgaben des Gesetzes findet man in zwei Sektionen:

- **Sektion 302**

Hier werden der Vorstandsvorsitzende und der Finanzvorstand verpflichtet, persönliche Erklärungen über die Korrektheit der Finanzberichterstattung abzugeben und zu bescheinigen, dass die geforderten Kontrollen und Verfahren effektiv durchgeführt wurden. Der Vorstandsvorsitzende und der Finanzvorstand können für die Korrektheit in die persönliche Haftung genommen werden.

- **Sektion 404**

Hier wird gefordert, dass das Unternehmen interne Kontrollen im Unternehmen etablieren, durchführen und dokumentieren muss, die sicherstellen, dass nicht unbemerkt oder vorsätzlich falsche Angaben in der Finanzberichterstattung auftauchen. Betroffen sind also insbesondere alle bilanzwirksamen Prozesse. Da auch diese Prozesse IT-gestützt sind, müssen die erwähnten internen Kontrollen auch in der IT bzw. den IT-Prozessen eingeführt werden.

Um SOX-Konformität zu erreichen, kann der 1992 veröffentlichte amerikanische Corporate-Governance-Ansatz „Internal Control Integrated Framework“ verwendet werden (meist wird der Begriff „COSO-Framework“ benutzt, weil der Ansatz vom COSO-Komitee³ stammt). Er definiert fünf Kernkomponenten für die Corporate Governance:

- **Control environment,**
d. h. die Einrichtung eines internen Kontrollsystems (IKS);
- **Risk assessment,**
d. h. Identifizierung und Analyse von Risiken im Umfeld der Finanzberichterstattung;
- **Control activities,**
d. h. die Durchführung interner Kontrollen;
- **Information and communication,**
d. h. die Dokumentation und Bereitstellung aller wichtigen Informationen;
- **Monitoring,**
d. h. laufende Überwachung der Durchführung/Umsetzung des Frameworks.

Für die IT kann man das COSO-Framework auf den COBIT-Standard⁴ mappen. Dazu werden die COBIT-Anforderungen einer oder mehreren COSO-Kernkomponenten zugeordnet.

³ Siehe www.coso.org

⁴ IT-Auditierungsstandard der ISACA (siehe www.isaca.org)

11.1.4.3 Combined Code (Großbritannien)

In den 90er-Jahren entstanden in Großbritannien drei Corporate-Governance-Ansätze (Cadbury Code, Greenbury Report, Hampel Report). Ende der 90er Jahre wurden sie zum „Combined Code“ verschmolzen. Britische Unternehmen müssen bei Unternehmensprüfungen die Konformität zu diesem Kodex erklären oder begründen, warum sie ihn nicht umsetzen. Der Combined Code besteht aus zwei Teilen:

- *Principles of Good Governance*
Dieser eher allgemeine erste Teil beschreibt Grundsätze für eine hochwertige Unternehmensverfassung und -überwachung.
- *Code of Best Practice*
In diesem Teil werden die im ersten Teil beschriebenen Grundsätze weiter aufgeschlüsselt und mit Anforderungen hinterlegt.

Es werden fünf Bereiche behandelt. Die ersten vier betreffen das Unternehmen selbst, der fünfte betrifft die Aktionäre.

- Aufsichtsrat
- Entlohnung der Aufsichtsratsmitglieder
- Beziehung zwischen dem Unternehmen und den Aktionären
- Rechenschaftspflicht und Wirtschaftsprüfung
- Institutionelle Investoren

Beispiel:

[A] Mitglieder des Aufsichtsrats

[A.5] Ernennung/Berufung neuer Aufsichtsratsmitglieder

Grundsatz: Es sollte ein formales und transparentes Verfahren für die Ernennung/Berufung neuer Aufsichtsratsmitglieder geben.

[A.5.1] Anforderung: Es sollte ein Gremium gebildet werden, das dem Aufsichtsrat Vorschläge bezüglich der Ernennung/Berufung neuer Aufsichtsratsmitglieder unterbreitet. Die Mehrheit der Gremiums-Mitglieder sollte nicht der Leitungsebene des Unternehmens angehören.

11.1.4.4 EuroSOX (EU-weit)

Auch in Europa gab es Prüfungsskandale (z. B. Parmalat in Italien), die den Handlungsbedarf der europäischen Union aufzeigten. Die EU reagierte mit der EuroSOX-Richtlinie (8. EU-Richtlinie), die seit Juni 2006 in Kraft ist. Dabei ergab sich das Problem, dass sich die Ansätze für Corporate Governance in den einzelnen Mitgliedsstaaten erheblich voneinander unterscheiden.

Daher ist EuroSOX nicht so streng wie SOX und überlässt den einzelnen Staaten Regeln für die Ausgestaltung der Corporate Governance. Definiert werden das Ziel, nicht die Form und die Mittel. Allerdings zeigt sich auch bei EuroSOX, dass ein Schwerpunkt bei der Einrichtung und Durchführung interner Kontrollen liegt. Daher ist ein internes Kontrollsystem (IKS) zu etablieren, dessen Wirksamkeit überprüft wird.

Die Richtlinie definiert keine konkreten Maßnahmen für einzelne Bereiche wie die Informationstechnik. Die IT ist jedoch mittelbar vom IKS betroffen, so dass etwa interne Kontrollen in den IT-Prozessen notwendig sind.

Ein weiterer Kernpunkt ist die Unabhängigkeit externer Prüfer, die in der Vergangenheit immer wieder untergraben wurde, denn Wirtschaftsprüfungsunternehmen sind privatwirtschaftliche Unternehmen – Mandate bedeuten Umsatz. So kam es in der Vergangenheit öfter zu Gefälligkeits-Testaten. Um das Mandat nicht zu verlieren, wurden Unregelmäßigkeiten nicht beanstandet. Dieser Missstand soll durch die Stärkung der Unabhängigkeit der Wirtschaftsprüfer in Zukunft bekämpft werden.

11.1.4.5 Bundesdatenschutzgesetz (BDSG)

In Deutschland lässt sich aus den durch das deutsche Grundgesetz garantierten Grundrechten das Recht einer Person auf informationelle Selbstbestimmung ableiten. Im Vordergrund stehen dabei Informationen, die sich dieser Person und nur dieser Person zuordnen lassen und deshalb als personenbezogene Daten bezeichnet werden.

Personenbezogene Daten werden als besonders schützenswert eingestuft. Aus diesem Grund hat der Gesetzgeber mit dem Bundesdatenschutzgesetz im Dezember 1990 eine gesetzliche Grundlage für die Behandlung personenbezogener Daten geschaffen. Im Fokus des Gesetzes stehen die Erhebung, Speicherung, Veränderung, Nutzung, Übermittlung und Löschung personenbezogener Daten.

Besondere Bedeutung kommt der *speichernden Stelle* zu – Institutionen, die über die Daten verfügen. Die Verantwortung für den sachgerechten Umgang mit personenbezogenen Daten obliegt vor allem diesen Stellen. Dabei wird zwischen öffentlichen Stellen wie Behörden und nicht-öffentlichen Stellen wie privatwirtschaftlichen Unternehmen unterschieden.

Bei der Verarbeitung von personenbezogenen Daten ist als Erstes zu klären, welche Datenschutzbestimmungen zur Anwendung kommen. Das BDSG gilt:

- für Bundesbehörden, aber nicht für Landesbehörden. Für Landesbehörden gilt das jeweilige Landesdatenschutzgesetz;
- für speichernde Stellen in Deutschland, aber nicht für Stellen im EU-Ausland. Für ausländische Stellen im EU-Rechtsraum gilt das Datenschutzrecht des jeweiligen Landes (Herkunftslandprinzip);
- für den Fall, dass andere Schutzvorschriften für die Daten existieren (z. B. die anwaltliche Schweigepflicht) gleichrangig neben diesen Vorschriften;
- nicht für personenbezogene Daten, die für persönliche, private Zwecke gesammelt werden.

Als Nächstes ist zu prüfen, ob die Erhebung der Daten nach den anzuwendenden Rechtsvorschriften notwendig und zulässig ist. Nach dem BDSG ist sie zulässig, wenn die Daten für den Geschäftszweck unbedingt benötigt werden (z. B. zur Abrechnung von Leistungen). Es gilt hier der Grundsatz, dass so wenig personenbezogene Daten wie möglich erhoben und verarbeitet werden sollen.

Bei einer zulässigen Erhebung und Speicherung gilt es dann die Schutzbestimmungen einzuhalten. Dies sind vor allem:

- die Wahrung der Vertraulichkeit der Daten (z. B. durch Anonymisierung oder getrennte Speicherung der Schlüsseldaten⁵);

⁵ Daten, anhand derer sich erkennen lässt, um welche Person es sich handelt.

- die Wahrung der Rechte des Betroffenen (Benachrichtigung über die Speicherung, Auskunftserteilung auf Anfrage, Berichtigung falscher Daten, Sperrung/Löschung in bestimmten Fällen⁶);
- die Beschränkung der Speicherung und Nutzung auf die Dauer des Geschäftszwecks.

Das Gesetz sieht vor, dass Stellen, die regelmäßig personenbezogene Daten verarbeiten, Datenschutzbeauftragte bestellen, die die Einhaltung der Datenschutzbestimmungen sicherstellen sollen.

11.1.4.6 Weitere Gesetze

Neben den dargestellten Gesetzen existieren noch eine Vielzahl gesetzlicher Regelungen, die bestimmte Informationsverarbeitungsbereiche betreffen (z.B. GoBS⁷), für bestimmte Branchen gelten (z.B. KWG⁸), sich auf bestimmte Anwendungen beziehen (z.B. ITK-Gesetze wie TKG⁹ oder IuKDG¹⁰) usw. Im Einzelfall muss daher geprüft werden, welche gesetzlichen Vorgaben anzuwenden sind. Diese Prüfung sollte durch einen kompetenten Rechtsexperten erfolgen.

11.1.5 Anforderungen an ein hochwertiges IT-Security-Management

Vor allem für die dem IT-Security-Management übergeordneten Bereiche stellt sich die Frage, woran man ein hochwertiges IT-Security-Management erkennt. Worauf ist bei der Etablierung dieser Managementfunktion also zu achten, um von einem qualitativ hochwertigen IT-Security-Management sprechen zu können? Die folgenden Anforderungen bzw. Kriterien sollen bei der Beantwortung dieser Fragen helfen:

- **Anforderung:** Das IT-Security-Management sollte den für die IT geforderten bzw. von der IT benötigten Schutz gewährleisten.

Wie man die Erfüllung der Anforderung feststellt: Die Anforderung kann als erfüllt angesehen werden, wenn im Fall der Bottom-up-IT-Security die durch die Risikoanalyse festgestellten Sicherheitsbedürfnisse oder im Fall der Top-down-IT-Security die sich aus der Schutzbedarfsanalyse ergebenden und in der IT-Security-Policy definierten Anforderungen im Bereich der IT durch die IT-Security befriedigt werden.

Das IT-Security-Management sollte über ein kontinuierlich arbeitendes Kontrollsystem verfügen, mit dem geprüft werden kann, inwieweit der Schutzbedarf befriedigt ist.

- Im Fall der Bottom-up-IT-Security muss das jeweils benötigte Schutzprofil erstellt und mit den Ergebnissen von Risikoanalysen, Sicherheitstests, Incident-Logs¹¹ usw. verglichen werden.
- Im Fall der Top-down-IT-Security muss der Status jeder Anforderung verfolgt und dokumentiert werden. Der quantitative und qualitative Erfüllungsgrad gibt dann Auskunft über den Stand der Umsetzung.

⁶ Siehe §35 Abs. 2 BDSG.

⁷ Grundsätze ordnungsmäßiger Speicherbuchführung (betrifft Buchhaltungsdaten)

⁸ Gesetz über das Kreditwesen (betrifft die Bankenbranche)

⁹ Telekommunikationsgesetz

¹⁰ Informations- und Kommunikationsdienstegesetz

¹¹ Protokollierungen tatsächlich aufgetretener sicherheitsrelevanter Vorfälle

- **Anforderung:** Der für die IT und ihre Objekte vorzusehende Schutz sollte angemessen und passgenau sein.

Wie man die Erfüllung der Anforderung feststellt: Die Anforderung kann als erfüllt angesehen werden, wenn Schutzmaßnahmen und Sicherheitslösungen auf das jeweilige Umfeld, die jeweilige Architektur sowie die darin existierenden Objekte zugeschnitten und die Schutzkonzepte sowie darin geplanten Sicherheitslösungen und -maßnahmen richtig dimensioniert sind, d. h. der Bedeutung des zu schützenden Objekts und dem bestehenden Risikopotenzial entsprechen.

Es darf nicht mit Kanonen auf Spatzen geschossen werden, aber mit einer Fliegenklatsche einen Raubvogel erschlagen zu wollen, ist ebenso unangemessen. Ungenaue Lösungen können sich negativ auf die Kostensituation der IT-Security, den technischen Aufwand bei Änderungen oder die Mitarbeiterzufriedenheit auswirken.

Die Berücksichtigung der Passgenauigkeit und Angemessenheit sollten bereits im Vorgehens- und Verfahrensmodell für die Sicherheitskonzepte verankert werden. Dort sind Bewertungsmaßstäbe zu hinterlegen, an denen sich die Bewertung der Passgenauigkeit und Angemessenheit orientieren kann. In die Bewertung selbst fließen auch viele subjektive Einschätzungen ein, die in einem Diskussionsprozess bestätigt oder verworfen werden.

- **Anforderung:** Die IT-Security bzw. das IT-Security-Management sollte über die Merkmale Steuerbarkeit und Reportbarkeit verfügen.

Wie man die Erfüllung der Anforderung feststellt: Die Anforderung kann als erfüllt angesehen werden, wenn Informationen über die zu managenden Elemente wie Sicherheitslage, Kostensituation, Sicherheitsfortschritt usw. kompakt, verständlich, aussagekräftig und zeitnah berichtet werden können und die Informationen in den Reports geeignet sind, um auf ihrer Grundlage Entscheidungen zu treffen (Investitionen, technische und/oder organisatorische Maßnahmen etc.).

Damit werden die dem IT-Security-Management übergeordneten Bereiche in die Lage versetzt, steuernd im Bereich der IT-Security mitzuwirken, ohne auf die innere Gestaltung Einfluss zu nehmen. Auch für den IT-Security-Manager hat dies Vorteile: Er bekommt leichter die Rückendeckung, die er für die von ihm getroffenen Entscheidungen und Maßnahmen braucht. Ebenso ist der Brückenschlag zu den Fachabteilungen unkomplizierter, wenn die Leitungsebene die IT-Security-Situation kennt und versteht.

Es sollte in der Praxis stetig überprüft werden, ob das Reporting erreicht, was es soll, und wo es Probleme mit dem Reporting gibt. Jedes Unternehmen und jede Führungskraft hat schließlich eigene Vorstellungen, wie ein Reporting aussehen sollte. Die Reportingmethodik sollte daher im kontinuierlichen Verbesserungsprozess berücksichtigt werden.

- **Anforderung:** IT-Security sollte praktikabel gestaltet sein.

Wie man die Erfüllung der Anforderung feststellt: Die Anforderung kann als erfüllt angesehen werden, wenn sowohl die sicherheitstechnischen Schutzmaßnahmen als auch die Methodiken des IT-Security-Managements in ihrer Anwendung angemessen, effektiv, durchführbar und im Unternehmen akzeptiert sind.

Fehlende Praktikabilität lässt sich beispielsweise daran erkennen, dass bürokratische Hürden und umfangreiche Verwaltungen bestehen, die Flexibilität für ungewöhnliche Fälle nicht vorhanden ist, Pragmatismus fehlt, Sicherheitsmechanismen umgangen bzw. ausgetrickst werden oder es viele Beschwerden der Mitarbeiter über die Handhabung der IT-Security gibt.

- **Anforderung:** Die IT-Security sollte wirtschaftlich arbeiten.

Wie man die Erfüllung der Anforderung feststellt: Die Anforderung kann als erfüllt angesehen werden, wenn Schutzmaßnahmen nicht teurer sind als der zu erwartende Schaden, wenn keine unnötigen oder gar unwirksame Sicherheitslösungen geplant werden und das IT-Security-Management selbst auf aufgeblähte Organisationsstrukturen und bürokratische Vorgehensweisen verzichtet.

- **Anforderung:** Sicherheitsanforderungen sollten skalierbar und nachvollziehbar sein.

Wie man die Erfüllung der Anforderung feststellt: Die Anforderung kann als erfüllt angesehen werden, wenn Sicherheitsanforderungen auf verschiedenen Ebenen des Unternehmens anwendbar sind, die Anforderungen je nach Sicherheitsklasse in Umfang und Schärfe variieren können und klar erkennbar ist, welchen Beitrag sie in welcher Hinsicht an welcher Stelle für die IT-Security leisten.

- **Anforderung:** Das dem IT-Security-Management zugrunde liegende Sicherheitsmanagementmodell sollte ganzheitlich und schlüssig sein.

Wie man die Erfüllung der Anforderung feststellt: Die Anforderung kann als erfüllt angesehen werden, wenn:

- das Modell alle IT-Lebenszyklusphasen berücksichtigt und für die einzelnen Phasen individuelle Verfahren und Vorgehensmodelle vorsieht (z. B. projektbegleitende Risikoanalysen in der Planungsphase);
 - das Modell alle Bereiche im Unternehmen berücksichtigt, die von der IT-Security berührt werden, die Bereiche einheitlich behandelt und in das Reporting einbezogen werden, auch wenn diese Bereiche nicht in der Hoheit des IT-Security-Managements liegen;
 - das Modell alle benötigten Security-Management-Bausteine wie Security Policy, Business Impact-Analyse, Notfallmanagement usw. enthält;
 - im Modell ein kontinuierlicher Security-Management-Prozess existiert.
- **Anforderung:** Sicherheitslösungen sollten möglichst zukunftssicher gestaltet werden.

Wie man die Erfüllung der Anforderung feststellt: Die Anforderung kann als erfüllt angesehen werden, wenn bei der Planung von Sicherheitslösungen Aspekte wie Flexibilität, Anpassbarkeit, Erweiterbarkeit, Ersetzbarkeit, Kompatibilität, Migration und Investitionsschutz betrachtet, gefordert und aktiv unterstützt werden. Besonders im IT-Bereich, der durch immer kürzere Innovations- und Release-Zyklen gekennzeichnet ist, gewinnen diese Aspekte immer mehr an Bedeutung.

Die hier aufgeführten Anforderungen sollten bei der Gestaltung des IT-Security-Managements berücksichtigt werden, doch wird kein Anspruch auf Vollständigkeit erhoben. Die weiteren Ausführungen in diesem Kapitel stellen Ansätze vor, mit denen sich ein IT-Security-Management realisieren lässt, das den in diesem Abschnitt beschriebenen Anforderungen genügt.



Praxistipp:

Gründen Sie eine Arbeitsgruppe im Sinne eines Qualitätszirkels, um die Arbeit des IT-Security-Managements von Zeit zu Zeit anhand der gezeigten Anforderungen zu reflektieren, oder beziehen Sie das Security-Management in die Überwachung des Qualitätsmanagements mit ein.

■ 11.2 Sicherheitsorganisation für die IT-Security

Einer der ersten Schritte beim Aufbau eines IT-Security-Managements besteht darin, Verantwortlichkeiten, Zuständigkeiten und Rollen für das Thema IT-Security organisatorisch im Unternehmen zu verankern. Dabei gilt es zu bedenken, dass ein Unternehmen keine homogene Einheit ist, die sachlogisch und zweckrational funktioniert, sondern ein komplexes System von Interessen, Macht, Konsens und Konflikten, aus dem heraus das Handeln des Unternehmens entsteht. Diese Tatsache zeigt sich auch, wenn es darum geht, die Sicherheitsorganisation für die IT-Security zu gestalten.

Jede Möglichkeit zur Gestaltung der Sicherheitsorganisation (siehe Abschnitt 11.2.1) berührt Macht- und Interessensbereiche. Mit der Wahl der Rollen und der Ausstattung dieser Rollen mit Kompetenzen und Rechten im Unternehmen können Personen oder Bereiche gestärkt, aber auch Konflikte vorprogrammiert werden. Daher ist es sehr wichtig, dass man nicht nur das offizielle Organigramm kennt, sondern auch das inoffizielle Netzwerk dieser Interessen und der verliehenen oder geliehenen Macht, um sie zu verfolgen und durchzusetzen.

11.2.1 Möglichkeiten für die Einordnung in die Organisation

Es gibt für Unternehmen keine feste Vorgabe, wie das IT-Security-Management zu gestalten und wer im Unternehmen dafür verantwortlich ist. Weil das Unternehmen frei ist bei der organisatorischen Gestaltung, ergibt sich eine Fülle von Möglichkeiten für die Definition verantwortlicher, zuständiger und kontrollierender Abteilungen, Teams, Stellen und Rollen.

Bei der Aufbauorganisation eines Unternehmens gibt es zwei Hauptrichtungen: Die vertikale Organisation spiegelt die Disziplinargewalt wider, die horizontale Organisation enthält die für das Unternehmen benötigten Tätigkeitsbereiche, die sich entweder an *Funktionen* (z. B. Einkaufsabteilung) oder an *Objekten* (z. B. IT-Bereich) orientieren.

Für das IT-Security-Managements muss als Erstes entschieden werden, ob die Einordnung nach der Funktion (d. h. Management von Sicherheit) oder nach dem Objekt (der IT) im Vordergrund stehen soll. Diese Entscheidung beeinflusst maßgeblich den „organisatorischen Pfad“, der für das IT-Security-Management in Frage kommt, was für die Effektivität entscheidend sein kann. Es muss jedoch immer beachtet werden, wie das jeweilige Unternehmensgefüge arbeitet und welche Einordnung daher am günstigsten erscheint. Eine generell richtige oder falsche Einordnung gibt es nicht.

11.2.1.1 IT-Security-Management als Teilfunktion des IT-Managements

Als das Thema IT-Security für Unternehmen relevant wurde, stand zunächst die Technik im Vordergrund. Firewalls oder Virens Scanner mussten beschafft und implementiert werden. Aus diesem Grund waren die Personen, die sich um das Management der IT-Security kümmern sollten, schnell gefunden: die Mitarbeiter der IT-Abteilung. Nur sie verfügten über das entsprechende IT-Know-how.

Mit der Zeit wurde die Aufgabe des IT-Sicherheitsmanagements immer komplexer. Zunehmend stellte man fest, dass für diese Aufgabe nicht nur IT-Know-how erforderlich war, son-

dern vor allem Qualifikationen wie methodisches Wissen, Koordinationsvermögen oder analytische Fähigkeiten gefragt sind. Die direkte Zuordnung des IT-Security-Managements zum IT-Lebenszyklusmanagement entsprach immer weniger den Erfordernissen dieser Managementfunktion.

Viele Unternehmen lösten deshalb das IT-Security-Management aus dem IT-Betrieb und definierten eigene verantwortliche Rollen wie IT-Security-Manager oder IT-Sicherheitsbeauftragte (siehe auch Abschnitt 11.2.2). Die Frage ist, wo diese Rollen im Unternehmen organisatorisch zweckmäßigerweise verankert werden.

Eine Möglichkeit besteht darin, in einem Bereich „IT“, der in den meisten Unternehmen existiert, alle IT-relevanten Funktionen (IT-Planung, IT-Betrieb, IT-Security-Management) als Teilbereiche zu realisieren. In diesem Fall steht das Objekt (die IT) im Vordergrund.

Vorteile:

- Einfache, objektbezogene Investitionssteuerung und -kontrolle ist möglich.
- Ein Ansprechpartner für alle Belange in der IT.
- Kurze Wege und gute Abstimmung zwischen den IT-Funktionen.

Nachteile:

- Oft kein eigenes IT-Security-Budget, d.h. das IT-Security-Management konkurriert mit anderen IT-Funktionen um das IT-Budget.
- Das IT-Security-Management ist disziplinarisch der IT-Leitung unterstellt und wird von den Interessen der IT-Leitung beeinflusst (keine Unabhängigkeit).

Viele IT-Leiter bemühen sich um die Einordnung des IT-Security-Managements in den IT-Bereich, weil sie damit die IT-Security unter Kontrolle halten können. Müssen die Berichtswege in der Hierarchie eingehalten werden, kann der IT-Leiter beispielsweise Schwachstellen, die vom Security-Management entdeckt und gemeldet werden, zumindest eine Zeit lang unter der Decke halten. Eine geschickte Budgetsteuerung kann das Security-Management stärken oder schwächen.

11.2.1.2 IT-Security-Management als Teil der Corporate Security

Stellt man nicht das Objekt, sondern die Funktion (das Security-Management) in den Mittelpunkt, gibt es einen Bereich „Unternehmenssicherheit“, in dem alle sicherheitsrelevanten Bereiche des Unternehmens als Teilbereiche realisiert werden (Objektschutz, Personenschutz, Arbeitssicherheit, Produktionssicherheit, Informationssicherheit usw.).

IT-Security-Management ist demnach losgelöst von anderen IT-Managementfunktionen. In der Corporate Security wird die Unternehmenssicherheit als Ganzes analysiert und gesteuert. Es wird somit leichter, die Risiko- bzw. Sicherheitslage des Unternehmens zu ermitteln. Die IT-Security wird zu einem Teilbereich der Unternehmenssicherheit, also zu einer „Unternehmenssicherheit angewendet auf die IT“ und gewinnt dadurch eine andere Bedeutung im Unternehmen.

Vorteile:

- Die Sicherheitsbereiche arbeiten mit einheitlichen Methodiken: ganzheitliches Security-Reporting wird möglich.
- Andere IT-Security-Management-Attention in der Unternehmensführung.
- Unabhängigkeit von den IT-Funktionen.

Nachteile:

- Hoher Aufwand bei der Zusammenführung der Sicherheitsbereiche.
- Abnehmende Identifizierung der IT mit dem Thema IT-Security.

11.2.1.3 IT-Security-Management als Teil der Corporate Compliance

Mit wachsender Bedeutung von Gesetzen und Richtlinien wie KonTraG oder SOX kristallisiert sich ein neuer Tätigkeitsbereich heraus: Corporate Compliance. Auch in Deutschland wächst die Zahl der Unternehmen, die die Position des Chief Compliance Officers (CCO) einrichten.

Aufgabe dieses neuen Tätigkeitsbereichs ist die Sicherstellung der Konformität einzelner Bereiche im Unternehmen zu

- Corporate-Governance-Gesetzen und -Richtlinien;
- externen und internen Vorgaben und Standards;
- Unternehmenszielen und -strategien.

Der Bereich ist üblicherweise beim Top-Management angesiedelt und berichtet direkt dem Vorstand.

Auch die Corporate Compliance kann nach Objekt und Funktion im Unternehmen heruntergebrochen werden (siehe zu dem Thema Compliance ausführlich Kapitel 13 dieses Handbuchs). Steht das Objekt im Vordergrund, ergibt sich im Falle des Objekts IT der Tätigkeitsbereich *IT-Governance*. Steht dagegen die Funktion im Vordergrund, ergibt sich im Fall des Security-Managements der Tätigkeitsbereich *Security-Governance*.

Der Trend ist zu beobachten, dass viele Unternehmen das IT-Security-Management der IT-Governance zuordnen. Doch damit ist die Problematik der Abhängigkeit vom IT-Bereich nicht gelöst. Der andere Weg zur Security-Governance erscheint schwierig, da die einzelnen Sicherheitsbereiche historisch gewachsen sind und die Bereichsleiter oft bei einer Konsolidierung einen Machtverlust befürchten.

11.2.1.4 IT-Security-Management als losgelöste Funktion

Eine weitere Möglichkeit besteht darin, das IT-Security-Management als Stabstelle losgelöst von jeglicher Linie zu realisieren. Weil die anderen Security-Management-Bereiche vor ähnlichen Einordnungsproblemen stehen, kann es leicht passieren, dass plötzlich eine Fülle von Stabstellen existiert, die ihrerseits unkoordiniert einzelne Security-Aspekte managen und alle einer Stelle berichten möchten, die sich „möglichst weit oben“ befindet, um eine entsprechende Rückendeckung zu erhalten. Demgegenüber steht der Vorteil, dass die Unabhängigkeit gewährleistet ist und die Stelle flexibel mit verschiedenen Organisationslinien arbeiten kann. Konfliktpotenzial gibt es trotzdem, z. B. wenn darum gestritten wird, ob Finanzmittel aus dem Security-Projektbudget oder einem Budget aus der Linie zur Verfügung gestellt werden sollen.

11.2.2 Rollen im IT-Security-Management

Um das Thema IT-Security-Management im Unternehmen umzusetzen, werden verschiedene sicherheitsbezogene Rollen definiert. Jede Rolle deckt einen bestimmten Teilbereich des Themas IT-Security-Management ab. Damit können einzelne Aspekte delegiert werden. Außerdem erzielt man eine Arbeitsteilung.

11.2.2.1 IT-Risk-Manager

Die Aufgabe des IT-Risk-Managers liegt in der Erkennung, der Bewertung und dem Management von IT-Risiken im Unternehmen. Er führt Risikoanalysen durch, etabliert und betreibt die IT-Risikomanagement- und Risikofrüherkennungssysteme, erstellt den Risikolagebericht und berät die Unternehmensleitung bei Risikoentscheidungen mit Bezug zur Informationstechnik.

11.2.2.2 IT-Security-Manager, Chief Security Officer (CSO)

Der IT-Security-Manager bzw. CSO spielt die Hauptrolle, wenn es um das Thema IT-Security-Management geht. Er ist zentraler Ansprechpartner sowohl für die Unternehmensleitung als auch für den IT-Bereich und arbeitet eng mit dem IT-Risk-Manager zusammen. Mit Hilfe der Risikoehebungen des Risk-Managers erarbeitet er Schutzbedarfsfeststellungen und wirkt bei der Erstellung entsprechender Schutzkonzepte mit. Er definiert IT-Sicherheitsstandards und verankert sie im Unternehmen. Beim Thema IT-Security ist es sinnvoll, wenn der IT-Security-Manager fachvorgesetzt ist.

11.2.2.3 IT-Sicherheitsbeauftragter

Die IT-Sicherheitsbeauftragten bilden die Brücke zwischen dem IT-Risk-Manager/IT-Security-Manager auf der einen Seite und der IT in den einzelnen Unternehmensbereichen auf der anderen. Sie entwickeln mit dem IT-Security-Manager zusammen Schutzkonzepte für einzelne IT-Lösungen und setzen sie in Zusammenarbeit mit dem IT-Bereich um. Sie führen vor Ort Sicherheitsuntersuchungen und Audits durch, begleiten Notfallübungen und sind vor Ort Ansprechpartner für die Erfüllung der Sicherheitsstandards und für alle Fragen der IT-Security. Durch ihren engen Kontakt zur Praxis liefern sie dem IT-Security-Manager wertvolle Informationen.

11.2.2.4 IT-Sicherheitsadministrator

Diese Rolle ist für die Umsetzung von Maßnahmen im Bereich der IT-Security zuständig. Er implementiert in Zusammenarbeit mit dem IT-Bereich Sicherheitslösungen und gewährleistet den sicheren IT-Betrieb. Er kennt sich technisch sehr gut mit den eingesetzten Technologien aus und kennt deren sicherheitstechnische Schwachstellen. Warnzeichen und sicherheitsrelevante Vorfälle bekommt er vor Ort mit und meldet sie dem IT-Security-Manager oder einem IT-Sicherheitsbeauftragten. Darüber hinaus ist er Ansprechpartner für alle technischen Detailfragen der IT-Security.

11.2.2.5 Datenschutzbeauftragter

Die Rolle des Datenschutzbeauftragten ergibt sich vor allem aus der gesetzlichen Verpflichtung zur Bestellung eines Datenschutzbeauftragten.¹² Er ist zuständig für den Schutz personenbezogener Daten, prüft die Zulässigkeit der Erhebung, Speicherung, Nutzung und Übermittlung solcher Daten, überwacht den korrekten Umgang mit den Daten und die Wahrung der Rechte von Betroffenen.

¹² Wann ein Unternehmen zur Bestellung eines Datenschutzbeauftragten verpflichtet ist, wird in Deutschland beispielsweise im BDSG ausgeführt.

11.2.3 Organisationsmodelle

Organisationsmodelle führen die beschriebenen Rollen und die Einordnung der IT-Security zusammen und bilden diese im Organigramm ab bzw. vereinbaren dazu Organisations- und Prozessanweisungen. Hierfür gibt es viele Gestaltungsmöglichkeiten, die von der Struktur und Philosophie des Unternehmens, der generellen Organisationsstrategie und auch den Faktoren Macht und Interessen beeinflusst werden. Alle nachfolgend gezeigten Beispiele wurden real existierenden Unternehmen entnommen, vereinfacht und anonymisiert.

11.2.3.1 IT-Security-Organisationsmodell orientiert am Objekt IT

In Abbildung 11.2 ist die Struktur eines Organisationsmodells zu sehen, das in den IT-Bereich integriert ist. In diesem Modell ist der IT-Leiter sehr mächtig und hat eine Schlüsselposition inne. Zwar wurde der IT-Security-Manager ihm nicht direkt disziplinarisch unterstellt, er ist aber vom IT-Leiter abhängig und hat, zumindest aus Sicht der organisatorischen Einordnung, die schlechteren Karten.

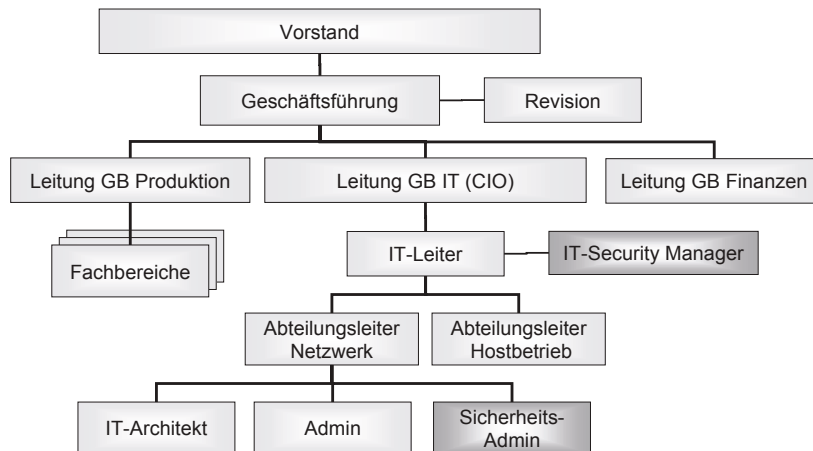


ABBILDUNG 11.2 Am Objekt orientiertes IT-Security-Organisationsmodell

Die ihm zuarbeitenden Sicherheitsadministratoren unterstehen ganz seiner Linie und stecken deshalb in einem Interessenskonflikt zwischen den Interessen des Abteilungsleiters und den Interessen des IT-Security-Managers. Der IT-Leiter kann den IT-Security-Manager austricksen, ausbluten lassen oder Druck über die Abteilungsleiter ausüben.

Selbst wenn sich die Unternehmensleitung zur IT-Security bekennt und dem IT-Security-Manager über Vorstandsbeschlüsse und Richtlinien die nötige Rückendeckung gibt, um die vorhandene Ungleichheit in der Machtverteilung auszugleichen, entsteht ein Konfliktpotenzial zwischen dem IT-Security-Manager und dem IT-Leiter. Dies führt mitunter zu einem Machtkampf, der nicht im Sinne des Unternehmens sein kann.

Als Vorteil dieser Variante gilt, dass der IT-Security-Manager fachlich eng mit dem IT-Leiter zusammenarbeitet und so kurze Wege existieren. Die Sicherheitsadministratoren sind als Linienposition voll in die IT eingebunden und haben dadurch einen besseren Einblick in IT-Projekte und den laufenden IT-Betrieb.

11.2.3.2 Organisationsmodell der geteilten IT-Security-Verantwortung

Abbildung 11.3 verdeutlicht die Variante, bei welcher der IT-Security-Manager unabhängig von der IT-Linie arbeitet. Der Weg zur Geschäftsführung ist kürzer als im ersten Beispiel, dadurch wird der Kontakt zur Geschäftsführung direkter. Der IT-Security-Manager berichtet daher direkt an die Geschäftsführung, die Berichte können nicht durch andere Stellen oder Positionen gefiltert oder geschönt werden.

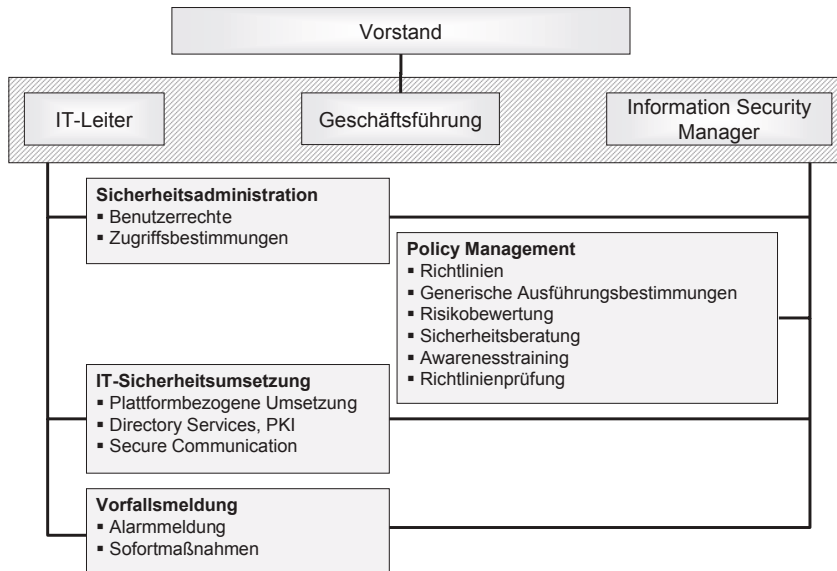


ABBILDUNG 11.3 Organisationsmodell der geteilten IT-Security-Verantwortung

IT-Leiter und IT-Security-Manager stehen auf der gleichen Höhe im Organigramm, was für ein ausgeglichenes Kräfteverhältnis spricht. Zwar sind immer noch Intrigen der einen oder anderen Seite möglich, aufgrund der direkten Anbindung der Geschäftsführung kann diese aber schnell intervenieren.

Sowohl der IT-Leiter als auch der IT-Security-Manager sind in die sicherheitsrelevanten IT-Themen eingebunden. Das kann beim IT-Security-Manager dazu führen, dass er leicht überfordert sein kann, wenn er nicht wie der IT-Leiter in der Lage ist, auf einen unterstützenden personellen Unterbau zurückzugreifen.

In diesem Modell entsteht das Konfliktpotenzial auf der Ebene der Themen: Wofür ist der IT-Bereich zuständig, wofür das Security-Management? Hier sollten sich beide Seiten nicht als Konkurrenz verstehen.

11.2.3.3 Verteilte Struktur für das IT-Security-Management

Ist das Unternehmen stark verteilt, kann eine Rolle allein die IT-Security im Gesamtunternehmen nicht mehr gewährleisten. Die Aufgaben müssen dezentralisiert werden. Eine diesbezügliche Möglichkeit zeigt Abbildung 11.4 (nächste Seite).

Auch hier findet sich die Position des IT-Security-Managers (in der Abbildung mit SM gekennzeichnet), allerdings besitzt er eine etwas andere Funktion. In den bisherigen Beispielen war

er der Dreh- und Angelpunkt für alle operativen Sicherheitsthemen. Nun bekommt er eine mehr koordinierende Funktion und ist nicht mehr in alle Themen eingebunden.

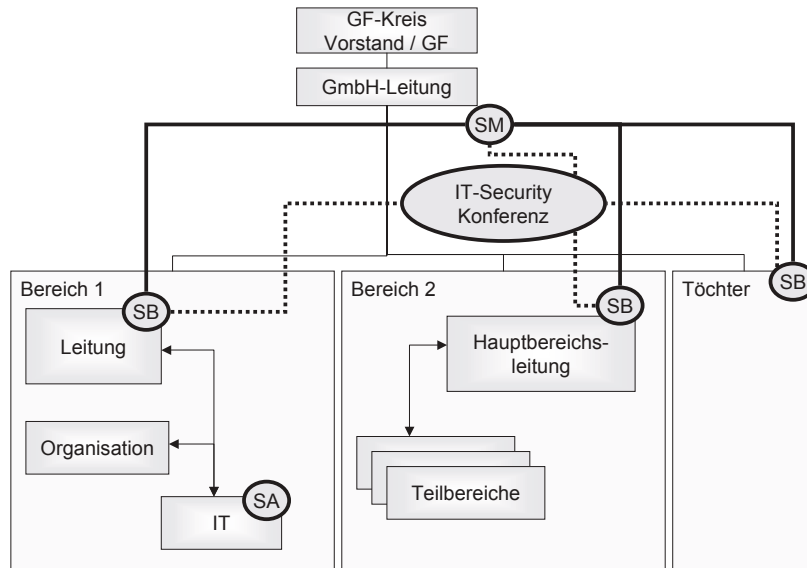


ABBILDUNG 11.4 Verteilte Struktur für das IT-Security-Management

Die Hauptakteure für die operativen Sicherheitsthemen sind nun die IT-Sicherheitsbeauftragten (in der Abbildung mit SB gekennzeichnet), die einerseits in ihrem Bereich an die Bereichsleitungen berichten, andererseits aber vom IT-Security-Manager koordiniert werden und ihn über die Sicherheitslage informieren. Nach innen verfügen die Beauftragten mit den IT-Sicherheitsadministratoren über unterstützende Personen für operative Tätigkeiten in der IT-Security.

Die Sicherheitslagen der Bereiche fließen beim IT-Security-Manager zusammen, der daraus den Gesamtlagebericht erstellt und an die Unternehmensleitung berichtet.

Alle IT-Sicherheitsbeauftragten und der IT-Security-Manager stimmen sich in regelmäßigen Meetings, Videokonferenzen o. Ä. („IT-Security-Konferenz“) ab und stellen in wichtigen Punkten die Einheitlichkeit (z. B. von Methodiken) sicher.

11.2.3.4 Gremienmodell für das IT-Security-Management

In diesem Modell wird die zentrale Figur des IT-Security-Managers durch ein oder mehrere Gremien ersetzt. Den IT-Security-Manager gibt es nach wie vor, er besitzt in diesem Modell aber weit weniger formale Macht.

Die eigentlichen Entscheidungen werden in den Gremien getroffen, wo sich Vertreter aller IT-Security-relevanten Bereiche befinden. Durch den gremienbasierten Aufbau des Security-Managements ist der Aufwand höher als bei den vorangegangenen Modellen. Das beginnt bei der Problematik, gemeinsame Termine zu finden, und zeigt sich auch an der Vielzahl von Interessen, die unter einen Hut gebracht werden müssen. Dies führt dazu, dass die Entscheidungsfindung mehr Zeit in Anspruch nimmt und oft Kompromisse in Kauf zu nehmen sind.

**Praxistipp:**

Richten Sie nur dann ein Gremium ein, wenn für Entscheidungen und Beschlüsse mehrere Verantwortliche beteiligt sein *müssen*. Überlegen Sie genau, wer in dem Gremium vertreten sein *muss*. Oft finden sich in der Praxis zu große Gremien, in denen wenige Wortführer den Ton angeben und andere nur ihre Zeit „absitzen“.

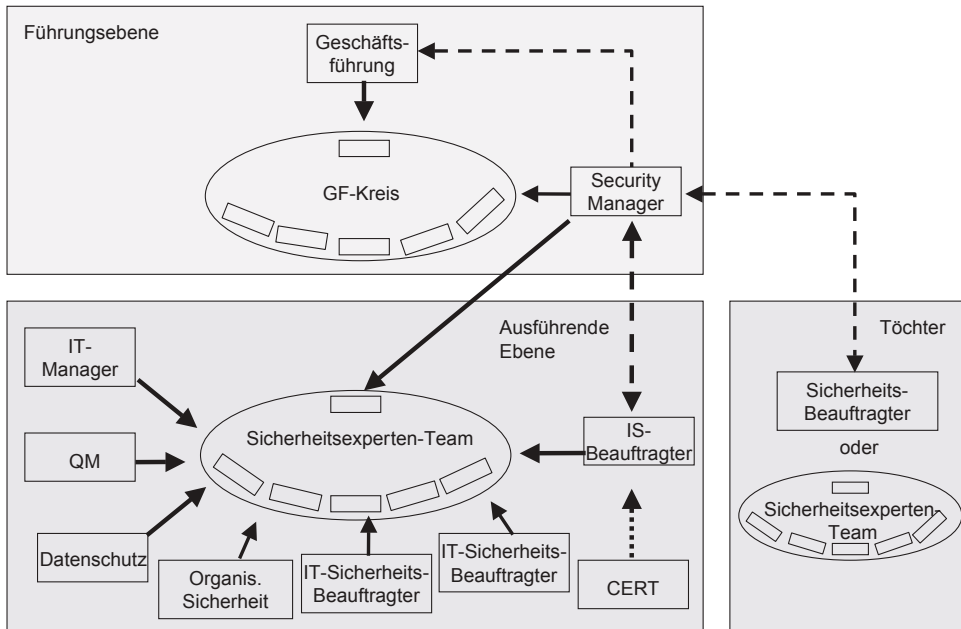


ABBILDUNG 11.5 Gremienmodell für das IT-Security-Management

11.2.4 Zusammenspiel mit anderen Sicherheitsbereichen

Die IT-Security ist einer von vielen Sicherheitsbereichen im Unternehmen. In der Vergangenheit entwickelten sich diese Bereiche unabhängig und isoliert voneinander und wurden nicht koordiniert. Diese Situation ist für das Unternehmen unbefriedigend, da es aufgrund verschiedener Strategien, Philosophien und Methodiken nicht leicht ist, Aussagen über die Gesamtsicherheitssituation des Unternehmens zu treffen.

Doch auch für die Sicherheitsbereiche im engeren Sinn ist dies nicht sinnvoll. Die IT-Security ist dafür ein gutes Beispiel. Die Sicherheit eines Servers hängt nicht nur von der IT ab (Hardware, Software, Netzwerk etc.), sondern beispielsweise auch von der Sicherheit des Gebäudes und des Raums, in dem sich der Server befindet. Für die Gebäudesicherheit ist aber ein anderer Sicherheitsbereich zuständig, z.B. das Facility Management.

Die IT-Security benötigt vom Facility Management in diesem Fall die Sicherheitslage des Gebäudes/Raums, im Gegenzug benötigt das Facility Management die Information, wie wich-

tig der Server für das Unternehmen ist, um die Sicherheitsmaßnahmen darauf abstimmen zu können. Ohne Einheitlichkeit bei Sicherheitsanforderungen und Metriken ist die Zusammenarbeit schwierig.

■ 11.3 Aufbau des IT-Security-Managements

Die ersten beiden Schritte zur Etablierung eines zweckmäßigen IT-Security-Managements wurden in den vorangegangenen Abschnitten erläutert und liegen hinter uns:

- Der Stellenwert sicherer Informationsverarbeitung und die Notwendigkeit für das Thema IT-Security wurden im Unternehmen erkannt.
- Eine für das Unternehmen passende Sicherheitsorganisation wurde definiert. Es ist festgelegt, wer (welche Rollen und Personen) sich um das Thema IT-Security kümmern soll und wie die Rollen/Personen organisatorisch in das Unternehmen eingebunden werden.

Nun geht es darum, das IT-Security-Management inhaltlich zu gestalten. Dieser Abschnitt soll die Frage beantworten, wie ein solches IT-Security-Management aufgebaut ist und in welche Teilaufgaben sich die Hauptaufgabe „Gewährleistung der benötigten IT-Security“ gliedert.

Grundsätzlich gibt es zwei Herangehensweisen an die Thematik des IT-Security-Managements:

- *Top-down-IT-Security-Management*

Die Top-down-Herangehensweise konzentriert sich auf den zu erreichenden Sollzustand für die IT-Security. In einem ersten Schritt wird zunächst dieser Sollzustand bzw. Zielzustand definiert. Für diese Definition können vordefinierte Sicherheitsstandards genutzt werden, was den Aufwand verringert. Ausgehend von diesem Sollzustand werden dann Maßnahmen umgesetzt und regelmäßig überprüft, wie nahe man dem Sollzustand gekommen ist.

- *Bottom-up-IT-Risk-Management*

Anders als bei der Top-down-Herangehensweise spielt der Sollzustand beim Bottom-up-Ansatz keine Rolle. Wichtig ist nur die jeweilige IST-Situation. Ausgehend von der IST-Situation werden die bestehenden Schwachstellen, Bedrohungen und Risiken ermittelt und aufgrund der Ergebnisse dann notwendige, risikomindernde Maßnahmen implementiert. So erreicht man einen neuen, sichereren IST-Zustand.



Praxistipp:

Arbeiten Sie sowohl top-down als auch bottom-up! Wenn Sie nur top-down arbeiten, fehlen Ihnen die Informationen über die bestehende Sicherheits- und Risikosituation. Arbeiten Sie hingegen nur bottom-up, *reagieren* Sie, statt proaktiv und zielgerichtet zu *agieren*.

Das Grundgerüst für das IT-Security-Management besteht in einem effektiven und effizienten Security-Managementsystem. Es besteht aus einer Vielzahl von Methodiken und Verfahren,

mit denen die benötigte Sicherheit gewährleistet wird. Die wichtigen Komponenten dieses Managementsystems sollen in den folgenden Abschnitten kurz dargestellt werden.

11.3.1 Sicherheitsrichtlinien

Das Fundament für das IT-Security-Management bilden Sicherheitsrichtlinien bzw. Security Policies. Diese Richtlinien oder Policies können sich auf bestimmte Unternehmensbereiche, bestimmte Technologien oder bestimmte Lebenszyklusphasen der IT beziehen. Es sollte eine unternehmensweite Basisrichtlinie existieren, die quasi als „Grundgesetz der IT-Security“ die Leitlinien der IT-Security enthält. Struktur und Inhalt einer solchen Richtlinie werden in Abschnitt 11.5.4 beschrieben.

11.3.2 Schutzbedarfsanalyse

Für die aufwandsoptimierte Realisierung der Informationssicherheit ist es elementar wichtig, erst einmal festzustellen, wie schutzbedürftig ein zu betrachtendes Objekt (Server, Gebäude, Prozess, IT-Verfahren etc.) ist. Dies wird in der Schutzbedarfsanalyse bzw. Schutzbedarfsfeststellung erhoben, für die es bislang kein einheitlich festgelegtes Vorgehen, sondern nur Best practices gibt, von denen eine Möglichkeit hier vorgestellt werden soll.

Die Schutzbedürftigkeit wird dabei in den einzelnen Sicherheitskriterien wie Verfügbarkeit, Vertraulichkeit usw. (siehe dazu Abschnitt 11.5.1) festgestellt.¹³ Jedem Kriterium werden relevante Schadenskategorien wie z. B. finanzielle Schäden (siehe dazu Abschnitt „Bestimmung der Schadenshöhe“ im Kapitel 12 „IT-Risikomanagement“) zugeordnet. Zur Abdeckung der Spannweite von „Kriterium ist überhaupt nicht gewährleistet“ bis „Kriterium ist vollständig gewährleistet“ werden in den einzelnen Schadenskategorien mehrere Schadensszenarien betrachtet.¹⁴

Diese Schritte sind vorbereitend nur einmal für alle Schutzbedarfsanalysen durchzuführen.

Beispiel:

Verfügbarkeit

- a) Gefahr für Leib und Leben
- b) Verstöße gegen Gesetze, Verträge etc.
- c) Finanzielle Auswirkungen
 - Gering (0 – 10.000 €)
 - Mittel (10.000 – 100.000 €)
 - Hoch (100.000 – 1 Mio. €)
 - Sehr hoch (> 1 Mio. €)
- d) Auswirkungen auf die Aufgabenerfüllung
- e) Imageschäden

¹³ Um Umfang und Aufwand in Grenzen zu halten, beschränken sich viele dieser Analysen auf die drei Kernkriterien Verfügbarkeit, Vertraulichkeit und Integrität.

¹⁴ In der Praxis findet man hierzu oft Metriken mit drei bis fünf Stufen.

In der konkreten Schutzbedarfsanalyse werden nun die Auswirkungen beurteilt, die sich ergeben, wenn das jeweilige Sicherheitskriterium nicht gewährleistet ist. Die Höhe der Auswirkungen kann, wie im Beispiel oben, in mehrere Klassen eingeteilt werden, es wird dann von Schutzbedarfskategorien oder -klassen gesprochen.

Beispiel:

Für den zentralen E-Mail-Server eines Unternehmens wird der Schutzbedarf hinsichtlich der Verfügbarkeit festgestellt. Es ergeben sich folgende Fragen:

- Wie groß ist die Gefahr für Leib und Leben bei Ausfall des E-Mail-Servers?
(z.B. Ausfall von Alarmierung-E-Mails für Produktionseinrichtungen)
- In welchem Ausmaß wird durch einen Ausfall gegen Gesetze verstoßen?
(z.B. gegen Aufbewahrungs- oder Bereitstellungsfristen)
- In welcher Höhe ergeben sich infolge eines Ausfalls monetäre Schäden?
(z.B. durch E-Mails, die aufgrund des Ausfalls nicht bearbeitet werden können)
- Inwiefern wird die Aufgabenerfüllung ver- oder behindert?
(z.B. Mitarbeiter, die aufgrund des Ausfalls nicht mehr arbeiten können)
- Wie sehr leidet das Image des Unternehmens?
(z.B. durch eine Pressemeldung, die die mangelnde Zuverlässigkeit des E-Mail-Dienstes des Unternehmen kritisiert)

Die Ergebnisse der einzelnen Schadensszenarien werden nach dem Maximumprinzip zusammengefasst, d.h. der höchste Wert wird der Gesamtwert für das Sicherheitskriterium.

11.3.3 Sicherheitskonzepte und Sicherheitslösungen

Auf der Grundlage der Risikoentscheidung entwickelt man nun Sicherheitskonzepte, d.h. es wird überlegt, auf welche Weise der sich ergebende Sicherheitsbedarf implementiert werden kann. Die Kombination aus technischen und/oder organisatorischen Maßnahmen, welche die benötigte Sicherheit realisiert, bezeichnet man als Sicherheitslösung.

11.3.4 IT-Security Reporting

Eine wichtige Aufgabe des IT-Security-Managements neben der Definition des SOLL-Zustandes und der Ermittlung der bestehenden Sicherheitssituation ist die Darstellung und das Reporting dieser Sicherheitssituation. Vor allem die Geschäftsleitung ist Adressat für das Reporting, da der Vorstand bzw. die Geschäftsleitung gesamtverantwortlich für die Informationssicherheit ist. Das Reporting sollte folgende Eigenschaften besitzen:

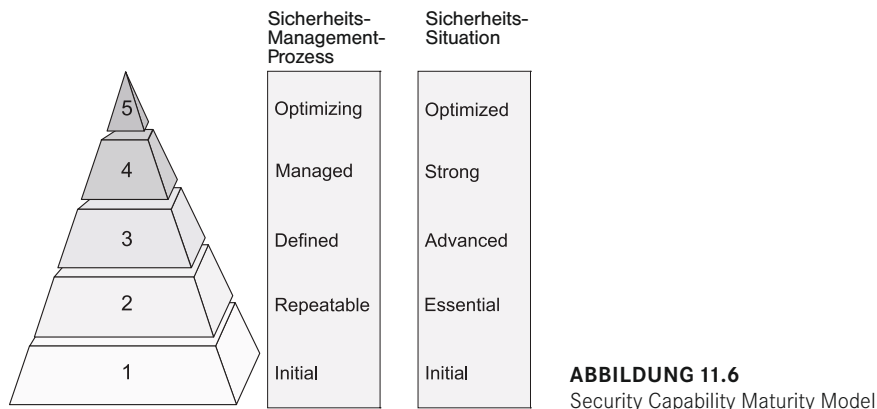
- Es sollte die Leitungsebene ausreichend über die Herausforderungen, Aufgaben und Aktivitäten der IT-Security informieren, ohne sie mit unwichtigen Details zu überfrachten.
- Es sollte eine Zusammenfassung geben, um die Sicherheitssituation möglichst „auf einen Blick“ darzustellen. Die Datengrundlage dieser Zusammenfassung sollte möglichst einfach nachgeschlagen werden können. In dieser Management Summary sollte der identifizierte Handlungsbedarf erkennbar sein.

- Die Form des Reportings sollte so gewählt sein, dass sie der Arbeitsweise und dem Kenntnisstand des Empfängers entspricht. So verbieten sich in einem Bericht an die Geschäftsleitung komplizierte technische Begriffe oder Zusammenhänge. Der Bericht muss in verständlicher Form abgefasst sein, d. h. verstanden werden können.
- Der Bericht sollte die Sicherheit nach gewünschten bzw. sinnvollen Gesichtspunkten gliedern (z. B. nach Sicherheitsbereichen, Sicherheitskriterien, Standorten, Kritikalität der Systeme o. Ä.).
- Der Bericht sollte geeignet sein, der Geschäftsleitung als objektives Steuerungsinstrument für die IT-Security zu dienen, d. h. er darf nicht zu sehr interessengeleitet sein und muss einen entscheidungsunterstützenden Charakter besitzen.

Das Unternehmen ist in der Gestaltung des Reportings völlig frei. Es haben sich in der Vergangenheit einige Arten von Reportingmöglichkeiten herauskristallisiert, die sich gut für ein solches Reporting eignen.

11.3.4.1 Security Capability Maturity Model

Das Security Capability Maturity Model (SCMM) ist die Anwendung des Capability Maturity Model (CMM), das aus dem Bereich der Softwareentwicklung stammt, auf die IT-Security. Es lässt sich sowohl auf die Reife der Sicherheitssituation als auch auf die Reife des Sicherheitsmanagementprozesses anwenden. In beiden Fällen existieren fünf Stufen, wie in Abbildung 11.6 zu sehen ist:



Bedeutung der fünf Stufen in Bezug auf die Reife des Sicherheitsmanagements:

- **Initial:** Unternehmen kümmert sich nicht um die IT-Security, Vorgehen im Bereich IT-Security ist chaotisch, nur intuitive Ad-hoc-Entscheidungen. Erfolge in der Informationssicherheit beruhen allein auf dem persönlichen Engagement einzelner Mitarbeiter.
- **Repeatable:** Es gibt Vorgehensmodelle für einzelne Aufgaben im Sicherheitsmanagement (z. B. für die Durchführung von Audits), die jedoch nicht unbedingt dokumentiert sein müssen. Erfahrungswerte werden weiter verwendet.
- **Defined:** Prozesse und Bausteine des IT-Security-Managements sind definiert, dokumentiert (und damit unabhängig von einzelnen Mitarbeitern) und werden im Unternehmen „gelebt“. Es sind Verantwortlichkeiten für die IT-Security benannt.

- *Managed*: Es existieren quantitative und qualitative Ziele für die IT-Security. Für die Ziele werden Messgrößen definiert und der Fortschritt gemessen und überwacht. Damit ist die Qualität der Informationssicherheit kontrollierbar.
- *Optimizing*: Es existiert ein kontinuierlicher Verbesserungsprozess, mit dessen Hilfe der Sicherheitsmanagementprozess weiterentwickelt und optimiert wird.

Bedeutung der fünf Stufen in Bezug auf die Höhe des Sicherheitsgrades der IST-Situation:

- *Initial*: Sicherheit ist in dieser Stufe Zufall, es ist keine geplante Sicherheit vorhanden. Organisierte Sicherheitslösungen sind weder im Einsatz noch geplant.
- *Essential*: Nur die nötigsten Sicherheitsvorkehrungen sind getroffen. Entweder sind dies Vorkehrungen, die selbstverständlich erscheinen (z.B.: Die Türen zu sensiblen Räumen sind verschlossen), oder sie sind unbedingt notwendig, um das Überleben des Unternehmens zu sichern.
- *Advanced*: In wichtigen Bereichen werden Sicherheitsmaßnahmen entsprechend dem Sicherheitsbedarf vorgesehen. Der Erfüllungsgrad der zugehörigen Sicherheitsanforderungen liegt in Stufe 3 bei unter 40%.
- *Strong*: Die Informationssicherheit wird flächendeckend angegangen. In allen Bereichen werden Sicherheitsmaßnahmen entsprechend dem Sicherheitsbedarf vorgesehen. Der Erfüllungsgrad der zugehörigen Sicherheitsanforderungen liegt zwischen 40% und 80%.
- *Optimized*: Die optimale Sicherheit ist erreicht. In allen Bereichen wurden entsprechend dem Sicherheitsbedarf und den Vorgaben der Security Policy Sicherheitsmaßnahmen umgesetzt. Die dafür definierten Anforderungen sind zu 80–100% erfüllt. Der Schutz berücksichtigt sowohl technische als auch organisatorische und rechtliche Aspekte. Die Sicherheitssituation wird von einem Sicherheitsmanagementprozess begleitet, der mindestens in die Stufe 4 einzuordnen ist.

Mit dem Erreichen der Stufe 5 ist die Arbeit nicht etwa abgeschlossen. Die Sicherheitssituation verändert sich durch neue Technologien, Architekturänderungen u. v. m. ständig, sodass es großer Anstrengungen bedarf, den hohen Reifegrad auch zu halten.

11.3.4.2 Grafische Darstellung der Sicherheitssituation

Um schnell – „auf einen Blick“ – zu erkennen, in welchen Bereichen die IT-Security stark ausgeprägt ist und wo sich Schwächen zeigen, eignen sich grafische Darstellungen. In Abbildung 11.7 werden die SCMM-Stufen auf sieben Sicherheitsbereiche (Physik, Netzwerke, Systeme, Anwendungen, Inhalte, Personen und Übergeordnetes) angewendet und als Spinnennetzdiagramm dargestellt. Während in diesem Beispiel die physikalische Sicherheit optimal ist, bestehen in der personellen Sicherheit starke Defizite.

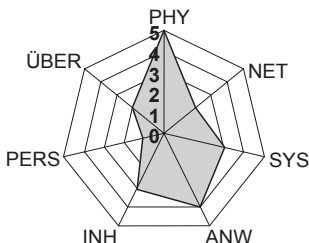


ABBILDUNG 11.7
Spinnennetzdiagramm
der IT-Security

Wendet man das SCMM nicht nur auf die Sicherheitsbereiche an, sondern betrachtet zusätzlich die drei Dimensionen technisch, organisatorisch und rechtlich, erhält man eine dreidimensionale Grafik (siehe Abbildung 11.8), die einer Landschaftskontur mit Hügeln und Tälern ähnelt und daher auch als Security Landscape bezeichnet wird.

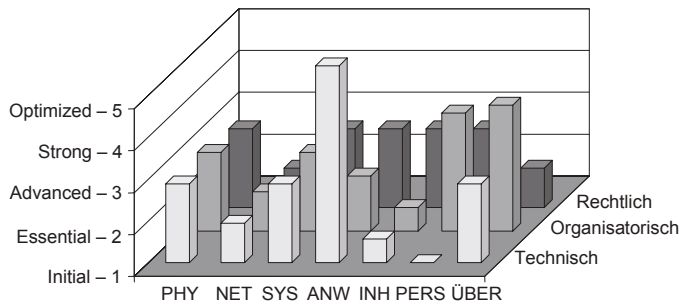


ABBILDUNG 11.8
Security Landscape

Die grafischen Darstellungen sind skalierbar. So kann es eine Security Landscape für das gesamte Unternehmen geben, für einen Standort oder ein bestimmtes Objekt (z. B. für einen Raum oder einen Server). Damit hat man ein leistungsfähiges Reportinginstrument, das sich zudem noch für weitere Zwecke, z. B. für die Investitionssteuerung, einsetzen lässt.

11.3.5 Information Security Circle

Der Information Security Circle bildet die Dynamik des Security-Managements ab. Basis ist ein 4-Phasen-Managementkreislauf mit den Phasen Identifikation, Konzeption, Umsetzung und Kontrolle, in den die Bausteine des Security-Managements integriert werden (Abbildung 11.9).

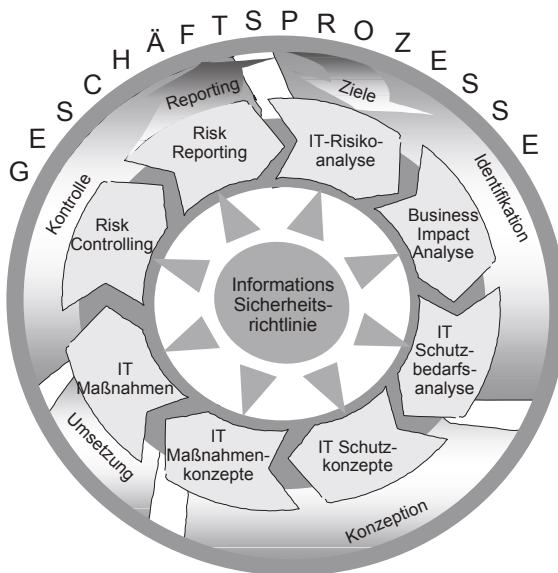


ABBILDUNG 11.9
Information Security Circle

Den Ausgangspunkt bildet dabei die Informationssicherheits-Richtlinie (Corporate Security Policy). Wichtig ist, dass die Schutzbedürfnisse als Ziele aus dem Geschäft kommen und die Ergebnisse des Kreislaufs über das Reporting wieder in das Geschäft (zur Leitungsebene) zurückfließen. Der Information Security Circle ist ein kontinuierlicher Kreislauf, der letztlich nie endet.

11.3.6 Notfallmanagement

Auch das beste Security-Management kann das Auftreten von Notfällen¹⁵ nicht vollständig verhindern. Tritt ein Notfall ein, geht es vor allem um Schadensbegrenzung. Bereits vor Auftreten des Notfalls wird innerhalb der Notfallvorsorge und Notfallplanung durchdacht, was in einem Notfall zu tun wäre. Diese Abläufe werden als Notfallkonzept dokumentiert und in angekündigten und unangekündigten Notfallübungen regelmäßig trainiert. Zentrales Instrument im Notfall ist das Notfallhandbuch, in dem wichtige Notfallmaßnahmen wie Alarmierungen, Sofortmaßnahmen und Vorgehensweisen zur Notfallbewältigung zu finden sind.

Im Notfall ändert sich die disziplinarische Hierarchie. Je nach Notfall geben unter Umständen externe Kräfte wie Polizei oder Feuerwehr den Ton an. Im Unternehmen übernimmt ein Krisenstab die Befehlsgewalt nach innen. Alle Anstrengungen richten sich nach der Rettung von Personen und der Sicherung des Notfallgebiets auf die Sicherung der Geschäftstätigkeit (Business Continuity) durch Weiterführung/Überbrückung der Geschäftsprozesse und ggf. Errichtung eines Notbetriebs, sowie auf die Wiederherstellung des Regelbetriebs (Disaster-Recovery, Business-Recovery, IT-Recovery). Mit der Feststellung des wiederhergestellten Regelbetriebs endet der Notfall.

■ 11.4 Einsatz von Sicherheitsstandards

Wie in anderen Managementbereichen haben sich auch für das IT-Sicherheitsmanagement bestimmte Vorgehensweisen herauskristallisiert, die ein effektives Management versprechen und in entsprechenden Standards formuliert wurden. Dabei zeigt sich, dass die einzelnen Standards für IT-Sicherheit zwar ein gemeinsames Grundverständnis besitzen, dennoch aber verschiedenen Philosophien folgen.

IT-Sicherheitsstandards lassen sich grob in 5 Gruppen einteilen:

1. Gesetze und Vorschriften mit Bezug auf die IT-Sicherheit (BDSG, KonTraG, SOX/Euro-SOX etc.)
2. Normen und technische Richtlinien für einzelne Sicherheitstechnologien (VDI/VDE-Normen, PCI-DSS, ISO 18033 etc.)

¹⁵ Hier verstanden als größere Schadensfälle.

3. Standards für Managementsysteme der Informationssicherheit (ISMS)
(ISO 27001, BSI-Grundschutz etc.)
4. IT-Standards, die den Aspekt IT-Sicherheit enthalten
(Cobit, ITIL etc.)
5. Standards zur Evaluierung von IT-Sicherheit
(Common Criteria, CMM etc.)

In diesem Kapitel soll aus Platzgründen nur auf wichtige Standards der Gruppe 3 – ISMS-Standards – eingegangen werden.

11.4.1 ISO/IEC 2700x (International)

Die von der International Standard Organization (ISO) herausgegebene Standardreihe 2700x umfasst die Einzelstandards:

- 27000: Information security management systems – Overview and vocabulary
Es werden in den Standards der Reihe 2700x verwendete Begrifflichkeiten erläutert.
- 27001: Information security management systems – Requirements
Spezifikation und Framework für ein ISMS. Es wird der Managementrahmen beschrieben, der für die Einführung und den Betrieb eines ISMS notwendig ist.
- 27002: Code of practice for information security management
Es wird ein generisches ISMS beschrieben, das 12 Bausteine umfasst. In jedem Baustein gibt es umzusetzende und zu prüfende Sicherheitsanforderungen (Controls).
- 27003: Information security management system implementation guidance
Darstellung der Projektschritte für die Definition und Einführung eines ISMS
- 27004: Information security management – Measurement
Es werden Kennzahlen dargestellt, mit denen die Effektivität eines ISMS gemessen werden kann.
- 27005: Information security risk management
Es wird beschrieben, wie ein generischer Risikomanagement-Prozess beschaffen ist. Risikomanagement wird hier nicht als eigenständige Unternehmensfunktion, sondern als Hilfsmittel zur Erzielung von Informationssicherheit aufgefasst.
- 27006: Requirements for bodies providing audit and certification of information security management systems.
Es werden formale Anforderungen für die Zertifizierung durch akkreditierte Unternehmen aufgelistet.

Weitere in diesem Zusammenhang zu erwähnende Standards sind ISO 27011 (für TK-Unternehmen), ISO 27031 (Business Continuity), ISO 27033-1 (Netzwerksicherheit) und ISO 27799 (ISM im Gesundheitswesen). Für die Praxis ist ISO 27002 der entscheidende Standard, für die Implementierung und Zertifizierung ist es ISO 27001.

11.4.2 IT-Grundschutz (Deutschland)

Die vom Bundesamt für Sicherheit in der Informationstechnik (BSI)¹⁶ herausgegebenen BSI-Standards definieren das Vorgehen für den Schutz von IT-Systemen mit maximal mittlerem Schutzbedarf (daher der Begriff Grundschutz). Bislang sind vier Standards definiert:

1. BSI-Standard 100-1: Managementsysteme für Informationssicherheit
Erweiterung des Grundschutzes, um kompatibel mit ISO 27001 zu sein.
2. BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
Schwerpunkt für die Anwendung/Realisierung des IT-Grundschutzes.
3. BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
Vorgehen für Systeme mit höherem Schutzbedarf.
4. BSI-Standard 100-4: Notfallmanagement

Die Grundlage für die operative Arbeit bilden die aus dem IT-Grundschutzhandbuch entstandenen drei IT-Grundschutzkataloge „BSI-Bausteine“, „Gefährdungen“ und „Maßnahmen“.

Für gebräuchliche IT-Objekte (z.B. Windows-Server oder Netzwerk-Switches) sind im gleichnamigen Katalog BSI-Bausteine definiert. Dort sind den IT-Objekten typische Gefährdungen zugeordnet sowie Sicherheitsmaßnahmen, um diesen Gefährdungen zu begegnen. Welche Maßnahme sich auf welche Gefährdung bezieht, lässt sich aus Kreuzreferenztabellen ablesen.

Die betrachtete Architektur¹⁷ (Infrastruktur, Netze, Systeme, Anwendungen usw.), im Grundschutz als IT-Verbund bezeichnet, wird Objekt für Objekt mit BSI-Bausteinen „nachgebaut“, was man als Modellierung bezeichnet. Gibt es für ein Objekt keinen BSI-Baustein, müssen die Gefährdungen und Maßnahmen „per Hand“ in einer eigenen Sicherheitsanalyse definiert werden. Ist der Schutzbedarf höher als „mittel“, ist eine Risikoanalyse durchzuführen. Hierfür liefert der BSI-Standard 100-3 die Methodik.

Schließlich wird überprüft, ob die für die vorhandenen Objekte aufgeführten Maßnahmen umgesetzt sind. Diese Prüfung wird als Basissicherheits-Check bezeichnet. Alle nicht umgesetzten Maßnahmen werden in einen Realisierungsplan aufgenommen und darin deren Umsetzung geplant.

11.4.3 Informationssicherheitshandbuch (Österreich)

Das vom Bundeskanzleramt in Kooperation mit dem Zentrum für sichere Informationstechnologie – Austria (A-SIT) – herausgegebene Informationssicherheitshandbuch versteht sich als konkrete Implementierungshilfe für die Realisierung der Informationssicherheit in Unternehmen und der öffentlichen Verwaltung.

Es gliedert sich in 15 Kapitel, in denen

- das ISMS als solches betrachtet wird;
- Bausteine des IS-Managements, wie die Informationssicherheits-Politik oder die Sicherheitsorganisation, behandelt werden;
- einzelne Methoden, wie die Klassifizierung von Informationen, beschrieben sind;

¹⁶ Das BSI ist eine nachgeordnete Behörde des Bundesministerium des Inneren (BMI).

¹⁷ z. B. eines IT-Verfahrens zur Unterstützung eines bestimmten Geschäftsprozesses

- verschiedene Sicherheitsbereiche, wie physische oder personelle Sicherheit, aufgeführt sind und
- einzelne, sicherheitsrelevante IT-Themen – wie E-Mail, Outsourcing oder E-Commerce – angesprochen werden.

Für jeden Abschnitt ist eine Referenz zur ISO-Reihe 2700x vermerkt, somit kann schnell festgestellt werden, welcher Teil der ISO-Standards dem Abschnitt entspricht.

Aufgrund der Breite der behandelten Themengebiete sind die einzelnen Themengebiete nicht vollständig dargestellt. Gefährdungen und Maßnahmen werden nur stichpunktartig erwähnt und nicht näher ausgeführt. Es ist daher eher ein guter Überblick als ein kompletter Standard.

11.4.4 Informatiksicherheit in der Bundesverwaltung (Schweiz)

Wie der Name schon erkennen lässt, ist die Informatiksicherheit stark auf die öffentliche Verwaltung ausgerichtet. Sie gliedert sich in fünf Ebenen.

Die grundlegendste Ebene bildet das IKT-Sicherheitsleitbild der Bundesverwaltung (2 Seiten), darauf aufbauend existiert die Bundesinformatikverordnung (BinfV) und die Informationsschutzverordnung (ISchV).

Allgemeine Ausführungen zur Informatiksicherheit finden sich auf der nächsten Ebene in den Weisungen des Informatikrates des Bundes (WIsB) und deren Anhänge. Hier finden sich Aussagen zu Zuständigkeiten, Sicherheitsverfahren (insbesondere wird auf ISO 27001 und IT-Grundschutz verwiesen) und die Netzwerksicherheit. Die letzte Ebene besteht in detaillierten Sicherheitskonzepten, auf deren Struktur oder Inhalt jedoch bewusst nicht näher eingegangen wird, so dass hier Freiraum in der Realisierung besteht.

■ 11.5 Sicherheit als Sollzustand vorgeben

Die Top-down-IT-Security definiert den SOLL-Zustand für die Sicherheit der IT. Sie gibt an, wie viel Sicherheit (kategorisiert durch Sicherheitsklassen) in welcher Hinsicht (gekennzeichnet durch Sicherheitskriterien und Themen) in welchen IT-Bereichen (angegeben durch Objektarten) gefordert wird. Dieser SOLL-Zustand wird mit Hilfe von Security Policies dokumentiert und richtet sich an einer vom IT-Security-Management mit dem Unternehmen abgestimmten Sicherheitsstrategie aus.

11.5.1 IT-Sicherheitskriterien

Der Begriff „Sicherheit“ beschreibt einen Zustand, der frei von Gefahren und Risiken ist, wobei es einen absolut risiko- bzw. gefahrenfreien Zustand nicht gibt. Sicherheit ist daher immer nur als ein relativer Zustand der Gefahrenfreiheit anzusehen. Für eine Aussage über die Sicherheit benötigt man drei Angaben:

- *Auf welches Objekt bezieht sich die Sicherheit?*
Ein Objekt kann eine Person sein, materielle (z. B. ein Server) oder immaterielle (z. B. Daten) Gegenstände, ein Zustand (z. B. Temperaturkonstanz) oder auch eine Handlung/ein Prozess (z. B. eine Datenübertragung).
- *Auf welche Situation bezieht sich die Sicherheit?*
Dieser Punkt beschreibt die situativen Rahmenbedingungen für das Objekt zum Zeitpunkt der Betrachtung der Sicherheit.
- *Sicherheit in welcher Hinsicht?*
Hier wird danach gefragt, nach welchem Aspekt die Sicherheit beurteilt wird.

Der letzte Punkt der Aufzählung führt zu den *Sicherheitskriterien*, anhand derer sich die Sicherheit eines Objekts beurteilen lässt. Diese Kriterien geben Auskunft darüber, welche Eigenschaften bei dem Objekt mit welcher Ausprägung erfüllt sein müssen, damit die Aussage gilt: „Das Objekt ist sicher.“ Anders ausgedrückt: Hier wird die Frage gestellt, woran sich die Sicherheit des Objekts festmachen lässt bzw. wie man sie feststellt.

Beispiel: Ein Geldschein kann sicher sein hinsichtlich seiner Echtheit, seiner Ursprünglichkeit (nicht wesentlich beschädigt, zerrissen o. Ä.) und seines Wertes. Das sind die drei maßgeblichen Sicherheitskriterien.

Die Frage nach solchen Sicherheitskriterien ist auch für die IT-Security sehr wichtig, denn die Aussage „Der Server ist nicht sicher“ ist zu global, um die Sicherheit beurteilen zu können, so dass sich sofort die Folgefrage stellt: „Nicht sicher in welcher Hinsicht?“



Praxistipp:

Beginnen Sie schon bei der Ermittlung der Sicherheitssituation damit, die IT-Sicherheitskriterien zu verwenden. Ordnen Sie Schwachstellen, Bedrohungen und Risiken (bottom-up) sowie Anforderungen und Ziele (top-down) den jeweiligen Sicherheitskriterien zu. Vergessen Sie die Kriterien nicht im Reporting!

Ähnlich wie beim Geldschein werden daher Eigenschaften für die IT definiert, an Hand derer sich die IT-Sicherheit beurteilen lässt. Diese Sicherheitskriterien werden dann verwendet, um eine passgenaue IT-Security gewährleisten zu können. Im Folgenden stellen wir die wichtigsten Kriterien kurz vor.

11.5.1.1 Verfügbarkeit

Die fundamentalste Forderung an die IT besteht darin, sich in einem Zustand zu befinden, in dem sie genutzt werden kann. Aus Sicht der IT-Security spricht man in diesem Fall davon, dass die IT „verfügbar“ ist. Die Verfügbarkeit eines IT-Systems ist die Wahrscheinlichkeit, dieses IT-System zu einem bestimmten Zeitpunkt in einem funktionstüchtigen Zustand anzutreffen. Die Verfügbarkeit wird als Prozentwert angegeben. 0% bedeutet, dass das IT-System nie funktioniert, bei 100% (theoretischer Wert) würde das IT-System nie ausfallen. In Tabelle 11.1 sind einige Verfügbarkeitswerte und die sich ergebenden Ausfallzeiten dargestellt.

TABELLE 11.1 Verfügbarkeiten und Ausfallzeiten

Verfügbarkeit ¹⁸	Ausfallzeit pro Jahr
90%	36,5 Tage
95%	18,25 Tage
99%	3,65 Tage
99,9%	8,76 Stunden
99,99%	52,56 Minuten
99,999% ¹⁹	5,26 Minuten

In der IT werden hoch anmutende prozentuale Verfügbarkeiten gefordert, die meist über 99% liegen. In Tabelle 11.1 wurden die Verfügbarkeitswerte in Ausfallzeiten umgerechnet. Man sieht, dass 99% für einen IT-Dienst doch eine relativ große Ausfallzeit bedeutet.

11.5.1.2 Vertraulichkeit

In einem Unternehmen existieren viele Informationen, die nur einem bestimmten Personenkreis zugänglich sein dürfen und als vertraulich einzustufen sind. Geraten solche Informationen in die falschen Hände (z. B. Entwicklungs- oder Angebotsinformationen), kann daraus für das Unternehmen ein großer Schaden entstehen. Daher ist die Wahrung der Vertraulichkeit solcher Informationen für die Sicherheit des Unternehmens ein wichtiges Kriterium.

Die Vertraulichkeit ist ein Maß dafür, wie vertraulich eine Information zu behandeln ist. Für die IT-Security bestimmt die Höhe der Vertraulichkeit Umfang und Strenge der Sicherheitsmaßnahmen, die zum Schutz der Objekte vor einem Vertraulichkeitsverlust ergriffen werden.

Die Vertraulichkeit wird mit Hilfe von Vertraulichkeitsstufen angegeben. Üblich sind Stufen wie „gering – mittel – hoch – sehr hoch“ oder „öffentlich – intern – vertraulich – streng vertraulich“.

11.5.1.3 Integrität/Ursprünglichkeit

Für die IT-Security ist es wichtig, dass Unbefugte nicht unbemerkt Informationen verändern können, da sonst mitunter ein großer Schaden droht. Man stelle sich eine Bank vor, bei der die Kurswerte des Online-Wertpapierhandels unbemerkt manipuliert werden können.

Man bezeichnet eine Information als integer, solange sie ihren ursprünglichen Inhalt besitzt und nicht unbefugt verändert wurde; in diesem Fall ist die Integrität WAHR. Ergibt eine Integritätsprüfung, dass die Information unbefugt verändert wurde, ist die Integrität FALSCH. Für jede kritische Information sollte die Möglichkeit der Integritätsprüfung bestehen.

11.5.1.4 Authentizität

Ähnlich wie die Manipulation von Daten, kann es auch verheerend sein, wenn es gelingt, eine Information „unterzuschieben“, z. B. bei einer E-Mail-Nachricht einen bestimmten Absender vorzutäuschen.

¹⁸ Kontinuierlich arbeitender IT-Dienst ohne Wartungszeiten, Werte gerundet.

¹⁹ Dieser Wert wird auch als „Five Nines“ bezeichnet.

Die Authentizität ist ein Maß dafür, ob man sich darauf verlassen kann, dass eine Information tatsächlich von demjenigen stammt, der als Urheber der Information angegeben ist. Technisch kann die Authentizität mit einer digitalen Signatur überprüfbar gemacht werden. Dazu entnimmt der Urheber Fragmente der Information und verschlüsselt („unterschreibt“ bzw. „signiert“) den daraus entstehenden Datenauszug (Hash) mit dem geheimen Schlüssel eines asymmetrischen Verschlüsselungsverfahrens. Da er dazu den geheimen Schlüssel benutzt, kann die Information nur von ihm signiert worden sein. Die Signatur kann mit dem zugehörigen öffentlichen Schlüssel geprüft werden.

11.5.1.5 Nachvollziehbarkeit

Mit der Nachvollziehbarkeit kann verfolgt werden, welche Aktionen mit einer Information oder Nachricht durchgeführt wurden und ggf. wer diese Aktionen durchgeführt hat. Dies ist besonders für die IT-Forensik und die IT-Revision von Bedeutung.

Die Nachvollziehbarkeit wird wie die Vertraulichkeit mittels der Stufen „gering – mittel – hoch – sehr hoch“ angegeben.

11.5.1.6 Konformität

Die Konformität ist ein Maß für die Übereinstimmung mit einem definierten Vergleichsgegenstand. Beispiel: Ein Unternehmen kann konform zu einem Sicherheitsstandard arbeiten, ein Netzwerk kann konform zur strukturierten Verkabelung aufgebaut sein, ein Administrator kann konform zu den Anforderungen für technisches Personal tätig sein.

Im Hinblick auf die Informationssicherheit spielt die Konformität zu Sicherheitsstandards die größte Rolle. Einige Sicherheitsstandards bieten die Möglichkeit der Zertifizierung, um die Konformität des Unternehmens mit dem jeweiligen Standard nachzuweisen.

Für die Darstellung der Konformität wird meist eine Prozentangabe gewählt, die Verwendung von Stufen ist ebenfalls möglich.

11.5.1.7 Verbindlichkeit

Die Verbindlichkeit bzw. Nicht-Abstreitbarkeit ist ein Beispiel für ein Sicherheitskriterium, das sich aus zwei anderen zusammensetzt. Ein solches Kriterium wird auch als „kombiniertes Sicherheitskriterium“ bezeichnet.

Die Verbindlichkeit setzt sich aus den beiden Kriterien Authentizität und Integrität zusammen. Beispiel: Wenn feststeht (z. B. durch eine digitale Signatur), dass ich der Absender einer Bestellung per E-Mail bin, und wenn weiterhin feststeht, dass diese E-Mail auf ihrem Weg vom Absender zum Empfänger nicht verändert wurde (ebenfalls durch digitale Signatur), dann kann ich nicht bestreiten, die Bestellung in der Form aufgegeben zu haben, wie sie beim Empfänger eingetroffen ist.

Da es auch hier um eine Prüfung geht, wird das Ergebnis als Wahrheitswert dargestellt.

11.5.2 Sicherheitsgrad und Sicherheitsklassen

Um eine Situation hinsichtlich der Sicherheit einschätzen zu können, bedarf es einer Maßgröße, die die Höhe der Sicherheit angibt. Dabei spannen sich zwei Extreme auf: *Sehr gefährlich* bzw. *sehr risikoreich* (0% Sicherheit) auf der einen Seite, *sehr sicher* (100% Sicherheit) auf der anderen.²⁰ Der Sicherheitsgrad trifft mit einem Wert zwischen 0% und 100% eine Aussage bezüglich der Höhe der Sicherheit. Dies kann die vorhandene Sicherheit (IST-Zustand) oder auch die geplante Sicherheit (SOLL-Zustand) sein. Hierbei gelten wieder die drei Angaben aus Abschnitt 11.5.1 zu Objekt, Situation und betrachtetem Aspekt.

Mit dem reinen prozentualen Zahlenwert zu arbeiten, ist in der Praxis nicht sehr sinnvoll. Daher wird diese recht feine Unterteilung oft in gröbere Stufen eingeteilt. Im Bereich zwischen 0% und 100% finden sich dann mehrere Sicherheitsklassen²¹, wie in Abbildung 11.10 zu sehen ist. Wie viele Sicherheitsklassen definiert werden, hängt davon ab, wie fein man den Bereich zwischen 0% und 100% einteilen möchte oder muss. Üblich sind 3 bis 5 Klassen, die man mit Zahlen (1, 2, 3, ...), Buchstaben (A, B, C, ...) oder Namen (Hochsicherheit, Grundschutz, ...) bezeichnet. Auch Farben werden verwendet, meist aber im Sinne der Angabe der Gefahrenhöhe (grün, gelb, rot ...).

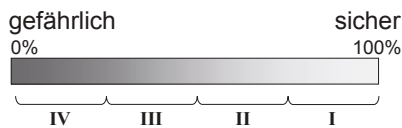


ABBILDUNG 11.10
Sicherheitsklassen

Sicherheitsklassen sind in der Praxis wichtig, weil sie das Sicherheitsmanagement erheblich vereinfachen. Voraussetzung ist jedoch, dass die Klassen einheitlich im Unternehmen verwendet werden, so dass jeder sofort weiß, welchen Schutz er von den einzelnen Klassen erwarten kann.

Statt die Sicherheit anhand vieler Sicherheitsanforderungen zu definieren, die für die einzelnen zu sichernden Objekte mühsam abgestimmt werden müssen, ist es unter Verwendung der Sicherheitsklassen möglich, ein bestimmtes Sicherheitsniveau anzugeben, bei dem unternehmensinterne Standards festlegen, welche Sicherheitsanforderungen dieses Niveau garantieren.



Beispiel: In einem IT-Projekt wird eine IT-Lösung entwickelt, in der ein zentrales Serversystem eingesetzt werden soll. Die IT-Security analysiert den Sicherheitsbedarf für das Serversystem (z. B. Sicherheit des Serverraums, der Stromversorgung, der Netzanbindung usw.) und ordnet die entsprechende Sicherheitsklasse zu (z. B. Serverraum: Klasse 2). Jeder Serverraum mit der Sicherheitsklasse 2 im Unternehmen erfüllt damit die räumliche Sicherheitsanforderung der geplanten IT-Lösung.

²⁰ Diese Extreme sind jedoch nur fiktive Werte, die in der Praxis nicht existieren.

²¹ Es finden sich dafür auch die Begriffe „Sicherheitsstufen“ oder „Schutzzklassen“.

11.5.3 Sicherheitsstrategien

„Wer das Ziel nicht kennt, kann den Weg nicht finden“ – diese Weisheit von Hans Domizlaff gilt auch für den IT-Security-Manager. Die Definition des Zielzustands für die IT-Security ist daher für das IT-Security-Management von großer Bedeutung. Gemäß dem Sprichwort „Viele Wege führen nach Rom“ lässt sich das Ziel auf vielen verschiedenen Wegen erreichen. Daher werden in der IT-Security Sicherheitsstrategien und Sicherheitsphilosophien festgelegt.

Eine Sicherheitsstrategie legt fest, wie die erforderliche Sicherheit im Unternehmen so zu erzielen ist, dass sie zum Unternehmen passt und im Unternehmen praktisch durchführ- und durchsetzbar ist. Die Sicherheitsstrategie ist unter anderem abhängig von

- der Unternehmensgröße,
- den Zielsetzungen,
- der Art, wie das Unternehmen „denkt“,
- den gewachsenen historischen Strukturen, Denkweisen und Traditionen sowie
- modernen Best-practice-Ansätzen.

Vier Strategien sollen im Folgenden anhand von Beispielen kurz vorgestellt werden.

11.5.3.1 Strategie der chinesischen Mauer

Diese Strategie, die oft auch unter dem entsprechenden englischen Begriff „Chinese Wall“ zu finden ist, geht davon aus, dass die Bedrohung für die Sicherheit des Unternehmens von außen kommt. Innerhalb des Unternehmens besteht bei dieser Strategie eine „Domain of trust“, d. h. man vertraut sich intern und ergreift zwischen internen Instanzen wie Mitarbeitern, Abteilungen usw. keine großen Sicherheitsmaßnahmen. Wie der Name schon andeutet, wird „um das Unternehmen herum eine große Mauer gebaut“, die Sicherheitsmaßnahmen konzentrieren sich auf die Schnittstellen zwischen dem Unternehmen und der Außenwelt. Somit gewinnen Funktionsbereiche wie die Warenannahme oder der Pförtnerdienst an Bedeutung: sie alle sind für die Sicherheit entscheidend.

11.5.3.2 Strategie der prozessbasierten Sicherheit

Das Konzept der prozessbasierten Sicherheit geht davon aus, dass es in einem Unternehmen eine Vielzahl von Prozesssträngen gibt, die parallel zueinander durch das Unternehmen laufen. Im Gegensatz zur „Chinese Wall“-Strategie verkleinert sich die Domain of trust auf alle internen Instanzen (Abteilungen, Arbeitsgruppen) eines einzelnen Prozesses. Innerhalb eines Prozesses gibt es Informationen, die erhoben, ausgetauscht und gespeichert werden müssen. Diese Informationen dürfen nur denjenigen zugänglich sein, die am Prozess beteiligt sind. Dies ist auch als „Need to know“-Prinzip bekannt, d. h. ein Mitarbeiter verfügt nur über diejenigen Informationen, die er für seine Funktion im jeweiligen Prozess benötigt.

11.5.3.3 Strategie der Sicherheit von innen nach außen

Bei dieser Strategie gibt es keine Domain of trust mehr. Jede Information ist ein schützenswertes Gut, unabhängig davon, in welchem Prozess die Information genutzt wird. Jede interne Instanz ist potenziell für diesen Schutz zuständig, unabhängig davon, welche Informationen in dieser Instanz genutzt werden. Dies bedeutet, dass auch innerhalb einer Arbeitsgruppe

jeder seine Informationen vor jedem anderen Kollegen schützt. Es bedeutet aber auch, dass dadurch jeder Mitarbeiter jedem Kollegen indirekt misstraut.

Der Schutz der Informationen wird bei dieser Strategie möglichst nahe an der Information selbst organisiert. Beispiel: Die Information befindet sich auf einer DVD im Aktenschrank. Sicherheit von außen nach innen würde zuerst das Gelände schützen, dann das Gebäude, den Raum und den Schrank. Sicherheit von innen nach außen schützt zuerst die Information auf der DVD (Verschlüsseln der Information) und dann den Schrank, den Raum usw.

11.5.3.4 Strategie der Sicherheit durch Eigentümerschaft

Es wird ein Eigentümer (Owner) für jede schützenswerte Information benannt. Der Eigentümer ist für den Schutz dieser Information verantwortlich. Er legt zusammen mit den Verantwortlichen für die IT-Security fest, wie hoch der Schutz sein muss und welcher Personenkreis über die Information verfügen darf. Diese Strategie, die auch unter ihrem englischen Namen „Security by Ownership“ bekannt ist, stellt also die Verantwortung für eine bestimmte Information in den Mittelpunkt der Überlegungen.

11.5.4 Sicherheitspolitik und Corporate IT-Security Policy

Der Begriff „Sicherheitspolitik“ wird in mehreren Bedeutungen verwendet. Zum einen bezeichnet er die taktische und politische Arbeit der für die IT-Security zuständigen Personen, um die Sicherheitssituation der IT des Unternehmens gemäß der Sicherheitsstrategie zu entwickeln, zum anderen wird damit das unternehmensweite Regelwerk bezeichnet, das den SOLL-Zustand für die IT-Security formuliert.

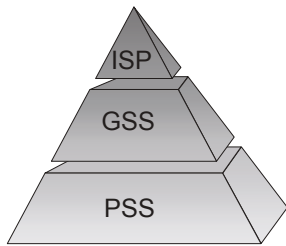
Um beide Bedeutungen besser auseinanderzuhalten, hat es sich als zweckmäßig erwiesen, für das Regelwerk den englischen Begriff „Security Policy“ zu benutzen. Im engeren Sinne dieser zweiten Bedeutung findet sich der Begriff „Sicherheitspolitik“ auch als Bezeichnung für das Dokument, das auf der obersten Ebene der Corporate IT-Security Policy grundsätzliche Aussagen zur IT-Security trifft.

Die Corporate IT-Security Policy ist das zentrale Element des Top-down-IT-Security-Managements. Sie dokumentiert die Grundsätze und Leitlinien der IT-Security und liefert Sicherheitsvorgaben für einzelne IT-relevante Bereiche im Unternehmen (z. B. IT-Netzwerke oder IT-Systeme). An dieser SOLL-Beschreibung orientiert sich dann das Handeln.

11.5.4.1 Dreistufiges Modell für die Corporate IT-Security Policy

Vor einigen Jahren herrschte noch einige Unklarheit darüber, wie eine Corporate IT-Security Policy zu gestalten sei und welchen Inhalt sie aufweisen solle. Zunehmend setzte sich ein dreistufiges Modell durch, das schon früh vom Bundesamt für Sicherheit in der Informationstechnik (BSI) propagiert wurde.

In diesem Modell existieren, wie der Name schon sagt, drei Stufen, wobei jede Stufe eine andere Aufgabe übernimmt. Zusammen bilden sie das Regelwerk, das den SOLL-Zustand der IT-Security beschreibt. Abbildung 11.11 (nächste Seite) zeigt die drei Stufen des Modells.



ISP:
Information Security Policy
Informationssicherheits-Politik

GSS:
Generic Security Standard
Generischer Sicherheitsstandard

PSS:
Product Specific Security Standard
Produktspezifischer Sicherheitsstandard

ABBILDUNG 11.11
Dreistufiges Security-Policy-Modell

11.5.4.2 Die Information Security Policy (ISP)

Die ISP kann quasi als das „IT-Security-Grundgesetz“ angesehen werden. Ähnlich wie das deutsche Grundgesetz im juristischen Bereich formuliert es im Bereich Sicherheit einen Rahmen für die IT-Security. Auf operative Aspekte wird bewusst nicht eingegangen. Beschrieben wird unter anderem:

- Für wen das Regelwerk gültig und bindend ist.
- Welche Begriffe verwendet werden, und in welcher Bedeutung sie das Unternehmen gebraucht.
- Welche Bedeutung der Informationssicherheit zukommt und wie sie im Unternehmen verstanden wird.
- Was unter schutzbedürftigen Werten zu verstehen ist (evtl. auch, welche es gibt), und wie die grundsätzlichen Sicherheitsziele aussehen.
- Wie das Security-Management aufgebaut ist und im Unternehmen verstanden werden sollte.
- Wie das Regelwerk der Security Policy aufgebaut ist und wie man es verwenden sollte.
- Was grundsätzlich von den Mitarbeitern in Bezug auf die Informationssicherheit erwartet wird.
- Welche Konsequenzen sich aus Verstößen ergeben.

Die Information Security Policy wird in der Regel vom Top-Management herausgegeben und dokumentiert damit das Commitment der Geschäftsleitung zur Informationssicherheit. Dies ist folgerichtig, denn die Geschäftsleitung und niemand anders ist gesamtverantwortlich für die Informationssicherheit, auch wenn sie fachlich nicht die erforderliche Expertise besitzt und die resultierenden Aufgaben delegieren muss.²²

Die ISP sollte in ausgedruckter Dokumentenform einen Umfang von 5–10 Seiten nicht überschreiten.

11.5.4.3 Der generische Sicherheitsstandard (GSS)

Die ISP ist aufgrund ihrer Abstraktheit und der recht allgemein gehaltenen Aussagen nicht als operatives Regelwerk geeignet. Diese Aufgabe kommt dem generischen Sicherheitsstandard (GSS) zu.

²² So wird auch die ISP nicht von der Geschäftsleitung erstellt, sondern vom IT-Security-Management. Die Geschäftsleitung unterschreibt sie jedoch und verleiht ihr somit entsprechend Bedeutung.

Der GSS beschreibt den SOLL-Zustand der Informationssicherheit mit Hilfe von Anforderungen, die aus Sicht der Informationssicherheit an die informationsverarbeitenden Bereiche des Unternehmens zu stellen sind.

Eine Anforderung wird mehreren Elementen zugeordnet:

- dem passenden Sicherheitsbereich, z.B. der physischen Sicherheit (Gebäude, Räume), der Netzwerksicherheit, der Systemsicherheit usw.;
- der in der Anforderung behandelten Objektart, z.B. Server, Raum, Person, Netzwerkelement usw.;
- dem in der Anforderung behandelten Thema, im Fall eines Raumes z.B. Brandschutz, Einbruchsschutz, Zutrittschutz usw.;
- den in Frage kommenden Sicherheitsklassen und Sicherheitskriterien.

Als Ergebnis der dargestellten Schritte liegt ein implementierungsunabhängiger, technologie-neutraler Anforderungskatalog vor, der den vollständigen ganzheitlichen SOLL-Sicherheitszustand enthält. Abbildung 11.12 zeigt, wie ein solcher Anforderungskatalog gestaltet werden kann. Von links sieht man die Sicherheitskriterien [1], das Thema [2], den Anforderungstext [3] und die Sicherheitsklassen [4].

11.2 SAP-Administratoren

Sicherheitskriterien					Thema	Nr.	Anforderung	Schutzklassen			
Verfügbarkeit	Integrität	Vertraulichkeit	Authentifizierbarkeit	Authentizität				I (Identifizierung)	II (Hoch)	III (Ganzheitlich)	IV (Trennung)
Benutzerverwaltung (Kap. 7.1.1)					Administratorrollen	1	2	3	4		
X	X	X	X	X							
X	X	X	X	X	Kennwörter		Die Rollen „Benutzeradministrator“ und „Berechtigungs-/Aktivierungsadministrator“ sollen personell getrennt sein. Diese Trennung darf auch im Vertretungsfall nicht aufgehoben werden.	X	X	X	
X	X	X	X	X							
X	X	X	X	X	„Standardbenutzer“		Die Rollen „Berechtigungsadministrator“ und „Aktivierungsadministrator“ sollen personell getrennt sein. Diese Trennung darf auch im Vertretungsfall nicht aufgehoben werden.	X	X	X	X
X	X	X	X	X							
X	X	X	X	X			Die Anforderungen des GSS sollen umgesetzt werden.	X	X	X	
X	X	X	X	X							
X	X	X	X	X			Die Tabelle „USR40“ soll mit verbotenen Zeichenkombinationen gefüllt werden.	X	X	X	
X	X	X	X	X							
X	X	X	X	X			Im Produkktivsystem ist sicherzustellen, dass der Benutzer „SAP***“ existiert.	X	X	X	X
X	X	X	X	X							
X	X	X	X	X			Im Produkktivsystem ist sicherzustellen, dass der Benutzer „SAP***“ in allen Mandanten deaktiviert wurde (Löschen aller Profile in der Profilliste und Sperren des Benutzers).	X	X	X	X
X	X	X	X	X							
X	X	X	X	X			Im Produkktivsystem ist sicherzustellen, dass der Benutzer „SAP***“ zur Gruppe „SUPER“ gehört.	X	X	X	X
X	X	X	X	X							
X	X	X	X	X			Durch Setzen der Parameter „login/no_automatic_user_SAP***“ (bzw. „login/no_automatic_user_SAPSTAR“) ist ein Zugriff auf den in Programmen festencodierten	X	X	X	
X	X	X	X	X							

ABBILDUNG 11.12 Ausschnitt aus einem GSS-Anforderungskatalog

Ein solcher GSS-Anforderungskatalog kann als ausgedrucktes Dokument je nach Ausprägung zwischen 60 und 120 Seiten umfassen. Für den Katalog kann man vordefinierte Anforderungen aus bekannten Sicherheitsstandards wie BSI (Grundsatzkataloge), BS7799 ff. (ISO 17799, ISO 27001), COBIT o.Ä. verwenden, was den Aufwand für die Erstellung des Katalogs verringert.

Die GSS-Anforderungen sollte man wirklich als Anforderungen (d.h.: was soll damit in Bezug auf die Sicherheit erreicht werden?) formulieren und nicht als Maßnahmen. Beispiel für eine Anforderung: „Sensible Räume sind vor unbefugtem Zutritt zu schützen.“ Dagegen wäre „An den Türen müssen elektronische Codeschlösser installiert werden“ eine Maßnahme.

Maßnahmen sind problematisch, denn zum einen wäre es vermessen, wenn der IT-Security-Manager die Maßnahmenkompetenz in allen Sicherheitsbereichen beanspruchen würde, zum

anderen kann eine Maßnahme aufgrund der Situation vor Ort nicht umsetzbar sein. Anforderungen müssen aber erfüllbar sein, sonst ergeben sie in der GSS keinen Sinn.

11.5.4.4 Der produktspezifische Sicherheitsstandard (PSS)

Die Ebene des PSS hat die Aufgabe, die generischen Anforderungen des GSS für eine bestimmte Technologie oder ein bestimmtes Produkt zu konkretisieren. Dort, wo die generischen Anforderungen nicht weiter konkretisiert werden müssen oder können, wird im PSS auf den GSS verwiesen. Dies verhindert unnötige Redundanzen. Die PSS bildet somit die Schnittstelle zwischen dem GSS auf der einen Seite und Administrationsleitfäden auf der anderen. Dies ist gleichzeitig der Übergang zwischen der IT-Security und dem IT-Betrieb. Im BSI-Modell der dreistufigen Sicherheitspolitik wird diese Ebene deshalb auch als „Product based Operating Manuals (POM)“ bezeichnet.

Im PSS wird beschrieben, wo und wie das jeweilige Produkt die GSS-Anforderungen erfüllt. Dies kann so weit gehen, dass detailliert für einzelne Anforderungen beschrieben wird, wie die erforderlichen Systemeinstellungen in den Bildschirmmasken vorzunehmen sind. Da man hierbei auch den Kompetenzbereich des IT-Betriebs berührt, sollte der PSS nicht völlig ohne Beteiligung der Administration erstellt werden. Auch die Frage der Pflege ist zu klären, da infolge von z.B. Release-Wechseln unter Umständen die Inhalte des PSS angepasst werden müssen.

Der Umfang eines PSS kann je nach Produkt recht hoch sein. Für komplexere Produkte kann er als ausgedrucktes Dokument durchaus 150–200 Seiten betragen. Daher wird man nicht für jedes eingesetzte Produkt einen PSS erstellen, sondern nur für sehr zentrale Produkte, für die die Informationssicherheit eine wichtige Rolle spielt.

11.5.5 Security Policy Management

Mit der Erstellung der Security Policy ist es noch nicht getan. Sie muss veröffentlicht, im Unternehmen verankert, umgesetzt und kontrolliert werden. Diese Aufgaben fasst man unter dem Begriff „Security Policy Management“ zusammen.

Security Policies, die ausschließlich als Textdokument existieren, findet man immer seltener. Die Gestaltungsform des Anforderungskatalogs legt es nahe, den Katalog strukturiert als Excel-Datei, Datenbank o.Ä. abzulegen. Auch ein vollständig webbasiertes, softwarebasiertes Security Policy Management ist möglich. Damit können Auswertungen nach Fragestellungen wie z.B.: „Wie viele Anforderungen sind bereits erfüllt?“ automatisiert ausgewertet und berichtet werden.

Die Aufgabe, den Status der Anforderungen zu pflegen, sollte nicht beim IT-Security-Manager hängen bleiben. Sinnvoller ist es, diese Aufgabe im Unternehmen an diejenigen Personen zu delegieren, die vor Ort für die jeweilige Objektart bzw. das jeweilige Thema zuständig sind. Dazu müssen Rollen definiert werden (z.B. Brandschutzbeauftragter), denen man dann die entsprechenden Anforderungen zuordnet.

Man könnte meinen, mit der Erstellung, Veröffentlichung und Delegation der Security Policy sei es getan, und die Rollen- bzw. Funktionsträger im Unternehmen würden nun aufgrund des durch die Security Policy definierten SOLL-Zustands die Anforderungen eigenverantwortlich umsetzen bzw. erfüllen.

Ein Blick in die Praxis zeigt, dass bei einer solchen Auffassung meist der Wunsch Vater des Gedankens ist. Dies hat vielerlei Gründe, unter anderem:

- *Die Funktionsträger verstehen die Anforderungen nicht.*
Sie verstehen nicht, was die Anforderung soll, was sie meint und wie Maßnahmen zu ihrer Erfüllung aussehen könnten. Deshalb ist es oft gut, wenn nicht nur der Anforderungstext aufgeführt wird, sondern auch Erklärungen, Beispiele oder auch Maßnahmenvorschläge dazu existieren.
- *Die Funktionsträger haben ganz andere Sorgen.*
Das kann daran liegen, dass die Personen mit zu vielen Aufgaben überfordert sind, dass andere Aufgaben dringlicher erscheinen oder einfach daran, dass die Personen in puncto Sicherheit träge und bequem sind. Geht es mit der Erfüllung der Anforderungen trotz Rücksprachen, Erinnerungen usw. nicht voran (was man am besten mit einem softwarebasierten Policy-Management verfolgt), muss die Situation eskaliert werden. Denken Sie daran, dass auch Ihnen der schwarze Peter zugeschoben werden kann, wenn etwas passiert. Wenn die Geschäftsleitung beschließt, dass das alles nicht so schlimm ist, sind Sie wenigstens aus dem Schneider.
- *Die Funktionsträger steuern bewusst dagegen.*
Manchmal ist auch Bössartigkeit im Spiel. Vielleicht will man Sie gegen die Wand laufen lassen, vielleicht langsam zermürben. Gutes Zureden wird nicht helfen, der Konflikt und die Fronten müssen geklärt werden. In dieser Situation ist Ihre Durchsetzungsfähigkeit gefragt. Nutzen Sie auch die Rückendeckung der Geschäftsleitung, bestehender Gesetze und Richtlinien usw. Achten Sie darauf, möglichst wenig Leichen im Keller zu haben.

11.5.6 IT-Security Auditing

Mit dem Delegieren der Verantwortung zur Erfüllung der Anforderungen delegieren Sie gleichzeitig auch die Verantwortung zur Meldung des Status der Anforderungen. Somit können Sie feststellen, ob und wie schnell einzelne Bereiche in der IT-Security vorankommen. Was aber, wenn ein Verantwortlicher Ihnen munter Erfüllungsmeldungen berichtet, die in Wahrheit gar nicht stimmen?

Auch hier gilt: Vertrauen ist gut, Kontrolle besser. Ein Mittel zur Kontrolle ist das IT-Security Auditing. Ein IT-Security Audit ist ein Sicherheitscheck mit Hilfe einer vorher festgelegten Checkliste. Es kann sowohl die IT-Security als auch das IT-Security-Management überprüft werden. Im ersten Fall enthält die Checkliste Punkte aus der Corporate IT-Security Policy, im zweiten werden Kriterien definiert, anhand derer sich überprüfen lässt, ob das Security-Management vorhanden und geeignet ist und ob es „gelebt“ wird. In beiden Fällen kann man vordefinierte Sicherheitsstandards als Grundlage betrachten.

Die Zielsetzung eines IT-Security Audits liegt vor allem darin, festzustellen, in welchen Punkten der berichtete IST-Zustand vom tatsächlichen abweicht. Falls die Konformität zu einem Standard nachgewiesen werden muss (IT-Security Compliance), gilt es weiterhin innerhalb eines IT-Security Audits herauszufinden, an welchen Stellen der Standard nicht erfüllt ist.

Sowohl die Abweichungen des berichteten vom tatsächlichen IST-Zustand wie auch die Standard-Abweichungen werden als sogenannte Findings („Gefundenes“) in einem Audit-Report

dokumentiert. Dem auditierten Bereich sollte die Möglichkeit zur Stellungnahme gegeben werden, um zu erklären, wie die Abweichungen aus seiner Sicht zu erklären sind und welche Gründe es dafür gibt.

11.5.7 Sicherheit in externen Partnerschaften

Bislang bezogen sich die Aussagen zum IT-Security-Management nur auf Bereiche innerhalb des Unternehmens. In der Praxis ist man jedoch auch mit vielen Situationen konfrontiert, in denen externe Partner involviert sind. Die Möglichkeiten für solche externe Partnerschaften sind vielfältig:

- Outsourcing von Teilen der IT-Hardware (z. B. Server-Hosting)
- Outsourcing von Teilen des IT-Betriebs (z. B. Fernwartung)
- Erbringung vollständiger IT-Dienste durch einen externen Partner (z. B. Communication Services, Helpdesk)
- Lieferanten und Kunden, die ebenfalls als externe Partner angesehen werden können und unter Umständen die IT-Security beeinträchtigen
- Einsatz externer Mitarbeiter (z. B. freiberuflicher Mitarbeiter in der Softwareentwicklung)
- Externe Berater usw.

In solchen externen Beziehungen entstehen durch die Partnerschaft selbst einige Informationsrisiken, die es zu berücksichtigen gilt. Dies sind beispielsweise:

- *Verfügbarkeitsrisiken*

Zur Beurteilung von Verfügbarkeitsrisiken muss man sich den Geschäftseinfluss der Leistung des externen Partners etwas näher anschauen. Ist die vom externen Partner zu erbringende Leistung sehr wichtig für das Unternehmen, steigen die Anforderungen an die Verfügbarkeit dieser Leistung und somit die Auswirkungen einer Nicht-Verfügbarkeit. Ein hierfür gern zitiertes Beispiel sind die WOW²³-Leistungen in der Logistik der Automobilindustrie.

Das Verfügbarkeitsrisiko scheint zunächst auf den externen Partner abgewälzt und der Ausfall über Vertragsstrafen abgesichert zu sein. Doch ein Ausfall erzeugt in der Regel Folgeschäden, die diese Absicherung übertreffen können und für die der externe Partner z. B. aufgrund von Haftungsbegrenzungen nicht immer in Anspruch genommen werden kann.

Das Unternehmen ist bei einer konsequenten Auslagerung nicht mehr in der Lage, einen Ausfall der externen Leistungen aus eigener Kraft zu kompensieren. Damit macht es sich von den Leistungen des externen Partners abhängig. Man mag argumentieren, dass das Unternehmen bei Schwierigkeiten den externen Partner jederzeit wechseln könne, doch ist ein Wechsel u. U. mit sehr hohen Aufwänden verbunden.

- *Vertraulichkeitsrisiken*

Der externe Partner bekommt durch die Zusammenarbeit unter Umständen einen tiefen Einblick in das Unternehmen. Dies betrifft zunächst den Vertragszweck als solchen, d. h. die dem externen Partner zur Verarbeitung übergebenen Daten, aber auch Informationen über interne Strukturen des Unternehmens, die aktuellen Probleme, die unternehmenspolitischen Interna usw.

²³ Warehouse on wheels (WOW) ist ein Logistikkonzept, welches das frühere Konzept des Just in time (JIT) abgelöst hat.

Solche „weichen“ Informationen sind für die Wettbewerber des Unternehmens sehr lukrativ. Es besteht daher das Risiko, dass solche Informationen vom externen Partner selbst oder einem seiner Mitarbeiter an Dritte weitergegeben werden. Daher sollte es selbstverständlich sein, Vertraulichkeitserklärungen abzuschließen, die sich nicht nur auf die verarbeiteten Daten, sondern auch auf solche weichen Informationen beziehen.

- *Integritätsrisiken*

Vor allem dann, wenn eine Kombination aus Informationstechnik des Unternehmens und Dienstleistungen von externen Partnern besteht, treten auch Integritätsrisiken auf. Ein Beispiel hierfür ist die Fernwartung von Systemen des Unternehmens durch darauf spezialisierte Dienstleister oder Hersteller. Externe Partner besitzen dabei Zugänge und Berechtigungen in den Systemen, die nicht immer dem „Need to know“-Prinzip entsprechen. Dadurch entsteht das Risiko, dass der externe Partner oder einer seiner Mitarbeiter vorsätzlich oder fahrlässig Sicherheitslöcher in die Systeme einbaut, Systeme manipuliert oder Daten verfälscht.

- *Know-how-Risiken*

Bereits bei den Vertraulichkeitsrisiken wurde angesprochen, dass der externe Partner in der Zusammenarbeit von vielen Dingen des Unternehmens Kenntnis erhält. Er nimmt dadurch viel Wissen und Know-how des Unternehmens auf. Gerade in Unternehmen, bei denen dieses Wissen einen großen Geschäftswert darstellt, besteht das Risiko, dass dieser Geschäftswert durch Mitarbeiter des externen Partners oder durch den externen Partner selbst kompromittiert und von ihm während oder nach Beendigung der Partnerschaft zum Nachteil des Unternehmens eingesetzt wird.

Auch auf der personellen Ebene besteht dieses Risiko in Form des Abwerbens von Mitarbeitern des Unternehmens, die als Know-how-Träger des Unternehmens für die Wahrung des angesprochenen Geschäftswertes notwendig sind. Man mag einwenden, dass dieses Risiko ganz allgemein und nicht nur in einer externen Partnerschaft besteht, doch steigt mit den direkten personellen Beziehungen dieses Risiko an.

- *Risiko in Bezug auf Schutzrechte*

Ist der externe Partner im Entwicklungsprozess involviert und steuert er zu einem Produkt eigene Ergebnisse bei (z.B. eine von ihm erstellte Software, die Teil des Produktes wird), sollte sichergestellt sein, dass das Unternehmen über die vollständigen Schutzrechte des Produktes verfügt bzw. eine Regelung darüber getroffen werden, wie mit integrierten externen Teilen umzugehen ist.

Bereits bei der Definition der Sicherheitsanforderungen beginnen oft die Probleme. Oft genug sind sie unvollständig, unverständlich, über- oder unterdimensioniert, zu schwammig formuliert oder fehlen ganz. Oft wird auch nicht geprüft, ob der externe Partner überhaupt in der Lage ist, die geforderte Sicherheit zu erbringen. Der externe Partner wird diese Frage immer bejahen, da er den Auftrag und kein schlechtes Image möchte.

Es kann auch passieren, dass der externe Partner die Sicherheitsanforderungen nicht ernst nimmt. Das kann daran liegen, dass der externe Partner andere Vorstellungen und Auffassungen zum Thema Sicherheit hat (z.B. eine andere Einschätzung der Bedrohungslage), das Thema am liebsten völlig ignorieren möchte oder gedankenlos handelt.

Ein weiteres Problem besteht in der Aktualität. Bei längerfristigen Partnerschaften müssen die Sicherheitsanforderungen regelmäßig auf Aktualität und Angemessenheit überprüft werden, sonst entspricht die ursprünglich geforderte und vereinbarte Sicherheit nicht mehr der aktuellen Situation und wird den Bedürfnissen des Unternehmens nicht gerecht.

Schließlich ist auch die mangelnde Kontrolle der Sicherheitsanforderungen ein Problem. Der externe Partner wird sich nur ungern „in die Karten schauen lassen“ und Kontrollen in seinem Unternehmen ablehnen.

Ein **Security Service Level Agreement (SSLA)** stellt eine Möglichkeit dar, die Sicherheitsaspekte in externen Partnerschaften zu berücksichtigen. Analog zu einem funktionalen Service Level Agreement (SLA) werden darin Vereinbarungen in Bezug auf sicherheitsrelevante Punkte (Security Services) der Partnerschaft getroffen. Für die Sicherheit werden zumeist qualitative Parameter und Kennzahlen (Levels) definiert, anhand derer man beurteilt, ob den Sicherheitsanforderungen Genüge getan wird oder nicht.

In einem solchen SSLA finden sich beispielsweise folgende Punkte:

- Garantien zur Gewährleistung der technischen Verfügbarkeit
Einsatz von fehlertoleranten oder hochverfügbaren Systemen, Beschaffungsgarantie von Ersatzteilen und -geräten innerhalb eines definierten Zeitraums, Nachweis über regelmäßige Wartung der Systeme, Überwachung der Systeme inkl. Früherkennung von Problemen, etc.
- Schutz vor Missbrauch der Systeme des Unternehmens
Einrichtung von Ausweissystemen und Zugangskontrollen, Einsatz mandantenfähiger²⁴ Systeme, Überprüfung der Vertrauenswürdigkeit von Administratoren, etc.
- Datensicherheit
Regelmäßige Datensicherung, redundante Speichersysteme, Manipulationsschutz, Verschlüsselung von Datenübertragungen, Verpflichtung der Mitarbeiter auf Vertraulichkeit und Datenschutz, etc.
- Mitwirkungspflichten, Zusammenarbeit im Notfall
- Kontroll- und Überwachungsbefugnisse des Auftraggebers
- Konsequenzen der Nichterfüllung

Probleme bereitet mitunter die rechtliche Einordnung von SLA und SSLA. Verschiedene gesetzliche Regelungen, die z. B. die Gewährleistung oder Haftung betreffen, beziehen sich auf einzelne Vertragstypen, die die oft aus dem angelsächsischen Rechtsraum stammenden SLAs in dieser Form nicht berücksichtigen. Deshalb sollten Sie solche Vereinbarungen immer rechtlich überprüfen lassen.

²⁴ Mandantenfähigkeit bedeutet die vollständige Isolierung von Anwendungen, Diensten und Daten auf Systemen, die für mehrere Unternehmen (Mandanten) genutzt werden.



Das Wichtigste – zusammengefasst

- **Betrachten Sie die IT-Sicherheit als elementaren Bestandteil von IT-Verfahren, IT-Prozessen, IT-Produkten und IT-Projekten!**

Kein Fußballtrainer stellt eine Mannschaft auf, die ausschließlich aus 11 Stürmern besteht. Erst die IT-Sicherheit macht Ihre IT-Verfahren zu einer zuverlässigen und vertrauenswürdigen Stütze der Geschäftsprozesse.

- **Nutzen Sie IT-Sicherheitsstandards!**

Sie geben Ihnen vordefinierte, meist praxiserprobte Methodiken an die Hand. Werden Sie aber nicht zum Sklaven des Standards. Er muss Ihnen dienen und zu Ihnen passen, nicht umgekehrt!

- **Kein Sicherheitskonzept ohne Schutzbedarfsanalyse!**

Nur wer weiß, welcher Schutz benötigt wird, kann Sicherheitslösungen adäquat planen und realisieren.

- **Schaffen Sie mit der Security Policy Klarheit über Sicherheitsanforderungen!**

Auf diese Weise wird die IT-Sicherheit strukturiert und mess- bzw. prüfbar.

- **Sorgen Sie für ein aussagekräftiges, verständliches und management-konformes Reporting!**

Damit schaffen Sie die Grundlage für die Involvierung der Leitungsebene und letztlich auch für Ihr Ansehen.

- **Planen, üben und treffen Sie Vorkehrungen für den Notfall!**

Im Ernstfall müssen Sie schnell reagieren und die richtigen Entscheidungen treffen.

11.6 Literatur

- [Cam11] *Campo, M.*: Bundesdatenschutzgesetz. Weka Media 2011
- [Eck08] *Eckert, C.*: IT-Sicherheit. Oldenbourg 2009
- [Froe11] *Frösche, H.-P.*: IT-Sicherheit & Datenschutz. Dpunkt 2011
- [Gola09] *Gola, C.*: The combined code of corporate governance. In: The UK banking system and its regulatory and supervisory framework. Palgrave Macmillan 2009
- [Grü07] *Gründer, T.*: Managementhandbuch IT-Sicherheit. Erich Schmidt 2007
- [Kron08] *Kronschnabl, S.*: IT-Security Governance. Universitätsverlag Regensburg 2008
- [Kub09] *Kubisch, S.*: Corporate Governance gemäß BilMoG und SOX. SIMAT 2009
- [Mül08] *Müller, K.-R.*: IT-Sicherheit mit System. Vieweg 2008
- [Pog07] *Poguntke, W.*: Basiswissen IT-Sicherheit. W3L-Verlag 2007
- [Schm06] *Schmidt, K.*: Der IT Security Manager. Hanser 2006
- [Spei07] *Speichert, H.*: Praxis des IT-Rechts. Vieweg 2007
- [Tar06] *Tarantino, A.*: Manager's Guide to Compliance. Wiley 2009
- [Wolf09] *Wolf, K.*: Risikomanagement und KonTraG. Gabler 2009

Klaus Schmidt



Fragen, die in diesem Kapitel beantwortet werden:

- Was steckt hinter dem Risikobegriff, und was ist der Unterschied zwischen Risiko und Gefahr?
- Welche Möglichkeiten der Risikowahrnehmung gibt es, und wie können diese in die Risikoanalyse und Risikobewertung einbezogen werden?
- Wie entstehen IT-Risiken, und wie kann daraufhin eine systematische Risiko-identifikation erfolgen?
- Was sind die zentralen Bestandteile einer Risikoanalyse, welche Methoden und Techniken bieten sich zur Durchführung an, und wie können die Ergebnisse dokumentiert und kommuniziert werden?
- Welche Möglichkeiten gibt es zur Darstellung und zum Reporting der Risiko-situation?
- Auf welche Weise können IT-Risiken gemanagt und bewältigt werden?
- Welche Risikobewältigungsstrategien stehen zur Wahl, und wann können diese sinnvoll eingesetzt werden?
- Wie kann der Risikomanagementprozess gestaltet werden, und welche Konsequenzen ergeben sich dadurch für die Organisation des IT-Risikomanagements?

Das Management von Risiken im Unternehmen ist eine generelle Unternehmensaufgabe und obliegt grundsätzlich dem Top-Management. Da in modernen Unternehmen mittlerweile die meisten Prozesse IT-gestützt ablaufen, besitzt die Informationstechnik einen großen Einfluss auf das Gesamtrisiko. Das IT-Risikomanagement gehört daher mittlerweile zu den wichtigen Aufgaben des IT-Managements und wird angesichts steigender Anforderungen an eine verantwortungsvolle Unternehmensführung (Corporate Governance) in seiner Bedeutung noch zunehmen.

■ 12.1 Risiko und Gefahr

Die Bezeichnung „IT-Risikomanagement“ sagt bereits, worum es geht: um das Management der IT- und Informationsrisiken im Unternehmen. Doch wie grenzt sich der Begriff des Risikos von dem verwandten Begriff der Gefahr ab?

12.1.1 Der Gefahrenbegriff



Der Begriff der Gefahr existiert wahrscheinlich schon so lange wie die menschliche Sprache, denn das, was der Begriff Gefahr beschreibt, begleitet uns tagtäglich in unserem Alltagsleben: Eine Gefahr beschreibt für eine gegebene Situation die Möglichkeit, in dieser Situation einen Schaden zu erleiden.

Beispiel: Wenn Dateien im World Wide Web heruntergeladen werden (die Gefahrensituation), besteht die Gefahr, dass schädliche Inhalte auf den Rechner gelangen.

Eine Gefahr wird durch die Gefahrenumstände bestimmt. Ob schädliche Inhalte auf den Rechner gelangen, hängt von diesen Gefahrenumständen ab; beispielsweise davon, von welchen Webseiten Dateien heruntergeladen wurden.

Eine Gefahr tritt auf. Sie gehört zu der Situation, die ich betrachte. Jede Situation stellt eine eigene, individuelle Gefahrensituation dar. Eine völlig gefahrlose Situation und somit absolute Sicherheit gibt es nicht.

12.1.2 Der Risikobegriff

Der Begriff „Risiko“ entstand im 16. Jahrhundert mit dem Aufkommen des Überseehandels. Mit dem regelmäßigen Bedienen von Handelsrouten wurden Seefahrten zu planmäßig durchgeführten Ereignissen, von denen man sich einen bestimmten Profit versprach. Durch die fehlende Kenntnis der geografischen Längenbestimmung bei der Navigation und die zahlreichen Gefahren auf See waren die Schiffe der damaligen Handelsflotten stark gefährdet, so dass man begann, im Voraus die möglichen Schäden und Verluste so gut es ging zu kalkulieren¹ und gegen den zu erwartenden Profit abzuwägen.

12.1.2.1 Abgrenzung von Risiko und Gefahr

Im allgemeinen Sprachgebrauch werden die Begriffe „Gefahr“ und „Risiko“ synonym gebraucht, weil beide das mögliche Eintreten eines negativen Ereignisses in einer Situation beschreiben und die Möglichkeit eines Schadens ausdrücken.

¹ Wahrscheinlichkeiten zur Risikoberechnung, wie wir sie heute kennen, waren zu dieser Zeit noch unbekannt.

Der grundsätzliche Unterschied ergibt sich bezüglich der Planmäßigkeit des Handelns:

- Einer Gefahr bin ich in einer Situation in der Gegenwart ausgesetzt, unabhängig davon, wie diese Situation entstand.
- Ein Risiko gehe ich in der Zukunft ein, um durch ein planvolles Handeln ein bestimmtes Ziel zu erreichen. Dabei besteht die Möglichkeit, das Ziel aufgrund eines Schadens, Verlustes o. Ä. nicht erreichen zu können.

Durch das zielgerichtete Handeln führe ich also die Situation bewusst herbei, in der ich dann Gefahren ausgesetzt bin.



Gefahren ist man in der Gegenwart ausgesetzt, Risiken geht man für die Zukunft ein.

Da man von Risiken spricht, wenn man sich noch nicht in der Situation befindet, in der der Schaden entstehen kann, ist es möglich, die Risiken im Vorfeld der Situation zu betrachten, abzuwägen und zu beeinflussen. Damit verbunden ist die Zurechenbarkeit eines Schadens, denn Risiken sind von Menschen bewusst eingegangene Wagnisse, um ein Ziel zu erreichen. Wir erleben beispielsweise, dass hinterfragt wird, ob das Eingehen bestimmter IT-Risiken (z. B. das PIN/TAN-Verfahren beim Online-Banking, das Eingeben der Kreditkartennummer beim Online-Kauf oder das Öffnen unbekannter E-Mail-Anhänge) angemessen oder schon in Richtung leichtsinniges Verhalten zu interpretieren ist.

Mit dem Begriff „Risiko“ sind folglich drei Aspekte untrennbar verbunden:

- *Auf die Zukunft gerichtete Betrachtung*

Da ein Risiko eine Schadensmöglichkeit darstellt, die erst in der Zukunft existiert, steht im Zentrum der Risikobetrachtung die Frage, welche Gefahrensituation sich in Zukunft ergeben wird, wenn man diesen oder jenen Weg beschreitet und Entscheidungen in die eine oder andere Richtung trifft. Aus der Beschäftigung mit dem Risiko möchte man eine Orientierung ableiten, welche Entscheidungen und Handlungen angesichts dieser Zukunftsabschätzung in der Gegenwart ratsam sind.

Wenn sich die Betrachtung auf die Gegenwart bezieht, hat man es (wie bereits dargestellt) nicht mit einem Risiko, sondern mit einer Gefahr zu tun.

- *Unsicherheit*

Risiko bedeutet immer, dass niemand weiß, wie etwas ausgehen und wie sich die Situation entwickeln wird. Bei der Ermittlung der Risikohöhe arbeitet man daher mit Wahrscheinlichkeiten, die man aus Erfahrungswerten, Expertise, Intuition oder dem Auswerten von Hinweisen und Anzeichen ableitet. Risiken der Vergangenheit sind dabei allenfalls als Erfahrungswerte interessant, da in der Regel die Situationen nicht vergleichbar sind. Wenn keine Unsicherheit besteht und die Entwicklung zuverlässig vorhersehbar ist, hat man es nicht mit einem Risiko, sondern mit einer Wirkung zu tun.

- *Möglichkeit eines Schadens oder einer negativen Entwicklung*

Es kann gut laufen, es kann aber auch schiefgehen – und genau auf diese negative bzw. schädigende Möglichkeit richtet sich der Blick bei der Risikobetrachtung. Würde die Schadensmöglichkeit fehlen und es nur eine positive Entwicklung geben, so hätte man es nicht mit einem Risiko, sondern mit einem Nutzen zu tun.

Die allgemeine Risiko-Definition einer „in der Zukunft liegenden Schadensmöglichkeit“ kann präzisiert werden als „Maß für die Möglichkeit, im Zusammenhang mit dem für die Zukunft geplanten Handeln einen bestimmten Schaden oder einen bestimmten Verlust zu erleiden“. Die Betriebswirtschaft definiert Risiko auch als „mögliche Abweichung von einer definierten Zielsetzung“.

12.1.2.2 Zusammenhang zwischen Risiken und dem Handeln

Mit jeder Art von Handeln – also bewusstem, zielgerichtetem Verhalten – sind automatisch Risiken verbunden. Habe ich vor, einen Rechner mit dem Internet zu verbinden, dann begeben sich mich bewusst in eine Situation, mit der bestimmte Schadenspotenziale verbunden sind. Diese Schadenspotenziale stellen für mich Risiken dar. Befinde ich mich in dieser Situation und bin dabei mit dem Internet verbunden, dann sind die Schadenspotenziale keine Risiken mehr, sondern sind zu Gefahren geworden.

Die primäre sprachliche Wurzel – lateinisch, „risicare“² – ist interessant, weil sie neben der Schadensmöglichkeit selbst auch die Einstellung gegenüber der Schadensmöglichkeit zeigt. Sie sieht in einem Risiko eine beeinflussbare Größe innerhalb eines aktiven Prozesses.

Wichtig ist, dass man auch dann Risiken eingeht, wenn man sich für eine andere, alternative Situation entscheidet. Entscheidet man überhaupt nicht, sieht man sich wiederum Gefahren durch die sich daraus ergebende Situation ausgesetzt. Gerade bei der IT-Sicherheit ist dies ein wichtiger Punkt: Man entkommt IT- und Informationsrisiken nicht, indem man nicht handelt, denn auch dann entsteht eine Situation mit bestimmten Gefahren. Um bei dem Beispiel zu bleiben: Natürlich könnte man auf den Internetzugang verzichten und so das Risiko schädlicher Inhalte vermeiden, doch würde man dann andere, z. B. betriebswirtschaftliche Nachteile erleiden.

12.1.2.3 Risiko und Chance

Im deutschen Sprachraum ist der Begriff „Risiko“ negativ besetzt. Risiken sind etwas Schlechtes, das es zu vermeiden gilt. Doch das Eingehen von Risiken ermöglicht erst das Erreichen von Zielen, daher bedeutet ein Risiko immer auch eine Chance (denn es kann ja auch gut gehen, und dann erreiche ich das Ziel).



„Risiko ist die Bugwelle des Erfolgs.“ (Carl Amery)

Besonders im angelsächsischen Raum wird Risiko deshalb durchaus auch positiv verstanden – „No risk, no fun“. Je verlockender das Ziel, desto größer die Motivation für das Ziel und damit meist auch die Risikobereitschaft.

² „Risicare“ (Klippen umschiffen) mündet in die italienischen Ausdrücke „rischiare“ (etwas wagen) und „risico“ bzw. „risco“ (Wagnis).



Praxistipp:

Es gibt eine Vielzahl von vorhandenen Risiken, beispielsweise Marktrisiken, Produktrisiken, Finanzrisiken, Prozessrisiken, Projektrisiken, IT-Risiken etc.

Es ist sinnvoll, zunächst abzugrenzen, welche Risiken betrachtet werden sollen oder müssen, und eine entsprechende Systematik der relevanten Risiken zu erstellen. Im Fall des IT-Risikomanagements sollten die wesentlichen IT-Risiken (etwa bezogen auf IT-Budgets, IT-Architekturen, IT-Projekte, IT-Prozesse, IT-Produkte und IT-Services sowie IT-Personal) klassifiziert und dann weiteren Analyse- und Handlungsaktivitäten zugrunde gelegt werden.

12.1.3 Risikowahrnehmung

Gefahren und Risiken sind keine objektiven, d. h. für alle Menschen gleichbedeutende Größen (wie z. B. die physikalische Größe der Länge), sie unterliegen vielmehr subjektiven Faktoren. Beispiele für Risiken:

- Risiken, die sich auf Situationen beziehen, die man selbst aktiv beeinflussen kann, schätzt man geringer ein als solche, denen man passiv ausgeliefert ist (in der Rolle des Beifahrers erlebt man die Verkehrssituation gefährlicher als in der des Fahrers).
- Unter Zeitdruck werden Gefahren höher eingeschätzt (Panikeffekt).
- Charaktereigenschaften, Gefühle und Überzeugungen beeinflussen die Einschätzung von Risiken (so beurteilen etwa Optimisten Risiken positiver als Pessimisten).
- Erfahrungen verändern die Einstellung gegenüber einem Risiko („ein gebranntes Kind scheut das Feuer“).
- Je weniger transparent ein Risiko ist, desto größer wird es eingeschätzt (eine Nacht im Dschungel zu verbringen, erscheint uns aufgrund der unbekannten Situation als risikoreich, auch wenn sie es möglicherweise – objektiv – gar nicht ist).
- Risiken, die sich allmählich akkumulieren, werden geringer eingeschätzt als plötzliche, seltene Risiken (Risikogewöhnung).
- Ein hoher Wissensstand in dem betrachteten Gebiet lässt uns Risiken anders beurteilen (Experten beurteilen Risiken anders als Laien).

Solche subjektiven Faktoren gilt es bei der Risikobewertung zu berücksichtigen. Gerade auch die mathematische Berechnung von Risiken führt dazu, ein Risiko als einen absoluten, objektiven Wert anzusehen. Das entspricht jedoch nicht der Wahrnehmung der Menschen.

■ 12.2 Entstehung von Risiken und Risiko-Identifikation

Damit ein Risiko entsteht, müssen mehrere Faktoren zusammenkommen. Das Wissen um diese Faktoren und ihr Zusammenwirken wird beim Risikomanagement angewendet, um Risiken zu eliminieren. Fehlt auch nur einer dieser Faktoren, kommt ein Risiko nicht zum Tragen.

In der Praxis kann zum einen von den einzelnen Faktoren auf das Risiko geschlossen werden, zum anderen lassen sich aus einem angenommenen Risiko aber auch jene Faktoren ermitteln, die zusammenwirken müssen, um dieses Risiko entstehen zu lassen.

12.2.1 Schwachstelle

Ausgangspunkt und Voraussetzung für ein IT-Risiko ist, dass das jeweils betrachtete Objekt³ nicht völlig gegen alle Gefahren abgesichert ist. Wäre dies der Fall, dann wäre das Objekt risikolos. Dieser Zustand ist in der Praxis jedoch nicht anzutreffen.⁴

Die Eigenschaften eines für die IT relevanten Objekts, die unter den Einsatzbedingungen in der Praxis zu einer gefährlichen Situation führen können, werden als Schwachstellen bezeichnet. Wichtig ist, dass die jeweilige Eigenschaft immer nur in einer bestimmten Konstellation eine Schwachstelle darstellt.

Beispiele für Schwachstellen:

- Ein Administrator-Account hat keinen Passwortschutz.
- Streng vertrauliche Daten werden im Klartext über die Leitung übertragen.
- Die Klimatisierung eines Serverraums ist angesichts der Größe des Raums unzureichend.
- Ein Laptop befindet sich ungesichert im Seminarraum eines Hotels.

Es gibt *potenzielle* Schwachstellen (Eigenschaften einer Objektart, die in vielen Fällen in der Praxis eine Schwachstelle darstellen)⁵ und *konkrete* Schwachstellen (Eigenschaften, die bei real vorhandenen Objekten unter den Einsatzbedingungen in der Praxis tatsächlich eine Schwachstelle darstellen).



Praxistipp:

Schwachstellen gibt es in allen Objekten der IT-Realität, und täglich kommen neue hinzu. Daher ist es in der Praxis fast unmöglich, auf jeden Fall aber wirtschaftlich nicht möglich, alle Schwachstellen zu kennen bzw. ermitteln zu wollen. Deshalb ist eine Konzentration und Schwerpunktsetzung für das Handeln oft unverzichtbar.

³ Der Begriff Objekt wird in diesem Kapitel als abstrakter Bezeichner verwendet. Neben physischen Objekten (z. B. ein Serverraum oder ein Router) umfasst der Begriff auch logische IT-Objekte (z. B. eine Software), Prozessobjekte oder personelle Objekte (z. B. ein Administrator).

⁴ Ein solcher Zustand wäre wirtschaftlich auch nicht vertretbar.

⁵ Aufgrund dieser Tatsache wird vermutet, dass dies auch bei den real vorhandenen Objekten der Fall sein könnte.

12.2.2 Angriffspfad

Die Existenz von Schwachstellen allein reicht noch nicht aus, damit ein Risiko entsteht, sie müssen auch zum Tragen kommen können. Betrachten wir die beiden letzten Schwachstellen etwas genauer:

Die Klimatisierungs-Schwachstelle könnte sich auf einen für 50 Server ausgelegten Serverraum beziehen, bei dem die Klimatisierung nur für 25 Server ausreichend ist. Solange weniger als 25 Server vorhanden sind oder sich von den 50 vorhandenen Servern nur 25 in Betrieb befinden, passiert – nichts. Die Schwachstelle kommt nicht zum Tragen.

Da in der Historie der IT-Sicherheit vorsätzliche Handlungen wie Hacker-Angriffe im Vordergrund standen, sagt man: „Die Schwachstelle ist nicht angreifbar“. Da es bei den oben beschriebenen Bedingungen keinen Weg gibt, die Schwachstelle anzugreifen, sagt man: „Es gibt keinen Angriffspfad zu dieser Schwachstelle“.

Die gleiche Frage gilt auch für die Laptop-Schwachstelle: Gibt es einen Angriffspfad, d. h. kann die Schwachstelle, dass der Laptop nicht an den Tisch gekettet ist, ausgenutzt werden und zum Tragen kommen? Solange der Eigentümer des Laptops anwesend ist oder der Raum in seiner Abwesenheit abgeschlossen wurde, existiert kein Angriffspfad für die Schwachstelle.⁶

Hier wird deutlich, dass bei den Angriffspfaden auch verknüpfte Bedingungen vorhanden sind. Nur unter der Bedingung, dass der Laptop-Eigentümer abwesend UND der Raum offen ist, existiert der Angriffspfad. Wurde der Raum abgeschlossen, dann deckt die äußere Sicherheit des Raumes die innere Unsicherheit des Laptops ab.

Zu einer Schwachstelle kann es viele Angriffspfade geben. Sie können u. a. technischer, prozessualer oder personeller Natur sein. Ein personeller Angriffspfad wäre das Social Engineering, bei dem versucht wird, Personen zu manipulieren. Im Laptop-Beispiel könnte eine Hotelangestellte so geschickt manipuliert werden, dass sie den abgeschlossenen Raum aufschließt und auf diese Weise ein Angriffspfad entsteht.

Es muss immer mindestens eine Schwachstelle und mindestens einen Angriffspfad zu einer Schwachstelle geben, damit sich eine gefährliche Situation⁷ entwickeln kann. Anders ausgedrückt, müssen alle Angriffspfade eliminiert werden, wenn man zuverlässig verhindern will, dass eine Schwachstelle zum Tragen kommt.

Nicht immer sind alle Angriffspfade offensichtlich. Ein Angriffspfad im Klimatisierungs-Beispiel ist die Zeit, denn die Schwachstelle kommt über die langsam steigende Temperatur zum Tragen. Wären die Server im Serverraum jeweils nur für 10 Minuten in Betrieb,⁸ käme die Schwachstelle auch bei 50 betriebenen Servern nicht zum Tragen.

⁶ Hier werden nur unbemerkt durchgeführte Angriffe unterstellt. Bei genügend krimineller Energie sind auch hier Angriffspfade durch schweren Raub oder Einbruch vorhanden, doch so weit gehen wir hier nicht.

⁷ Man spricht hier von einem „sicherheitsrelevanten Ereignis“, also einem Ereignis, das die Sicherheit des betrachteten Objekts berührt.

⁸ Unter der Annahme, dass innerhalb von 10 Minuten die Temperatur zwar steigt, aber noch keine Ausfälle bewirkt.

12.2.3 Auslöser

Auch bei dem Vorhandensein von Schwachstellen und Angriffspfad tritt das Risiko noch nicht ein. Im Laptop-Beispiel kann der ungesicherte Laptop viele Male in offenen Räumen stehen, und nichts passiert. Hinzu kommen muss ein aktives Element, um das sicherheitsrelevante Ereignis auszulösen, d.h., dass eine Schwachstelle über einen Angriffspfad zum Tragen kommt.

Dieses aktive Element wird in der IT-Sicherheit häufig als „Angreifer“ bezeichnet. Ein Angreifer ist eine Person, die eine Motivation besitzt, das sicherheitsrelevante Ereignis bewusst herbeizuführen (Angriff) und angreifbare Schwachstellen vorsätzlich auszunutzen.

Doch das aktive Element muss keine Person sein, auch ein Blitz oder eine zu hohe Temperatur kann ein auslösendes, aktives Element darstellen. Daher spricht man allgemein von einem Auslöser.

Beispiele für Auslöser:

- Vorsätzliche Taten: Angriffe, Sabotage, Terrorismus etc.
- Höhere Gewalt/Naturereignisse: Brände, Überschwemmungen, Blitzschlag etc.
- Umwelteinflüsse: Feuchtigkeit, Temperatur, Staub, Schmutz etc.
- Technisches Versagen: Technische Defekte
- Menschliches Versagen: Fehlbedienungen, Unachtsamkeit, Unterlassungen etc.

Wie wahrscheinlich die Existenz eines Auslösers ist, wird bestimmt durch die Art des Auslösers (Blitz, Kälte, personeller Angreifer, Kurzschluss). Bei personellen Angreifern spielt auch die Motivation für einen Angriff (z.B. auf ein verhasstes Unternehmen) und die Schwierigkeit eines Angriffs eine Rolle.

12.2.4 Bedrohung

Unter einer Bedrohung versteht man das Zusammenwirken der Faktoren Schwachstelle, Angriffspfad und Auslöser. Je nachdem, ob es sich nur um mögliche oder um real vorhandene Faktoren handelt, spricht man von potenziellen oder akuten Bedrohungen.

12.2.4.1 Potenzielle Bedrohung

Eine potenzielle oder auch latente Bedrohung ist eine denkbare und mehr oder weniger wahrscheinliche Bedrohung. Beispiel: „Diebstahl eines ungesicherten Laptops in einem offenen Seminarraum durch einen Hotelangestellten“.

Mindestens einer der Faktoren Schwachstelle, Angriffspfad und Auslöser ist nur ein *möglicher* Faktor, dessen reale Existenz nicht feststeht. Daher ist nicht vorhersehbar, ob das Ereignis „Diebstahl des Laptops“ jemals eintritt. Ob die betrachtete Bedrohungssituation vertretbar ist, hängt davon ab, wie wichtig, vertraulich und unwiederbringlich die Daten auf dem Laptop sind und wie wertvoll der Laptop selbst ist.

12.2.4.2 Akute Bedrohung

Wenn alle drei Faktoren real existieren, d.h. wenn es den ungesicherten Laptop im offenen Seminarraum und auch denjenigen, der ihn stehlen will, tatsächlich gibt, wird aus der potenziellen Bedrohung eine akute. Das Risiko kann nun jeden Moment eintreten. Eine akute Bedrohung ist eine dynamische Situation, sie kann sehr schnell auch wieder aufgehoben sein, z.B. wenn der Eigentümer des Laptops um die Ecke kommt und so kein Angriffspfad mehr existiert, den Laptop unbemerkt zu entwenden.

Abbildung 12.1 fasst die Zusammenhänge von der Schwachstelle bis zur Bedrohung noch einmal grafisch zusammen.

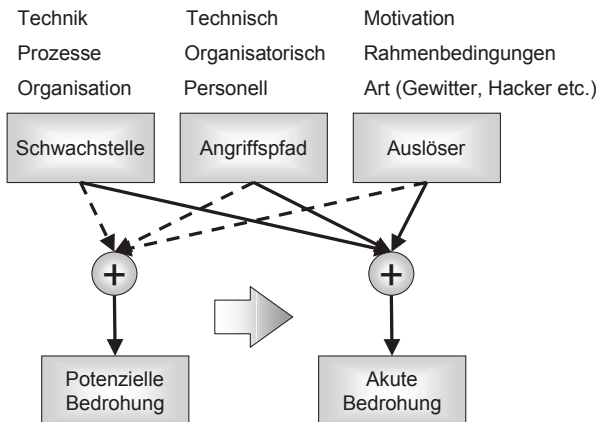


ABBILDUNG 12.1

Von der Schwachstelle zur Bedrohung

12.3 Risikoszenario

Bei der akuten Bedrohung ist der Eintritt des Risikos zwar jederzeit möglich, aber es ist noch nichts passiert. Das ändert sich, wenn die akute Bedrohung zur Realität wird.

12.3.1 Sicherheitsrelevantes Ereignis

In dem Augenblick, in dem der Auslöser aktiv wird und die Schwachstelle über den Angriffspfad tatsächlich ausnutzt, wird die akute Bedrohung zum sicherheitsrelevanten Ereignis (SRE) – „es passiert“. Im Laptop-Beispiel würde der Hotelangestellte in den Seminarraum gehen und den Laptop an sich nehmen.

Die Ausprägung des SRE wird beeinflusst durch die Art der Einwirkung (Umwelteinfluss, Fehlbedienung, vorsätzlicher Angriff), der Anzahl und Wichtigkeit der betroffenen Objekte und der Fähigkeiten des Angreifers (im Falle eines vorsätzlichen Angriffs).

12.3.2 Wirkungsszenario

Mit dem SRE startet das Risiko- bzw. Wirkungsszenario.⁹ Das Risikoszenario ist eine gedankliche Vorstellung des Eintretens eines Risikos. Das Szenario betrachtet, wie sich die Situation mit dem Eintreten des Risikos entwickelt. Bei komplexen Risikoszenarien werden mehrere Wirkungsstränge und Wirkungsketten ausgelöst, wie Abbildung 12.2 zeigt.

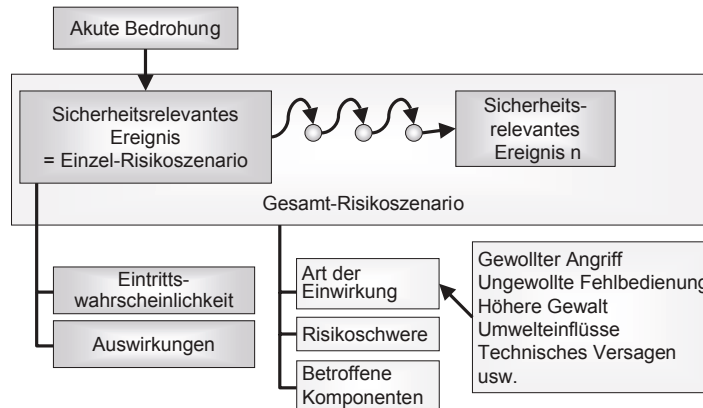


ABBILDUNG 12.2
Risikoszenario

Im Klimatisierungs-Beispiel bestünde das SRE (und damit der Beginn des Wirkungsszenarios), wenn sich nach einiger Zeit aufgrund der erhöhten Temperatur der Serverbetrieb nicht mehr aufrechterhalten lässt. Der primäre Wirkungsstrang (Hauptstrang) ist: „Serverausfall aufgrund zu hoher Temperatur“. Er beginnt, wenn der erste Server ausfällt (d.h. sich selbst herunterfährt), und besteht aus vielen mehr oder weniger parallelen Ereignissen, denn die Temperatur wirkt auf alle Server gleichzeitig ein und führt dazu, dass ein Server nach dem anderen ausfällt.

Neben dem Hauptstrang gibt es einen Nebenstrang „Nachlassen der Wärmeerzeugung“ (positive Auswirkung), da durch den Ausfall eines Servers dieser Server keine Wärme mehr produziert. Dieser Nebenstrang kann dafür sorgen, dass nicht alle Server ausfallen.

Die Wirkungsstränge zeigen ein dynamisches und oft unberechenbares Verhalten. Haupt- und Nebenstränge können unterschiedlich schnell ablaufen, Stränge können auslaufen, sich in mehrere Stränge verästeln, Nebenwirkungen können zu Hauptwirkungen werden und umgekehrt. Das macht es bei komplexeren Risiken schwierig bis unmöglich, den genauen Verlauf der Wirkungsstränge vorherzusagen. So könnte im Beispiel bei einer bestimmten Temperaturbelastung auch die Klimaanlage ausfallen, was unweigerlich zum Ausfall aller Server führt.

In einem Wirkungsstrang zieht eine Auswirkung meist andere Auswirkungen nach sich. In diesem Fall spricht man von einer Wirkungskette. Im Laptop-Beispiel würde der Verlust des Laptops den Verlust der Daten nach sich ziehen, was zum Abbruch des Seminars führen würde, der wiederum einen Imageschaden nach sich zieht.

⁹ Es wird von einem Wirkungsszenario und nicht nur von einem Schadensszenario gesprochen, da ein SRE sowohl negative (Schäden) als auch positive Auswirkungen haben kann.

Das Eintreten eines Risikos kann die Wahrscheinlichkeit anderer Risiken beeinflussen oder sogar andere Risiken auslösen. Geschieht dies mehrfach hintereinander, spricht man von einer Kettenreaktion.

**Beachten Sie:**

In der Praxis zeigt sich, dass es mehrere Verläufe für ein eingetretenes Risiko gibt. Daher kann es zu einem Risiko mehrere Risikoszenarien mit unterschiedlicher Eintrittswahrscheinlichkeit und unterschiedlichen Auswirkungen geben.

■ 12.4 IT-Risikoanalyse

Die Methode der IT-Risikoanalyse bildet mit dem Risiko-Managementkreislauf den Kern des Risikomanagements. Sie ist die zentrale Methodik für die Ermittlung, Bewertung und Darstellung von IT- und Informationsrisiken.

12.4.1 Kernbestandteile der IT-Risikoanalyse

Wenn Schwachstellen, Angriffspfade und Auslöser die Faktoren dafür sind, dass ein Risiko entstehen kann, liegt auf der Hand, dass es bei der IT-Risikoanalyse darum geht, diese Faktoren zu ermitteln. Außerdem werden die daraus resultierenden, sicherheitsrelevanten Ereignisse und Wirkungsszenarien betrachtet und bewertet. Die Ergebnisse sollten in einer überschaubaren und präsentierbaren Form dokumentiert werden.

12.4.2 Arten von IT-Risikoanalysen

Es existieren verschiedene Möglichkeiten, eine Risikoanalyse zu gestalten. Hier gibt es kein Richtig oder Falsch, vielmehr muss vor der Durchführung einer solchen Analyse entschieden werden, welche Ziele man mit der Analyse verfolgt und welcher Aufwand betrieben werden kann. Für die Darstellung der einzelnen Phasen einer IT-Risikoanalyse in diesem Kapitel wird die vollständige IT-Risikoanalyse zugrunde gelegt.

12.4.2.1 Verkürzte IT-Risikoanalyse

Bei der verkürzten IT-Risikoanalyse wird zunächst – wenn etwa der Fokus auf Sicherheitsrisiken liegt – ein Katalog mit Sicherheitsanforderungen für die IT-relevanten Objekte erstellt. In der eigentlichen Analysephase erhebt man nun zu jeder Sicherheitsanforderung des Katalogs den IST-Zustand des Objekts. Ergibt sich eine Abweichung, so stellt diese Abweichung eine Schwachstelle dar. Der Schwachstelle wird dann ein Risiko zugeordnet, das anschließend hinsichtlich der Eintrittswahrscheinlichkeit und der Schadenshöhe bewertet wird.

Die verkürzte Risikoanalyse stellt keine Risikoanalyse im eigentlichen Sinn dar, sie entspricht eher einem Audit. Ein Audit ist eine Überprüfung mittels SOLL/IST-Vergleich. Von Vorteil ist eine schnelle und einfache Durchführung, von Nachteil die Beschränkung auf die Punkte des Katalogs und die meist nur intuitive Zuordnung der Risiken.

12.4.2.2 Vollständige IT-Risikoanalyse

Die vollständige IT-Risikoanalyse ermittelt in einer IST-Aufnahme die IT-relevanten Objekte und deren Einsatzbedingungen. In einer Schwachstellenanalyse werden die Eigenschaften der Objekte ermittelt, die unter diesen Einsatzbedingungen Schwachstellen darstellen. In einer Bedrohungsanalyse werden die Bedrohungen ermittelt, die sich aus den Schwachstellen und den vorhandenen Angriffspfaden und Auslösern ergeben könnten (potenzielle Bedrohungen) oder tatsächlich vorhanden sind (akute Bedrohungen). In einem weiteren Schritt wird das aus den Bedrohungen resultierende Risiko festgestellt und hinsichtlich der Eintrittswahrscheinlichkeit und der Schadenshöhe bewertet.

12.4.2.3 Umfassende IT-Risikoanalyse

Die umfassende IT-Risikoanalyse entspricht der vollständigen IT-Risikoanalyse mit der Erweiterung, dass zur Ermittlung der Schadenshöhe eine umfassende Analyse der sicherheitsrelevanten Ereignisse und der Wirkungsszenarien erfolgt. Haupt- und Nebenwirkungen, positive und negative Auswirkungen, der zeitliche Verlauf der Wirkungen und wer wie davon betroffen wäre (Mitarbeiter, Öffentlichkeit, Verträge, Prozesse usw.), wird für jedes sicherheitsrelevante Ereignis detailliert durchgespielt und ggf. simuliert.

12.4.3 IST-Aufnahme

Die IT-Risikoanalyse ist eine Bottom-Up-Methodik, bei der von der bestehenden Situation ausgegangen wird und die damit verbundenen Risiken ermittelt werden. Daher kommt der IST-Aufnahme eine besondere Bedeutung zu. Nur wenn es gelingt, die bestehende Situation im Hinblick auf die IT genügend detailliert und vollständig aufzunehmen, sind auch die Ergebnisse der IT-Risikoanalyse ausreichend aussagekräftig.

12.4.3.1 Abgrenzung des Analysebereichs

In einem ersten Schritt wird der Analysebereich abgegrenzt. Was soll Bestandteil der Betrachtung sein und was nicht? Eine IT-Risikoanalyse kann für einen beliebigen Bereich erstellt werden, z. B. für bestimmte Geschäftsprozesse, IT-Prozesse, einen bestimmten Server, einen Unternehmensstandort, eine IT-Lösung (Applikation), eine bestimmte IT-Infrastruktur oder für ein IT-Projekt. Die Abgrenzung kann statisch (welche IT-relevanten Objekte, Personen, Stakeholder werden betrachtet?) und/oder dynamisch (welche Abläufe/Prozesse werden ab wann bis wohin betrachtet?) erfolgen.

12.4.3.2 Prozessaufnahme und Geschäftseinflussanalyse

Aus Sicht der Unternehmensführung stehen in vielen Fällen Geschäftsprozesse im Fokus der Betrachtung, denn dort entsteht in der Regel der geschäftliche Schaden. Sofern das Unternehmen nicht schon prozessorientiert arbeitet, müssen zunächst die Prozesse aufgenommen werden. Dies geschieht bei der IT-Risikoanalyse nicht so detailliert wie beim Business Process

Reengineering, sondern konzentriert sich auf die wesentlichen Prozessschritte. Zusätzlich können die aufgenommenen Prozesse hinsichtlich ihrer geschäftlichen Bedeutung priorisiert werden. Als Nächstes wird aufgenommen, welche IT-Objekte an welcher Stelle in den Prozessen in welcher Weise eingesetzt bzw. welche Software-Anwendungen und -dienste in den Prozessen genutzt werden.

In einem weiteren Schritt wird mit Hilfe der Methodik „Business Impact Analyse“ der Geschäftseinfluss der einzelnen IT-Objekte aufgenommen. Dazu nimmt man etwa unterschiedliche Sicherheitsbeeinträchtigungen eines IT-Objekts an und ermittelt die Auswirkungen auf die Geschäftsprozesse.

Beispiel: Innerhalb eines Bestellprozesses werden Bestellungen in einen Fileserver eingespielt. Nun wird nach den geschäftlichen Auswirkungen von Sicherheitsbeeinträchtigungen gefragt: Welchen Einfluss auf das Geschäft des Unternehmen hat es, wenn eine Serverfunktion oder der ganze Server für 5 Minuten, 1 Stunde, 1 Tag oder 1 Woche ausfällt? Welchen Einfluss hat es, wenn eine einzelne Bestellinformation, eine vollständige Bestellung, alle Bestellungen oder deren Übertragung abgehört oder manipuliert wird?

12.4.3.3 Architektur- und Abhängigkeitsanalyse

In der Architekturanalyse wird die Statik der IT ergründet. Welche IT-Objekte (IT-Infrastruktur und ihre Elemente, IT-Applikationen etc.) sind vorhanden? Wie sind sie miteinander verschaltet? Hierzu werden IT-Architekturdokumentationen wie Netzwerkpläne, Systemaufstellungen, Inventarlisten, Verbindungspläne, Architekturübersichten o. Ä. herangezogen. Die Kenntnis der Struktur der IT-Architektur ist wichtig, um beispielsweise kritische Elemente erkennen zu können.

Des Weiteren wäre die Frage zu beantworten, welche Objekte von anderen IT-Objekten abhängig sind. In der Praxis hat man es mit einem Geflecht einzelner IT-Komponenten zu tun, die für den Anwender nicht transparent sind. Die Abhängigkeit einer Anwendung von Servern, Datenbanken, Netzwerken usw. ist nicht immer einfach nachzuvollziehen.

Für die Dokumentation der Abhängigkeiten existiert die Methodik der Abhängigkeitsmatrix (siehe Abbildung 12.3). Dazu werden in einer Tabelle die IT-Objekte jeweils vertikal (welche Objekte sind abhängig?) und horizontal (von welchen Objekten sind die Objekte abhängig?) aufgetragen. In den Schnittpunkten der Komponenten trägt man dann die Informationen zur Abhängigkeit ein:

- Besteht eine Abhängigkeit?
- Wenn ja, in welcher Richtung? Verläuft sie uni- oder bidirektional?

	Objekt A	Objekt B	Objekt C	Objekt X
Objekt A		hoch	gering	mittel
Objekt B	gering		mittel	mittel
Objekt C	unbekannt	hoch		unbekannt
Objekt X	gering	mittel	gering	

ABBILDUNG 12.3
Abhängigkeitsmatrix

- Wie groß ist die Abhängigkeit?
Stark: Ohne das andere Objekt kann die Funktion nicht erbracht werden.
Mittel: Die Funktion ist ohne das andere Objekt eingeschränkt.
Gering: Das andere Objekt spielt nur bei Nuancen der Funktion eine Rolle

Außerhalb der IT liegende Abhängigkeiten des Prozesses (z. B. von der Mitarbeiter-Qualifikation oder der Materialgüte) werden bei der IST-Aufnahme für eine IT-Risikoanalyse nicht betrachtet.

12.4.4 Schwachstellenanalyse

Nach der IST-Aufnahme sind die Statik und Dynamik der IT-relevanten Objekte, deren Zusammenspiel und deren Einsatzbedingungen bekannt. Nun geht es darum, technische und organisatorische Eigenschaften und Umstände in der Statik und Dynamik der Objekte zu identifizieren, die unter diesen Einsatzbedingungen Schwachstellen darstellen.

Es gibt mehrere Möglichkeiten, IT-Schwachstellen aufzuspüren:

- *Vulnerability Scanning*
Unter diesem Begriff wird eine toolgestützte, automatisierte Schwachstellensuche verstanden. Das Vulnerability Scanning wird vornehmlich auf der Netzwerkebene, der Betriebssystemebene und der Anwendungsebene (z. B. für die Überprüfung von Webservern und Webapplikationen) eingesetzt.
Im World Wide Web gibt es eine Fülle kostenfreier und kostenpflichtiger einzelner Tools und ganzer Softwarepakete, die für das Vulnerability Scanning verwendet werden können, wie z. B. ISS (Internet Security Scanner), Nessus, N-Stalker, Nmap, Webshag usw.
- *Penetration Tests und Tiger Teams*
Bei einem Penetration Test wird das Analyseobjekt mit Wissen des Eigentümers angegriffen. Dies wird auch als „freundlicher Angriff“ bezeichnet. Ein Unternehmen könnte beispielsweise seiner IT-Security-Mannschaft den Auftrag geben, zu versuchen, die E-Mails des Vorstandsvorsitzenden auszuspähen.
Während das Vulnerability Scanning lediglich eine vordefinierte Liste potenzieller Schwachstellen überprüft, handelt es sich bei einem Penetration Test um einen intelligent vorbereiteten und durchgeführten Angriff.
Ein *Tiger Team* im Sinne der IT-Risikoanalyse ist eine Gruppe von IT-Sicherheitsexperten, die mit dem freundlichen Angriff beauftragt wird und über Fähigkeiten verfügt, wie man sie auch bei professionellen Angreifern finden würde. Aufgrund der hohen Spezialisierung auf solche Angriffe ist ein *Tiger Team* einem unternehmensinternen Team meist weit überlegen.
- *Vordefinierte IS-Standards*
Insbesondere für die Durchführung von verkürzten IT-Risikoanalysen interessant sind nationale und internationale Standards für die Informationssicherheit (IS), wie ISO 27001 (weltweiter ISMS-Standard der ISO¹⁰), COBIT (weltweiter Auditierungsstandard der ISACA¹¹) oder die IT-Grundschutzkataloge (deutsche Standards des BSI¹²).

¹⁰ ISO = International Organization for Standardization, ISMS = Information Security Management System

¹¹ ISACA = Information Systems and Control Association

¹² BSI = Bundesamt für Sicherheit in der Informationstechnik

Aus den Anforderungen bzw. Gefährdungskatalogen lassen sich potenzielle Schwachstellen ableiten, die in der Praxis überprüft werden können.

- *Computer Emergency Response Teams (CERT)*

Ein CERT ist eine Stelle, die sich mit IT-Sicherheit beschäftigt. Sie stellt Unternehmen und bei dem CERT registrierten Personen Informationen zu aufgetretenen Sicherheitsvorfällen und Sicherheitslücken zur Verfügung. Ein CERT verbreitet Warnungen, wenn neue Sicherheitslücken (potenzielle Schwachstellen) bekannt werden.

In Deutschland seit langem bekannt ist das DFN-CERT des Deutschen Forschungsnetzes. Daneben gibt es das CERT-Bund (auf Behörden ausgerichtet) und das Bürger-CERT (auf Privatpersonen ausgerichtet) des BSI, oder auch Branchen- und Unternehmens-CERTs wie das S-CERT der Sparkassenorganisation oder das Telekom-CERT.

- *Eigene Recherche*

Eine weitere, wenn auch zeitraubende, Möglichkeit ist die eigene Recherche nach Schwachstellen. Die Informationsmöglichkeiten über potenzielle IT-Schwachstellen sind mittlerweile nur noch schwer überschaubar. Neben Zeitschriften, Pressemeldungen, Herstellerinformationen und anderen Publikationen findet man vor allem im World Wide Web eine Vielzahl von IT-Security-Foren und „schwarzen Brettern“ zu den unterschiedlichsten Themen.

Bei den ersten beiden Punkten geht es um das Aufspüren tatsächlich vorhandener, meist technischer Schwachstellen in den untersuchten Systemen. Die anderen Punkte liefern potenzielle Schwachstellen, bei denen dann geprüft werden muss, inwieweit sie bei den eingesetzten IT-Objekten auch real vorhanden sind.

12.4.5 Bedrohungsanalyse

Nach dem Sammeln der potenziellen Schwachstellen steht noch nicht fest, ob die Schwachstellen unter den vorhandenen Einsatzbedingungen auch tatsächlich ein Risiko entstehen lassen können. Daher schließt sich der Schwachstellenanalyse die Bedrohungsanalyse an.

Innerhalb der Bedrohungsanalyse wird ermittelt, inwieweit die gefundenen Schwachstellen in der Realität zum Tragen kommen können.

Beispiel: In der Schwachstellenanalyse einer Webapplikation wurde die potenzielle Schwachstelle „Applikation führt keine Kontrolle von Eingaben in Textfeldern durch“ überprüft, und es wurde festgestellt, dass diese Schwachstelle tatsächlich vorhanden ist. Würde die Applikation die Überprüfung der Benutzerexistenz mit dem SQL-Statement

```
SELECT COUNT(*) FROM users WHERE user='...Eingabe...' AND pass='...Eingabe...'
```

in einer Datenbank durchführen,¹³ dann könnte die Schwachstelle durch die Eingabe der Zeichenkette ' OR 1=1 OR ' in das Textfeld für das Passwort zum Tragen kommen. Es entstünde das Statement (nun mit den Eingabewerten):

```
SELECT COUNT(*) FROM users WHERE user='egal' AND pass='' OR 1=1 OR ''
```

und die Applikation würde annehmen, der Benutzer hätte das richtige Passwort eingegeben. Der Angriffspfad ist das SQL-Statement, denn würde die Applikation die Überprüfung anders durchführen, z.B. indem die Eingabewerte der Textfelder einzeln mit den Vorgabe-

¹³ Wenn das Ergebnis der Abfrage größer null ist, dann existiert der Benutzer.

werten der Datenbank verglichen würden, bestünde die Schwachstelle zwar weiterhin, könnte aber in der Überprüfung der Benutzerexistenz nicht mehr zum Tragen kommen.

Der dritte Faktor des Auslösers wird bei IT-Bedrohungen im Falle bewusster Handlungen meist als gegeben vorausgesetzt. Es wird also nicht weiter betrachtet, ob es tatsächlich jemanden gibt, der eine Motivation besitzt, die Webapplikation auszutricksen. Das ist etwas anderes, wenn der Auslöser beispielsweise ein Naturereignis wie ein Erdbeben ist. In diesem Fall würde man sich schon überlegen, wie groß die Möglichkeit für ein solches Naturereignis ist.

Die Bedrohungsanalyse kann auch in umgekehrter Richtung erfolgen, indem man von einer Bedrohung bzw. einem Bedrohungsszenario ausgeht und dann ergründet, ob, und wenn ja, wie dieses Szenario in der vorhandenen Realität entstehen kann. In diesem Beispiel könnte man von der Bedrohung „Benutzerauthentifikation austricksen“ ausgehen und sich fragen, wie ein solches Austricksen möglich werden könnte (Angriffspfad suchen). Der Nachteil dieser Methode liegt darin, dass man nur die Bedrohungen betrachtet, von denen man ausgeht. Vielleicht können aus den Schwachstellen aber noch ganz andere Bedrohungen entstehen.

12.4.6 Risikofeststellung und -bewertung

Wenn nach Abschluss der Bedrohungsanalyse die potenziellen und akuten Bedrohungen vorliegen, können die aus den Bedrohungen resultierenden Risiken eingeschätzt werden. Ein Risiko wurde definiert als Maß für die Möglichkeit, einen bestimmten Schaden zu erleiden. Zum ersten Mal wird in der IT-Risikoanalyse nun der mögliche Schaden betrachtet.

12.4.6.1 Die Risikoformel

Die Risikoformel ist ein einfaches mathematisches Verfahren zur Berechnung der Höhe eines Risikos. Dabei wird davon ausgegangen, dass das Risiko umso höher ist, je größer der Schaden bzw. Verlust ist und je wahrscheinlicher es ist, diesen Schaden bzw. Verlust zu erleiden. Beide Faktoren werden in der Risikoformel multiplikativ verknüpft:



Risiko = Eintrittswahrscheinlichkeit × Schadenshöhe

Daraus ergibt sich, dass für die Risikofeststellung die beiden Faktoren Eintrittswahrscheinlichkeit und Schadenshöhe bestimmt werden müssen.

12.4.6.2 Bestimmung der Eintrittswahrscheinlichkeit

Wahrscheinlichkeiten werden in der Mathematik mit einem Wahrscheinlichkeitswert angegeben, d. h. einem Wert zwischen 0 (ausgeschlossen, tritt nie auf) und 1 (sicher, tritt auf jeden Fall auf), der auch oft als Prozentwert zwischen 0% und 100% zu finden ist.

Mathematisch werden Wahrscheinlichkeiten über statistische Häufigkeiten berechnet. Um die Ausfallwahrscheinlichkeit eines Linux-Servers zu ermitteln, wird eine bestimmte Anzahl von Linux-Servern über einen bestimmten Zeitraum beobachtet und die Anzahl der Ausfälle fest-

gehalten.¹⁴ Daraus lässt sich ableiten, wie wahrscheinlich ein Ausfall in der Zukunft ist. Hierbei gibt es drei Probleme:

1. Die Struktur des Analyseobjekts¹⁵ und dessen Einsatzbedingungen müssen vergleichbar sein, was sie in der Praxis nur selten sind. Wir erinnern uns an den unzureichend klimatisierten Serverraum – eine solche Einsatzbedingung würde den Wahrscheinlichkeitswert deutlich verfälschen.
2. Die Vielzahl unterschiedlicher IT-Objekte (schon jedes Release eines IT-Produkts liefert andere Werte) würde eine unüberschaubare Menge an Werten erzeugen.
3. Für seltene Ereignisse ist keine Beobachtung möglich, der Zeitraum müsste so groß gewählt werden, dass durch den Technologiefortschritt keine zwei vergleichbaren Szenarien vorhanden wären.

Aus diesen Gründen wird die Wahrscheinlichkeit nicht statistisch berechnet, sondern eingeschätzt. Verbreitet ist die Einteilung in mehrere **Wahrscheinlichkeitsstufen**,¹⁶ wobei sich die Wahrscheinlichkeit immer auf einen bestimmten Zeitraum (z.B. die nächsten 12 Monate) bezieht.

Beispiel: Die Wahrscheinlichkeit dafür, dass das Risiko innerhalb des Zeitraums eintreten wird, ist:

- Sehr gering (0–20%): Es ist sehr unwahrscheinlich, dass das Risiko eintritt.
- Eher gering (20–50%): Die Möglichkeit, dass das Risiko nicht eintritt, ist größer als die Möglichkeit, dass es eintritt.
- Eher hoch (50–80%): Die Möglichkeit, dass das Risiko eintritt, ist größer als die Möglichkeit, dass es nicht eintritt.
- Sehr hoch (80–100%): Es kann als relativ sicher gelten, dass das Risiko eintritt.



Praxistipp:

Die Einschätzung der Risikowahrscheinlichkeit ist immer subjektiver Natur und von der Erfahrung und dem Gespür der beurteilenden Person abhängig. Fragen für die Einordnung eines Risikos in diese Stufen:

- Sind ähnliche Fälle bekannt, in denen das Risiko auftrat?
- Sind Risikofaktoren vorhanden, die das Auftreten des Risikos wahrscheinlicher machen?
- Gibt es Anhaltspunkte dafür, dass das Risiko auftreten könnte?
- Gibt es Vorkehrungen für den Fall, dass das sicherheitsrelevante Ereignis eintritt?

12.4.6.3 Bestimmung der Schadenshöhe

Zur Bestimmung der möglichen Schäden wird das gesamte Risikoszenario ausgewertet, das sich ergibt, wenn die jeweilige akute Bedrohung zu dem entsprechenden sicherheitsrelevanten Ereignis führt. Dabei müssen die Wirkungsstränge und Wirkungsketten berücksichtigt

¹⁴ Je länger der Zeitraum und je größer die Anzahl der Server dabei ist, desto genauer wird das Ergebnis.

¹⁵ Im Fall des Linux-Servers: Der Releasestand der Distribution, der eingesetzte Kernel, die Konfiguration usw.

¹⁶ Als Begriffe werden hier auch Wahrscheinlichkeitsklassen oder -kategorien verwendet.

werden und somit auch die zeitliche Komponente, denn je länger z. B. ein Ausfall anhält, desto größer werden die Schäden.

Ist das Risikoszenario schon einmal eingetreten, sind die Auswirkungen bekannt, ansonsten müssen die Wirkungsstränge gedanklich durchgespielt werden. Die Bandbreite reicht hier vom

- Best-Case-Szenario (alles, was gut gehen kann, geht auch gut) bis zum
- Worst-Case-Szenario (alles, was schiefgehen kann, geht auch schief).

Risikoszenarien haben durchaus auch positive Auswirkungen, die man bei der Bestimmung der Schadenshöhe aber nicht berücksichtigt bzw. gegengerechnet.

Zunächst wird bestimmt, welcher Art die zu erwartenden Schäden sind. Hierbei helfen Schadenskategorien:

- *Personenschäden* (Verlust von Leib und Leben; Beeinträchtigung der körperlichen oder geistig/seelischen Unversehrtheit)
- *Verstöße* (gegen Gesetze, Vorschriften und Richtlinien, Rechte,¹⁷ Verträge und Vereinbarungen)
- *Finanzielle Schäden* (direkte finanzielle Auswirkungen)
- *Betriebliche Schäden* (Beeinträchtigung der Aufgabenerfüllung)
- *Imageschäden* (negative Außenwirkung, Vertrauensverlust)
- *Immaterielle Schäden* (z. B. Verlust unwiederbringlicher/ideeller Werte)

Ob ein Schaden als schlimm oder harmlos angesehen wird, hängt davon ab, wo das Unternehmen die Prioritäten setzt. Daher bezeichnet der Begriff der Schadenspriorität, an welchen Aspekten sich die Beurteilung des Schadens orientiert:

- *Geschäftsorientiert*
Die Auswirkungen auf die geschäftliche Tätigkeit (Abwicklung der Geschäftsprozesse, Einhaltung von Liefervereinbarungen, Aufgabenerfüllung) steht im Vordergrund.
- *Wertorientiert*
Der Wert (materiell und immateriell) der im Risikoszenario betroffenen IT-Objekte steht im Vordergrund.
- *Finanzorientiert*
Der direkte, durch den Schaden verursachte Abfluss an finanziellen Mitteln steht im Vordergrund.
- *Ethikorientiert*
Die ethischen und moralischen Auswirkungen und deren Vertretbarkeit stehen im Vordergrund.

Nachdem als Ergebnis der Analyse des Wirkungsszenarios die Art der Schäden und die Schadenspriorität feststehen, wird der Schaden bewertet.

Eine weit verbreitete Möglichkeit ist die Angabe einer Schadenssumme. Dazu werden alle Einzelschäden unabhängig von der Schadenskategorie monetär bewertet und zu einer Gesamtschadenssumme aufaddiert. Das Problem dabei liegt darin, mit welchem Betrag ein Schaden anzusetzen ist. Gerade bei Image- und Personenschäden ist das nicht einfach – welcher Geldbetrag ist einem Menschenleben angemessen?

¹⁷ Insbesondere das informationelle Selbstbestimmungsrecht

Eine weitere Möglichkeit besteht darin, die Schadenshöhe mit Hilfe mehrerer Stufen einzuschätzen, so wie es weiter oben mit der Eintrittswahrscheinlichkeit getan wurde. Bei der Verwendung der gleichen Metrik ergeben sich die folgenden Stufen:

Sehr gering

- *Im finanziellen Bereich:* kein spürbarer finanzieller Verlust.
- *Im geschäftlichen Bereich:* unbedeutende Auswirkungen auf die geschäftliche Tätigkeit, z. B. begründet in:
 - einer minimalen Beeinträchtigung der Geschäftsprozesse;
 - einer Ordnungswidrigkeit mit unwesentlichen Konsequenzen (z. B. kleines Bußgeld);
 - einem Vertragsverstoß ohne merkbare Auswirkungen auf die Wertschöpfungskette;
 - einer kaum spürbaren Beeinträchtigung des Ansehens und Rufs des Unternehmens.
- *Im materiellen Bereich:* ein minimaler Sachschaden, dessen Wiederbeschaffung keine Probleme bereitet.
- *Im personellen Bereich:* nur minimale, kurzzeitige gesundheitliche Beeinträchtigungen.

Eher gering

- *Im finanziellen Bereich:* ein kleinerer, tragbarer finanzieller Verlust.
- *Im geschäftlichen Bereich:* kleinere Auswirkungen auf die geschäftliche Tätigkeit, z. B. begründet in:
 - einer mäßigen Beeinträchtigung der Geschäftsprozesse;
 - einem Gesetzesverstoß mit geringen Konsequenzen;
 - einem Vertragsverstoß mit geringen Auswirkungen auf die Wertschöpfungskette;
 - einer Beeinträchtigung des Ansehens und des Rufs des Unternehmens in Fachkreisen.
- *Im materiellen Bereich:* ein geringerer Sachschaden, dessen Wiederbeschaffung nicht schwierig ist.
- *Im personellen Bereich:* leichte Verletzungen, die vollständig ausheilen.

Eher hoch

- *Im finanziellen Bereich:* ein großer, aber noch verkraftbarer finanzieller Verlust.
- *Im geschäftlichen Bereich:* größere Auswirkungen auf die geschäftliche Tätigkeit, z. B. begründet in:
 - einer massiven Beeinträchtigung oder kürzeren Verhinderung der Geschäftstätigkeit;
 - einem Verstoß gegen Gesetze und Vorschriften mit empfindlichen Folgen, jedoch ohne Gefährdung des Unternehmens;
 - einem Vertragsverstoß mit empfindlichen, aber verkraftbaren Konsequenzen für die Wertschöpfung des Unternehmens;
 - einer starken Beschädigung des Ansehens und Rufs des Unternehmens.
- *Im materiellen Bereich:* ein höherer Sachschaden mit der Vernichtung schwer wiederbeschaffbarer Gegenstände.
- *Im personellen Bereich:* starke, aber nicht unheilbare Verletzungen.

Sehr hoch

- *Im finanziellen Bereich:* ein sehr hoher finanzieller Verlust, der eine ernste Gefahr für die Finanzstabilität des Unternehmens darstellt.
- *Im geschäftlichen Bereich:* sehr große Auswirkungen auf die geschäftliche Tätigkeit bis zur existentiellen Bedrohung, z. B. begründet in:
 - einer längeren Verhinderung der Geschäftstätigkeit oder der Kernprozesse;
 - einem fundamentalen Verstoß gegen Gesetze und Vorschriften, der die Schließung des Unternehmens oder extrem hohe Geldbußen nach sich zieht;
 - einem Vertragsverstoß mit weit reichenden Konsequenzen für die Wertschöpfung des Unternehmens;
 - der Zerstörung von Ansehen und Ruf des Unternehmens auf breiter Ebene.
- *Im materiellen Bereich:* ein sehr hoher Sachschaden mit der Vernichtung unwiederbringlicher Gegenstände.
- *Im personellen Bereich:* der Verlust von Menschenleben oder Entstehung von Invalidität.

12.4.6.4 Probleme der Risikoformel

So plausibel die Risikoformel auch ist, sie hat ihre Tücken. Es ergeben sich vor allem vier Probleme:

- Der Wert für die Eintrittswahrscheinlichkeit ist in den meisten Fällen nicht statistisch abgesichert. Diese Tatsache wurde bereits angesprochen. Damit wird die Risikoformel manipulierbar. Sie kann, je nach Zweck, dazu genutzt werden, ein Risiko möglichst groß oder möglichst klein darzustellen. Das gilt umso mehr, wenn zur Untermauerung des Wertes nicht vergleichbare Daten verwendet werden.
- Es wird eine Genauigkeit vorgetäuscht, die nicht vorhanden ist. Das ist eine Folge davon, dass die Eintrittswahrscheinlichkeit als Zahlenwert angegeben wird. Wie schon erwähnt, resultiert der Wert für die Eintrittswahrscheinlichkeit nur selten aus einer gesicherten mathematischen Datenbasis, sondern wird geschätzt. Eine solche Schätzung kann naturgemäß keinen mathematisch fundierten Wert liefern. Kleinere Unterschiede in den Werten (z. B. zwischen 0,79 und 0,81) sind daher nicht nachvollziehbar.
- Aufgrund der multiplikativen Verknüpfung sind viele kleine Schäden ein ebenso hohes Risiko wie ein einziger, großer Schaden.
Beispiel: Jeden Tag (bei 360 Tagen Betrieb im Jahr) fällt ein nicht sehr bedeutender Server für durchschnittlich 5 Minuten aus, pro Minute entstehen 50 Euro Schaden. Einmal im Jahr fällt der zentrale Server für durchschnittlich 10 Minuten aus, pro Minute entstehen 9000 Euro Schaden. Welches Szenario ist schlimmer? Monetär gesehen sind beide mit 90.000 Euro Gesamtschaden gleich schlimm. Das widerspricht jedoch der Risikowahrnehmung in der Realität.
- Die Schadenshöhe wird in einem einzigen Wert zusammengefasst. Es bleibt meist unklar, ob ein Best Case, Worst Case oder sonstiges Szenario zugrunde gelegt wurde. Ebenso unklar bleibt, ob berücksichtigt wurde, wann das auslösende, sicherheitsrelevante Ereignis entdeckt wird. Es ist ein großer Unterschied, ob Maßnahmen, die dem Risiko entgegenwirken, schon bei der Entstehung des Schadens ergriffen werden können oder erst dann, wenn der Schaden in vollem Umfang eingetreten ist.

Aus den genannten Gründen sollte eine unkritische Verwendung der Risikoformel nicht erfolgen, sondern es sollte ein Bewusstsein für die genannten Aspekte gegeben sein.

12.4.6.5 Berechnung einer Risikoprioritätsziffer (RPZ)

Die Berechnung einer Risikoprioritätsziffer bietet die Möglichkeit, einige der mit der Risikoformel verbundenen Probleme zu umgehen oder zumindest abzuschwächen. Das Verfahren zur RPZ-Berechnung stammt aus einer Methodik des Qualitätsmanagements, der Failure Mode and Effects Analysis (FMEA), die Ende 1949 in der US Army entstand, über die NASA und die US-Automobilindustrie 1988 in den ISO-9000-Standard einfluss und 1997 von der Connector GmbH für die Durchführung von IT-Risikoanalysen adaptiert wurde. Die RPZ besteht demnach aus drei Faktoren:

- *Auftrittswahrscheinlichkeit $p(A)$*

Die Auftrittswahrscheinlichkeit¹⁸ gibt an, wie groß die Wahrscheinlichkeit ist, dass das sicherheitsrelevante Ereignis und somit das Wirkungsszenario zum Tragen kommt. Dieser Wert wird nicht mathematisch errechnet, sondern eingeschätzt. Er wird auch nicht als stetiger mathematischer Zahlenwert angegeben, sondern als Ganzzahl mit einem Wert zwischen 1 und 10.

Der Wert 1 steht für „sehr unwahrscheinlich“, der Wert 10 für „sehr wahrscheinlich“. In der Praxis verdichtet man oft die sich daraus ergebenden 10 Stufen nochmals zu vier Stufen, indem man nur die Werte 1 (sehr unwahrscheinlich), 4 (eher unwahrscheinlich), 7 (eher wahrscheinlich) und 10 (sehr wahrscheinlich) verwendet.

- *Entdeckungswahrscheinlichkeit $p(E)$*

Ein Faktor, der durch die RPZ neu eingeführt wird, ist die Entdeckungswahrscheinlichkeit. Auch für die Entdeckungswahrscheinlichkeit sind 10 Stufen (Werte 1 bis 10) vorgesehen. Zu beachten ist dabei, dass der Wert 1 für die größte und der Wert 10 für die kleinste Wahrscheinlichkeit für eine Entdeckung steht. Bei der Auftrittswahrscheinlichkeit ist es genau umgekehrt.

Die Entdeckungswahrscheinlichkeit lässt sich auf zweierlei Weise interpretieren: Zum einen als Maß dafür, wann (zu welchem Zeitpunkt) das sicherheitsrelevante Ereignis entdeckt wird, und zum anderen, ob es überhaupt entdeckt wird (unabhängig davon, wann dies geschieht). Ebenso wie bei der Auftrittswahrscheinlichkeit ist eine Verdichtung auf die vier Stufen 1, 4, 7 und 10 möglich. Mögliche Metriken hierfür wären:

Wert	Wahrscheinlichkeit der Entdeckung	Zeitpunkt der Entdeckung
1	sehr wahrscheinlich bis relativ sicher	noch bevor das SRE eintritt (fällt z. B. bei einem Audit oder einer Wartung auf)
4	eher wahrscheinlich	nach dem SRE während des Wirkungsszenarios (z. B. bei entstehendem Brand im Serverraum)
7	eher unwahrscheinlich	erst nach Ablauf des Wirkungsszenarios und Eintritt des Schadens (z. B. nach einer Löschung aufgrund einer Fehlbedienung)
10	sehr unwahrscheinlich bis unmöglich	auch nicht nach Ablauf des Wirkungsszenarios (z. B. wenn sich ein Hacker ohne Spuren zu hinterlassen eine Datei kopiert)

¹⁸ In der ursprünglichen FMEA befindet sich stattdessen der Faktor „Fehlerexistenz“, der bei Risikobetrachtungen jedoch keinen Sinn ergibt.

▪ *Schwere der Auswirkungen S*

Mit diesem Wert wird das Wirkungsszenario eingeschätzt, das infolge des sicherheitsrelevanten Ereignisses entsteht. Positive Auswirkungen werden wiederum nicht betrachtet. Analog zu den beiden anderen Faktoren gibt es hier keinen mathematischen oder monetären Wert, sondern wieder die 10 Stufen von 1 bis 10. Bei dem Wert 1 wären die Auswirkungen kaum spürbar, bei 10 wären sie akut existenzgefährdend.

Alle drei Faktoren werden zur Berechnung der Risikoprioritätsziffer miteinander multipliziert, was zu einem Gesamtwert zwischen 1 (fast überhaupt kein Risiko) und 1000 (äußerst hohes, existenzielles Risiko) führt:



$$\text{RPZ} = p(\text{Auftritt}) \times p(\text{Entdeckung}) \times \text{Schwere der Auswirkungen}$$

In der Praxis wird oft so vorgegangen, dass der gesamte Wertebereich (1–1000) in mehrere Bereiche eingeteilt wird. Diese geben Auskunft darüber, welches Gewicht das Risiko hat und welcher Handlungsbedarf aufgrund des RPZ-Werts gesehen wird. Man ordnet dann alle Risikoszenarien mit ihrem RPZ-Wert diesen Bereichen zu. Eine Möglichkeit für eine solche Einteilung wäre:

RPZ-Wert	Gewicht des Risikos	Handlungsbedarf
1–149	geringfügig	kein oder nur geringer Handlungsbedarf
150–299	erträglich	mäßiger, aber unkritischer Handlungsbedarf
300–499	beträchtlich	größerer, drängender Handlungsbedarf
über 500	schwerwiegend	sofortiger und erheblicher Handlungsbedarf

12.4.7 Risikodarstellung und Risikodokumentation

Den Abschluss der Analysephase innerhalb der IT-Risikoanalyse bildet die Risikodarstellung, die die gesamte Risikosituation, die auch als Risikolage bezeichnet wird, umfasst. Sinn und Zweck der Risikodarstellung ist die Information der Risikoeigentümer (Risk Owner, meist das Management des Bereichs, in dem das Risiko zum Tragen kommen würde; in letzter Instanz ist dies die Unternehmensführung).

12.4.7.1 Risikomatrix und RPZ-Würfel

Die Risikomatrix ist eine grafische Darstellung der Risikosituation in einem zweidimensionalen Koordinatensystem (siehe Abbildung 12.4). Sie orientiert sich an den Faktoren der Risikoformel: Die Eintrittswahrscheinlichkeit $p(E)$ bildet die x-Achse und die Schadenshöhe S die y-Achse.

In dieses Koordinatensystem werden die Risikoszenarien an der Position eingetragen, die den Werten von Eintrittswahrscheinlichkeit und Schadenshöhe des Szenarios entsprechen. Dies geschieht beispielsweise, indem die Szenarien durchnummeriert und die Zahlen in kleinen Kreisen in die Risikomatrix eingetragen werden, so wie es in der obigen Abbildung zu sehen ist. Mit dem Eintragen aller Szenarien entsteht auf diese Weise ein Überblick über die gesamte Risikosituation der jeweiligen Organisation bzw. der jeweiligen IT-Objekte.

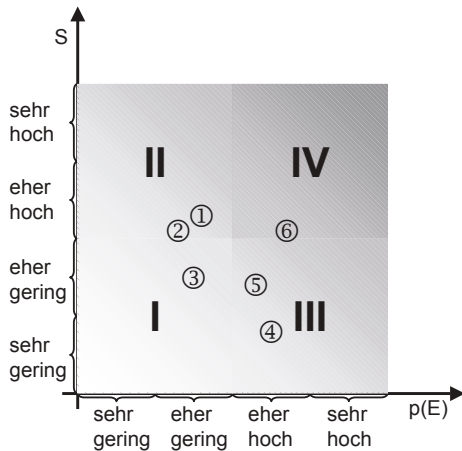


ABBILDUNG 12.4
Risikomatrix

Für die Bewertung der Risikosituation wird die Fläche, die das Koordinatensystem bildet, in vier Quadranten eingeteilt und diesen jeweils adäquate Handlungssituationen (Maßnahmen) zugeordnet:

■ *Quadrant I (Akzeptieren)*

Quadrant I enthält die Risikoszenarien, die ein geringes Risiko darstellen. Sowohl Eintrittswahrscheinlichkeit als auch Schadenshöhe sind gering oder sehr gering. Diese Risiken können getragen werden, ohne dass es zu gravierenden negativen Folgen kommt. Sie werden in der Praxis daher meist akzeptiert. Wichtig ist, diese Risiken trotzdem nicht aus den Augen zu verlieren und sie zu beobachten, da sie sich im Laufe der Zeit in andere Quadranten bewegen können.

■ *Quadrant II (Versichern und Reagieren)*

In Quadrant II befinden sich Risikoszenarien mit einer mäßigen Risikohöhe. Da die Eintrittswahrscheinlichkeit gering bis sehr gering ist, ist es oft nicht sinnvoll, großartige Maßnahmen zu ergreifen, um den Risiken zu begegnen.

Sofern es möglich ist, ist das Versichern dieser Risiken an dieser Stelle eine gute Handlungsoption. Ansonsten bietet es sich an, sich gut auf den Ernstfall vorzubereiten und dann schnell und effektiv zu handeln. Etwas schwieriger wird es, wenn der zu erwartende Schaden unwiederbringliche Verluste enthält. Hier wird man trotz geringer Eintrittswahrscheinlichkeit nicht um Schutzmaßnahmen herumkommen.

■ *Quadrant III (Vorsorgen)*

Bedingt durch die multiplikative Berechnung des Risikos ist die Höhe der Risiken in Quadrant III mit der Höhe der Risiken im Quadranten II vergleichbar, doch sie entsteht auf andere Weise. Die Eintrittswahrscheinlichkeit ist hoch bis sehr hoch, was bedeutet, dass mit dem Eintritt dieser Risiken eine Konfrontation zu erwarten ist. Aus diesem Grund sind hier präventive Maßnahmen (Vorsorgemaßnahmen) sinnvoll.

■ *Quadrant IV (Handeln)*

Quadrant IV ist der Hochrisikobereich. Hier ist ein zeitnahes, entschlossenes Handeln notwendig, um die Risikoszenarien in andere Quadranten zu bringen. Kein Risikoszenario sollte längere Zeit im Quadrant IV bleiben.

Aufgrund der zweidimensionalen Struktur reicht die Risikomatrix nicht mehr aus, wenn die Risikosituation dargestellt werden soll, die sich ergibt, wenn die Risikoszenarien mit Hilfe der Risikoprioritätsziffer (RPZ) festgestellt werden. Da sich die RPZ aus drei Faktoren zusammensetzt, wird die Matrix zu einem Würfel.

Aus den vier Quadranten werden aufgrund der z-Achse nun acht Segmente, wie Abbildung 12.5 zeigt. Das kleinste Risiko ist links-unten-vorne, das größte rechts-oben-hinten.

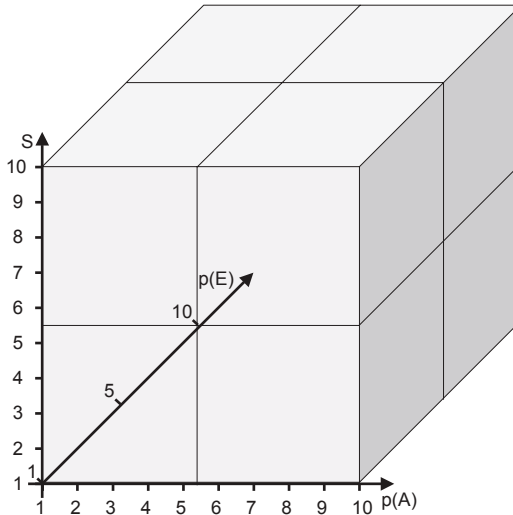


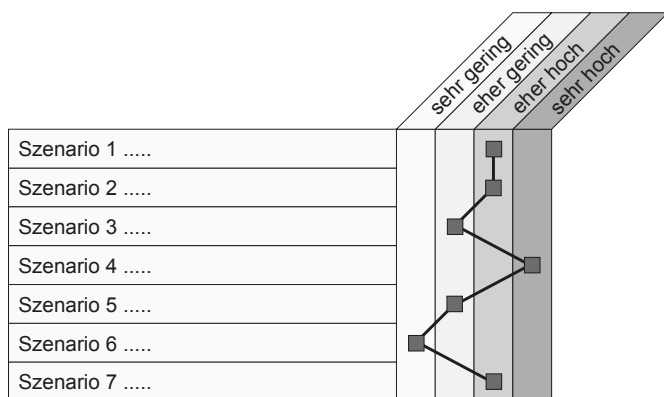
ABBILDUNG 12.5
RPZ-Würfel

Diese Darstellungsform wird vorwiegend bei automatisch erzeugten Darstellungen mit veränderbarer Perspektive verwendet, für die Papierform ist sie weniger geeignet, da die Übersichtlichkeit leidet und zudem ein höherer manueller Aufwand entsteht. In der Praxis werden Auftretis- und Entdeckungswahrscheinlichkeit manchmal auch zu einem einzigen Faktor zusammengezogen, wodurch die Risikomatrix wieder anwendbar wird.

12.4.7.2 Risikoprofil

Ein Risikoprofil besteht aus den in Listenform aufgeführten Risikoszenarien. Für die Angabe der Risikohöhe werden Spalten für die verwendeten Risikostufen bzw. Schadenssummen vorgesehen. Jedem Risikoszenario wird gemäß dem Ergebnis der Risikoformel eine bestimmte Risikostufe bzw. Schadenssumme zugeordnet und durch einen Punkt in der jeweiligen Spalte markiert. Zum Schluss werden die Punkte durch eine Linie miteinander verbunden, wodurch sich ein bestimmter vertikaler Risikoverlauf ergibt (siehe Abbildung 12.6).

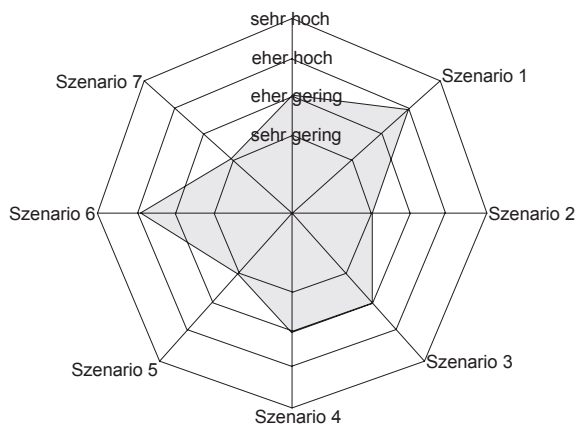
Der Vorteil des Risikoprofils liegt darin, dass Veränderungen sehr gut visualisiert werden können. Es ist sehr einfach möglich, die Situation zu einem bestimmten Zeitpunkt einzutragen und nach einer bestimmten Zeit eine neue Situation zu erfassen (z. B. durch eine andere Farbe). Ebenso ist es möglich, ein SOLL-Profil zu erstellen und nach dem Eintragen des IST-Profiles die Abweichungen zu analysieren.

**ABBILDUNG 12.6**

Risikoprofil

12.4.7.3 Risiko-Netzdiagramm

Das Risiko-Netzdiagramm enthält die gleichen Informationen wie das Risikoprofil, aber in einer etwas anderen Darstellung (siehe Abbildung 12.7). Die Darstellung ähnelt einem Spinnennetz, wie die nachfolgende Abbildung zeigt:

**ABBILDUNG 12.7**

Risiko-Netzdiagramm

Die Risikostufen bzw. Schadenssummen werden von innen nach außen aufgetragen, die Querverbindungen repräsentieren die Risikoszenarien. Analog zum Risikoprofil werden die Werte der Risikoszenarien eingetragen und die Punkte miteinander verbunden. Beim Netzdiagramm entsteht so eine Fläche, die die gesamte Risikosituation abbildet.

Durch das Eintragen mehrerer Flächen übereinander können Abweichungen erkannt werden. Das Risiko-Netzdiagramm ist sehr übersichtlich, eignet sich jedoch nur für eine kleine Anzahl von Risikoszenarien.

12.4.7.4 IT Risk Landscape

Definiert man ein räumliches Koordinatensystem mit IT-Risikobereichen,¹⁹ Betrachtungsräumen und der Risikohöhe und trägt die IT-Risiken in Form von vertikalen Balken ein, entsteht die IT Risk Landscape. Ein Beispiel zeigt die Abbildung 12.8.

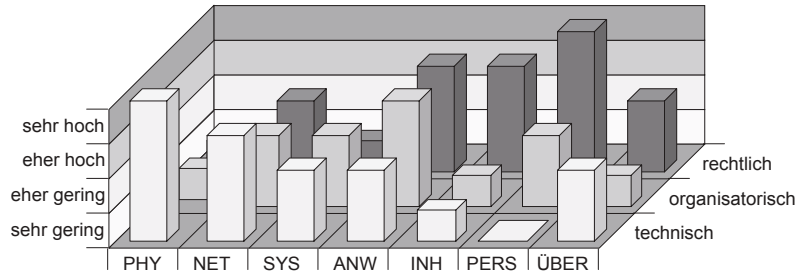


ABBILDUNG 12.8 IT Risk Landscape

Die einzelnen Szenarien sind nun nicht mehr erkennbar, dafür wird ein strukturierter, grafischer Überblick über die gesamte Risikosituation geboten. Kritische Bereiche lassen sich mit der IT Risk Landscape leicht identifizieren. Auch ist ersichtlich, wie homogen die Risikosituation beschaffen ist, d. h. wie groß die Unterschiede der Risikohöhen in den einzelnen Bereichen ausfallen.

12.4.7.5 IT Risk Scorecard

Die Risikodarstellung kann auch mit Hilfe der Balanced Scorecard (BSC) erfolgen (siehe Abbildung 12.9). Dazu werden die vier Perspektiven entsprechend angepasst:

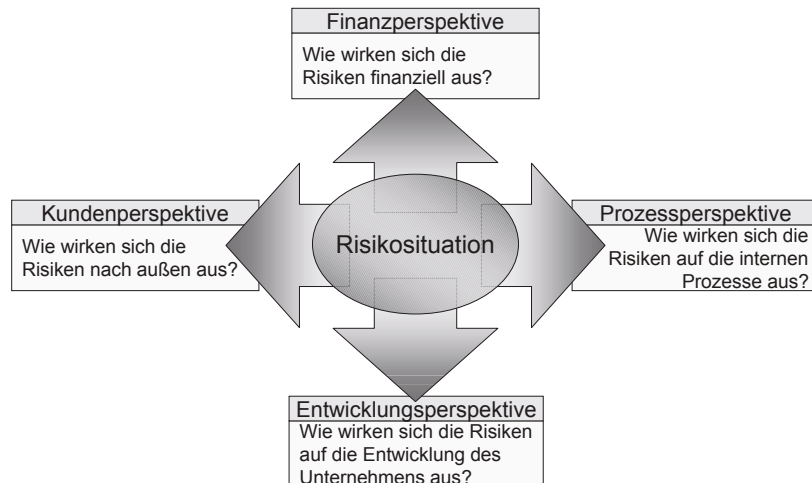


ABBILDUNG 12.9 Balanced Scorecard

¹⁹ Hier: Physik, Netzwerke, Systeme, Anwendungen, Inhalte, Personen und Übergeordnetes

- *Finanzperspektive*

Die Finanzperspektive spiegelt die finanzielle Schadenskategorie wider, d. h. die finanziellen Auswirkungen der Risiken. Die primäre Kennzahl ist die Schadenssumme, die sich ergibt, wenn die Risiken der Risikosituation gemäß ihrer Eintrittswahrscheinlichkeit eintreten.

- *Prozessperspektive*

Die Prozessperspektive spiegelt die geschäftliche Schadenskategorie wider, d. h. die Auswirkungen der Risiken auf die internen Prozesse.

- *Entwicklungsperspektive*

Die Entwicklungsperspektive betrachtet die Auswirkungen des Risikoeintritts auf die Entwicklungschancen des Unternehmens, setzt ergänzend aber auch den Fokus auf die Mitarbeiterinnen und Mitarbeiter des Unternehmens (bzw. der IT-Organisation).

- *Kundenperspektive*

Die Kundenperspektive spiegelt die Schadenskategorie der negativen Außenwirkung wider. Zum einen geht es um die Auswirkungen, die der Eintritt von Risiken für andere (Kunden, Geschäftspartner) besitzt und zum anderen um die Einwirkung auf das Unternehmen als Reaktion der Umwelt auf den Eintritt von Risiken.

12.4.7.6 Risikolagebericht

Die Gesamtheit der Risiken bildet die Risikosituation, die auch als Risikolage bezeichnet wird. Der Risikolagebericht gibt darüber Auskunft, welche Risiken im Unternehmen existieren und wie das Unternehmen dazu steht. Die Erstellung des Risikolageberichts ist dabei nicht nur Eigeninteresse des Unternehmens: Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) verpflichtet Aktiengesellschaften und große Kapitalgesellschaften zur Erstellung eines solchen Risikolageberichts.

Im Vordergrund des Berichts stehen die existenzgefährdenden Risiken des Unternehmens. Sie müssen bekannt sein und gemanagt werden. Daher werden die Risiken zunächst nach der Risikostufe und anschließend nach der Risikokategorie sortiert. Um im Bericht zu vermerken, wie das Unternehmen zu den Risiken steht, ist ein weiterer Schritt notwendig: die Risikoentscheidung.

■ 12.5 Risikoentscheidung

Nach der Risikoerhebung und -darstellung ist die erste und wichtigste Phase des Risikomanagements abgeschlossen. Nun geht es darum, zu beschließen, wie mit den Risiken umgegangen werden soll. Die wichtigsten Fragen, die sich im Zuge der Risikoentscheidung stellen und auf die eine Antwort gefunden werden muss, sind:

- Welche Risiken erscheinen tragbar und welche nicht?
- Welche Risiken sollen akzeptiert werden?
- Welche Risikobewältigungsstrategien sollen für welche Risiken angewendet werden?
- Gegen welche Risiken lässt sich nichts unternehmen?

12.5.1 Risikotragfähigkeit

Bereits zu Beginn dieses Kapitels wurde ausgeführt, dass zielgerichtetes Handeln und Risiko zusammengehören. Das Ziel bzw. der Nutzen des Handelns muss es jedoch auch wert sein, die damit verbundenen Risiken einzugehen. Innerhalb der Risikoentscheidung findet nun genau diese Abwägung statt. Es gilt festzulegen, welches Risiko als angemessen bzw. tragfähig betrachtet wird.

Ein Risiko ist im Allgemeinen dann tragfähig, wenn in einem bestimmten Zeitraum die Schadenserwartung²⁰ um einiges kleiner ist als die Nutzenerwartung. Die Risikotragfähigkeit gibt an, welche Schadenserwartung in diesem Zeitraum mit einer bestimmten Sicherheit nicht überschritten wird.

In der Praxis nähert man sich dem Thema oft dadurch an, dass eine maximal tolerierbare Schadenssumme pro Zeitraum festgesetzt wird. Alle Risiken, die dazu führen, dass die Risikosituation diese Grenze überschreitet, werden als nicht tragbar eingestuft.

12.5.2 Risikobereitschaft

Als weiterer Faktor für die Bestimmung des tragbaren Risikos kommt die Risikobereitschaft der Risikoentscheider hinzu. Sie bewegt sich zwischen

- Risikofreude (Risiken werden als unausweichlich, herausfordernd oder gar spannend empfunden) und
- Risikoaversion (Risiken werden als störend, belastend oder beängstigend empfunden).

Auch andere psychologische Aspekte wie beispielsweise die Einschätzung der Beherrschbarkeit der Risiken fließen mit ein.

12.5.3 Risikoakzeptanz

Eine der zentralen Entscheidungen im Risikoentscheidungsprozess ist die Frage, welche Risiken akzeptiert werden sollen. Akzeptierte Risiken werden so belassen, wie sie sind – sowohl die Risiken selbst als auch deren Eintritt werden bewusst in Kauf genommen.

Die Risikoakzeptanz korrespondiert mit der Frage, ob die Risiken tragbar oder nicht tragbar sind (siehe Abbildung 12.10).

Beispiele:

- Der Vorstand eines Unternehmens, dessen Rechenzentrum in der Einflugschneise eines großen Flughafens liegt, entscheidet per Vorstandsbeschluss, dass das Risiko des Absturzes eines Flugzeuges auf das Rechenzentrum akzeptiert wird (entspricht einem Risiko im Quadrant IV).
- Aufgrund einer Security-Policy-Anforderung für die Verschlüsselung von Kommunikationsverbindungen innerhalb eines Unternehmens werden die Leitungen der Not-Telefone in den Aufzügen verschlüsselt (entspricht einem Risiko im Quadrant I).

²⁰ Unter der Annahme, dass sich die Schäden beheben lassen.

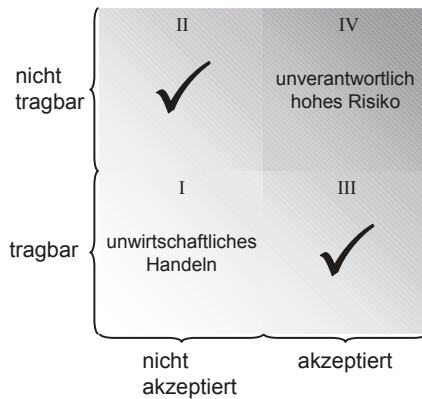


ABBILDUNG 12.10
Akzeptanz vs. Tragbarkeit

12.5.4 Risikopriorisierung

Es ist notwendig, alle nicht akzeptierten Risiken einem Priorisierungsprozess zu unterwerfen. Für die Entscheidung, ob ein Risiko eine hohe Prioritätsstufe erhält, können verschiedene Kriterien zum Einsatz kommen:

- Höhe des Risikos
- Einfachheit bzw. Kosteneffizienz von entgegenwirkenden Maßnahmen
- Wirkungsstärke von entgegenwirkenden Maßnahmen
- Wichtigkeit der von den Risiken betroffenen Komponenten und Bereiche

Mit der Priorisierung steht fest, in welcher Reihenfolge Risikobewältigungsstrategien für die Risiken konzipiert und umgesetzt werden.

12.5.5 Risikobewältigungsstrategien

Alle nicht akzeptierten und priorisierten Risiken müssen bewältigt werden. Dazu gibt es mehrere Möglichkeiten, die im Folgenden erläutert werden.

12.5.5.1 Risikovermeidung bzw. -umgehung

Wie zu Beginn des Kapitels beschrieben wurde, ist ein Risiko mit einem zielgerichteten Handeln verbunden. Eine Möglichkeit zur Risikobewältigung besteht daher darin, das jeweilige Risiko ganz zu vermeiden, indem für das zielgerichtete Handeln eine Variante gewählt wird, bei der das Risiko nicht vorhanden ist.

Beispiel: Stellt sich bei der Planung für ein neues Rechenzentrum im Rahmen einer durchgeführten Risikoanalyse heraus, dass das Risiko einer Überflutung oder Überschwemmung existiert, dann bestünde eine Risikovermeidungsmaßnahme darin, das Rechenzentrum an einem anderen Standort zu planen.

Zu beachten wäre, dass jede Variante mit Risiken verbunden ist. Es geht also darum, eine Variante mit möglichst wenig oder möglichst unkritischen Risiken zu finden, wobei die Wahl

nicht frei ist, da funktionale und betriebswirtschaftliche Aspekte den Entscheidungshorizont einschränken.

12.5.5.2 Risikoeliminierung

Ziel der Risikoeliminierung ist es, einen oder mehrere risikobildende Faktoren zu beseitigen, so dass das Risiko nicht eintreten kann. Im Falle von IT-Risiken geht man in der Regel davon aus, dass an der Existenz des Faktors „Auslöser“ nichts geändert werden kann. Somit konzentrieren sich die Maßnahmen auf die Faktoren „Schwachstelle“ und „Angriffspfad“.

- *Schwachstelle eliminieren*

Mit der Eliminierung der Schwachstelle, die zu einem Risiko führen kann, wird das Risiko an seiner Wurzel gepackt. Eine zentrale Frage dabei ist der Aufwand für die Beseitigung der Schwachstelle.

Beispiele: Unsichere Administrator-Passwörter in einem IT-System (geringer Aufwand), unzureichende Klimatisierung im Serverraum (höherer Aufwand).

Nicht alle Schwachstellen können beseitigt werden. Die Eigenschaft eines Laptops, als kleines, mobiles Gerät leicht transportierbar zu sein, stellt im Hinblick auf eine mögliche Entwendung eine systemimmanente Schwachstelle dar. Die Schwachstelle selbst lässt sich nicht eliminieren, allenfalls kann das Risiko durch zusätzliche Maßnahmen (z. B. Stahlseil-Sicherung) vermindert werden.

- *Angriffspfad eliminieren*

Bei der Eliminierung der Angriffspfade verhindert man, dass der Auslöser (z. B. ein „Hacker“) an die Schwachstellen herankommt und sie ausnutzen kann. Es gibt fast immer mehrere Möglichkeiten für die Eliminierung, die geprüft und über die entschieden werden muss.

Beispiel: Um zu verhindern, dass ein Hacker in ein wichtiges IT-System im Unternehmen eindringt, könnte das IT-System von allen Netzanbindungen nach außen getrennt oder mit Hilfe einer Firewall oder eines VLAN abgeschottet werden. Welche Maßnahme realistisch ist und Nachteile vermeidet, die für das Unternehmen nicht hinnehmbar sind, muss innerhalb der Risikoentscheidung festgelegt werden.

12.5.5.3 Risikoverminderung

Lassen sich die risikobildenden Faktoren nicht eliminieren, dann besteht in den meisten Fällen zumindest die Möglichkeit, mit zusätzlichen Maßnahmen das Risiko zu vermindern. Hierbei gibt es wiederum zwei Varianten:

- *Eintrittswahrscheinlichkeit reduzieren*

Die Maßnahmen zur Reduzierung der Eintrittswahrscheinlichkeit zielen darauf ab, das Eintreten des Risikos zu erschweren. Bei dem Laptop-Beispiel zielt die Maßnahme, den Laptop über ein Stahlseil am Tisch anzuketten, darauf, dass es damit wesentlich erschwert wird, den Laptop zu entwenden. Das Bedrohungsszenario „Hotelangestellter nimmt den Laptop vom Tisch“ wird damit wirksam verhindert, nicht aber die Bedrohung, dass ein mit schwerem Werkzeug (Bolzenschneider) ausgerüsteter Angreifer das Seil kappt und den Laptop entwendet. Daher stellt sich bei allen Maßnahmen immer die Frage: Gegen welche Bedrohungsszenarien will oder muss der Schutz wirksam sein, und wie wahrscheinlich sind sie?

- *Schadenshöhe reduzieren*

Ein etwas anderer Weg wird beschritten, wenn Maßnahmen dazu dienen, die Schadenshöhe zu reduzieren. Dies wird oft getan, wenn es keine Möglichkeit gibt, das Risiko zu eliminie-

ren oder die Eintrittswahrscheinlichkeit zu reduzieren. Im Laptop-Beispiel wäre es möglich, dass der größte Schaden dadurch entsteht, dass die auf dem Laptop gespeicherten Daten durch die Entwendung nicht mehr zur Verfügung stehen.²¹ Eine schadensmindernde Maßnahme wäre, die Daten zusätzlich auf einem USB-Stick, den der Eigentümer ständig bei sich trägt, zu speichern. Das Risiko der Entwendung bliebe mit unverminderter Wahrscheinlichkeit bestehen, der Schaden wäre aber auf den Verlust der Laptop-Hardware begrenzt.

Bei Risiken, die sehr unwahrscheinlich sind, aber ein hohes Schadenpotenzial besitzen, ist die reaktive Schadensbegrenzung oft der einzige Weg. Man bereitet sich intensiv auf den Ernstfall vor, um dann schnell und effektiv zu handeln und den Schaden sofort zu begrenzen.

12.5.5.4 Risikoabwälzung

Bisher wurde im Laptop-Beispiel immer davon ausgegangen, dass der Eigentümer das Risiko zu tragen hat, doch ist das nicht zwingend der Fall. Es ist auch möglich, das Risiko auf einen Dritten zu übertragen. In diesem Fall spricht man von einem abgewälzten Risiko.

Die bekannteste Form der Abwälzung ist das Versichern der Risiken, was sich immer dann anbietet, wenn ein hoher Schaden zu erwarten ist, der Eintritt des Schadens aber relativ unwahrscheinlich erscheint. In diesem Fall sind aufwändige Maßnahmen aufgrund der geringen Eintrittswahrscheinlichkeit nicht sinnvoll, das Risiko kann aufgrund des hohen Schadenspotenzials aber nicht ignoriert werden.

Eine Versicherung ist immer nur ein finanzieller Ausgleich für einen entstandenen Schaden. Bezieht sich das Risiko auf unwiederbringliche Objekte oder drohen immaterielle Schäden, nützt eine Versicherung nur sehr bedingt. Zudem schließen Versicherungsgesellschaften Risiken aus, die von ihnen wirtschaftlich nicht gedeckt werden können.

Im Laptop-Beispiel ist die Laptop-Hardware mit einer IT-Versicherung gegen Diebstahl versicherbar, nicht jedoch die Daten auf dem Laptop. Der Ausfall eines Seminars infolge des Diebstahls lässt sich wiederum in die Versicherung einbeziehen.

12.5.6 Restrisikodeklaration

Die nach der Anwendung der Risikobewältigungsstrategien verbliebenen Risiken bezeichnet man als **Restrisiken** (in Abbildung 12.11 mit RR gekennzeichnet).

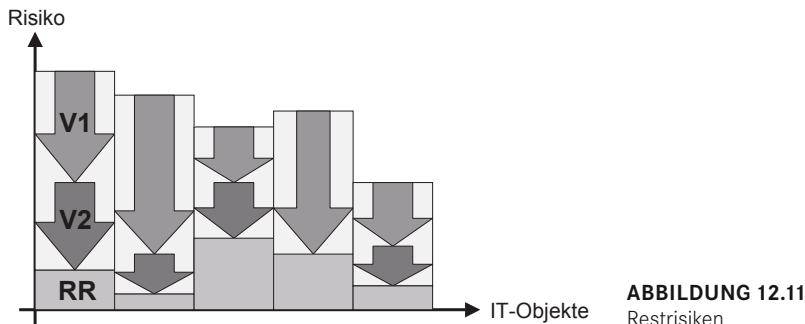


ABBILDUNG 12.11
Restrisiken

²¹ Wir gehen davon aus, dass die Daten nicht vertraulich sind.

Abbildung 12.11 zeigt, wie das für ein IT-Objekt bestehende Risiko zunächst durch technische oder organisatorische Maßnahmen in der Infrastruktur vermindert wird (mit V1 in der Abbildung gekennzeichnete Maßnahmen wie unternehmensweiter Netzwerksicherheit oder allgemeinem Virenschutz). Für das verbliebene Risiko wird ein spezielles Sicherheitskonzept mit risikovermindernden Maßnahmen erstellt (mit V2 in der Abbildung gekennzeichnete Maßnahmen, z.B. eine Stahlseilsicherung für Laptops).

Für die Behandlung von Restrisiken gibt es zwei Möglichkeiten:

- Entweder ist es nicht möglich, ihnen zu begegnen, oder
- es wird innerhalb der Risikoentscheidung beschlossen, ihnen nicht zu begegnen.

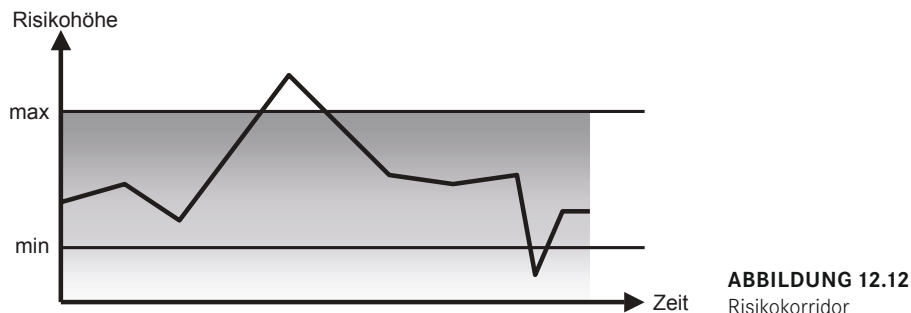
In der Restrisikodeklaration werden diese Restrisiken aufgeführt. Neben der Dokumentation der Restrisiken dient die Restrisikodeklaration auch der Risikoübernahme, d.h. die Risiken werden einer verantwortlichen Stelle (Risk Owner) zugeordnet und von ihr übernommen.²²

■ 12.6 IT-Risikosituation managen

Nachdem die Risiken erhoben sind und die Risikoentscheidung durchlaufen wurde, gilt es die gesamte Risikosituation zu managen. Je nach definiertem Scope kann das die Risikosituation eines Servers, eines Geschäftsprozesses, eines Standorts oder eines gesamten Unternehmens sein.

12.6.1 Risikokorridor

Ziel des IT-Risikomanagements ist es, die Risikosituation so zu steuern, dass sie sich innerhalb eines definierten Bereichs bewegt. Dieser Bereich wird als Risikokorridor bezeichnet (siehe Abbildung 12.12).



Der Maximalwert gibt an, wie groß das Gesamtrisiko höchstens werden darf (z.B. maximale Schadenssumme). Der Minimalwert zeigt entsprechend das kleinste vertretbare Gesamtrisiko

²² In der Praxis wird die Übernahme in der Restrisikodeklaration auch per Unterschrift bestätigt.

an. Während der erste Wert leicht nachvollziehbar ist, scheint der zweite Wert unlogisch zu sein. Ist es nicht so, dass die Lage umso besser ist, je kleiner das Gesamtrisiko ausfällt, und ist daher der Idealzustand nicht eine Risikohöhe von null?

Nun, in der Theorie schon. In der Praxis bedeutet eine Reduzierung der Risikohöhe aber Aufwand und somit Kosten, wie Abbildung 12.13 zeigt:

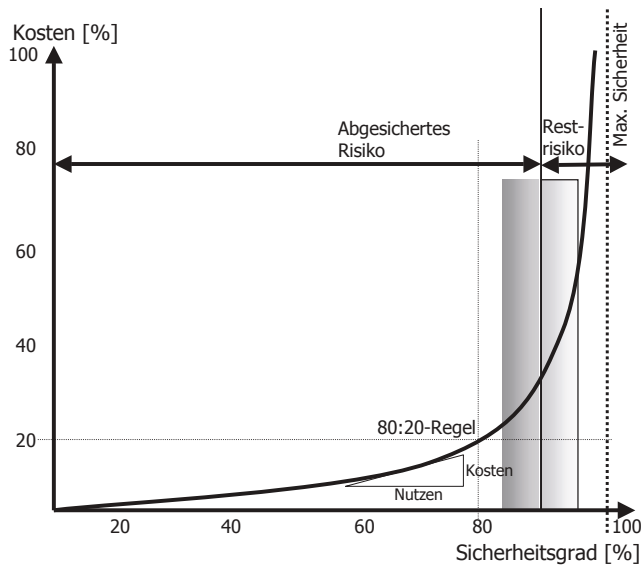


ABBILDUNG 12.13
Risikokorridor und Sicherheitsaufwand

Die Aufwandskurve steigt bei zunehmendem Sicherheitsgrad exponentiell an. Das Nutzen/Kosten-Verhältnis wird so bei steigendem Sicherheitsgrad nicht nur immer schlechter, sondern „immer gravierender schlecht“. In der Abbildung ist der Risikokorridor um 90° gedreht eingezeichnet. Der Aufwand, der betrieben werden muss, um im Risikokorridor bis zum Minimalwert zu gelangen (rechte Flanke des Korridors), ist bereits enorm. Das erklärt den Minimalwert: Es ist unwirtschaftlich, die Risikohöhe nach Erreichen des Minimalwerts noch weiter zu reduzieren.

Die Kunst ist zunächst, festzustellen, an welcher Stelle im Risikokorridor sich die aktuelle Risikosituation befindet. Hierfür gibt es unterschiedliche Vorgehensweisen:

- Für die Risikoszenarien werden mit Hilfe der Risikoformel Schadenswerte berechnet und die Gesamtheit der Schadenswerte über statistische Verfahren zu einem Punkt verdichtet.
- Es wird ein Anforderungskatalog aufgestellt. Sind alle Anforderungen erfüllt, entspricht das dem Minimalwert im Korridor. Die Anzahl der erfüllten Anforderungen bestimmt, wo sich die Situation im Korridor befindet.
- Es werden Risikoindikatoren definiert (z.B. die Anzahl der Tage seit dem letzten Update des Virenschanners). Für jeden Indikator wird eine Metrik erstellt (z.B. letztes Update in dieser Stunde = Minimalwert, 14 Tage = Maximalwert im Korridor). Die Gesamtheit der aktuellen Werte wird dann über statistische Verfahren zu einem Punkt verdichtet.

Es muss festgelegt werden, wie zeitnah der Risikokorridor gesteuert werden muss. Das bestimmt, wie oft die Risikosituation zu erheben ist.

12.6.2 Risikofrüherkennung

Je früher erkannt wird, dass das Eintreten eines Risikos bevorsteht, desto besser kann man reagieren und desto geringer fällt in der Regel der Schaden aus. Die daraus resultierende Wichtigkeit einer Risikofrüherkennung hat auch der Gesetzgeber erkannt und in das KonTraG die Verpflichtung zur Einrichtung einer Risikofrüherkennung existenzgefährdender Risiken aufgenommen.

Für die Früherkennung wird die Tatsache genutzt, dass sich der Eintritt bei vielen Risiken ankündigt (avisierende Risiken) oder der Eintritt aufgrund von Risikoindikatoren absehbar ist (schleichende Risiken).

Beispiel: Aufgrund der Tatsache, dass Festplatten über feinmechanische Komponenten verfügen, existiert das schleichende Risiko eines Hardware-Defekts. Je intensiver die Festplatte genutzt wird und je älter die Festplatte ist, desto größer wird das Risiko. Für die Früherkennung würden diese Daten innerhalb einer Festplattenverwaltung geführt und eine Warnung ausgegeben, wenn vordefinierte Schwellenwerte überschritten werden.

Hardware-Defekte kündigen sich in vielen Fällen vor dem Eintritt durch Schwankungen der Zugriffszeit, fehlerhafte Zugriffe, mehrfaches Wiederanlaufen der Platte oder ungewöhnliche Geräusche an. Anhand solcher Indikatoren erkennt das Früherkennungssystem, dass der Eintritt bevorsteht, und gibt eine entsprechende Warnung aus.

12.6.3 IT-Risikomanagementprozess

Aufgrund der hohen Dynamik der Informationstechnik infolge des technischen Fortschritts, des Entstehens und Bekanntwerdens neuer Schwachstellen und fast ständiger IT-Architekturveränderungen reicht es nicht aus, die Risiken nur einmal zu erheben. Es ist vielmehr notwendig, die Risikosituation kontinuierlich zu beobachten, Änderungen zu berücksichtigen, durchgeführte Maßnahmen auf ihre Wirksamkeit zu prüfen und Verbesserungen zu planen. Der IT-Risikomanagementprozess ist ein Managementrahmen für alle diese Aufgaben.

In der Praxis durchgesetzt hat sich der Vier-Phasen-Managementkreislauf, den es in zwei Ausprägungen gibt:

- *Top-down-Kreislauf (vom Soll zum Ist)*

Der bekannteste Top-down-Kreislauf ist der PDCA-Zyklus von Edward Demming, der die Phasen „Plan“ (Ziele setzen und Maßnahmen planen), „Do“ (Maßnahmen umsetzen), „Check“ (Maßnahmen überprüfen) und „Act“ (aufgrund der Überprüfung handeln) vorsieht.

- *Bottom-up-Kreislauf (vom Ist zum Soll)*

Die Phasen des Bottom-up-Kreislaufs sind: Analysieren (Aufnehmen und Bewerten), Entscheiden, Konzipieren (von Maßnahmen), Implementieren (der Maßnahmen).

Wie der Name Kreislauf schon andeutet, wiederholen sich die vier Phasen immer wieder. Beim PDCA-Zyklus werden nach der Anpassung der Maßnahmen wieder neue Ziele definiert, beim Bottom-up-Kreislauf wird nach der Implementierung der Maßnahmen wieder die neu entstandene Situation analysiert.

Für das IT-Risikomanagement eignet sich der Bottom-up-Kreislauf, weil auch die Risikoanalyse selbst nach dem Bottom-up-Prinzip arbeitet.

Phase 1: Analysieren

In der Phase „Analysieren“ findet sich die Risikoanalyse, die eine bestehende Situation aufnimmt und bewertet. Hat sich die Situation seit der letzten Risikoanalyse nur in bestimmten Bereichen verändert, so kann die Aufnahme auf diese Bereiche beschränkt werden. Eine weitere Möglichkeit besteht darin, nur verkürzte Risikoanalysen durchzuführen.

Phase 2: Entscheiden

In der Phase „Entscheiden“ befindet sich die Risikoentscheidung. Durch sie ergibt sich der mit Maßnahmen abzudeckende Handlungsbedarf.

Phase 3: Konzipieren

In der dritten Phase werden dem Handlungsbedarf entsprechende Maßnahmen geplant. Dabei stehen folgende Fragen im Vordergrund:

- *Gegen was oder wen sollen die Objekte geschützt werden?*
Einen vollkommenen Schutz gibt es nicht. Es ist demnach immer die Frage, wie stark der Schutz ausgeprägt sein muss. In Abschnitt 12.6.1 wurde gezeigt, dass ein stärkerer Schutz höhere Kosten bedeutet, daher muss genau ausgelotet werden, wie hoch man die Hürde legt, die ein Angreifer überwinden muss.
Hier hilft die Top-down-Methodik der Schutzbedarfsanalyse, so wie sie in Kapitel 11 beschrieben ist.
- *Was soll die Maßnahme bewirken?*
Entdecken: Die Maßnahme sorgt dafür, dass ein für das Objekt sicherheitsrelevantes Ereignis entdeckt und ggf. erfasst wird, die Maßnahme unterbindet das Ereignis aber nicht. Beispiele: Zugriffsprotokollierung oder Videoüberwachung.
Melden: Die Maßnahme sorgt dafür, dass eine festgelegte Stelle oder Person über das entdeckte, sicherheitsrelevante Ereignis informiert wird. Beispiel: Alarmedung eines Intrusion Detection Systems an den Administrator.
Stören: Die Maßnahme sorgt dafür, dass der Auslöser (z.B. Angreifer) in seiner Aktivität gehemmt bzw. gestört wird. Beispiel: Alarmanlage mit schrillum Alarmton.
Begrenzen: Die Maßnahme sorgt dafür, dass die Auswirkungen reduziert werden. Beispiel: Ein Identity Management System wird nach 50 automatisiert ausgelösten Löschungen gestoppt, um eine Massenlöschung aufgrund eines Fehlers zu verhindern.
Verhindern: Die Maßnahme sorgt dafür, dass das sicherheitsrelevante Ereignis nicht eintreten kann. Beispiel: Die unbefugte Benutzung eines Terminals wird durch eine biometrische Authentifizierung abgewendet.
- *Auf welcher Ebene soll der Schutz realisiert werden?*
Um zu verhindern, dass ein Unbefugter einen PC benutzt, kann ich eine softwarebasierte Anmeldung realisieren, ich kann aber auch die Stromzufuhr durch einen Schlüsselschalter sperren oder den Raum abschließen.
Ob eine Maßnahme auf einer bestimmten Ebene durchführbar, sinnvoll und praxistauglich ist, hängt von der jeweiligen Situation „vor Ort“ ab. Ein beliebter Fehler besteht darin, Maßnahmen zu definieren, ohne die jeweilige Situation genau zu kennen. So kam es schon vor, dass bewegliche Kameras in explosionsgeschützten Räumen gefordert wurden oder Chipkartenleser in Thin-Clients, obwohl das zu diesem Zeitpunkt technisch gar nicht möglich war.

Phase 4: Implementieren

In der vierten Phase werden die Maßnahmen umgesetzt. Dabei wird zwischen technischer und organisatorischer Implementierung unterschieden. In vielen Fällen besitzt eine Maßnahme sowohl technische als auch organisatorische Aspekte.

Beispiel: Installation von Handfeuerlöschern. Die technische Implementierung ist das Anbringen der Feuerlöscher, die organisatorische Implementierung die Dokumentation der vorhandenen Feuerlöscher, der Wartungsplan und die Schulung der Mitarbeiter hinsichtlich der Benutzung.

Durch die Implementierung der Maßnahmen verändert sich die Risikosituation, was ja beabsichtigt ist. Daher startet nun wieder Phase 1, in der überprüft wird, ob die Maßnahmen die gewünschte Wirkung erzielen und wie die neu entstandene Risikosituation zu bewerten ist.



Das Wichtigste – zusammengefasst

- **Nehmen Sie für Ihr Unternehmen eine Einordnung zum IT-Risikomanagement vor!**

Ein grundlegendes Verständnis zum Thema „Risikomanagement“ und ein entsprechendes Risikobewusstsein ist auf allen Ebenen einer Unternehmensorganisation wesentlich. Die letztendliche Verantwortung liegt gerade bei diesem Managementthema – und das ist rechtlich vielfach dokumentiert – bei der Unternehmensführung.

- **Nutzen Sie für das Aufspüren von Schwachstellen externe Informationsdienste und Security-Tools!**

Mit automatisierten Security-Checks, die oft vollständiger sind als manuelle, sparen Sie Zeit.

- **Berücksichtigen Sie bei der Risikominimierung neben den Schwachstellen immer auch die Angriffspfade!**

Nicht alle Schwachstellen müssen oder können beseitigt werden, daher sollte stets geprüft werden, ob das Risiko nicht über die Angriffspfade gemindert werden kann.

- **Vorsicht bei der Verwendung der Risikoformel!**

Versuchen Sie nicht, die Risiken exakt berechnen zu wollen, arbeiten Sie lieber mit Risikoklassen.

- **Vergessen Sie bei der Schadensbetrachtung nicht die Entdeckungswahrscheinlichkeit!**

Die Schadenshöhe steigt in der Regel bei unentdeckten Risikoereignissen an, daher ist es für die Beurteilung der Risiken wichtig, zu identifizieren, ob das Risikoereignis überhaupt entdeckt werden kann und wenn ja, wann es entdeckt wird.

- **Begreifen Sie Risikomanagement als kontinuierlichen Prozess!**

Steuern Sie die Risikosituation mit dem Risikokorridor in einem Vier-Phasen-Managementkreislauf. Gegebenenfalls kann auch hier zur Unterstützung ein spezielles Risikomanagement-Tool zum Einsatz kommen.

■ 12.7 Literatur

- [Bos08] *Bostrom, A.*: Risk assessment, modeling and decision support. Springer, 2008
- [Hil08] *Hildebrand, K.*: Compliance & Risk Management. dpunkt, 2008
- [Kön11] *Königs, H.-P.*: IT-Risiko-Management mit System. Vieweg-Teubner, 2011
- [Pro08] *Prokein, O.*: IT-Risikomanagement. Gabler, 2008
- [Schm06] *Schmidt, K.*: Der IT Security Manager. Hanser, 2006
- [Sei06] *Seibold, H.*: IT-Risikomanagement. Oldenbourg, 2006
- [Stal08] *Stallinger, M.*: IT-Governance im Kontext Risikomanagement. VDM, 2008
- [Thie08] *Thies, K.*: Management operationaler IT- und Prozessrisiken. Springer, 2008
- [Tiet11] *Tietjen, T.*: FMEA-Praxis. Hanser, 2011
- [Wolf09] *Wolf, K.*: Risikomanagement und KonTraG. Gabler, 2009

Michael Klotz



Fragen, die in diesem Kapitel beantwortet werden:

- Was bedeutet der Begriff „Compliance“ bzw. „compliant sein“?
- Woher kommen die Vorgaben, die zu beachten sind, wenn ein Unternehmen compliant sein will?
- Was ist unter IT-Compliance zu verstehen, und wie stellt sich die „Legal IT-Compliance“ als Kern der IT-Compliance dar?
- Wie ordnet sich IT-Compliance in das IT-Governance Framework „COBIT“ ein?
- Was sind Ziele und Nutzen von IT-Compliance?
- Aus welchen Elementen setzt sich ein Managementsystem für IT-Compliance zusammen?
- Aus welchen Aufgabenbereichen setzt sich ein allgemeiner IT-Compliance-Prozess zusammen, und wie lässt sich IT-Compliance in der Aufbauorganisation verankern?

■ 13.1 Begriff und Aktualität von Compliance

Wegen Gesetzesverstößen in den Bereichen des Kartell- oder Produktrechts werden Bußgelder in Millionenhöhe verhängt. Vorstände müssen wegen Bestechung, schwarzen Kassen und anderen illegalen Praktiken ihren Posten räumen. Auch wird immer wieder von verlorenen oder gestohlenen Daten berichtet, die mitunter Gegenstand von Erpressungsversuchen sind. Zudem halten Bespitzelungsskandale Vorstände und Aufsichtsräte, aber natürlich auch die Betroffenen und die gesamte Öffentlichkeit in Atem. Mit der viel beschworenen verantwortungsvollen Unternehmensführung scheint es allzu häufig nicht gut bestellt zu sein. So verwundert es nicht, dass (mangelhafte) Compliance seit einiger Zeit nicht nur Tagungsthema und Gegenstand von Fachpublikationen ist, sondern oft sogar den Weg in die Tagespresse findet.

Wie kommt es dazu? Als Ursache dieser Entwicklung beklagen viele Unternehmen eine ständig zunehmende Zahl an Regularien, d. h. Vorgaben aus Gesetzen, Verordnungen, Normen,

Standards usw. Für Unternehmen aller Größenordnungen bedeutet dies wachsende Risiken aus potenziellen Regelverstößen – die sich allerdings schon allein deswegen ergeben können, weil ein Überblick mittlerweile kaum noch möglich ist. Die Vermeidung derartiger Risiken durch Sicherstellung der Befolgung von Vorgaben ist Zielsetzung der Corporate Compliance, im IT-Bereich speziell der IT-Compliance.

13.1.1 Begriffliche Grundlagen

Compliance ist ein noch recht junges Teilgebiet des Managements. Schon deshalb ist die Bedeutung von „Compliance“ nicht leicht zu fassen. Der Begriff stammt aus der angelsächsischen Rechtsterminologie (vgl. [Hau10], S. 2) und muss erst in die von Wissenschaft und Praxis verwendete Fachterminologie eingeordnet werden. Ohne eine derartige systematische Einordnung droht eine „Aufladung“ des Compliance-Begriffs mit vorschnellen Identifizierungen und beliebigen, im Zweifelsfall schwammigen Bezügen zur Unternehmenswirklichkeit. Die Folge sind Unsicherheit und mangelnde Orientierung, schlimmstenfalls auch Fehlallokationen von Managementkapazität und Finanzmitteln. Es ist also nötig, sich mit der Begrifflichkeit auseinanderzusetzen, um auf der Basis eines geklärten und gemeinsamen Verständnisses die erforderlichen Maßnahmen ergreifen zu können. Dabei lassen sich in Bezug auf Compliance einige Grundhaltungen identifizieren (vgl. ebd., S. 3f.):

- Das allgemeine Empfinden von Führungsverantwortlichen ist das der „Überregulierung“, also der ausufernden Vorgaben durch Rechtsnormen, aber auch durch Vorgaben von Regulierungs- und Aufsichtsbehörden.
- Non-Compliance, also das Vorliegen von Verstößen gegen Compliance-Vorgaben, wird als wirtschaftliches Risiko für das Unternehmen und die das Unternehmen als Organe vertretenden Personen der Unternehmensleitung gesehen. Gerade die persönliche Betroffenheit der verantwortlichen Führungskräfte ist ein zentraler Treiber von Compliance-Maßnahmen.
- Die Risikosichtweise erfordert bewusste Entscheidungen darüber, welche Compliance-Risiken akzeptabel sind und welche Compliance-Risiken im Rahmen eines Risikomanagements gesteuert werden müssen.
- Das Steuern von Compliance-Risiken erfordert ein entsprechendes Compliance-Managementsystem, das dem Eintritt von Schadensfällen durch Non-Compliance entgegenwirken soll.

In einem allgemeinen, grundlegenden Verständnis handelt ein Unternehmen dann „compliant“, wenn es in seiner Geschäftstätigkeit bestimmte relevante Vorgaben befolgt. Neben „Befolgung“ werden auch Begriffe wie „Übereinstimmung“, „Einhaltung“, „Konformität“, „Erfüllung“ oder „Entsprechung“ verwendet. Welche Vorgaben relevant sind, ist einerseits unternehmensextern vorgegeben (wie beispielsweise bei Gesetzen), andererseits selbst gewählt (z. B. bei unternehmensinternen Richtlinien). Dementsprechend lässt sich der Compliance-Begriff wie folgt fassen:



Compliance liegt vor, wenn alle für das Unternehmen verbindlich vorgegebenen bzw. als verbindlich akzeptierten Vorgaben nachweislich eingehalten werden.

Dort, wo ein Unternehmen nicht compliant ist, liegt ein Compliance-Verstoß, häufig auch als „Non-Compliance“ bezeichnet, vor. Sehen wir uns die Compliance-Definition genauer an.

1. Das Satzglied „Compliance liegt vor“ bezeichnet einen Zustand (und keine Struktur, keinen Prozess, kein Konzept o.Ä.), wobei natürlich adäquate Strukturen eingerichtet und Prozesse gestaltet werden müssen, um Compliance zu erreichen. Dieser Zustand stellt sich nicht von selbst ein, sondern ist durch geeignete Maßnahmen anzustreben. Damit wird deutlich, dass es sich bei Compliance um ein Ziel (einen Zielzustand) handelt. Diesem Ziel nähert man sich mal mehr, mal weniger – vor allem, weil Rechtsnormen und sonstige Regelungen einer kontinuierlichen Veränderung unterliegen und in ihrer Zahl tendenziell steigen (was zu der von Unternehmen beklagten Überregulierung führt). Diese Erkenntnis sollte aber nicht entmutigend wirken – Compliance ist vielmehr als „regulatives Ideal“ anzusehen, das in seiner Gesamtheit nie finalistisch erreichbar ist und dem sich Unternehmen insofern nur asymptotisch nähern können. Damit bezeichnet Compliance einen Zustand, der immer „noch nicht ist“, aber als „moving target“ auch nie komplett eintreten wird (was höchstwahrscheinlich auch unwirtschaftlich wäre). Jeder Zustand von Compliance ist somit notwendig mit einem gewissen Ausmaß an Non-Compliance verbunden. Hieraus folgt für die Compliance-Verantwortlichen, dass sie Unsicherheit und ein entsprechendes Risiko akzeptieren müssen. Die Vorgaben einzelner Regelwerke können aber – und müssen teilweise – sehr wohl vollständig eingehalten werden. Hierzu ist es erforderlich zu klären, welche Regelwerke entsprechend zu priorisieren sind.
2. Die Satzglieder „nachweislich“ und „eingehalten werden“ verweisen darauf, dass eine Zielerreichung nicht nur zu postulieren, sondern auch nachzuweisen ist. Dies ist vor allem dann der Fall, wenn Dritte berechnete Interessen am Vorliegen von Compliance geltend machen – ein pures Versprechen des Einhaltens von Vorgaben reicht dann nicht aus. Die nicht nur potenzielle, sondern faktische Nachweisbarkeit (z. B. mittels archivierter Dokumente, Verfahrensanweisungen, Prüfprotokollen, Prozessbeschreibungen, Kontrollbelegen) ist unternehmensintern gegenüber Aufsichtsorganen und Prüfungsinstitutionen (z. B. Wirtschaftsprüfer, interne Revision) notwendig, aber auch, um sich unternehmensextern im Verdachts- und Streitfall exkulpieren zu können – wie folgendes Beispiel zeigt.

Beispiel:

Das Landgericht München I gab in seinem Urteil vom 5. April 2007 (Az. 5 HKO 15964/06) einer Anfechtungsklage, mit der der Hauptversammlungsbeschluss zur Entlastung des Vorstands für nichtig erklärt werden sollte, statt. Bei dem betreffenden Elektronik-Großhandelsunternehmen war nach Einschätzung des den Jahresabschluss testierenden Wirtschaftsprüfers zwar ein Überwachungssystem zur Erkennung bestandsgefährdender Entwicklungen eingerichtet, es mangelte aber an einer hinreichenden formellen Dokumentation desselben. Diese Dokumentation, die auch die wesentliche Grundlage ist, um ein Risikomanagementsystem im Unternehmen zu kommunizieren, sah das Gericht als zentrale Aufgabe des Vorstandes an und stufte die unterbliebene Dokumentation als wesentlichen Verstoß gegen § 91 Abs. 2 AktG ein.

§ 91 AktG

(2) Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.

Die Erfüllung von Dokumentationspflichten ist jedoch nicht nur von Gesetzes wegen erforderlich. Eine vollständige und qualitativ hochwertige Dokumentation ist Voraussetzung, um den zentralen Managementanforderungen der kaufmännischen Sorgfalt, der Transparenz und Kontrolle zu genügen, ohne die eine den Erwartungen und Anforderungen der verschiedenen Stakeholder (Anteilseigner, Abschlussprüfer, Analysten etc.) entsprechende Unternehmensführung heute nicht mehr denkbar ist.

- Die oben genannte Compliance-Definition adressiert ein Unternehmen und damit sein gesetzlich vorgesehenes Vertretungsorgan, d.h. den Vorstand, die Geschäftsführung, den geschäftsführenden Inhaber. Compliance liegt somit im Verantwortungsbereich der Unternehmensleitung und muss insofern Gegenstand des Führungssystems eines Unternehmens sein. Konkret bedeutet dies für die Unternehmensleitung, dass das Erreichen von Compliance eine Zielsetzung der Einrichtung und Nutzung eines Internen Kontrollsystems (IKS) sowie interner und externer Prüfungen darstellen muss. Hieraus resultiert die Notwendigkeit, dass sich die Unternehmensleitung zu Compliance verpflichtet und als treibende Kraft agiert. Dies zeigt sich beispielsweise in einem unmissverständlichen Bekenntnis zu Compliance, verbunden mit einer konsequenten Sanktionierung von Verstößen, siehe Abbildung 13.1.

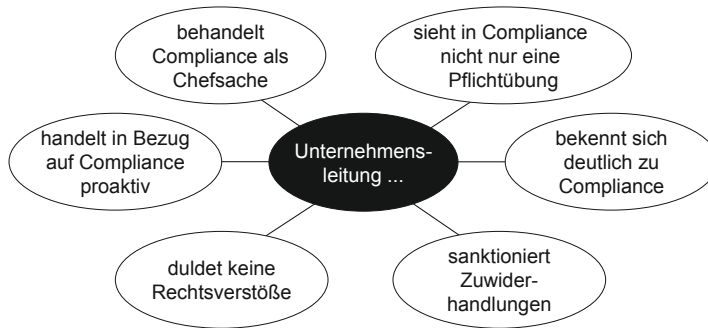


ABBILDUNG 13.1
Commitment der
Unternehmensleitung



Praxistipp: Ohne das Commitment der Unternehmensleitung geht es nicht.

Der wesentliche Erfolgsfaktor für Compliance ist der Rückhalt und das aktive Eintreten der Unternehmensleitung. Diese muss die Bedeutung von Compliance für das Unternehmen anerkennen. Das sichtbarste Zeichen hierfür ist, wenn die Verantwortung für Compliance einem Mitglied des Top-Managements übertragen wird. Gleiches gilt auf der Ebene der Unternehmens-IT, auf der die IT-Leitung bzw. der Chief Information Officer (CIO) IT-Compliance als ihre bzw. seine Verantwortung (im doppelten Sinne) wahrnehmen muss.

- Das vierte und zentrale Element der Compliance-Definition bilden die einzuhaltenden Vorgaben. Sofern sie aus Gesetzen stammen, bedeutet dies, dass sich Unternehmen an geltendes Recht zu halten haben – was eigentlich eine Selbstverständlichkeit sein sollte. Neben Gesetzen, oder besser Rechtsnormen, hat ein Unternehmen jedoch auch weitere Vorgaben aus unterschiedlichen Regelwerken zu beachten (siehe Abbildung 13.2). Diese erstrecken sich auf Verträge, die die Gruppe der rechtlichen Vorgaben ergänzen, sowie auf unterneh-

mensinterne und -externe Regelwerke. Die unternehmensexternen Regelwerke beinhalten vor allem Normen und Standards, die für ein Unternehmen ebenso von existenzieller Bedeutung sein können wie die Befolgung gesetzlicher Vorgaben. Dies gilt vor allem für Standards, die sich in einer Branche durchgesetzt haben und hier eine grundlegende Voraussetzung für Marktzutritt und Geschäftstätigkeit darstellen (z.B. Zertifizierungen). Interne Regelwerke (Richtlinien, Hausstandards etc.) dienen in vielen Fällen dazu, die Beachtung der Anforderungen aller anderen Regelwerke sicherzustellen, indem sie konkrete Handlungsanweisungen für die Organisationsmitglieder vorgeben (nach [KI09a], S. 4).

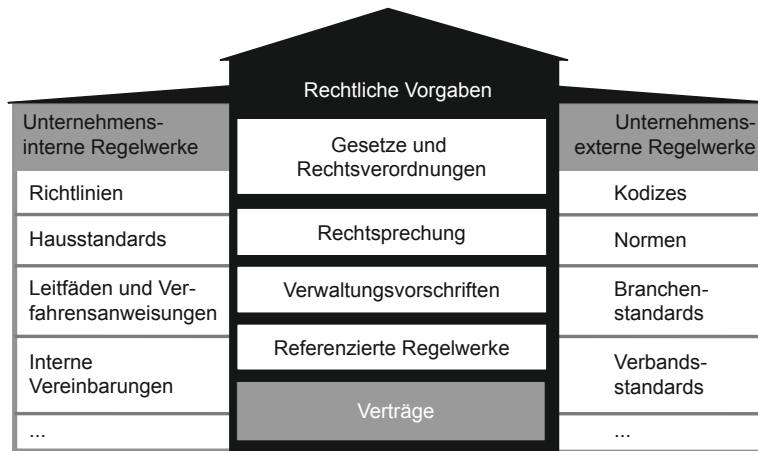


ABBILDUNG 13.2 Quellen von Compliance-Vorgaben – das „House of Compliance“

13.1.2 Beispiele von Compliance-Verstößen

Zahlreiche Beispiele der jüngsten Vergangenheit, in denen sich Unternehmen nicht an (vor allem gesetzliche) Vorgaben gehalten haben und damit eben „nicht compliant“ waren, verdeutlichen die generelle Relevanz der Compliance-Thematik.

Beispiele:

- Im November 2006 wurden von US-amerikanischen Behörden Vorwürfe gegen die Siemens AG wegen schwarzer Kassen, Bestechung und illegaler Geschäfte laut. Die Aufarbeitung zog sich über vier Jahre hin. Vorstände verloren ihre Posten oder leisteten, wie der ehemalige Vorstands- und Aufsichtsratsvorsitzende Heinrich von Pierer, hohe Wiedergutmachungszahlungen. Bis Ende 2009 entstanden Siemens Kosten in Höhe von ca. zwei Mrd. € für Anwalts- und Gerichtskosten, Straf- und Steuernachzahlungen (vgl. z.B. [Sp09]).
- Seit 2004 ermittelte die Börsenaufsicht der USA, die SEC (Securities and Exchange Commission), gegen den Daimler-Konzern, der damals noch unter dem Namen DaimlerChrysler firmierte. Der Autohersteller zahlte im Jahr 2010 im Rahmen eines Vergleichs mit der SEC und dem US-Justizministerium insgesamt ca. 134 Mio. €, weil in mindestens 22 Ländern über zehn Jahre (1998 bis 2008) hinweg Regierungsbeamte mit Bargeld und Geschenken bestochen wurden, um an Aufträge zu gelangen. Im Zuge unternehmensinterner Ermittlungen wurden insgesamt 45 Manager entlassen (vgl. z.B. [Sp10a]).

- Die EU-Kommission verhängte im Juni 2010 Bußgelder in der Gesamtsumme von 518 Mio. € gegenüber 17 Herstellern von Spannstahl, die mindestens 18 Jahre lang Preise abgesprochen und Märkte in fast allen EU-Ländern untereinander aufgeteilt hatten. Die Saerstahl-Tochter DWK Drahtwerk Köln machte von der Kronzeugenregelung Gebrauch und arbeitete mit der Kommission zusammen. Aus diesem Grunde ging sie straffrei aus. Die Westfälische Drahtindustrie GmbH wurde dagegen mit einer Geldbuße in Höhe von 56 Mio. € bestraft (vgl. z. B. [Sp10b]).
- Ende 2010 erklärte sich die Toyota Motor Corporation gegenüber der US-Verkehrsaufsicht NHTSA (National Highway Traffic Safety Administration) zu einer Strafzahlung in Höhe von 24,6 Mio. € bereit. Toyota wurde vorgeworfen, Defekte im Beschleunigungs- und Lenksystem seiner Kraftfahrzeuge verheimlicht und in nur unzureichendem Maße gemeldet zu haben. Die Behörden hatten die Mängel mit vielen Verkehrsunfällen, in die Toyota-Fahrzeuge verwickelt waren, in Verbindung gebracht. So musste Toyota allein in den USA insgesamt elf Mio. Fahrzeuge zurückrufen. Insgesamt wurden von US-Behörden gegen Toyota drei Strafen im Volumen von zusammen fast 50 Mio. \$ verhängt (vgl. z. B. [MM10]).

In diesen Beispielen stehen Gesetzesverstöße im Vordergrund. Dass sie als Beispiele für Non-Compliance publik werden, liegt daran, dass es hier jeweils Einrichtungen gibt, die an der Entdeckung und Aufklärung ein eigenes professionelles Interesse haben und Verstöße aktiv verfolgen. Ähnliches gilt für Vertragsverstöße, an deren Verfolgung die Vertragspartner ein verständliches Interesse haben. Diese Fokussierung und die für Unternehmen damit verbundenen Risiken von Rechts- und Vertragsverstößen führen mitunter zu einer Verengung des Compliance-Begriffs auf eine sog. „Legal Compliance“, die die Konformität mit rechtlichen Rahmenbedingungen zum Ziel hat. Dass dieser Fokus, der aber gleichsam den Kern von Compliance darstellt (und unten in Abschnitt 13.7 beschrieben wird), derzeit gerade in der Corporate Compliance im Vordergrund steht, hängt auch damit zusammen, dass für das Topmanagement eines Unternehmens neben einem Karriereknick auch persönliche Haftungsrisiken bis hin zu strafrechtlichen Konsequenzen drohen (siehe hierzu die Ausführungen in Kapitel 14 „Rechtliche Rahmenbedingungen“, Abschnitt 14.1.3).

Vor allem größere Unternehmen haben in den letzten Jahren mit der Etablierung eines eigenständigen Compliance-Bereichs, der an die Unternehmensleitung berichtet, reagiert. Dies erfolgte oftmals als Teil eines Maßnahmenbündels zur Sicherstellung einer ordnungsgemäßen Unternehmensführung, die von aktuellen Konzepten und Vorschriften zur Corporate Governance genauso wie von Politik und Öffentlichkeit gefordert wird. Als zentrale Regelung schreibt der Deutsche Corporate Governance Kodex (DCGK) die Verpflichtung des Vorstands für die Einhaltung gesetzlicher Bestimmungen fest (vgl. Kapitel 14 „Rechtliche Rahmenbedingungen“, Abschnitt 14.1.1). Weiterhin erfährt die Institutionalisierung von Compliance in denjenigen Branchen einen Schub, wo regulatorische Vorgaben die Einrichtung einer Compliance-Funktion vorschreiben.

Beispiel:

Die von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) als Rundschreiben veröffentlichten „Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten nach §§ 31ff. WpHG für Wertpapierdienstleistungsunternehmen“ (MaComp) schreiben in BT 1.1 vor, dass Wertpapierdienstleistungsunternehmen *„eine dauerhafte und wirksame Compliance-Funktion einrichten und*

ausstatten“ müssen. Diese Funktion „berät die operativen Bereiche und überwacht und bewertet die im Unternehmen aufgestellten Grundsätze und eingerichteten Verfahren sowie die zur Behebung von Defiziten getroffenen Maßnahmen. Zusätzlich berichtet sie gegenüber der Geschäftsleitung und dem Aufsichtsorgan“ (BT 1.2).



Praxistipp: IT-Compliance muss auf Corporate Compliance aufsetzen.

Überlegungen zur IT-Compliance müssen die vorhandenen Strukturen, Verfahren und Prozesse der Corporate Compliance als Ausgangspunkt nehmen. Diese stellen den Rahmen für IT-Compliance dar. Die IT-Compliance wird sich nicht völlig unabhängig von der Corporate Compliance etablieren lassen. IT-Compliance kann somit nie ein Projekt sein, das ausschließlich der IT-Funktion zugeordnet ist.

■ 13.2 IT-Compliance

13.2.1 Begriffliche Grundlagen

Auch die IT-Funktion eines Unternehmens ist – wie jeder andere Unternehmensbereich auch – Gegenstand von Compliance bzw. Compliance-Verstößen. Dies liegt schon allein daran, dass es verschiedene Gesetze gibt, die die Art und Weise der Nutzung von IT direkt oder indirekt adressieren. Gerade Verstöße gegen das Datenschutzgesetz erlangten in jüngster Vergangenheit eine beträchtliche öffentliche Aufmerksamkeit (siehe Tabelle 13.1).

TABELLE 13.1 Beispiele von Non-Compliance

Institution	Fall
Lidl	Die Discount-Kette Lidl ließ ihre Mitarbeiter von Detekteien per Videokamera überwachen. Hierdurch sollten Ladendiebstahl und Fehlverhalten aufgedeckt werden. Protokolliert wurden jedoch auch Details aus dem Privatleben der Mitarbeiter. Lidl wurde 2008 vom Innenministerium Baden-Württemberg zu einer Strafzahlung in Höhe von 1,462 Mio. € verpflichtet (vgl. z. B. [AG08]).
Deutsche Bahn	Die Deutsche Bahn AG hatte seit 1998 ihre Mitarbeiter dreimal einem Massen-Screening unterzogen. Ziel dieser Aktionen war das Aufdecken von Auftragsvergaben an Scheinfirmen. Am 19.10.2009 erteilte der Berliner Datenschutzbeauftragte einen Bußgeldbescheid in Höhe von 1.123.503,50 €, der von der Deutschen Bahn akzeptiert wurde (vgl. z. B. [St09]).
Einwohnermeldeämter	Durch einen Fernsehbericht stellte sich 2008 heraus, dass persönliche Daten von Bürgern aus rund 200 deutschen Städten und Gemeinden über einen längeren Zeitraum frei im Internet zugänglich waren. Die verantwortliche Softwarefirma hatte aus Versehen die für den Zugang erforderlichen Passwörter auf ihrer eigenen Internetseite veröffentlicht (vgl. z. B. [Hei08]).

Institution	Fall
T-Mobile Deutschland	2008 berichtete ein Nachrichtenmagazin über einen Diebstahl von Daten von über 17 Mio. T-Mobile-Mobilfunkkunden, der bereits 2006 erfolgt war. Unter den Daten waren auch Geheimnummern und Adressen von Politikern, hochrangigen Managern und anderen Personen, für die die Verbreitung derartiger Daten ein Sicherheitsrisiko darstellt. Daraufhin beauftragte das Innenministerium das Bundeskriminalamt mit der Durchführung von Gefährdungsanalysen (vgl. z. B. [St08]).
BBK Gesundheit	Bei der Betriebskrankenkasse Gesundheit hatten Mitarbeiter eines externen Dienstleisters Zugang zu Daten der Versicherten. Die Telefon-Hotline war an einen Subunternehmer vergeben worden, der wiederum Hilfskräfte beauftragte, die freien Zugang zu den medizinischen Daten der Versicherten hatten. So sah sich die Betriebskrankenkasse einem Erpressungsversuch ausgesetzt und erfuhr durch einen Bericht im Fernsehen im Februar 2010 eine negative Publizität. Erst nach dem Vorfall entschied sich die Organisation zu einer Zertifizierung nach ISO/IEC 27001 (vgl. z. B. [St10], [BKK10]).

In den ausgewählten Fällen spielt die Nutzung von Daten sowie von Informations- und Kommunikationstechnologien eine zentrale Rolle. Bei den beiden erstgenannten Beispielen ist mit dem vorsätzlichen Missbrauch personenbezogener Daten ein Verstoß gegen gesetzliche Regelungen offensichtlich, auch wenn dem jeweiligen Datenmissbrauch ein durchaus berechtigtes Unternehmensinteresse (Aufdecken von Diebstahl und Betrug) zugrunde lag. In den drei letztgenannten Fällen mangelte es offenbar an effektiven Maßnahmen der Überprüfung eines Dienstleisters und des Zugriffsschutzes sowie an entsprechenden Kontrollen, wie sie sowohl von gesetzlichen Regelungen als auch von Normen und Standards des IT-Sicherheitsmanagements gefordert werden.

Vor allem in den Fällen von Gesetzesverletzungen ist davon auszugehen, dass die betroffenen Unternehmen neben Schadensersatzzahlungen und gesetzlich vorgesehenen Strafen in der Öffentlichkeit eine Schädigung ihrer Reputation, verbunden mit Verlust von Vertrauen und Kundenbindung, erlitten haben. Dies soll jedoch nicht heißen, dass die mangelnde Befolgung der sonstigen Regelwerke von geringerer Bedeutung ist. Verträge sehen bei Verletzung vertraglicher Vereinbarungen mitunter empfindliche Strafzahlungen vor. Zudem dürften schwerwiegende Vertragsverletzungen in der Regel zu einer Beendigung der Geschäftsbeziehung führen, was entsprechende Umsatz- und Imageverluste nach sich zieht. Der Verlust von Zertifikaten als Folge mangelnder Konformität mit am Markt üblichen Standards kann Nachteile bei der Auftragsgewinnung bewirken, wenn beispielsweise in einer Ausschreibung der Nachweis bestimmter Zertifikate als Teilnahmevoraussetzung vorgeschrieben ist. Und die mangelnde Befolgung unternehmensinterner Regelungen führt wiederum zum Verstoß gegen externe Vorgaben, aber auch zu internen Ineffizienzen, Kontrollverlust und operationellen Risiken.



Praxistipp: Aus schlechten Beispielen anderer lernen.

Analysieren Sie systematisch die negativen Auswirkungen, die mangelnde IT-Compliance haben kann. So können Sie die Bedeutung der Compliance für die Unternehmens-IT wie auch das Unternehmen insgesamt verdeutlichen. Die veröffentlichten Fälle von Non-Compliance können hierbei durchaus hilfreich sein. Je realistischer Sie die Folgen identifizieren, auf die eigene Situation übertragen und veranschaulichen, umso eher lässt sich ein Handlungsdruck in Sachen IT-Compliance begründen.

Diese Beispiele zeigen, dass die im Unternehmen eingesetzte Informationstechnik eine wesentliche Rolle bei der Compliance-Thematik spielt. Hieraus resultiert eine durchaus neue Verantwortung für die IT-Abteilung, die den effektiven und effizienten Einsatz der Informationstechnik sicherstellt. Traditionell unterstützt die IT-Abteilung die Geschäftsprozesse der Unternehmensbereiche durch den Betrieb der Fachanwendungen. Diese Unterstützung muss sich heute auch auf die Compliance in der Durchführung der Geschäftsprozesse erstrecken, beispielsweise durch die Implementierung automatisierter Kontrollen. Zudem hat die IT-Funktion auch direkt an sie gerichtete Compliance-Vorgaben zu erfüllen. Damit steht „IT-Compliance“ als Teilbereich des IT-Managements zur Debatte. Wie prägt sich dieser Teilbereich der Compliance aus?

IT-Compliance materialisiert sich letztlich im Vorhandensein und Funktionieren spezifischer informations- und kommunikationstechnischer Einrichtungen, im Vorliegen von Systemdokumentationen, IT-Richtlinien, Kontrollergebnissen und Notfallplänen, korrekten und gesicherten Daten, Regelungen für den Datenzugriff u.v.a.m. Dennoch steht all dies nicht für die Bedeutung des Begriffs „IT-Compliance“. Nicht der unmittelbare Zweck, der mit dem Vorhandensein der verschiedenen Gerätschaften, Dokumente etc. verbunden ist, wird vom Compliance-Begriff adressiert, sondern eine Nebenbedingung steht hier im Vordergrund: die der Befolgung relevanter Vorgaben. Diese Vorgaben, die technischer, organisatorischer oder personeller Art sein können, erweisen sich in der Regel als Mittel zum Zweck. So soll beispielsweise die Beschränkung des Datenzugriffs (Mittel) Datenmissbrauch und somit die Beeinträchtigung des Unternehmenswertes (Zweck) verhindern. Umfang und Art der Beschränkung werden hierbei internen Vorgaben eines Berechtigungskonzeptes, vertraglichen Vereinbarungen, gesetzlichen Anforderungen, z. B. des Bundesdatenschutzgesetzes (BDSG), oder akzeptierten IT-Normen und IT-Standards, z. B. der ISO/IEC 27002 oder den Grundsatzkatalogen des BSI (Bundesamt für Sicherheit in der Informationstechnik), zu genügen haben, vgl. Abbildung 13.3.

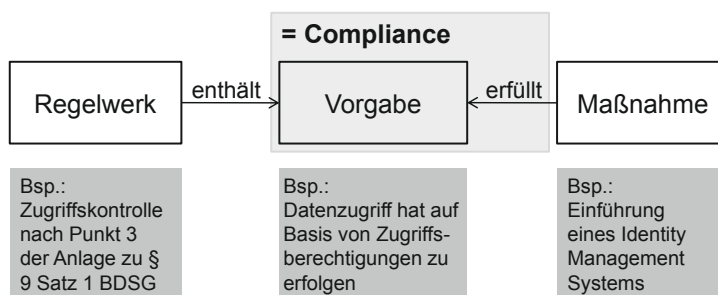


ABBILDUNG 13.3
IT-Compliance als
Erfüllung von Vorgaben

Die Erfüllung von Vorgaben ist somit auch die Basis für den Begriff der IT-Compliance als Spezialisierung des allgemeinen Compliance-Begriffs:



IT-Compliance bezeichnet einen Zustand, in dem alle die IT des Unternehmens betreffenden und verbindlich vorgegebenen bzw. als verbindlich akzeptierten Vorgaben nachweislich eingehalten werden.

Hierbei ist es unerheblich, ob die IT-Leistungen ausschließlich unternehmensintern oder (teilweise) durch externe IT-Dienstleister (im Rahmen von Entwicklungs-, Hosting-, Outsourcing-Verträgen o. Ä.) erbracht werden.

13.2.2 IT-Compliance als Verhalten

Ausgehend von wohlbekannten Unternehmensskandalen (z.B. Enron und Worldcom in den USA, Schneider und Balsam in Deutschland), bei denen beträchtlicher Schaden durch betrügerisches Handeln entstanden ist, hat sich Compliance als Forderung nach einem regelkonformen Verhalten der Unternehmensmitglieder entwickelt. Übertragen auf die Unternehmens-IT ist IT-Compliance ein Verhalten, bei dem von den Unternehmensmitgliedern und ggf. beauftragten Externen alle für die IT des Unternehmens relevanten bzw. als relevant akzeptierten internen und externen Regelwerke beachtet und eingehalten werden. Gegenstand der IT-Compliance sind bei dieser Sichtweise vor allem verhaltensbeeinflussende, -steuernde oder kontrollierende Maßnahmen. Hierbei steht die Befolgung von rechtlichen Vorgaben, aber auch von ethisch fundierten Handlungsprinzipien im Vordergrund. Ein hierfür häufig genutztes Instrument sind Verhaltensnormen, die von den Mitarbeitern beispielsweise fordern, dass sie

- ihre informationsbezogenen Aufgaben mit Ehrlichkeit, Sorgfalt und Kompetenz wahrnehmen;
- alle für die IT des Unternehmens relevanten bzw. als relevant akzeptierten internen und externen Regelwerke einhalten und die damit verbundenen ethischen Werte achten (z.B. das dem Datenschutz zugrunde liegende informationelle Selbstbestimmungsrecht von Betroffenen);
- Daten von Kunden, Lieferanten und anderen Geschäftspartnern sowie sensible Unternehmensdaten vertraulich behandeln;
- Daten und die IT-Infrastruktur als Vermögenswerte begreifen und entsprechend schützen.

Soweit diese Verhaltenserwartungen explizit festgehalten werden, entstehen Verhaltenskodizes, die den Mitarbeitern eine Orientierung geben, wie sie in bestimmten Entscheidungssituationen agieren sollen, aber auch, welche Sanktionen bei Verstößen drohen. Vom Kodex angebotene Orientierungen sollten weitestgehend konkretisiert werden, letztlich bis hin zu Verfahrensanweisungen, denen verbindlich zu folgen ist (z.B. für den Umgang mit personenbezogenen Daten, mit als vertraulich klassifizierten Dokumenten oder mit Passwörtern und Zugangscodes).

Eine sensible Frage in diesem Zusammenhang ist die Aufforderung, dass Mitarbeiter Verstöße gegen den Verhaltenskodex melden sollen. Es wird von der Einrichtung eines generellen Hinweisgebersystems abhängen, inwieweit dies in einem Unternehmen hinsichtlich der IT-Compliance praktiziert wird. In jedem Falle bedarf es jedoch spezifischer Informations- und Bera-

tungsstrukturen, die den Mitarbeitern eine Hilfestellung bieten, z. B. eine Compliance-Helpline oder Compliance-Schulungsangebote. Eine sowohl initiale als auch kontinuierliche Mitarbeiterschulung ist eine der Kernmaßnahmen sowohl der Corporate als auch der IT-Compliance. Natürlich können präventiv wirkende Kodizes, Schulungsmaßnahmen und Beratung kein vorsätzliches Missachten oder gar kriminelles Handeln verhindern. Insofern ist eine Ergänzung um kontrollierende und entdeckende Maßnahmen erforderlich, die von der Implementierung einzelner Kontrollen bis hin zur Einrichtung eines Anti-Fraud-Managementsystems reichen. Neben der fachlichen Kompetenz fokussiert die Verhaltensperspektive die mit der Aufgabendurchführung verknüpfte persönliche Verantwortung, die sich in arbeitsteiligen Organisationen über die Delegation entlang den hierarchischen Weisungsbeziehungen ergibt. Hier werden sinnvollerweise unabdingbare Pflichten zu regeln sein, die sich auf wesentliche Aufgaben richten, beispielsweise in den Bereichen IT-Sicherheit, IT-Risikomanagement oder Einhaltung von IT-Verträgen. Der Nachvollziehbarkeit der Übertragung von Verantwortung ist hierbei besondere Aufmerksamkeit zu widmen (nach [KI09b]).



Praxistipp: Mit den Personal- und Organisationsfunktionen zusammenarbeiten.

Die Verhaltensperspektive führt in der Praxis dazu, dass die IT-Compliance mit den Personal- und Organisationsfunktionen eng zusammenarbeiten muss, und zwar sowohl was die nachweisliche Qualifizierung der Belegschaft als auch die formale Grundlage der Delegation von Verantwortlichkeiten anbelangt. Diese Zusammenarbeit sollte von Beginn an praktiziert werden.

13.2.3 Compliance der IT-Funktion vs. IT-gestützte Corporate Compliance

In der Literatur, bei Fachdiskussionen und praktischen Anwendungsbeispielen lassen sich zwei Auffassungen von IT-Compliance ausmachen. Eine häufig anzutreffende Sichtweise versteht IT-Compliance als Einsatz von Soft- und Hardwareprodukten, mit deren Hilfe die Einhaltung von Regelwerken sichergestellt werden kann. In diesem Sinne handelt es sich um eine „IT-gestützte Corporate Compliance“. Diese Interpretation wird vor allem von Herstellern vertreten, die Lösungen für Security- oder Content-Management, Archivierung, Verschlüsselung, Nutzer-, Zugangs- und Lizenzverwaltung u. a. m. anbieten. Aber auch auf Unternehmensseite wird dieser Sicht gerne gefolgt, belegt doch der Einsatz derartiger Systeme das Bemühen um Compliance. Dass diese Auffassung ihre Berechtigung hat, kann nicht im Geringsten bezweifelt werden. Im Gegenteil: Ohne die genannten Lösungen sind die zahlreichen Anforderungen aus den verschiedenen Regelwerken nicht in den Griff zu bekommen. Die mit den Lösungen verbundene Automatisierung von Kontrollen führt zu einem IT-gestützten Internen Kontrollsystem, das somit ebenfalls Teil der IT-Compliance wird (nach [RS09], S. 163).

Die zweite Sichtweise fragt danach, welche Vorgaben aus Gesetzen, Normen, Standards, Verträgen und anderen Regelwerken die IT selbst als Unternehmensfunktion zu erfüllen hat. Hier richten sich Anforderungen direkt an die Planung, die Entwicklung und den Betrieb von Informationssystemen. Da diese Aufgaben ganz überwiegend im Verantwortungsbereich der IT-Abteilung eines Unternehmens liegen, steht hier somit die „Compliance der IT-Funktion“ im

Mittelpunkt der Betrachtung. Auch diese Sichtweise ist vollauf berechtigt, ist sie doch Teil der Führungsverantwortung der IT-Leitung.

In der Praxis sind beide Sichtweisen zusammenzubringen. Zunächst einmal ist es sinnvoll, sich die grundlegenden Unterschiede zwischen den beiden Interpretationsmöglichkeiten zu verdeutlichen (siehe Abbildung 13.4).

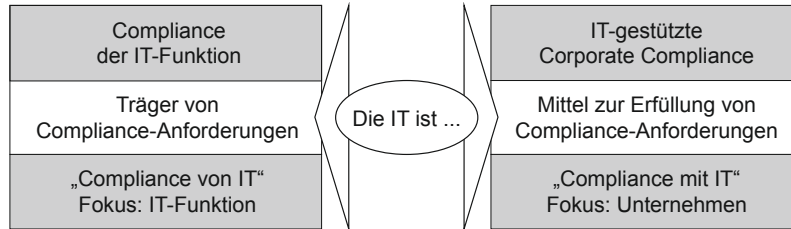


ABBILDUNG 13.4 Compliance der IT-Funktion vs. IT-gestützte Corporate Compliance

Die Sichtweise „Compliance der IT-Funktion“ betrachtet die IT selbst als Träger von Compliance-Anforderungen. Hier stellen sich beispielsweise folgende Fragen (nach [KD08], S. 9f.):

- Welche Rechtsnormen und ggf. sonstigen Regelwerke sind für die IT des Unternehmens relevant?
- Welche Compliance-Anforderungen haben die einzelnen Bereiche der IT (Infrastruktur, Datenhaltung, Betrieb, Prozesse etc.) zu erfüllen?
- Welche IT-gestützten Prozesse und Anwendungen sind betroffen, und welche Anforderungen sind von ihnen zu erfüllen?
- Welche Risiken resultieren in welcher Höhe aus fehlender oder mangelhafter Compliance der IT?
- Welche technischen, organisatorischen und personellen Maßnahmen sind für die Gewährleistung von Compliance der IT zu ergreifen?

IT-gestützte Corporate Compliance bedeutet, dass IT als Mittel zum Erreichen von Compliance in allen Unternehmensbereichen genutzt wird. Bei dieser Sichtweise stellen sich beispielsweise folgende Fragen:

- Welche Compliance-Anforderungen haben die Geschäftsprozesse zu erfüllen?
- Welche Compliance-Anforderungen kann eine spezifische Hard- oder Software adressieren?
- Welche Hard- oder Softwarelösung ist für die Erfüllung der Compliance-Anforderungen am besten geeignet?
- Wie sind die verfügbaren Compliance-Tools aufeinander abzustimmen?

Es ist offensichtlich, dass beide Sichtweisen ineinandergreifen und insofern beide notwendig sind, um Compliance im Allgemeinen und Compliance der IT im Speziellen zu erreichen. Im Ergebnis liegt ein IT-gestütztes Management von Vorgaben vor, die sich sowohl an das Unternehmen insgesamt und seine verschiedenen Unternehmensfunktionen als auch speziell an die IT-Funktion richten. Eine Trennung beider Sichtweisen in der Praxis scheint kein gangbarer Weg. Insofern gilt:



IT-Compliance = IT-gestützte Corporate Compliance + Compliance der IT-Funktion

Eine weitgehende IT-Unterstützung bei der Einhaltung von Compliance ist letztlich die einzige Möglichkeit, die Vielzahl heutiger Compliance-Anforderungen zu erfüllen. Dies gilt insbesondere für die kontinuierliche Überwachung des IT-Betriebs auf Compliance-Verstöße.

Beispiel:

Das Bundesdatenschutzgesetz richtet spezifische Anforderungen an die Haltung personenbezogener Daten. Zum Schutz dieser Daten sind nach § 9 BDSG und der zugehörigen Anlage 1 zahlreiche Kontrollen zu implementieren (z.B. Zutritts-, Zugriffs- oder Verfügbarkeitskontrollen). Um diese Vorgabe zu erfüllen, sind zuerst organisatorische und personelle Maßnahmen zu ergreifen, z.B. die Durchführung von Risiko- und Schutzbedarfsanalysen, die Festlegung von Zugriffsberechtigungen, die Planung und Durchführung von Schulungsmaßnahmen, die Regelung von Zutritts- und Zugangsrechten, das Erlassen von Vorschriften für die Verarbeitung von personenbezogenen Daten und die Verpflichtung der Mitarbeiter auf diese Vorschriften. Zu einem Großteil führen diese Maßnahmen aber letztlich zu technischen Lösungen, z.B. einer automatisierten, funktionsbasierten Zugriffssteuerung, einer systemgesteuerten Passwortvergabe oder einer automatischen Datensicherung.

Im Kern wird eine IT-gestützte Compliance aus folgenden Elementen bestehen, siehe Abbildung 13.5.

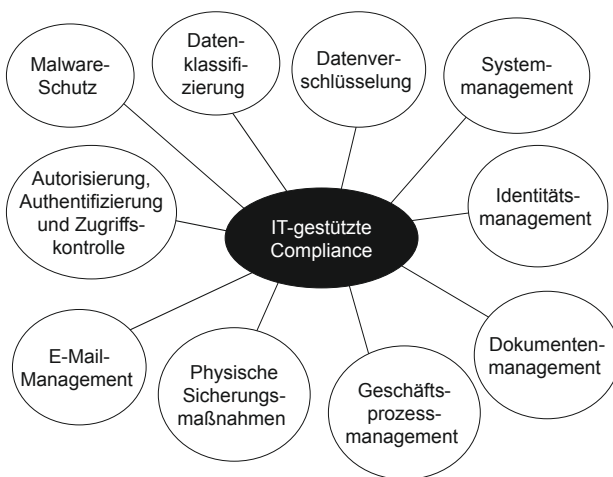


ABBILDUNG 13.5

IT-Lösungen als Elemente einer IT-gestützten Compliance

- **Datenklassifizierung**
Um Daten entsprechend ihrer Verwendung optimal bereitstellen, speichern, schützen und archivieren zu können, ist es erforderlich, sie zu klassifizieren und ihren Schutzbedarf festzustellen.
- **Datenverschlüsselung**
Die Datenverschlüsselung sorgt für den Schutz der Daten bei Übertragung, Speicherung und Archivierung. Der Umfang der Verschlüsselung richtet sich nach dem Schutzbedarf von Daten.
- **Autorisierung/Authentifizierung/Zugriffskontrolle**
Systeme für die Autorisierung, Authentifizierung und Zugriffskontrolle stellen die Vertraulichkeit, die Integrität und den Schutz von (insbesondere personenbezogenen) Daten sicher.

- **Identitätsmanagement**
Identitätsmanagement stellt sicher, dass nur autorisierte Personen entsprechend ihren Rollen Zugriffsrechte auf Daten haben. Außerdem unterstützt das Identitätsmanagement die Transparenz und Nachvollziehbarkeit beim Zugriff auf informationstechnische Ressourcen.
- **Dokumentenmanagement**
Mit Dokumentenmanagement-Systemen lassen sich Zugriffe auf sensible Daten und Dokumente regeln, kontrollieren und nachvollziehen.
- **Geschäftsprozessmanagement**
Systeme für Geschäftsprozessmanagement unterstützen die transparente und ordnungsmäßige Aufgabendurchführung unter Berücksichtigung von Compliance-Anforderungen, beispielsweise durch Kontroll- und Freigabeworkflows.
- **Systemmanagement**
Neben einer auf Effizienz des Systembetriebs ausgerichteten Zielsetzung bieten Systemmanagement-Tools auch Compliance-Funktionalitäten für die Aufzeichnung und Verfolgung von Zugriffen und Änderungen an Daten, Dokumenten, Konfigurationen etc. sowie für die IT-Sicherheit (z. B. Wiederherstellung oder Intrusion Detection und Prevention).
- **Malware-Schutz**
Der Schutz vor Malware, d. h. bösartiger Software (Viren, Spyware etc.) ist grundlegend zur Wahrung von Vertraulichkeit, Verfügbarkeit und Integrität von Daten.
- **Physische Sicherungsmaßnahmen**
Physische Sicherungsmaßnahmen wirken vor allem durch bauliche und technische Maßnahmen unterstützend, z. B. durch einen Zugangs- und Feuerschutz oder die Sicherstellung der Stromversorgung.
- **E-Mail-Management-Systeme**
E-Mail-Management-Systeme sorgen für die regelkonforme Nutzung, Versendung, Verteilung und Archivierung von E-Mails in allen Bestandteilen, also auch mit (digitalen) Signaturen und Anhängen.



Praxistipp: Ein integrativer Ansatz ist unumgänglich.

Damit die einzelnen informationstechnischen Lösungen für eine IT-gestützte Compliance effektiv und effizient arbeiten können, müssen sie in einem Gesamtkonzept aufeinander abgestimmt sein.

13.2.4 „Governance – Risk – Compliance“ und IT-Compliance

Governance, Risikomanagement und Compliance auf der Unternehmensebene verweisen aufeinander. Aufgrund der inhaltlichen Zusammenhänge wird neuerdings von der Trias „Governance – Risk – Compliance“ (GRC) gesprochen, die eine integrierte Strategie und ein gemeinsames Management erfordert. Dieser allgemeine GRC-Zusammenhang ergibt sich auch für die IT.

- **Governance – Compliance:**
Regelwerke der Corporate Governance lassen sich heutzutage häufig nur noch erfüllen, wenn entsprechende IT-Maßnahmen ergriffen werden. Die Ordnungsmäßigkeit sowohl der

Entwicklung als auch des Betriebs von IT-Anwendungen muss vor allem hinsichtlich der Finanzberichterstattung nachgewiesen werden können (nach [JG07], S. 17f.). Corporate Governance zieht somit eine spezialisierte IT-Governance nach sich. Diese richtet sich auf die Regelung von Verantwortlichkeiten und Entscheidungsrechten sowie von entsprechenden Prozessen und Verfahren mit dem Ziel, aus der IT-Nutzung einen maximalen Wertbeitrag für das Unternehmen zu ziehen. Hierzu gehört auch die Einrichtung eines IT-Kontrollsystems als Bestandteil des unternehmensweiten Internen Kontrollsystems (IKS), mit dem die Steuerung und Überwachung der IT im Unternehmen sichergestellt werden soll. Für die Ausgestaltung des IT-Kontrollsystems liegen wiederum einschlägige Standards vor, die insofern Gegenstand der IT-Compliance sind, z. B. COBIT (siehe Abschnitt 13.3).

■ Risikomanagement – Compliance:

Ein IT-Risikomanagement als Teil eines unternehmensweiten Risikomanagements richtet sich speziell auf die IT-Risiken des Unternehmens. Als Schnittmenge von IT-Risiken einerseits und von mit Regelverstößen verbundenen Risiken, d. h. Compliance-Risiken, andererseits ergeben sich die IT-Compliance-Risiken (siehe Abbildung 13.6). In einer risikoorientierten Sichtweise adressiert IT-Compliance IT-Risiken, die dadurch entstehen, dass die Informations- und Kommunikationssysteme eines Unternehmens nicht wie geplant funktionieren, schlecht organisiert sind, nicht wie erforderlich betrieben und genutzt werden, unzureichend verfügbar oder ungenügend gesichert sind, manipuliert oder missbraucht werden können usw., sodass hierdurch vor allem gesetzliche Vorgaben potenziell nicht oder nur mangelhaft erfüllt werden.

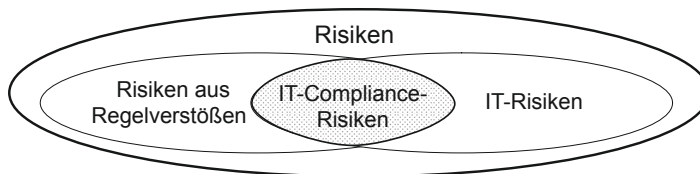


ABBILDUNG 13.6
IT-Compliance-Risiken
als Schnittmenge

Beispiel:

Die AXA Konzern AG unterliegt als Tochtergesellschaft der an der New York Stock Exchange (NYSE) notierten Pariser Muttergesellschaft den Regelungen des „Sarbanes-Oxley Act“ (SOX). IT-Risiken wurden im Rahmen eines Projektes zur Einführung eines IKS für die Cash- und Jahresabschlussprozesse bei der Datenaufbereitung und -haltung sowie der manuellen Eingabe und Weiterleitung von Daten gesehen. Hinsichtlich der SOX-Anforderungen wurde die Heterogenität der Systemlandschaft insgesamt als problematisch beurteilt. Compliance-Risiken ergaben sich aufgrund der zahlreichen Schnittstellen bei der Pflege und der Datenübertragung zwischen den verschiedenen Anwendungssystemen, da hierdurch die Zuverlässigkeit der Kontrollen des IKS nicht beurteilt werden konnte (nach [MK06], S. 141 ff.).

Im Ergebnis erfährt die GRC-Trias eine Spezialisierung im IT-Bereich, was vielfältige Koordinationsaufgaben bedingt. So muss sich jede Spezialisierung in den jeweiligen generellen Bereich eingliedern, also z. B. die IT-Compliance in die generellen Compliance-Aktivitäten des Unternehmens. Zudem muss jede Spezialisierung wegen der konzeptionellen, methodischen und strukturellen Überschneidungen auch mit den anderen Spezialisierungen abgestimmt werden, die IT-Compliance folglich mit IT-Governance und IT-Risikomanagement (vgl. Abbildung 13.7, nächste Seite).

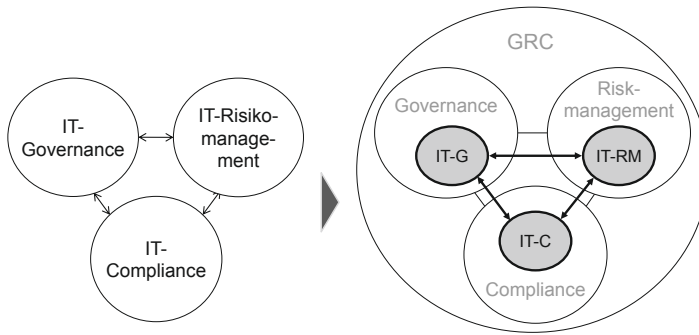


ABBILDUNG 13.7
Bezüge der IT-Compliance



Praxistipp: GRC-Zusammenhänge klären.

Die unternehmensspezifische Klärung der Zusammenhänge zwischen den Strukturen von Governance, Risikomanagement und Compliance ist ebenso schwierig wie notwendig. Ansonsten drohen Ineffizienzen, Doppelinvestitionen, Verschwendung von Managementkapazität oder gar konkurrierende Verantwortlichkeiten, die sich gegenseitig neutralisieren.

■ 13.3 IT-Compliance nach COBIT

13.3.1 COBIT als IT-Governance Framework

Bei COBIT (Control Objectives for Information and Related Technology) handelt es sich um ein Referenzmodell („Framework“), das Unternehmen eine methodische Unterstützung bietet, um IT-Ressourcen (d.h. Anwendungen, Informationen, IT-Infrastruktur und Personal) für die Erreichung von Wettbewerbsvorteilen zu nutzen (nach [ITGI05], S. 12). Seit 1993 wurde COBIT vom internationalen Prüfungsverband ISACA (Information Systems Audit and Control Association) entwickelt und erstmals Ende 1995 veröffentlicht. Aktuell liegt COBIT in der Version 4.1 vor (die deutsche Ausgabe in der Version 4.0).

Die erste Version von COBIT legte den Schwerpunkt auf sogenannte Kontrollziele und adressierte damit vor allem die Arbeit von Wirtschaftsprüfern. Die Verfolgung dieser Kontrollziele, ihre regelmäßige, systematische Überprüfung und die Umsetzung entsprechender Maßnahmen sollen einen effizienten und effektiven Einsatz der Informations- und Kommunikationstechnologie im Unternehmen gewährleisten. Im Verlauf der letzten Jahre entwickelte sich COBIT zunehmend zum Managementinstrument, mit dem die IT nicht nur nachgelagert geprüft, sondern proaktiv gestaltet werden kann.

COBIT berücksichtigt wichtige IT-Normen und -Standards (z.B. ITIL, CMMI, ISO/IEC 27002) und kann aufgrund seiner übergeordneten Management- und Steuerungssicht als Integrator

dienen, wenn ein Unternehmen diese Normen und Standards gleichzeitig nutzen will (vgl. [ITGI05], S. 197). COBIT definiert insgesamt 34 IT-Prozesse in den vier Domänen

- Planung und Organisation (engl. Plan and Organize – PO),
- Beschaffung und Implementierung (engl. Acquire and Implement – AI),
- Betrieb und Unterstützung (engl. Deliver and Support – DS),
- Überwachung und Bewertung (engl. Monitor and Evaluate – ME)

Je Prozess gibt man sowohl die von diesem Prozess unterstützten Geschäftsziele an als auch ein übergeordnetes Kontrollziel, das in 3 bis 30 Detailziele untergliedert wird.

COBIT richtet sich explizit auch an diejenigen internen und externen Stakeholder, die Compliance-Funktionen übernehmen. So sieht das Rollenmodell von COBIT eine Rolle „Compliance, Audit, Risk und Security“ vor, die die Gruppen, die eine Überwachungsfunktion, aber keine operative Verantwortung in der IT wahrnehmen, zusammenfasst. Darüber hinaus berücksichtigt COBIT die Compliance-Thematik im Wesentlichen in zweierlei Hinsicht:

- Zum einen wird Compliance als eine der allgemeinen Geschäftsanforderungen betrachtet, die bei der Nutzung von Informationen und Informationstechnik zu erfüllen sind. Fragen der Compliance werden somit in verschiedenen Prozessen über alle vier Domänen hinweg behandelt.
- Zum anderen widmet sich einer der 34 IT-Prozesse speziell der Sicherstellung von Compliance. Dies ist der Prozess ME 3 („Stelle Compliance mit Vorgaben sicher“) der COBIT-Domäne „Überwachung und Bewertung“.

13.3.2 Compliance als allgemeine Geschäftsanforderung

Die allgemeinen Anforderungen an Geschäftsinformationen werden von COBIT als „Informationskriterien“ (engl. information criteria) bezeichnet. Aus dem Verständnis der Informationskriterien ergibt sich der von COBIT verwendete Compliance-Begriff (nach [ITGI05], S. 14):



Compliance nach COBIT umfasst die Einhaltung von Gesetzen, Regulativen und vertraglichen Vereinbarungen im Rahmen von Geschäftsprozessen. Hierbei sind externe Vorschriften ebenso wie interne Richtlinien zu berücksichtigen.

Jeder IT-Prozess hat zur Erfüllung von Geschäftsanforderungen beizutragen. Durch „Key Goal Indicators“ (KGI) wird gemessen, inwieweit er hierin erfolgreich ist. Diese Messung richtet sich auch auf die Bestätigung der Compliance der unterstützten Geschäftsprozesse (ebd., S. 25). Weiterhin wird jeder in COBIT beschriebene IT-Prozess systematisch dahingehend charakterisiert, welche der Geschäftsanforderungen er unterstützt. Tabelle 13.2 listet diejenigen IT-Prozesse der vier COBIT-Domänen auf, die zur Erfüllung von Compliance beitragen. Hinsichtlich des Unterstützungsumfanges nimmt COBIT eine 2-stufige Differenzierung (primär, sekundär) danach vor, wie bedeutend der Beitrag eines Prozesses ist. Den in der Tabelle aufgeführten Prozessen wird bis auf Prozess ME 3 durchgängig eine sekundäre Bedeutung zugemessen.

TABELLE 13.2 Compliance-Inhalte der COBIT-Prozesse

Notation	Prozess	Compliance-Bezug
PO 6	Kommuniziere Ziele und Richtung des Managements	Im Rahmen dieses Prozesses sind Richtlinien zu erstellen, die die Nutzung der IT leiten. Hierzu ist eine IT-Kontrollumgebung einzurichten. Bestandteil dieser Richtlinien ist auch die Verpflichtung zu Compliance, die durch geeignete Kontrollen und Prüfungen im gesamten Unternehmen sicherzustellen ist.
PO 9	Beurteile und manage IT-Risiken	Hier wird die mangelnde Erfüllung externer Anforderungen (vor allem aus Verordnungen und rechtlichen Vorgaben) als potenzielles IT-Risiko eingestuft, das es im Rahmen eines IT-Risikomanagements zu steuern gilt.
AI 4	Ermögliche Betrieb und Verwendung	Die Verantwortung für die fachliche Nutzung von Anwendungen liegt nach COBIT in der Fachabteilung bzw. beim Geschäftsprozess-eigner. Diese Verantwortung richtet sich auch auf Compliance-Anforderungen, die der Geschäftsprozess zu erfüllen hat und deren Einhaltung durch entsprechende Kontrollen sicherzustellen ist.
AI 5	Beschaffe IT- Ressourcen	In diesem Prozess sind alle diejenigen Aktivitäten compliance-relevant, die sich auf vertragliche Anforderungen beziehen. Dies sind vor allem die Entwicklung von IT-Beschaffungsrichtlinien, die Auswahl von Lieferanten, die Vertragsgestaltung und die Durchführung der Beschaffung. Hierbei stellt ein Vertragsmanagement die Compliance mit vertraglichen Vorgaben für die gesamte Unternehmens-IT nachweislich sicher.
DS 1	Definiere und manage Service Levels	Fragen der Compliance werden im Service-Level-Management dann relevant, wenn die zu vereinbarenden Service-Level-Agreements (SLAs) oder Operating-Level-Agreements (OLAs) Compliance-Anforderungen berücksichtigen müssen. Die entsprechenden Festlegungen sind auch Gegenstand der Überwachung, des Berichtswesens und etwaiger Reviews.
DS 2	Manage Leistungen von Dritten	Das Management von Drittleistungen hat sich explizit auch auf die Erfüllung von Compliance-Anforderungen durch den Lieferanten zu richten. Die Anzahl der Fälle von Non-Compliance ist ein Indikator der Leistungsmessung.
DS 5	Stelle Security von Systemen sicher	Hier stehen die Compliance von IT-Sicherheitsrichtlinien und die Umsetzung zahlreicher Compliance-relevanter Einzelfragen, wie Berechtigungskonzepte, Funktionstrennungen, Dokumentationsverpflichtungen oder Sicherheitszertifizierungen, im Vordergrund.
ME 1	Monitore und evaluiere IT-Performance	Die Leistungsüberwachung hat sich auch auf das Erreichen von Compliance zu beziehen. Hierfür sind geeignete Leistungsindikatoren zu bestimmen und in das Berichtssystem aufzunehmen.
ME 2	Monitore und evaluiere Internal Controls	Ziel dieses Prozesses ist es, eine Aussage darüber zu erhalten, ob/ inwieweit Gesetze und Vorschriften eingehalten werden. Hierzu soll sich das Interne Kontrollsystem der IT an Richtlinien und Normen orientieren. Rechtliche, regulatorische und vertragliche Anforderungen müssen durch das IT-Kontrollsystem abgedeckt sein, wobei sich die Kontrollen auch auf externe Dienstleister zu erstrecken haben.

Notation	Prozess	Compliance-Bezug
ME 3	Stelle Compliance mit Vorgaben sicher	Dies ist der zentrale IT-Prozess, durch den Compliance sichergestellt werden soll (er wird im folgenden Abschnitt 13.3.3 ausführlich beschrieben).
ME 4	Sorge für IT-Governance	Auch dieser Prozess zielt auf die Einhaltung von Gesetzen und Vorschriften. Konkret wird gefordert, dass durch eine interne oder externe Prüfung „die Compliance der IT mit ihren Richtlinien, Standards und Verfahren sowie mit allgemein anerkannten Praktiken“ bestätigt wird ([ITGI05], S. 185).

13.3.3 Der COBIT-Prozess zur Sicherstellung von Compliance

Der Prozess „Stelle Compliance mit Vorgaben sicher“ (engl. Ensure Regulatory Compliance) ist als dritter Prozess in die Domäne „Überwachung und Bewertung“ eingeordnet (im Folgenden nach [ITGI05], S. 179 ff.). Die Prozessbezeichnung stellt gleichzeitig das übergeordnete Kontrollziel dar, das erreicht ist, wenn eine *„positive Bestätigung der Einhaltung von Gesetzen und Vorschriften vorliegt“* (ebd., S. 179). Eine derartige Bestätigung allein wird für eine Messung der Zielerreichung jedoch nicht als ausreichend angesehen. Vielmehr soll die Messung der Zielerreichung anhand folgender Indikatoren erfolgen:

- den Kosten von Non-Compliance, wobei Straf- und Vergleichszahlungen explizit genannt werden;
- der durchschnittlichen Zeitdauer zwischen dem Auftreten externer Compliance-Probleme und deren Lösung;
- der Häufigkeit von Compliance-Reviews.

Die genauere Prozessbeschreibung gliedert sich in fünf detaillierte Kontrollziele, die als normative Aussagen den Inhalt und den Umfang des Managements der IT-Compliance nach COBIT wiedergeben (siehe Abbildung 13.8).

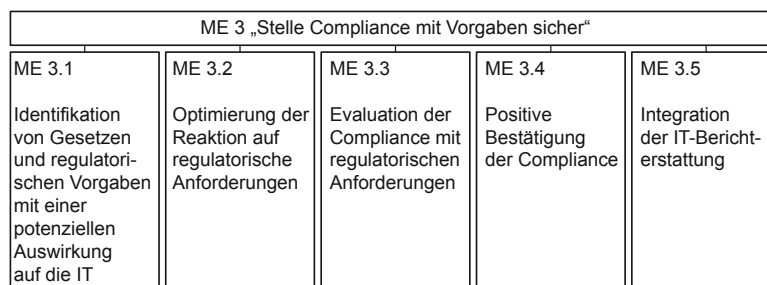


ABBILDUNG. 13.8 Detaillierte Kontrollziele des COBIT-Prozesses ME 3 - Stelle Compliance mit Vorgaben sicher

In ME 3.1 findet sich eine Aussage zum Umfang der zu berücksichtigenden Compliance-Anforderungen. Diese resultieren aus rechtlichen und sonstigen regulatorischen Vorgaben sowie aus Verträgen und Richtlinien. Als spezielle Rechtsgebiete werden u. a. Datenschutz,

Urheberrecht sowie Regelungen zur Gesundheit und Arbeitnehmersicherheit genannt. Um zeitnah auf diese Vorgaben reagieren und Compliance herstellen zu können, bedarf es eines entsprechenden internen Prozesses der Identifikation sowie der Umsetzung durch IT-Richtlinien, -Standards und -Verfahren, die regelmäßig zu bewerten und zu optimieren sind (ME 3.2). Sodann ist die Einhaltung der Compliance-Anforderungen zu prüfen und zu beurteilen (ME 3.3). Das Ergebnis ist entsprechend zu berichten und geht in die Leistungsdarstellung der IT-Funktion ein. Wurden Compliance-Lücken festgestellt, sind Maßnahmen einzuleiten, und zwar vor allem hinsichtlich einer Anpassung der IT-Richtlinien, -Standards und -Verfahren. COBIT siedelt die Verantwortung hierfür bei den Prozesseignern (engl. process owner) an (ME 3.4). Die Ergebnisse hinsichtlich der IT-Compliance sind in die generelle Berichterstattung der Corporate Compliance zu integrieren (ME 3.5).

In seinem RACI-Modell (R = responsible, A = accountable, C = consulted, I = informed) ordnet COBIT die Rechenschaftspflicht in Bezug auf die Compliance der IT-Funktion dem CIO zu. Für die Durchführung verantwortlich zeichnen die Mitglieder der Führungsebene unterhalb des CIO, die Leitungen für IT-Betrieb, -Entwicklung und -Administration, ebenso der IT-Chefarchitekt sowie die Compliance-affinen Stellen mit Kontroll- und Berichtsverantwortung (Corporate Compliance, Audit, Risiko und Sicherheit).

In den von COBIT angebotenen Zielen und Metriken lässt sich erkennen, dass die Schulung von Mitarbeitern hinsichtlich ihrer Compliance-Verantwortung von großer Bedeutung ist. So stellt die Anzahl der Compliance-bezogenen Schulungstage pro IT-Mitarbeiter einen der vorgeschlagenen Leistungsindikatoren dar. Andere Indikatoren beziehen sich darauf, wie schnell Compliance-Anforderungen identifiziert werden und ihre Erfüllung umgesetzt wird. Ein weiterer Indikator für die IT-Zielsetzung, IT-Compliance mit Gesetzen und Vorschriften sicherzustellen, ist die Anzahl der Fälle von Non-Compliance, die an die Unternehmensleitung gemeldet oder die öffentlich publik geworden sind.

COBIT bietet zudem als Grundlage einer Bewertung für jeden IT-Prozess ein Maturitätsmodell an, das an das Reifegradmodell von CMMI (Capability Maturity Model Integration) angelehnt ist. Für ME 3 enthält Tabelle 13.3. die wesentlichen Merkmale des Maturitätsmodells.

TABELLE 13.3 Maturitätsmodell des COBIT-Prozesses ME 3 – Stelle Compliance mit Vorgaben sicher.

Stufe	Merkmale
0 (nicht existent)	▪ Bewusstsein für Compliance-Anforderungen ist nur gering ausgeprägt. ▪ Prozess zur Einhaltung von Compliance-Anforderungen ist nicht vorhanden.
1 (initial)	▪ Bewusstsein für Compliance-Anforderungen ist vorhanden. ▪ Informelle Prozesse zur Aufrechterhaltung von Compliance im Rahmen von Projekten oder als Folge von Audits werden befolgt.
2 (wiederholbar, aber intuitiv)	▪ Bewusstsein für Compliance-Anforderungen ist vorhanden und Notwendigkeit wird kommuniziert. ▪ Bereichsspezifische Compliance-Verfahren sind definiert. ▪ Wissen und Verantwortung von Einzelpersonen stehen im Vordergrund. ▪ Compliance-Schulungen erfolgen informell.

Stufe	Merkmale
3 (definiert)	▪ Richtlinien, Verfahren und Prozesse sind entwickelt, dokumentiert und kommuniziert, werden aber nicht durchgängig angewendet. ▪ Eine Überwachung erfolgt nur eingeschränkt. ▪ Manche Compliance-Anforderungen werden nicht erfüllt. ▪ Compliance-Schulungen werden für den Bereich der gesetzlichen und regulatorischen Vorgaben angeboten.
4 (gemanaged und messbar)	▪ Verständnis für Compliance ist umfassend vorhanden. ▪ Ein formelles Compliance-Schulungsprogramm existiert. ▪ Standardisierte Compliance-Prozesse zur Überwachung von Non-Compliance sind etabliert. ▪ Reviews des Umfeldes werden genutzt. ▪ Ursachen von Non-Compliance werden identifiziert und beseitigt.
5 (optimiert)	▪ Eine zentrale Compliance-Funktion, die den Compliance-Prozess steuert, ist etabliert. ▪ Das Wissen über externe Anforderung ist umfangreich vorhanden und wird intern kommuniziert. ▪ Das Unternehmen ist in externe Plattformen integriert und kann auf externe Anforderungen Einfluss nehmen. ▪ Ein Compliance-Überwachungsprozess, der auch ein Self-Assessment beinhaltet, ist implementiert, sodass Non-Compliance nur selten auftritt. ▪ Compliance-Schulungen müssen nur noch für neue Mitarbeiter oder bei wesentlichen Veränderungen durchgeführt werden.



Praxistipp: Eigene Konzeption der IT-Compliance an COBIT orientieren.

COBIT ist das führende Framework für das IT-Management – gerade auch aus Sicht von Wirtschaftsprüfern bzw. externen IT-Auditoren. Der Compliance-Teil von COBIT bietet eine gute Grundlage für eigene Konzeptionen und hat den Vorteil, dass er in ein umfangreiches IT-Governance Framework integriert ist. COBIT kann deswegen gut als Ausgangspunkt für die Konzeption der IT-Compliance dienen.

■ 13.4 Nutzen von IT-Compliance

Neben der selbstverständlichen Pflicht zur Erfüllung gesetzlicher Vorschriften soll IT-Compliance ein Unternehmen vor allem vor wirtschaftlichen Nachteilen als Folge von Rechtsverletzungen bewahren. Es sollen insbesondere Schadensersatzpflichten, Strafen, Buß- und Zwangsgelder, aber auch erhöhte Steuerzahlungen aufgrund von Schätzungen des Finanzamts vermieden werden. So kann beispielsweise ein Schaden entstehen, wenn ein Unternehmen im Rahmen einer gerichtlichen Auseinandersetzung beweishebliche Daten und Dokumente

nicht vorlegen und damit seiner Beweisspflicht nicht nachkommen kann. Wird im Zusammenhang mit steuerrelevanten Unterlagen gegen Archivierungspflichten verstoßen, drohen Strafzahlungen wegen Steuerverkürzung. Zusätzlich zu diesen monetären Schäden ist auch ein potenzieller Imageschaden zu bedenken. Dieser kann sich leicht einstellen, wenn etwa gegen Datenschutznormen verstoßen wird oder Kundendaten missbraucht werden. Die Folgen können eine negative Publizität, Nachteile bei der Vergabe öffentlicher Aufträge oder gar Kundenabwanderungen sein.

Neben dieser Schutzfunktion, die auf die Vermeidung von Nachteilen zielt, ist IT-Compliance mit folgenden teils direkten, teils indirekten Vorteilen verbunden (siehe Abbildung 13.9).

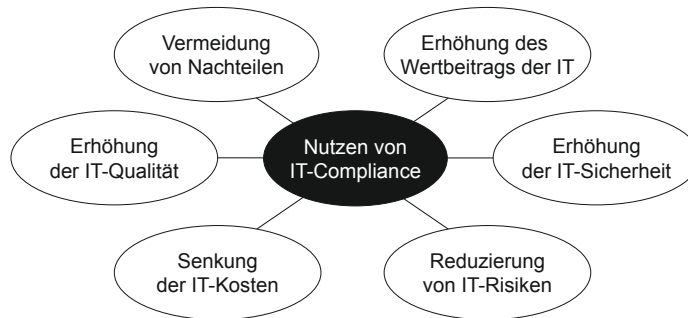


ABBILDUNG 13.9
Nutzen von IT-Compliance

■ Wertbeitrag

Wenn die IT eines Unternehmens ihre Compliance nachweisen kann, führt dies auf vielfältigen Wegen zu einer Erhöhung des Unternehmenswertes. Erweisen sich bestimmte Standards (z. B. Sicherheitszertifikate) als Markteintrittsbarrieren, ist der Wertbeitrag der IT offensichtlich. Ohne die Konformität zu derartigen externen Vorgaben könnten Umsatzchancen nicht genutzt werden. Andererseits kann mangelnde IT-Compliance zu Abschlüssen bei der Bestimmung des Unternehmenswertes im Falle von Unternehmenstransaktionen führen, wenn sich während einer Due-Diligence-Prüfung IT-Compliance-Risiken offenbaren. Gerät ein Unternehmen mit negativen Schlagzeilen in die Presse (beispielsweise wegen mangelndem Datenschutz), werden hierdurch auch wirtschaftliche Nachteile zu befürchten sein. Kundenverluste können den Produktabsatz reduzieren und aufwändige PR-Kampagnen erforderlich machen.

■ IT-Qualität

Viele Maßnahmen zur Herstellung von IT-Compliance tragen zu einer höheren Qualität von IT-Prozessen bei. Eine systematische Konzeption von Abläufen, verbunden mit ihrer Dokumentation und IT-technischen Unterstützung, wird in der Regel zu einer Erhöhung der Produktivität und zur Möglichkeit einer kontinuierlichen Verbesserung führen. Vor allem eine Konformität mit Best-Practice-Verfahren führt zu einer Steigerung der Prozessqualität, häufig verbunden mit einer höheren Nachvollziehbarkeit und Sicherheit in den betroffenen IT-Prozessen. So dient beispielsweise die Zuordnung von Personen zu Aufgaben und Rollen dem Nachweis der ordnungsmäßigen Bearbeitung (kritischer) Transaktionen durch autorisierte Personen. Eine qualitätssteigernde Wirkung liegt weiterhin vor, wenn Compliance-Anforderungen und Kontrollen als Elemente des IKS systematisch aufeinander abgestimmt werden. Hieraus resultiert eine höhere Transparenz, die die gesamte IT-Architektur umfasst und letztlich ein effektives Enterprise Architecture Management (EAM) unterstützt. Eine in

diesem Sinne verbesserte Qualität führt zu einer Reduzierung der Komplexität der IT-Infrastruktur und somit zu einer verbesserten Steuerungsfähigkeit, aber auch Auditierbarkeit der IT.

■ IT-Sicherheit

Hinsichtlich des IT-Sicherheitsmanagements liegen Normen und Standards vor (z.B. die ISO/IEC Normen-Reihe 2700x oder die Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik – BSI), mit denen die Unternehmens-IT gegebenenfalls compliant zu sein hat. Darüber hinaus adressieren Maßnahmen der IT-Compliance, die die Ordnungsmäßigkeit des IT-Betriebs sicherstellen, besonders die IT-Sicherheitsziele der Vertraulichkeit, Verfügbarkeit und Integrität. Hieraus resultieren Synergiepotenziale, die bei einer abgestimmten Vorgehensweise realisiert werden können. Auf diese Weise entfaltet IT-Compliance zusätzliche Nutzenpotenziale für die IT-Sicherheit.

■ IT-Risiken

Ähnliches wie für die IT-Sicherheit gilt für das IT-Risikomanagement. Auch hier existieren Normen und Standards für die Unternehmens-IT, z. B. die Norm „ISO/IEC 27005 – Information Security Risk Management“ oder das „Risk IT Framework“ der ISACA, die es zu erfüllen gilt, wenn sie für das Unternehmen als verbindlich erachtet werden. Aber selbst wenn dies nicht der Fall ist, ergeben sich Synergieeffekte für das IT-Risikomanagement, das durch gleichgerichtete Maßnahmen der IT-Compliance verstärkt wird. Somit entfaltet IT-Compliance auch für das Management von IT-Risiken zusätzliche Nutzenpotenziale – insbesondere dann, wenn eine Integration mit dem IT-Sicherheitsmanagement erfolgt (dass dies erforderlich ist, lässt sich schon daran erkennen, dass die ISO/IEC 27005 Teil der ISO/IEC Normen-Reihe 2700x ist).

■ IT-Kosten

Die verschiedenen Maßnahmen der IT-Compliance verursachen selbstverständlich Kosten. Da die Maßnahmen aber auch aus Gründen der Risikoreduzierung und der Erhöhung der IT-Sicherheit erfolgen, lassen sich die damit verbundenen Kosten oft nicht eindeutig der IT-Compliance zurechnen. Dies gilt natürlich auch umgekehrt für die Kosteneinsparungen, die sich unter anderem aus der Automatisierung manueller Arbeitsabläufe (beispielsweise bei der Überwachung oder im Reporting), geringeren Kosten in der IT-Administration und -Wartung oder bei der Durchführung von Prüfungshandlungen ergeben. Der quantitative wirtschaftliche Nutzen von Maßnahmen der IT-Compliance kann – wenn überhaupt – somit nur in einem größeren Zusammenhang ermittelt werden. Trotzdem gilt, dass IT-Compliance zwar Investitionen erfordert, aber auch zur Reduzierung von IT-Kosten beiträgt.



Praxistipp: Keine Nutzenbetrachtung von IT-Compliance ohne Nutzenverfolgung.

Ohne eine Nutzenbetrachtung wird kein Business Case für IT-Compliance auskommen. Insofern müssen Sie unbedingt den Nutzen detailliert abschätzen. Dies ist allerdings in den meisten Fällen nicht leicht. Nutzen Sie bereits vorhandene Erfahrungen und bewerten Sie kritisch, inwieweit mit den Maßnahmen der IT-Compliance ein intendierter Nutzen auch wirklich realisiert wurde. Nur so lässt sich eine realistische Sicht auf den Nutzen von IT-Compliance erreichen.

■ 13.5 Beteiligte und Interessenlagen

Der Kreis der grundsätzlich an der Herstellung von IT-Compliance beteiligten Personen und Gruppen erweist sich als durchaus umfangreich. Auch wenn in der fachlichen Diskussion oftmals ein „IT-Compliance-Officer“ im Mittelpunkt steht, hat die aufbauorganisatorische Gestaltung alle Beteiligten im Rahmen eines Stakeholder-Ansatzes einzubeziehen (siehe Abbildung 13.10) und ihre Aufgaben- und Verantwortungsteilung in Bezug auf IT-Compliance zu regeln.

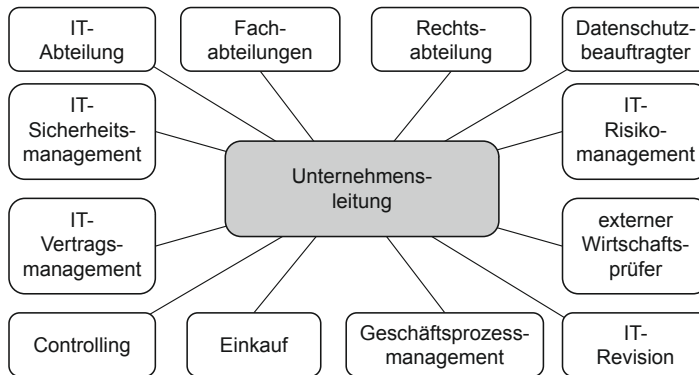


ABBILDUNG 13.10
An IT-Compliance beteiligte Stakeholder

Die Hauptverantwortung für IT-Compliance kommt der Unternehmensleitung zu. Dies ergibt sich aus expliziten gesetzlichen Vorgaben sowie generellen Sorgfaltspflichten der Unternehmensorgane (zwecks Vermeidung eines Organisationsverschuldens). Vor allem das KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) hat mit der persönlichen Inanspruchnahme von Vorstandsmitgliedern dafür gesorgt, dass Compliance heute die Aufmerksamkeit der Unternehmensleitung erlangt. So drohen ihr nämlich bei Verstößen gegen Compliance-Anforderungen die Verweigerung der Entlastung, eine Abberufung, eine außerordentliche fristlose Kündigung oder gar eine persönliche Haftung.

Die Unternehmensleitung muss zur Wahrnehmung ihrer Compliance-Verantwortung konzeptionelle und operative Aufgaben und die hierfür erforderlichen Befugnisse delegieren. Der Kreis der hierfür zur Verfügung stehenden Funktionsträger hängt von der Unternehmensgröße, der Gesellschaftsform und der Branchenzugehörigkeit ab. In jedem Falle sind aber die IT-Abteilung und die Fachabteilungen als Hauptbeteiligte einzubeziehen.

Die IT-Abteilung und ihre Leitung bzw. der CIO haben den Großteil an Maßnahmen zur Erfüllung der Compliance-Anforderungen zu planen und durchzuführen, zumindest soweit es die informations- und kommunikationstechnischen Mittel anbelangt. Hierbei sind die Entwicklung und der Betrieb von IT-Systemen selbst an IT-Standards (wie der Information Technology Infrastructure Library – ITIL) auszurichten, oder die Anforderungen aus Gesetzen (wie beispielsweise dem BDSG) sind direkt umzusetzen. Hierzu müssen IT-Kontrollen eingeführt werden, entweder als prozessintegrierte Kontrollen einzelner IT-Anwendungen (z. B. Eingabeprüfungen) oder als generelle IT-Kontrollen, die auf die gesamte IT wirken. Beispiele für generelle IT-Kontrollen sind Benutzerberechtigungskonzepte, Zugriffsschutzverfahren und Change-Management-Verfahren.

Auch die Fachabteilungen tragen eine Verantwortung für die Erfüllung von Compliance-Anforderungen – und zwar immer dann, wenn bereichsbezogene organisatorische oder personelle Maßnahmen ergriffen und entsprechende Kontrollen eingeführt werden. Vor allem die „Awareness“ für IT-Compliance, insbesondere für Datenschutz und Datensicherheit, muss bei den IT-Nutzern in den Fachabteilungen entwickelt werden.

In größeren Unternehmen sind weiterhin eine ganze Reihe von Stellen und Funktionen potenziell mit IT-Compliance befasst:

- Die unternehmensinterne Rechtsabteilung stellt in der Regel im Auftrag der Unternehmensleitung die Einhaltung von rechtlichen Vorgaben im Unternehmen sicher. Die juristische Beurteilung gesetzlicher und vertraglicher Anforderungen an die IT ist eine Kernkompetenz der Rechtsabteilung, der somit eine wichtige Verantwortung auch für die IT-Compliance zukommt.
- Eine weitere Schnittstelle ergibt sich zum Geschäftsprozessmanagement hinsichtlich der Compliance von Geschäftsprozessen. Soweit Stellen mit spezialisierter Prozessverantwortung eingerichtet sind, ist zu prüfen, ob und gegebenenfalls inwieweit ihr Verantwortungsbereich um Aspekte der IT-Compliance zu erweitern ist.
- Der oben beschriebene inhaltliche Zusammenhang zwischen IT-Risikomanagement und IT-Compliance erfordert auch auf institutioneller Ebene eine Zusammenarbeit zwischen den entsprechenden organisatorischen Einheiten. Soweit sich das Risikomanagement auf existenzgefährdende Unternehmensrisiken konzentriert, werden in Bezug auf die IT die Bereiche des Notfalls- und Kontinuitätsmanagements im Vordergrund stehen. Ein weiterer Bereich der Zusammenarbeit kann das Management von IT-Projektrisiken sein, wenn für die Unternehmensentwicklung wesentliche IT-Entwicklungen betroffen sind.
- Ähnliches gilt für das IT-Sicherheitsmanagement. Zahlreiche Regelwerke (bspw. BDSG, ISO/IEC 27001, ITIL) stellen Anforderungen an die Sicherheit der IT-Systeme bzw. ihre Komponenten (z. B. IT-Infrastruktur, IT-Anwendungen, Daten, IT-Prozesse). Viele IT-Sicherheitslösungen können dazu beitragen, Anforderungen der IT-Compliance zu erfüllen (wie das obige Beispiel für das BDSG zeigt).
- Mit dem Vertragsmanagement sind in manchen Unternehmen anstelle der Rechtsabteilung die Einkaufsabteilung oder das Controlling befasst, sodass diese Stellen mitunter auch Überwachungs- und Steuerungsaufgaben bei der Durchführung von IT-Verträgen wahrnehmen. Falls vertraglich geregelte Leistungen im Rahmen von IT-Projekten erbracht werden, kann das Vertragscontrolling auch Aufgabe des IT-Projektmanagements sein.
- Mit dem durch das Bundesdatenschutzgesetz in § 4f BDSG vorgeschriebenen Datenschutzbeauftragten gibt es zudem eine Stelle im Unternehmen, die bezogen auf das Gebiet des Datenschutzes bereits eine Compliance-Funktion wahrnimmt.
- Wenn Buchführung und Finanztransaktionen des Unternehmens IT-gestützt erfolgen, ist die Ordnungsmäßigkeit der IT Gegenstand sowohl der externen Jahresabschlussprüfung als auch der internen Revision. Hierzu haben beide Prüfungsinstanzen unter anderem die Angemessenheit und Wirksamkeit des IT-Kontrollsystems zu beurteilen, indem sie die Durchführung verschiedener IT-Kontrollen prüfen. Hierbei orientieren sie sich an entsprechenden Standards und Normen zum Prüfwesen, zur IT-Sicherheit und zum IT-Risikomanagement.

Neben den hier aufgeführten gibt es weitere Stellen und Funktionen, die sich nach Branchen-erfordernissen richten (z.B. in der Banken-, Telekommunikations- oder Pharmabranche). Auch hier gibt es häufig Bezüge zur IT-Compliance, sodass diese Stellen ebenfalls zu beteiligen sind. Für eine diesbezügliche Klärung sollte die unternehmensinterne Rechtsabteilung der erste Ansprechpartner sein.

Das Interesse der Stelleninhaber und Funktionsträger an IT-Compliance wird sich nach dem Inhalt und Umfang der an sie delegierten Verantwortung richten. In jedem Falle ist eine persönliche Haftung zu befürchten, und zwar nicht nur für die Unternehmensleitung. Bei einer nicht regelkonformen Aufgabenausführung können auch Mitarbeiter prinzipiell zur Verantwortung gezogen und haftbar gemacht werden. Für ausführende Mitarbeiter ergibt sich dies aus den Regelungen zur Arbeitnehmerhaftung.

In vielen Unternehmen stellt sich derzeit die Herausforderung, überhaupt erst einmal eine allgemeine Compliance-Funktion einzurichten, in die es wiederum die Verantwortung für IT-Compliance zu integrieren gilt. In dieser Konstellation bietet sich für die Beteiligten die Chance, den eigenen Aufgaben- und Verantwortungsbereich zu erweitern. Mitunter können sich so auch neue Karrierepfade eröffnen. Auf der anderen Seite droht neue Konkurrenz um Ressourcen und Einfluss. Diese Unsicherheiten gilt es bei der institutionellen Verankerung von (IT-)Compliance im Unternehmen durch eine klare Aufgaben- und Verantwortungsteilung zu beseitigen. Es ist zentrale Verantwortung der Unternehmensleitung, die Klärung dieser Fragen zu initiieren und durchzusetzen.



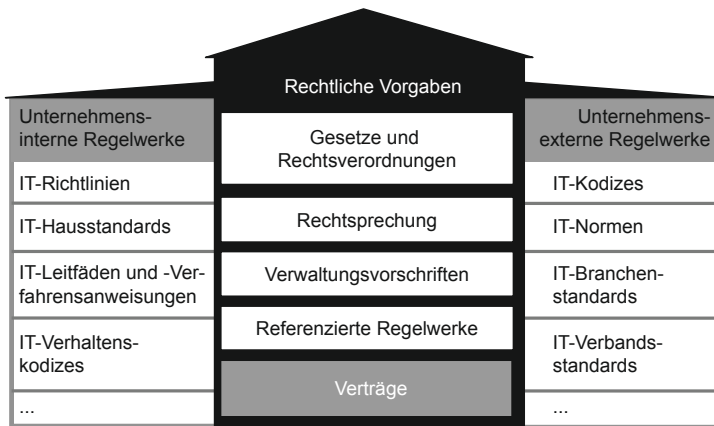
Praxistipp: IT-Compliance benötigt Stakeholder-Management.

Vor allem in der Implementierungsphase von IT-Compliance ist ein systematisches Stakeholder-Management erforderlich. Das Stakeholder-Management hat die Anforderungen und Erwartungen der Stakeholder zu ermitteln und bei der Konzeption und Umsetzung zu berücksichtigen. Während der gesamten Einführung ist die Kommunikation so zu steuern, dass die Bedürfnisse der Stakeholder erkannt und – soweit möglich – erfüllt sowie Probleme gemeinsam identifiziert und gelöst werden können.

■ 13.6 IT-relevante Regelwerke

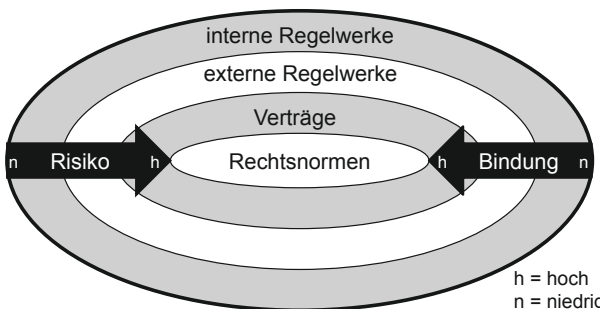
13.6.1 Klassifikation der Regelwerke

Wie für die Corporate Compliance lassen sich auch für die IT-Compliance grundsätzlich drei Gruppen von Regelwerken unterscheiden, die in ihrer Summe ein Grundgerüst für eine systematische Analyse von Compliance-Anforderungen darstellen (siehe Abbildung 13.11):

**ABBILDUNG 13.11**House of
IT-Compliance

- rechtliche Vorgaben an die IT, d. h. Rechtsnormen (also vom Gesetzgeber erlassene Gesetze sowie auf deren Grundlage von den Verwaltungen erlassene Rechtsverordnungen), Rechtsprechung, Verwaltungsvorschriften und weitere Regelwerke, auf die in Gesetzen, Rechtsverordnungen und Verwaltungsvorschriften verwiesen wird oder die von der Rechtsprechung zur Auslegung herangezogen werden, sowie Verträge, die ein Unternehmen mit Kunden, Lieferanten und sonstigen Marktpartnern abschließt und die IT-relevante Vereinbarungen enthalten;
- unternehmensexterne, auf IT bezogene Regelwerke, wie IT-Kodizes, IT-Normen oder IT-Standards vielfältiger Institutionen;
- unternehmensinterne Regelwerke, wie IT-Richtlinien, IT-Organisations- oder Verfahrensanweisungen, Verhaltenskodizes, Service-Level-Agreements (SLAs) oder Hausstandards, soweit sie IT-relevante Vorgaben enthalten.

Mit der Überlegung, dass sowohl der Bindungsgrad als auch das Risiko bei einem Verstoß in der genannten Reihenfolge tendenziell abnehmen, ergibt sich das in Abbildung 13.12 dargestellte „Zwiebelmodell“.

**ABBILDUNG 13.12**

Zwiebelmodell für Compliance-relevante Regelwerke

Bei Rechtsnormen und Verträgen ergeben sich höhere Risiken, weil hier oft ein monetäres Strafmaß entweder gesetzlich oder vertraglich geregelt ist bzw. aus Vertragsverletzungen teilweise bestandsgefährdende Schadensersatzpflichten resultieren können. Außerdem kommen in diesen Fällen häufig Vertrauensverlust und Imageschäden hinzu, die das Schadensausmaß zusätzlich erhöhen. Durch strafverfolgende Institutionen bzw. Vertragspartner, die ihre Inter-

essen wahren wollen, ergibt sich auch eher die Wahrscheinlichkeit, dass ein Verstoß reklamiert und ein Anspruch verfolgt und durchgesetzt wird.

Bei den externen Regelwerken ist zu beachten, dass diese ggf. aufgrund Verweis oder Heranziehung zur Auslegung der Rechtsnormen letztlich deren Bindungswirkung und das daraus resultierende Risiko teilen. Die Regelwerke dieser Gruppe erlangen dann eine höhere Bindungswirkung, wenn ihre Einhaltung von Dritten (z. B. Wirtschaftsprüfern, Kunden) eingefordert wird.



Praxistipp: Entscheiden, welche Regelwerke berücksichtigt werden.

Der Umfang von und der Aufwand für IT-Compliance hängt wesentlich davon ab, welche Regelwerke im Verantwortungsbereich der IT-Compliance liegen. Soll nur eine Beschränkung auf rechtliche Regelwerke – und somit auf Legal IT-Compliance – erfolgen? Oder werden auch weitere interne und externe Regelwerke einbezogen? Und wenn ja, welche? Diese Fragen sind als konstitutive Entscheidungen der IT-Compliance anzusehen; sie müssen von der Unternehmensleitung und der IT-Leitung vor der strukturellen Implementierung von IT-Compliance beantwortet werden.

13.6.2 Rechtliche Vorgaben

Gesetze und Rechtsverordnungen

Im Zentrum der rechtlichen Vorgaben stehen Rechtsnormen, also Gesetze und Rechtsverordnungen. Die Notwendigkeit zur Einhaltung der IT-Compliance ergibt sich nicht nur aus Gesetzen, die sich schon vom Namen her offensichtlich auf die IT beziehen, wie beispielsweise das Bundesdatenschutzgesetz, das Signaturgesetz oder das Telemediengesetz. Vielmehr regeln zahlreiche weitere Gesetze den IT-Einsatz im Unternehmen, z. B. das Betriebsverfassungsgesetz, das Strafgesetzbuch sowie hinsichtlich der Buchführungs- und steuerlichen Pflichten das Handelsgesetzbuch und die Abgabenordnung nebst Teilen der einzelnen Steuergesetze. Vertragliche Anforderungen sind insbesondere im Bürgerlichen Gesetzbuch geregelt. Tabelle 13.4 enthält die für IT-Compliance wesentlichen nationalen Gesetze. Weiterhin zählen zu dieser Gruppe die Rechtsentwicklungen, die sich auf EU-Ebene vollziehen (z. B. Basel II oder die 8. EU-Richtlinie, auch kurz „Euro-SOX“ genannt).

TABELLE 13.4 Für IT-Compliance relevante Gesetze

Abkürzung	Gesetz
AO	Abgabenordnung
BGB	Bürgerliches Gesetzbuch
BGB-InfoV	Verordnung über Informations- und Nachweispflichten nach bürgerlichem Recht
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
EStG	Einkommensteuergesetz
HGB	Handelsgesetzbuch

Abkürzung	Gesetz
KStG	Körperschaftsteuergesetz
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
UrhG	Urheberrechtsgesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
ZPO	Zivilprozessordnung

Rechtsprechung

Zu den rechtlichen Vorgaben zählt weiterhin die Rechtsprechung, die die Rechtsnormen auslegt und damit wesentlich deren Inhalt bestimmt. Dies betrifft in besonderem Maße sogenannte unbestimmte Rechtsbegriffe bzw. Generalklauseln. Beispiele hierfür sind die „übliche Beschaffenheit“, die das Vorliegen eines Mangels im Werkvertragsrecht bestimmt, oder die „im Verkehr erforderliche Sorgfalt“, deren Missachtung den Vorwurf fahrlässigen Verhaltens begründet.

Beispiel:

Das Oberlandesgericht Hamm hat in seinem Urteil vom 01.12.2003 (Az. 13 U 133/03) eine unterlassene Datensicherung bei Schäden, die durch Datenverluste entstehen, als Mitverschulden gewertet. In dem entschiedenen Fall war bei einer Reparatur durch eine beauftragte Computerfirma ein Datenverlust infolge eines Server-Absturzes entstanden. Das Gericht stellte fest, dass eine Datensicherung täglich zu erfolgen hat, eine Vollsicherung mindestens einmal wöchentlich. Da in dem Fall Letztere nicht einmal monatlich erfolgt war, wurde der Schaden der klagenden Auftraggeberin allein zugerechnet und ihr Schadensersatzanspruch abgewiesen.

Verwaltungsvorschriften

Auch ohne dass es sich um Rechtsnormen im engeren Sinne handelt, sind für IT-Compliance ferner Regelwerke relevant, die von den zuständigen (Aufsichts-)Behörden zur Interpretation und Ausführung der Rechtsnormen aufgestellt oder erklärtermaßen herangezogen werden. Diese Regelwerke bewirken rechtlich eine Selbstbindung der Verwaltung, indem sie die Anwendung der Rechtsnormen durch die Verwaltung bestimmen. Zudem ist die Entwicklung zu beobachten, dass es zunehmend Darlegungen gibt, wie spezielle Fragen zur Nutzung von IT aus Sicht der Verwaltung zu handhaben sind – allerdings ohne bindende Wirkung. Hieraus ergeben sich zum Teil recht komplexe Verweisungsstrukturen der verschiedenen Vorschriften.

Beispiel:

Sowohl die „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme“ (GoBS) als auch die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ (GDPdU) wurden vom Bundesministerium für Finanzen (BMF) als Verwaltungsanweisung erlassen. Sie interpretieren die Regelungen der Abgabenordnung zu den Anforderungen an die ordnungsgemäße Buchführung beim Einsatz IT-gestützter Buchhaltungssysteme und bei Verwendung digitaler Unterlagen. Als regulatorische Grundlage sind weiterhin folgende Regelwerke relevant (nach [KS11], S. 10f.):

- Häufig gestellte Fragen beantwortet das BMF in einem Fragen- und Antwortenkatalog, der laufend aktualisiert wird und mittlerweile in der 7. Fassung vom 22.01.2009 vorliegt.

Das BMF weist jedoch explizit darauf hin, dass dieser Fragenkatalog nur als Orientierungshilfe dient und für die Prüfungsdienste nicht die bindende Wirkung eines BMF-Schreibens hat.

- Die GDPdU machen keine konkreten Angaben über das Format des zu überlassenden Datenträgers. Es wird allerdings gefordert, dass alle zur Auswertung der überlassenen Daten notwendigen Informationen ebenfalls bereitgestellt werden. Das BMF empfiehlt in der „Information zum ‚Beschreibungsstandard für die Datenträgerüberlassung‘“ einen Beschreibungsstandard der Audicon GmbH, der ein Verfahren zur Beschreibung der Daten, Datenstrukturen und Verknüpfungen konkretisiert.
- Bei Nichterfüllung der zeitnahen Mitwirkungspflichten des Steuerpflichtigen kann die Finanzbehörde ein Verzögerungsgeld verhängen. Die Höhe des Verzögerungsgeldes beträgt gem. § 146 Abs. 2b AO mindestens 2.500,- € und höchstens 250.000,- €. Zum Verzögerungsgeld gibt es einen separaten Fragen-Antwort-Katalog des BMF vom 22. April 2010.

In Bezug genommene Regelwerke

Regelwerke, die als solche keinen Rechtsnormcharakter haben und sowohl von Verwaltungen wie auch von privatrechtlichen Institutionen (z. B. dem DIN Deutsches Institut für Normung) stammen können, haben für die IT-Compliance die gleiche Bedeutung wie Rechtsnormen, wenn sie durch ausdrückliche Verweisung in diese einbezogen werden.

Beispiel:

Die von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) erstmals am 20. 12. 2005 per Rundschreiben herausgegebenen MaRisk (Mindestanforderungen an das Risikomanagement) konkretisieren das von Kreditinstituten nach § 25a Abs. 1 KWG (Kreditwesengesetz) einzurichtende Risikomanagement. Die der MaRisk zugehörige Erläuterung verweist sowohl auf die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebenen IT-Grundsatzkataloge als auch auf die ISO 17799, siehe Tabelle 13.5. Dies hat zur Folge, dass Kreditinstitute, um keinen Beanstandungen der BaFin ausgesetzt zu sein, ein diesen Normen und Standards entsprechendes Sicherheitsniveau zu realisieren haben.

TABELLE 13.5 Auszug aus MaRisk Anlage 1: MaRisk - Regelungstext mit Erläuterungen in der Fassung vom 04.05.2006 (entnommen aus [BF06])

AT 7.2 Technisch-organisatorische Ausstattung	
1 ...	
2 Die IT-Systeme (Hardware- und Software-Komponenten) und die zugehörigen IT-Prozesse müssen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen. Für diese Zwecke ist bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen. Ihre Eignung ist regelmäßig von den fachlich und technisch zuständigen Mitarbeitern zu überprüfen.	Standards zur Ausgestaltung der IT-Systeme Zu solchen Standards zählen z. B. das IT-Grundsatzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der internationale Sicherheitsstandard ISO 17799 der International Standards Organization. Das Abstellen auf gängige Standards zielt nicht auf die Verwendung von Standardhardware bzw. -software ab; Eigenentwicklungen sind grundsätzlich ebenso möglich.
3 ...	

13.6.3 Verträge

Vertragsverstöße stellen für ein Unternehmen operationelle Risiken dar, die es mittels einer effektiven und effizienten Vertragssteuerung zu managen gilt. Zwei Gruppen von Verträgen sind hier von Bedeutung:

- Verträge allgemeiner Art, deren Vertragsgegenstand sich nicht auf IT-Belange konzentriert, die aber einzelne IT-relevante Regelungen enthalten (beispielsweise zum Austausch oder zur Aufbewahrung von Informationen) oder die dem Vertragsdokument als IT-Objekt einen schutzwürdigen Status zuerkennen (was gewöhnlich durch eine Geheimhaltungsvereinbarung geschieht);
- spezifische IT-Verträge, deren Vertragsgegenstand sich auf IT-Leistungen bezieht und die dadurch direkt relevant sind für IT-Compliance (z.B. IT-Entwicklungs- oder Schulungsverträge, Softwareüberlassungs- und Softwarepflegeverträge, Providerverträge).

Während das Vertragscontrolling Leistungserbringer und -empfänger kontinuierlich im Auge behalten muss, stehen aus Compliance-Sicht nur diejenigen vertraglichen Vereinbarungen im Fokus, aus denen sich IT-spezifische Pflichten und Obliegenheiten des Unternehmens als Vertragspartner ergeben. Diese beziehen sich z.B. auf die Erfüllung von Dokumentationspflichten sowie Geheimhaltungsabreden. In Bezug auf das Risikomanagement stehen solche Regelungen im Vordergrund, aus denen sich Risiken hinsichtlich von Schadensersatzansprüchen oder Vertragsstrafen ergeben.

13.6.4 Unternehmensexterne Regelwerke

In die Gruppe der unternehmensexternen Regelwerke fallen viele derjenigen Regelwerke, die derzeit im IT-Management große Aufmerksamkeit erfahren, vor allem die als „Framework“, „Referenzmodell“ oder „Best-Practice-Modell“ gehandelten IT-Standards, wie CMMI (Capability Maturity Model Integration), ITIL und COBIT. Insgesamt sind die in dieser Gruppe vertretenen Regelwerke höchst unterschiedlich. Die Spannbreite reicht von IT-Richtlinien supranationaler Organisationen, wie der OECD (Organisation for Economic Co-operation and Development), über nationale und internationale IT-Normen (z.B. ISO/IEC 20000, ISO/IEC 2700x), Standards internationaler und nationaler Verbandsorganisationen und behördlicher Einrichtungen bis hin zu Empfehlungen oder Konzepten, die sich im Laufe der Zeit durch Informations- und Erfahrungsaustausch in der Fachwelt herausgebildet haben.

Beispiel für eine internationale Richtlinie

Die „Guidelines for the Security of Information Systems and Networks“ der OECD wurden am 25. Juli 2002 vom Rat der OECD angenommen und verabschiedet. Das übergeordnete Ziel besteht darin, gemeinsam eine „Kultur der Sicherheit“ im Internet zu etablieren. Die Richtlinie beschreibt die übergeordnete Zielsetzung der IT-Sicherheit aus Sicht der OECD-Staaten und plädiert für ein Mehr an Sicherheitsbewusstsein und Sicherheitsverantwortung. Sie umfasst neun Empfehlungen, die in ihrer Allgemeinheit jedoch auch weitestgehend für Unternehmen zutreffen. Einzelne Empfehlungen richten sich auf die Durchführung von Risikoanalysen, die Bedeutung von IT-Sicherheit als integralem Bestandteil von Systementwurf und -implementierung oder die wiederkehrende Überprüfung von Informationssystemen und IT-Infrastruktur hinsichtlich ihrer Sicherheit.

Aus Sicht der IT-Compliance sind in dieser Gruppe vor allem Regelwerke von hoher Relevanz, die als Basis für Testierungen oder Zertifizierungen dienen. Hierzu zählen insbesondere die bereits erwähnten Prüfungs- und Rechnungslegungsstandards des IDW. In Bezug auf die Abschlussprüfung sind dies z. B. der IDW Prüfungsstandard (PS) 330 und die Stellungnahmen des IDW-Fachausschusses für Informationstechnologie zur Rechnungslegung (RS FAIT) 1 bis 3. Im betrieblichen Alltag sind an vielen Stellen mittlerweile Normen und Standards maßgebend, so auch für die IT, wobei die Grenzen mitunter fließend erscheinen und die Verbindlichkeit der verschiedenen Regelwerke oft nicht deutlich wird.



Exkurs: Normen vs. Standards

Da Normen eine Spezialisierung von Standards darstellen, hat die Begriffsklärung beim Begriff des Standards anzusetzen. Ein Standard ist zunächst ein Regelwerk, das beschreibt, wie etwas zu tun, zu lösen oder handzuhaben ist. Nun stellt jedoch nicht jede Zusammenfassung von Richtlinien, Best-Practices, Empfehlungen u. Ä. sofort einen Standard dar. Zur bloßen Existenz eines schriftlichen Regelwerkes muss hinzukommen, dass die als Standard beschriebenen Regeln breit akzeptiert und angewendet werden. Der Akzeptanzbereich kann dabei geographisch (z. B. auf einen Staat oder eine Staatengemeinschaft) oder auf eine nationale, internationale oder globale Anwendergruppe (z. B. Softwareentwickler, Projektmanager) beschränkt sein. Die Anwendergruppe muss zudem den Standard nicht nur kennen und akzeptieren, sondern auch wirklich praktisch nutzen. Aus dieser Nutzung muss sich außerdem eine Rückkopplung für die Weiterentwicklung des Standards ergeben.

Eine Norm ist nun ein Standard, der von einer offiziellen Normungsorganisation als Ergebnis eines systematischen, festgelegten Normungsverfahrens beschlossen und veröffentlicht wurde. Eine Norm ist ein *„Dokument, das mit Konsens erstellt und von einer anerkannten Institution angenommen wurde und das für die allgemeine und wiederkehrende Anwendung Regeln, Leitlinien oder Merkmale für Tätigkeiten oder deren Ergebnisse festlegt, wobei ein optimaler Ordnungsgrad in einem gegebenen Zusammenhang angestrebt wird“* ([DIN04], S. 23). Aufgrund des formalisierten Erstellungsprozesses beinhalten Normen in der Regel nicht den innovativsten Stand eines Anwendungsgebietes, sondern schreiben vielmehr die durch praktische Bewährung allgemein anerkannten Regeln eines (häufig technischen) Anwendungsbereiches fest. Ihre Einhaltung wird zudem mitunter in nationalen und internationalen Vorschriften, d. h. Gesetzen und Verordnungen, verbindlich vorgeschrieben.

Normen stellen somit eine Teilmenge von Standards dar; sie werden mitunter auch als „de-jure-Standard“ bezeichnet. Eine Norm gewinnt dadurch einen offiziellen Charakter, dass die jeweilige Normungsorganisation in der Lage ist, die Norm in ihrem Geltungsbereich (fachlich) durchzusetzen.

Für IT-Compliance relevante Normungsorganisationen sind zuständig:

- auf internationaler Ebene die „International Standardization Organization“ (ISO);
- auf europäischer Ebene das Europäische Komitee für Normung (Comité Européen de Normalisation – CEN);
- in Deutschland das „Deutsche Institut für Normung e. V.“ (DIN).

Weiterhin ist die International Electrotechnical Commission (IEC) von Bedeutung, die im Bereich der Informationstechnologie mit der ISO das gemeinsame „ISO/IEC Joint Technical Committee 1“ (JTC1) unterhält. Normen, die aus der Arbeit dieses Komitees resultieren, erhalten eine ISO/IEC-Kennung. ISO-Normen werden von den zuständigen Normenausschüssen des DIN kontinuierlich daraufhin geprüft, ob sie als „DIN ISO“-Norm übernommen werden sollen. Europäische EN-Normen werden vom DIN grundsätzlich als „DIN EN“-Norm übernommen. Normen, die sowohl vom DIN und der ISO als auch vom CEN verabschiedet wurden, werden als „DIN EN ISO“-Norm gekennzeichnet.

Beispiel für einen IT-Standard

Die ITIL (Information Technology Infrastructure Library) ist eine umfassende, nicht proprietäre, öffentlich publizierte Verfahrensempfehlung für die Planung, den Betrieb, die Überwachung und die Steuerung von IT-Services. Sie ist insofern der zentrale IT-Standard für das IT-Servicemanagement (ITSM). Erarbeitet wurde die ITIL durch die Central Computer and Telecommunications Agency (CCTA), eine IT-Dienstleistungsorganisation der britischen Regierung, in Zusammenarbeit mit Experten, Beratern und erfahrenen Berufspraktikern. Den Kern bilden in der aktuellen dritten Version fünf Bücher zu Servicestrategie (engl. Service Strategy), Service-Entwurf (engl. Service Design), Serviceüberführung (engl. Service Transition), Servicebetrieb (engl. Service Operation) und zur kontinuierlichen Serviceverbesserung (engl. Continual Service Improvement). ITIL versteht sich als Best-Practice-Sammlung. Eine Zertifizierungsmöglichkeit gibt es auf einer individuellen Ebene bzw. institutionell nach ISO/IEC 20000. Heute besteht die ITIL-„Bewegung“ aus allen Ingredienzen eines professionellen Managementkonzeptes: Trainingsangebote inkl. qualifizierter Zertifikatsabschlüsse, Beratung und unabhängiger Erfahrungsaustausch innerhalb spezieller Organisationen, Umsetzungshilfen und Softwaretools.

Beispiel für eine IT-Norm

Die Norm „ISO/IEC 20000“ wurde im Dezember 2005 von der ISO als internationale Norm zum IT-Servicemanagement verabschiedet. Die ISO/IEC 20000 basiert auf der britischen Norm BS 15000 und ergänzt das Normenwerk von ISO und IEC im Bereich des Software- und System-Engineering. International ist dafür das Gremium ISO/IEC JTC 1/SC7 zuständig. In Deutschland arbeitet das nationale Spiegelgremium „NI-07 Software und System-Engineering“ mit Experten aus Hochschulen, Bundesbehörden, IT-Beratungsfirmen, Telekommunikationsunternehmen und Forschungseinrichtungen an diesen Normen mit. Allerdings wurde die ISO/IEC 20000 noch nicht als DIN ISO-Norm veröffentlicht. Zumindest ist seit Ende 2010 die Arbeit an der DIN ISO/IEC 20000-1 im Gange, die aber erst Ende 2013 abgeschlossen sein soll (nach [DIN11], S. 86).

Die Norm besteht aus zwei Teilen:

- a) ISO/IEC 20000-1:2011 – Information technology – Service management – Part 1: Specification: Dieser Teil der Norm enthält eine formelle Spezifikation. Hier finden sich die Vorgaben, die eine Organisation umsetzen und nachweislich gewährleisten muss, um eine ISO/IEC 20000-Zertifizierung zu erhalten.
- b) ISO 20000-2:2005 – Information technology – Service management – Part 2: Code of practice: Im zweiten Teil werden die Anforderungen des ersten Teils durch Erläuterungen

und Best-Practice-Beispiele ergänzt. Außerdem sind hier die Leitlinien und Empfehlungen für die ITSM-Prozesse zu finden. Damit dient dieser Teil als Leitlinie für Auditoren und bietet Hilfen für Dienstleister, die Serviceverbesserungen oder Audits nach ISO/IEC 20000-1 planen.

Die ISO/IEC 20000 bietet einen messbaren Qualitätsstandard für das IT-Service-Management. Sie spezifiziert die hierzu notwendigen IT-Prozesse, die eine Organisation etablieren muss, um IT-Services in definierter Qualität bereitzustellen und steuern zu können. Als solche beinhaltet sie Prozesse wie Incident Management, Problem Management oder Change Management und führt durch die Anwendung des ISO-typischen Optimierungsmodells „Plan-Do-Check-Act“ (PDCA) zu einem kontinuierlichen Verbesserungsprozess in der IT.

Die Norm ist an den Prozessbeschreibungen, wie sie durch ITIL beschrieben sind, ausgerichtet und ergänzt diese komplementär. Ein entscheidender Punkt ist die Messbarkeit bei ISO/IEC 20000. Unternehmen können sich mit der ISO/IEC 20000 nach einheitlichen und zertifizierbaren Kriterien messen lassen. Sie kann damit Unternehmen als Referenzwert zur Kontrolle der eigenen IT-Prozesse dienen, aber auch bei der Auswahl geeigneter ITSM-Software unterstützen. Außerdem haben Unternehmen mit der ISO/IEC 20000 eine Orientierungshilfe für die Auswahl von und die Zusammenarbeit mit externen IT-Dienstleistern.

13.6.5 Unternehmensinterne Regelwerke

Bei unternehmensinternen Regelungen ist die Bindungswirkung auf dasjenige Unternehmen beschränkt, das die jeweilige Regelung in Kraft setzt. Beispiele für unternehmensinterne Regelungen aus dem IT-Bereich sind interne IT-Richtlinien oder -Verfahrensvorgaben zur IT-Sicherheit (z. B. IT-Sicherheitsvorschriften, E-Mail-Richtlinien, Regelungen zum Umgang mit Passwörtern). Aber auch zwischen der IT-Abteilung und den Fachabteilungen vereinbarte Service-Level-Agreements zählen zu dieser Gruppe.

Interne Regelwerke sind aus zweierlei Hinsicht Compliance-relevant. Zum einen dienen sie in vielen Fällen dazu, die Beachtung der Anforderungen aller anderen Regelwerke sicherzustellen, indem sie konkrete Handlungsanweisungen für die Organisationsmitglieder vorgeben. Hierdurch dokumentieren sie zum anderen nach außen, dass externen Verpflichtungen, insbesondere rechtlichen Vorgaben, nachgekommen wird.



Praxistipp: Synergien realisieren durch Konsolidierung der Vorgaben

Die Vorgaben aus den verschiedenen Regelwerken überlappen sich zum Teil beträchtlich. IT-Compliance sollte dafür Sorge tragen, dass die Vorgaben über die verschiedenen Regelwerke hinweg zusammengefasst werden, um eine getrennte, doppelte Realisierung von Compliance-Maßnahmen zu verhindern. Hierin liegt ein beträchtliches Synergiepotenzial von IT-Compliance.

■ 13.7 Kernbereiche der Legal IT-Compliance

In diesem Kapitel wird ausschließlich auf die Einhaltung von Gesetzesnormen abgestellt. Derart fokussiert bewahrt IT-Compliance ein Unternehmen vor allem vor wirtschaftlichen Nachteilen als Folge von Rechtsverletzungen. Diese sogenannte „Legal IT-Compliance“ adressiert diejenigen betrieblichen Handlungsfelder, die unabhängig vom konkreten Geschäftsfeld eines Unternehmens zumeist mit Hilfe der IT – und damit gegebenenfalls auch von der IT-Abteilung des Unternehmens – bearbeitet werden; siehe Abbildung 13.13 (im Folgenden nach [KD09]).

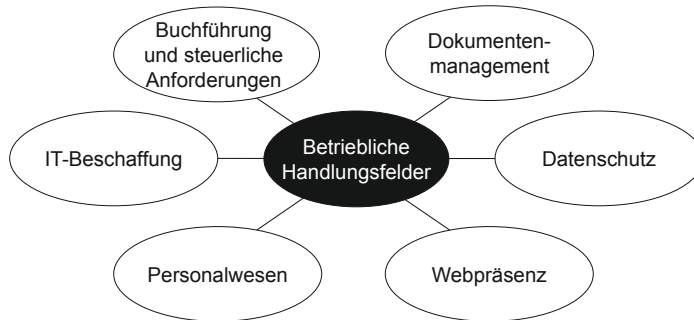


ABBILDUNG 13.13
Für IT-Compliance
relevante betriebliche
Handlungsfelder

Für eine realistische Bewertung der aus den verschiedenen Regelwerken resultierenden Compliance-Anforderungen ist das Wissen um die negativen Folgen bei fehlender oder mangelhafter Compliance von Bedeutung. Aus diesem Grunde werden im Folgenden auch die jeweiligen Rechtsfolgen bei Verletzung der Anforderungen dargestellt.



Praxistipp: IT-Compliance ist auch in KMU von Bedeutung.

Der Umfang der relevanten Handlungsfelder zeigt, dass nicht nur Großunternehmen, sondern auch mittelständische und sogar kleine Unternehmen von IT-Compliance betroffen sind und IT-Compliance somit auch dort der Aufmerksamkeit der Unternehmensführung bedarf.

13.7.1 Buchführung und steuerliche Anforderungen

Die Buchführung in Unternehmen erfolgt heute fast ausnahmslos IT-gestützt. Sie ist somit ein zentraler Bereich der IT-Compliance, ganz gleich, ob die mit Hilfe der IT erstellten Aufzeichnungen in Papierform vorgehalten werden, die Buchführungsdaten ausschließlich auf Datenträgern vorliegen oder die Belege lediglich maschinenlesbar archiviert werden.

Die steuerlichen Pflichten greifen grundsätzlich – soweit nicht aus speziellen Steuergesetzen zusätzliche Aufzeichnungspflichten resultieren – auf die Aufzeichnungspflichten zurück, die für das Unternehmen aufgrund anderer Gesetze begründet sind, indem § 140 AO bestimmt, dass diese Aufzeichnungspflichten auch für die Besteuerung zu erfüllen sind. Diese Pflichten ergeben sich insbesondere aus der Pflicht zur Führung kaufmännischer Bücher aus den

§§ 238 ff. HGB hinsichtlich der Aufzeichnungen zu Wareneingang und -ausgang aus §§ 143 f. AO und aus zahlreichen anderen, insbesondere branchenbezogenen Gesetzen. Ferner können sich Pflichten zudem aus ausländischem Recht ableiten, wenn dieses z.B. für im Ausland tätige deutsche (Tochter-)Unternehmen gilt.

Die grundsätzliche Anforderung an die zu führenden Aufzeichnungen ist in § 145 AO dahingehend definiert, „dass sie einem sachverständigen Dritten innerhalb angemessener Zeit einen Überblick über die Geschäftsvorfälle und über die Lage des Unternehmens vermitteln“ können, wobei „die Geschäftsvorfälle ... sich in ihrer Entstehung und Abwicklung verfolgen lassen“ müssen. Die Aufzeichnungen sind „vollständig, richtig, zeitgerecht und geordnet“ vorzunehmen (§ 146 Abs. 1 AO). Diese Aufzeichnungen können auch auf Datenträgern erfolgen, wenn das dabei angewendete Verfahren den „Grundsätzen ordnungsgemäßer Buchführung“ entspricht, wobei insbesondere sichergestellt werden muss, dass „während der Dauer der Aufbewahrungsfrist die Daten jederzeit verfügbar sind und unverzüglich lesbar gemacht werden können“ (§ 146 Abs. 5 AO). Entsprechende Anforderungen gelten gemäß § 147 Abs. 2 AO für die Aufbewahrung von Unterlagen auf Bildträgern oder anderen Datenträgern.

Indem die gesetzliche Regelung auf die „Grundsätze ordnungsgemäßer Buchführung“ als Generalklausel und auf die unbestimmten Rechtsbegriffe „unverzüglich“ und „jederzeit“ zurückgreift, wird die Definition der konkreten Anforderungen der Interpretation durch die Verwaltungspraxis und die Rechtsprechung überlassen. Dies hat den Vorteil, dass eine Anpassung an technische Entwicklungen ohne Gesetzesänderung möglich ist. Für die IT-Compliance ergibt sich hieraus jedoch die Notwendigkeit, weitere Regelwerke – insbesondere die von der Finanzverwaltung als Verwaltungsanweisung aufgestellten GoBS und GDPdU (siehe Abschnitt 13.6.2) – und die hierzu vorhandene Rechtsprechung zu berücksichtigen.

Zu berücksichtigen ist ferner, dass der Gesetzgeber weitere Pflichten des Steuerpflichtigen eingeführt hat, um den Finanzbehörden die Prüfung derartiger Aufzeichnungen zu ermöglichen. Nach § 147 Abs. 5 AO hat das Unternehmen die Hilfsmittel zur Verfügung zu stellen, um die Unterlagen lesbar zu machen. Noch weitergehend muss der Steuerpflichtige nach § 147 Abs. 6 AO bei einer Erstellung der Aufzeichnungen mit Hilfe eines IT-Systems nicht nur die „Einsicht“ in diese Daten ermöglichen, sondern nach Vorgabe der Betriebsprüfung die Daten selbst auswerten oder den Finanzbehörden auf einem verwertbaren lesbaren Datenträger zur Verfügung stellen. Folglich müssen die Programme so eingerichtet sein, dass im Rahmen einer Außenprüfung ein Zugang für den Betriebsprüfer – sinnvollerweise mit auf diese Daten eingeschränkten Berechtigungen – zur Verfügung gestellt bzw. eine Konvertierung der Daten auf einen Datenträger zur Übergabe an das Finanzamt in einem lesbaren Format ermöglicht werden kann. Die eingesetzten Programme müssen somit entweder „handelsübliche“ Formate verwenden oder zumindest das Konvertieren in diese ermöglichen.

Die steuerlichen Aufzeichnungspflichten dienen der Beweisführung für die der Besteuerung zu Grunde liegenden Sachverhalte. Die Verletzung der Anforderungen kann für das Unternehmen und gegebenenfalls auch für dessen verantwortliche Personen gravierende Auswirkungen haben. Erfüllen die Aufzeichnungen die dargestellten Anforderungen nicht, können sie die Beweisfunktion nicht oder nur eingeschränkt wahrnehmen. Wenn die Aufzeichnungen hierdurch unvollständig, formell oder sachlich unrichtig sind, kann das Finanzamt die Besteuerungsgrundlagen gemäß § 162 AO abweichend von den Aufzeichnungen schätzen, ohne dass es auf die Gründe hierfür oder ein Verschulden des Steuerpflichtigen ankommt. Bei dieser Schätzung ist auch ein „Unsicherheitszuschlag“ in bestimmten Grenzen zulässig.

Darüber hinaus ist die Gewährung von zahlreichen Steuervergünstigungen (z. B. die sofortige Abzugsfähigkeit von geringwertigen Wirtschaftsgütern (GWG) nach § 6 Abs. 2 Satz 4 EStG, die Inanspruchnahme von Sonderabschreibungen nach § 7 Abs. 8 EStG oder die Steuerver-schonung von steuerbegünstigten Körperschaften nach § 63 Abs. 3 KStG) von der korrekten Führung der Aufzeichnungen abhängig. Eine Nichtbeachtung der vorgenannten Anforderungen kann zu einem Wegfall dieser Steuervergünstigungen führen.

Die nicht ordnungsgemäße Erfüllung der Aufzeichnungspflichten kann darüber hinaus gemäß § 379 Abs. 1 Nr. 2 AO als Ordnungswidrigkeit der Steuergefährdung ein Bußgeld bis zu 5.000,- € nach sich ziehen. Eine nicht den Anforderungen entsprechende Aufbewahrung der steuerlich relevanten Unterlagen kann den Straftatbestand der Urkundenunterdrückung erfüllen – sanktioniert mit einer Freiheitsstrafe bis zu fünf Jahren oder einer Geldstrafe. Auch eine Strafbarkeit wegen Steuerhinterziehung oder Steuerverkürzung kann – abhängig vom konkreten Sachverhalt – nicht ausgeschlossen werden, wenn aufgrund der unzureichenden Aufzeichnungen zumindest mit bedingtem Vorsatz falsche Angaben über die Besteuerungsgrundlagen gemacht werden.



Praxistipp: Es gilt die persönliche Haftung des Topmanagements zu vermeiden.

Die Verantwortung für die Einhaltung der steuerlichen Pflichten – und somit auch der vorstehend dargestellten Aufzeichnungspflichten – trifft grundsätzlich die gesellschaftsrechtlich Verantwortlichen (also Vorstand, Geschäftsführer, Inhaber) des Unternehmens. Diese Verantwortung kann strafrechtlicher Art sein, aber auch eine persönliche Haftung für eventuelle Steuerverbindlichkeiten beinhalten.

13.7.2 Dokumentenmanagement

Die Geschäftskorrespondenz von Unternehmen wird heute in zunehmendem Maße digital – per E-Mail, Instant Messaging oder als (Fax-)Datei – geführt, wobei häufig bereits auf Ausdrucke verzichtet wird. Zunehmend wird auch die Archivierung aus Gründen der vereinfachten Zugänglichkeit sowie der Kosten- und Platzersparnis nur noch in Dateiform vorgenommen. Damit zusammenhängend obliegen die grundsätzliche Verwaltung und Archivierung dieser Korrespondenz der IT-Abteilung eines Unternehmens und stellen somit einen Bereich der IT-Compliance dar. Die hierbei zu beachtenden Anforderungen sind vielfältig. So ist bei der Gestaltung der Geschäftskorrespondenz, für die von der IT mit Textvorlagen bzw. „Signaturen“ für die E-Mails Vorgaben gemacht werden, zu beachten, dass gemäß § 37 a HGB bzw. den entsprechenden Vorschriften für spezielle Rechtsformen auf allen Geschäftsbriefen, zu denen auch E-Mails gehören, Angaben zur Firmierung, Vertretung und Handelsregistereintragung enthalten sein müssen.

Nicht nur aus Gründen der Besteuerung, sondern auch handelsrechtlich ist das Unternehmen zur Aufbewahrung der erhaltenen Handelsbriefe und von Wiedergaben der versendeten Handelsbriefe – nach der Definition des § 257 Abs. 2 HGB alle Schriftstücke, die ein Handelsgeschäft betreffen – verpflichtet. Die Aufbewahrung kann zwar auch auf Datenträgern erfolgen, die jedoch wiederum verfügbar und jederzeit lesbar sein müssen (§§ 238 Abs. 2, 257 HGB).

Angesichts der technisch einfachen Veränderbarkeit von Dateien erfordert eine elektronische Archivierung besondere Vorkehrungen, um ggf. den „Originalzustand“ eines Dokuments nachweisen zu können. Diese reichen – je nach Relevanz und Sensibilität des Dokuments – von einer belegbaren Speicherung auf einem nicht veränderbaren Datenträger über die Verwendung digitaler Signaturen bis hin zu Escrow-Vereinbarungen, d. h. der Aufbewahrung der Dateien bei einem Treuhänder, der dafür einsteht, dass diese nicht verändert worden sind. Gerade wenn Fälschungsvorwürfe nicht ausgeschlossen werden können, kann auch die körperliche Aufbewahrung der Originale erforderlich sein. Zumindest bei sensiblen Dokumenten, die dem Nachweis des Inhalts wichtiger Vereinbarungen oder der Abgabe bestimmender Erklärungen dienen, ist es darüber hinaus sinnvoll, zur Vermeidung der Veränderung auf der Empfängerseite digitale Signaturen zu verwenden und eventuelle Signaturen der eingehenden Korrespondenz zu überprüfen. Aufgabe der IT ist es hierbei, die entsprechenden technischen Möglichkeiten im gesamten Unternehmen zur Verfügung zu stellen, Verfahrensanweisungen für deren Einsatz vorzugeben und die Verwendung zu kontrollieren.

Mindestangaben auf elektronischen Geschäftsbriefen (z. B. nach 35 a Abs. 1 S. 1 GmbHG) können vom Registergericht mit Zwangsgeld durchgesetzt werden. Bei Verstoß gegen diese Verpflichtung können sich jedoch weitere, durchaus schwerwiegendere Nachteile für das Unternehmen ergeben, z. B. als Resultat von Beweisschwierigkeiten in Prozessen. Die Durchsetzung oder Abwehr vertraglicher Ansprüche setzen meist voraus, dass das Unternehmen in der Lage ist, das Zustandekommen von Vereinbarungen, die Abgabe bestimmter Erklärungen und insbesondere auch deren Inhalt in prozessual von den Gerichten verwertbarer Form nachzuweisen. Können diese Dokumente nicht oder in keiner verwertbaren Form – lesbar und ggf. nachweisbar inhaltlich unverändert – vorgelegt werden oder kann der Zugang von Erklärungen nicht nachgewiesen werden, so wird das Unternehmen seine Ansprüche nicht durchsetzen bzw. gegen es gerichtete Ansprüche abwehren können. Auch dies kann u. U. zu erheblichen, mitunter existenzbedrohenden Schäden führen.

Die mangelhafte Aufbewahrung und Sicherung von Dokumenten kann auch dann zu gravierenden prozessualen Nachteilen für das Unternehmen führen, wenn der Prozessgegner den Beweis zu führen hat, jedoch dem Unternehmen vom Gericht nach § 425 ZPO (Zivilprozessordnung) aufgegeben wird, in seinem Besitz befindliche Unterlagen vorzulegen. Gemäß § 427 ZPO kann in diesem Fall die Nichtvorlage durch das Unternehmen dazu führen, dass der Beweis durch den Gegner als geführt gilt, insbesondere wenn es – z. B. auf Grund der handelsrechtlichen Regelungen – zur Aufbewahrung der Urkunde verpflichtet gewesen ist.



Praxistipp: Eine systematische Archivierung ist unabdingbar.

Bei einer vollständigen oder teilweisen Archivierung der Geschäftskorrespondenz auf Datenträgern muss die IT deren geordnete Ablage und Auffindbarkeit ebenso wie deren Lesbarkeit auch in Zukunft und auch im Falle von Programmwechseln sicherstellen. Dies stellt erhebliche Anforderungen an das Dokumentenmanagement und die Archivierungstechnik, z. B. hinsichtlich Format, Speicherort der Daten, Wiederauffindbarkeit und Reproduzierbarkeit.

13.7.3 Datenschutz

Datenschutz ist nicht nur im Bereich der IT ein Thema. Da heute jedoch zumindest die Speicherung und Verarbeitung und im Bereich des E-Commerce auch die Erhebung der Daten überwiegend digital erfolgt, ist in den Unternehmen zumeist in erster Linie die IT-Abteilung betroffen. Die Einhaltung der entsprechenden gesetzlichen Regelungen ist somit auch ein wesentliches Thema der IT-Compliance.

Zu beachten ist der Grundsatz, wonach jegliche Erhebung, Verarbeitung (einschließlich Speicherung und Übermittlung) oder sonstige Nutzung personenbezogener Daten – nach der gesetzlichen Definition des § 3 Abs. 1 BDSG sind dies Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person, wobei dies weit ausgelegt wird – nach dem Grundsatz des § 4 Abs. 1 BDSG nur dann zulässig ist, wenn dies eine Rechtsvorschrift gestattet oder der Betroffene eingewilligt hat. Ansonsten ist die Bearbeitung personenbezogener Daten unzulässig und stellt einen Gesetzesverstoß dar.

Für Unternehmen finden sich die gesetzlichen Regelungen, die die Bearbeitung personenbezogener Daten betreffen, in erster Linie in den §§ 27 ff. BDSG, für Diensteanbieter ferner in den §§ 14, 15 TMG. Diese Vorschriften können im Wesentlichen grob dahingehend zusammengefasst werden, dass die Nutzung personenbezogener Daten nur „zur Erfüllung eigener Geschäftszwecke“ zulässig ist, soweit dies für die Abwicklung von Verträgen mit dem Betroffenen notwendig ist. Es müssen ferner Vorkehrungen getroffen werden, um die verschiedenen Vorschriften über die Benachrichtigung des Betroffenen und die Berichtigung oder Sperrung von Daten einzuhalten.



Praxistipp: Vorsicht bei Data-Warehouse- und CRM-Anwendungen!

Beim Umgang mit personenbezogenen Daten ist jeweils eine genaue Prüfung für jede Nutzung – z. B. für die interne Auswertung von Kundendaten in Data-Warehouse-Anwendungen bzw. Systemen für das Customer-Relationship-Management (CRM) – vorzunehmen, ob diese Nutzung (weitere Speicherung, Übermittlung an andere Stellen, Auswertung) von den konkreten Vertragszwecken und somit von den Ermächtigungsvorschriften der §§ 27 ff. BDSG gedeckt ist.

Diese strenge Zweckbestimmung ist auch bei der Einwilligung des Betroffenen zu beachten, die sich immer nur auf bestimmte Zwecke bezieht, die dem Betroffenen auch eindeutig mitzuteilen sind (§ 4 a BDSG). Unter den Voraussetzungen des § 13 Abs. 2 TMG kann die Einwilligung auch elektronisch erteilt werden, im Übrigen ist gesetzliche Schriftform erforderlich. Soll die Nutzung der personenbezogenen Daten somit auf der Grundlage von Einwilligungen der Betroffenen erfolgen, muss genau geprüft werden, ob diese Einwilligungen – und zwar in der gebotenen Form – vorliegen, ob sie wirksam zu Stande gekommen sind (was eine ausreichende Unterrichtung des Betroffenen voraussetzt) und ob der vorgesehene Zweck der Nutzung von der Einwilligung abgedeckt ist.

Werden diese Prüfungen nicht bzw. nicht sorgfältig vorgenommen, besteht angesichts der recht engen rechtlichen Zulässigkeit der Nutzung personenbezogener Daten eine hohe Wahrscheinlichkeit, dass mit dieser Nutzung datenschutzrechtliche Bestimmungen verletzt werden. Derzeit muss wohl konstatiert werden, dass in der Praxis bislang noch keine allzu große

Sensibilität hinsichtlich dieser Vorschriften gegeben ist und die wohl zahlreichen Verstöße überwiegend unbeanstandet und ungeahndet bleiben. Vor dem Hintergrund aktueller Skandale (vgl. Abschnitt 13.2.1) zeigt sich jedoch, dass derartige Rechtsverletzungen gravierende Folgen für das Unternehmen und die Vertretungsberechtigten haben können. Verstöße gegen die Datenschutzbestimmungen stellen gemäß § 43 BDSG und § 16 TMG Ordnungswidrigkeiten dar, die nach der derzeitigen Gesetzeslage mit einem Bußgeld in Höhe von 25.000,- bzw. 50.000,- € sanktioniert sind. In besonders schweren Fällen kann das Bußgeld bis zu 250.000,- € betragen bzw. eine Straftat darstellen, wobei die Strafdrohung bis zu zwei Jahren beträgt. Daneben kann die Aufsichtsbehörde einschreiten und Betroffene können Unterlassungsansprüche geltend machen; die hieraus resultierenden theoretisch möglichen Schadensersatzansprüche sind jedoch (noch) wenig praxisrelevant.

13.7.4 Webpräsenz

Die Betreuung der Website, die heute wohl praktisch jedes Unternehmen hat, stellt eine typische Aufgabe der IT-Abteilung dar. Bei der inhaltlichen Gestaltung der Website sind zahlreiche Vorschriften zu beachten, deren Zahl sich noch erhöht, wenn über die Website nicht nur eine Präsentation des Unternehmens erfolgt, sondern diese dem operativen Geschäft dient. Demgemäß ergibt sich hieraus ein wesentlicher Bereich für die IT-Compliance, wobei zu beachten ist, dass auch bei einer Übertragung der Gestaltung an externe Dienstleister die Verantwortung beim Unternehmen und dessen Vertretungsorganen verbleibt.

Den Diensteanbieter – nach der Definition des § 2 Nr. 1 TMG jeder, der eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung ermöglicht, somit auch derjenige, der eine Website „ins Netz stellt“ – treffen nach §§ 5, 6 TMG umfangreiche Informationspflichten (Angaben zum Unternehmen, Erreichbarkeit, zu eventuellen Aufsichtsbehörden sowie zur Erkennbarkeit einer kommerziellen Kommunikation), die in wesentlichen Teilen üblicherweise durch ein sorgfältig gestaltetes Impressum erfüllt werden. Werden über die Website auch Vertragsabschlüsse vorgenommen, betreibt das Unternehmen E-Commerce im engeren Sinne. In diesem Fall kommen die (teilweise identischen) Informationspflichten für den elektronischen Geschäftsverkehr und den dann auch immer vorliegenden Vertragsabschluss im Fernabsatz nach §§ 312 e, 312 c BGB und § 3, 1 BGB-InfoV (Verordnung über Informations- und Nachweispflichten nach bürgerlichem Recht) hinzu. Darüber hinaus sind in diesem Fall die Anforderungen an die Gestaltung des technischen Ablaufs für den Vertragsabschluss zu berücksichtigen: So muss eine Möglichkeit zur Korrektur von Eingabefehlern bestehen, der Vertrag muss durch das Unternehmen unverzüglich elektronisch bestätigt werden, der Inhalt und die Bedingungen des zu Stande gekommenen Vertrages müssen gespeichert werden und für den Kunden abrufbar sein (§ 312 e Abs. 1 BGB).

Keine Besonderheit der IT stellen die sonstigen Anforderungen an die inhaltliche Ausgestaltung der Website dar, die natürlich die allgemeinen gesetzlichen Anforderungen einhalten muss. Sie darf z. B. nicht gegen allgemeine oder spezielle Strafnormen (z. B. Einschränkungen der Werbung für Arzneimittel) verstoßen, keine unlautere geschäftliche Handlung i. S. d. § 3 UWG (Gesetz gegen den unlauteren Wettbewerb) oder auch keine irreführende Werbung i. S. d. § 5 UWG darstellen. Bei der Gestaltung sind somit die einzelnen in den §§ 4 bis 7 UWG aufgeführten Tatbestände unlauteren Verhaltens sowie die äußerst umfangreiche, zur Konkre-

tisierung dieser Generalklauseln ergangene Rechtsprechung zu berücksichtigen. In der Regel ist die Marketing-Abteilung mit diesen Fragen befasst. Häufig wird die Verantwortlichkeit bei entsprechenden Marketingmaßnahmen im Web jedoch zusammen mit der technischen Betreuung in der IT-Abteilung angesiedelt.

Ein besonderes Risiko von Rechtsverletzungen im Zusammenhang mit dem Webauftritt besteht erfahrungsgemäß im Bereich des Urheberrechts. Dieses wird aufgrund der leichten Verfügbarkeit von digitalen Dokumenten, Grafiken, Bildern und sonstigen Inhalten gerade im „Netz“ leicht und deshalb vielfältig – häufig ohne jedes Unrechtsbewusstsein – verletzt. Weil die Tatsache, dass Dateien „im Netz“ verfügbar sind, entgegen einer sehr weit verbreiteten Auffassung keinen Verzicht auf deren urheberrechtlichen Schutz darstellt, müssen die Regelungen des Urheberrechts – und auch z.B. des Markenrechts – bei der Gestaltung der Website sehr genau beachtet werden. Hiernach sind alle „Sprachwerke“ (also Texte gleich welchen Inhalts und welcher technischen Form) sowie Darstellungen wissenschaftlicher und technischer Art (z. B. Stadtpläne, Grafiken, Tabellen) und auch Lichtbilder gegen jede nicht vom Rechteinhaber gestattete Vervielfältigung, sonstige Verwertung und Veränderung geschützt. Die Publikation von Inhalten auf einer Website erfolgt in der Regel durch eine Vervielfältigung, indem die Daten in den dann aus dem Web abrufbaren Speicherplatz kopiert werden, und stellt eine ebenfalls dem Rechteinhaber vorbehaltene öffentliche Zugänglichmachung dar, erfordert somit entsprechende Nutzungs- und Verwertungsrechte. Bevor Texte oder Grafiken, z.B. aus Produktbesprechungen, von anderen Websites übernommen werden, Bilder aus entsprechenden Sammlungen eingestellt werden oder – z. B. zur Beschreibung der Anfahrt zum Unternehmen – Stadtplanausschnitte übernommen oder entsprechende Webinhalte in Frames oder in anderer Form in der Website nutzbar gemacht werden, gilt es, den jeweiligen Rechteinhaber festzustellen. Außerdem muss man sicherstellen, dass entsprechende Nutzungsrechte für die konkret vorgesehene Nutzung belastbar eingeräumt werden oder ausnahmsweise eine Nutzung kraft gesetzlicher Gestattung, z. B. im Rahmen des Zitatrechts, ohne Einräumung von Rechten durch den Rechteinhaber zulässig ist. Dies betrifft auch die Digitalisierung und Einstellung von Texten, Grafiken oder Bildern, die für andere Nutzungsarten – z.B. in einem Firmenprospekt – unter Einräumung der Nutzungsrechte erstellt und/oder zur Verfügung gestellt wurden.

Bei der Beauftragung Dritter mit der Gestaltung der Website sollte man zusätzlich vom Dienstleister der Nachweis verlangen, dass die entsprechenden Rechte komplett eingeräumt wurden. Soweit Texte, Bilder oder andere schutzfähige Werke für die Website erstellt werden, ist darauf zu achten, dass eine für diese Nutzungsart ausreichende Übertragung der Nutzungsrechte (§§ 31 ff. UrhG) erfolgt. Ebenso gilt es zu beachten, dass bei der Verwendung von Marken, z.B. zur Beschreibung von Fremdprodukten oder von Kooperationspartnern, entweder definitiv keine markenmäßige Verwendung vorliegt oder die Gestattung des Markeninhabers eingeholt wurde.

Ein weiteres häufig anzutreffendes Risiko bei der Gestaltung des Webauftritts eines Unternehmens ist die Haftung für fremde Inhalte, die auf der Website oder über diese zugänglich gemacht werden (dass eine Haftung für eigene, selbst erstellte oder eingestellte Inhalte der Website nach den allgemeinen Vorschriften und Regelungen besteht, ist ebenso wie bei allen anderen Äußerungen und Publikationen selbstverständlich). Zwar ist die Haftung des Diensteanbieters für fremde Inhalte durch §§ 7 ff. TMG eingeschränkt, er kann jedoch trotzdem auf Unterlassung in Anspruch genommen werden. Zudem greift dieser Haftungsausschluss bei einer Speicherung dieser fremden Inhalte nur dann, wenn sie dem Unternehmen als Dienst-

anbieter der Website nicht bekannt gewesen sind und die beanstandeten Daten unverzüglich nach Kenntnis entfernt oder gesperrt worden sind (§ 10 TMG). Lässt das Unternehmen auf seiner Website das Einstellen von Inhalten durch Dritte zu (z. B. Kooperationspartnern bei „Plattformen“ oder Kunden im Rahmen von Blogs oder Diskussionsforen), muss auf Hinweise bzgl. rechtswidriger Inhalte (sei es strafrechtlicher oder auch z. B. urheberrechtlicher Natur) sofort reagiert werden, um das Haftungsprivileg nicht zu verlieren.

Bei entsprechender Einbeziehung des von Dritten stammenden Inhalts kann darüber hinaus die Gefahr bestehen, dass diese als in den Inhalt der eigenen Unternehmens-Website übernommen angesehen werden, für den dieses voll haftet.



Praxistipp: Vorsicht bei Verwendung von Links

Für die Inhalte anderer Websites, auf die ein Unternehmen auf seiner eigenen Website verlinkt, besteht zwar grundsätzlich keine Haftung. Trotzdem kann diese nicht ausgeschlossen werden, so dass im Einzelfall eine Mitwirkung an einer Rechtsverletzung, die mittels dieser Inhalte durch den Dritten begangen wird, angenommen werden kann. Achten Sie deshalb darauf, Links nur auf Websites vertrauenswürdiger Anbieter zu setzen. Prüfen Sie diese regelmäßig, ob sich die Inhalte – oder sogar der Diensteanbieter – geändert haben.

Die Verletzung der Informationspflichten nach §§ 5, 6 TMG stellt nach § 13 TMG eine Ordnungswidrigkeit dar, die mit einem Bußgeld von bis zu 50.000,- € belegt werden kann. Wirtschaftlich zumeist gravierender ist jedoch die Gefahr, sich wegen einer Verletzung der Informationspflichten oder einer nicht den gesetzlichen Anforderungen entsprechenden Gestaltung des Webauftritts Abmahnungen durch Konkurrenten oder Verbänden auszusetzen. Die Kosten hierfür können erheblich sein, denn der Gegenstandswert, der für die Bemessung der Gebühren der beauftragten Anwälte und der Gerichte maßgeblich ist, richtet sich nach der wirtschaftlichen Bedeutung des Webauftritts und somit des Unternehmens – und ist somit grundsätzlich nach oben offen; in der Regel beträgt der Gegenstandswert mindestens 30.000,- €. Ergibt eine gerichtliche Unterlassungsanordnung oder wird zur Vermeidung eines gerichtlichen Verfahrens eine strafbewehrte Unterlassungserklärung abgegeben, kann eine Wiederholung des Fehlers zu erheblichen Ordnungsgeldern oder Vertragsstrafen führen. Entsprechendes gilt für die Verletzung der UWG-Regelungen, die von Konkurrenten und Verbänden verfolgt werden.

Im Bereich des elektronischen Geschäftsverkehrs kann die Verletzung der dargestellten Anforderungen dazu führen, dass Verträge nicht wirksam zu Stande gekommen sind bzw. sich die Kunden – gegebenenfalls auch nach langer Zeit und nach Erhalt der Waren – vom Vertrag lösen können, was zu erheblichen Verlusten und insbesondere auch zu hohen Handling-Kosten des Unternehmens führen kann. Des Weiteren können u. U. Schadensersatzansprüche der Kunden begründet werden. Gerade im „Massengeschäft“ stellen die hierbei entstehenden Rechtsverfolgungskosten (auch auf Seiten des Kunden, die gegebenenfalls zu erstatten sind) den maßgeblichen Kostenfaktor dar.

Die Verletzung der Urheber- oder Markenrechte ist gemäß §§ 106 UrhG, 143 MarkenG strafbar, wobei die Strafandrohung mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe recht hoch ist. Zudem setzt sich das Unternehmen zivilrechtlich Unterlassungs- und Schadensersatzansprü-

chen aus, die aus der vom Rechteinhaber ansonsten für die Nutzung verlangten Vergütung (nach dessen Preisgestaltung!) zuzüglich eines eventuellen „Strafaufschlags“ bestehen. Noch belastender sind mitunter die von den Gerichten für die Schaffung der Grundlage des Schadensersatzanspruchs zuerkannten Auskunftsansprüche über Art und Umfang der Nutzung, die zu recht umfassenden Auskünften über den Geschäftsbetrieb führen können.

Die Haftung für fremde Inhalte kann – je nachdem, welche Rechtsverletzungen vorliegen – sowohl eine strafrechtliche Haftung als auch die zivilrechtliche Haftung für Schadensersatzansprüche umfassen, unabhängig davon, dass auch in diesem Zusammenhang das Unternehmen den Unterlassungsansprüchen mit entsprechenden Kostenfolgen ausgesetzt ist. Die wirtschaftlichen und sonstigen Folgen für das Unternehmen sind somit kaum kalkulierbar.

13.7.5 Personalwesen

Der IT-Einsatz im Unternehmen ist in vielfältiger Hinsicht auch durch arbeitsrechtliche Normen geregelt. Für die IT-Compliance sind nicht nur diese Normen, sondern auch die umfangreiche Rechtsprechung zu berücksichtigen, welche die Pflichten erst konkretisiert.

Über die geplante Einführung von IT-Systemen, die Erweiterung ihres Einsatzes und die Einführung neuer Programme ist der Betriebsrat nach §§ 80 Abs. 2, 90 BetrVG (Betriebsverfassungsgesetz) unverzüglich zu unterrichten. Dem Betriebsrat steht darüber hinaus ein Mitbestimmungsrecht zu. Die Maßnahme darf somit nur mit seiner Zustimmung in Form einer Betriebsvereinbarung durchgeführt werden, wenn es sich beim betreffenden IT-System gemäß § 87 Abs. 1 Nr. 6 BetrVG um eine Einrichtung handelt, die dazu bestimmt ist, die Leistung oder das Verhalten von Arbeitnehmern zu überwachen. Diese „Bestimmung“ wird von der Rechtsprechung bereits dann angenommen, wenn die Einrichtung – insbesondere z.B. aufgrund entsprechender Gestaltung der eingesetzten Programme – dazu geeignet ist, leistungs- oder verhaltensrelevante Daten bestimmter Arbeitnehmer zu erfassen, unabhängig davon, ob diese ausgewertet werden oder ausgewertet werden sollen. Da heute die meisten Programme standardmäßig Protokollfunktionen enthalten, sind diese weiten, von der Rechtsprechung definierten Voraussetzungen des Mitbestimmungsrechts des Betriebsrats in der Regel schon bei der Einführung neuer Programme, häufig auch schon bei der Einführung neuer Hardware gegeben. Die IT-Abteilung muss somit jede Änderung in der IT des Unternehmens nicht nur rechtzeitig dem Betriebsrat mitteilen, sondern auch daraufhin überprüfen, ob in den Programmen derartige arbeitnehmerbezogene Daten erfasst werden. Wenn diese Erfassung nicht durch Änderung des Programms ausgeschlossen werden kann, muss das Mitbestimmungsverfahren gegenüber dem Betriebsrat eingeleitet werden.

Wird den Arbeitnehmern des Unternehmens – was häufig bereits durch sogenannte „betriebliche Übung“ auf Grund der bisherigen Handhabung der Fall ist – die private Internet- und E-Mail-Nutzung gestattet, ist es sinnvoll, durch einzelvertragliche Vereinbarungen, entsprechende Weisungen oder im Rahmen einer Betriebsvereinbarung die Bedingungen festzuschreiben, unter denen diese Möglichkeit genutzt werden kann. Ohne eine derartige Regelung ist nach der Rechtsprechung des Landgerichts Köln jegliche Nutzung, die die Betriebstätigkeit nicht stört, keine erheblichen unzumutbaren Kosten verursacht und das Betriebssystem nicht gefährdet, gestattet (Urteil vom 11. 2. 2005, Az. 4 Sa 1018/04). Diese Grenzen sind jedoch so fließend und weit, dass eine sinnvolle Eingrenzung der Nutzung kaum durchsetzbar ist. Die

Regelung der grundsätzlich eingeräumten privaten Nutzung stellt eine Regelung der Ordnung und des Verhaltens der Arbeitnehmer im Betrieb i.S.d. § 87 Abs. 1 Nr. 1 BetrVG dar, sodass das Mitbestimmungsrecht des Betriebsrats zu beachten ist, somit die Regelungen nur aufgrund einer Betriebsvereinbarung eingeführt werden können. Die IT-Abteilung muss somit die Prüfung veranlassen, ob eine private Nutzung den Arbeitnehmern eingeräumt werden soll (oder bereits eingeräumt worden ist), und in diesem Fall auf die Vereinbarung entsprechender Verhaltensregeln hinwirken.

Zu beachten sind ferner die Bestimmungen der §§ 88ff. TKG, da die Einräumung der privaten Nutzung von Internet und E-Mail als Anbieten von Übertragungswegen an Dritte i.S.d. § 3 Nr. 10 TKG angesehen wird, der Arbeitgeber somit Telekommunikationsdienste i.S.d. § 88 Abs. 2 TKG erbringt. Demgemäß sind bei der Nutzung von Internet und E-Mail die Bestimmungen zum Fernmeldegeheimnis und die besonderen Bestimmungen des Datenschutzes zu beachten.



Praxistipp: Private E-Mailnutzung muss geregelt werden.

Die IT-Abteilung hat darauf hinzuwirken, dass im Zusammenhang mit der Regelung der privaten Nutzung von Internet und E-Mail-Verkehr die individuelle Einwilligung der Arbeitnehmer zu einer gegebenenfalls gewünschten Überwachung dieser Nutzung – die sich jedoch keinesfalls auf den Inhalt der E-Mails beziehen darf – erteilt wird. Andernfalls sind derartige Überwachungsmaßnahmen nicht zulässig, insbesondere dann, wenn eine Abrechnung der privaten Nutzung nicht erfolgt und somit keine Abrechnungsdaten erhoben werden müssen.

Verletzungen der Bestimmungen des TKG stellen gemäß §§ 148f. TKG Straftaten (insbesondere die unzulässige Ermittlung des Inhalts von Nachrichten) oder Ordnungswidrigkeiten dar. Die Verletzung der Informationspflichten gegenüber dem Betriebsrat stellt gemäß § 121 BetrVG eine mit einer Geldbuße bis zu 10.000,- € bewehrte Ordnungswidrigkeit dar. Insbesondere löst die Verletzung der Mitbestimmungsrechte einen Unterlassungsanspruch des Betriebsrates aus, sodass dieser die Einführung neuer Programme oder Hardware verhindern oder die Rückgängigmachung verlangen kann, bis eine Betriebsvereinbarung zu Stande gekommen ist. Gegenüber dem einzelnen Arbeitnehmer können Maßnahmen, die unter Verletzung des Mitbestimmungsrechts vorgenommen worden sind, nicht durchgesetzt werden. Dies kann zu einer erheblichen Verzögerung oder gar einer Verhinderung der vorgesehenen Maßnahmen führen und somit zu einer erheblichen Störung des Geschäftsbetriebs, wenn Investitionen oder operative Maßnahmen nicht durchgeführt werden können.

13.7.6 IT-Beschaffung

Gewöhnlich ist die IT-Abteilung eines Unternehmens an Stelle oder neben dem Einkauf für die Beschaffung von Hard- und Software zuständig. Bestandteil von Beschaffungsaktivitäten ist die Gestaltung einer vertraglichen Grundlage, die wiederum Basis eines erforderlichen Vertragscontrollings hinsichtlich der Einhaltung von vertraglichen Vereinbarungen zu Abnahmeverfahren, Fertigstellungs- oder Gewährleistungsfristen, Anzeige- und Dokumentationspflichten usw. ist. Aus einem derartigen IT-Vertragscontrolling ergeben sich weitere Anforderungen an die IT-Compliance.

Da das Gewährleistungsrecht des BGB sowohl im Kauf- als auch im Werkvertragsrecht in erster Linie auf die vereinbarte Sollbeschaffenheit abstellt (§§ 437 Abs.1, 633 Abs. 2 BGB), ist die IT-Abteilung gehalten, in den Verträgen für eine möglichst genaue, gegebenenfalls funktionale Leistungsbeschreibung zu sorgen und deren Einhaltung dann durch Abgleich mit der tatsächlichen Beschaffenheit der Hard- oder Software zu überprüfen. Soweit es mangels derartiger Vereinbarungen auf die übliche Beschaffenheit eines Kaufgegenstandes oder Werkes ankommt, sind für diese Feststellung eventuell hierfür vorhandene Regelwerke (z.B. DIN-Normen, Empfehlungen zur Strukturierung von Software-Quellcode) sowie die hierzu ergangene Rechtsprechung (so verlangt diese beispielsweise auch ohne gesonderte vertragliche Vereinbarung für Software ein „Handbuch“ mit Bedienungsanleitung und Dokumentation) heranzuziehen.

Bei einem Kaufvertrag (das Kaufrecht ist aufgrund der Verweisung in § 651 BGB auch auf die Lieferung herzustellender beweglicher Sachen und somit regelmäßig auch auf Softwareerstellung anzuwenden) ist zu beachten, dass § 377 HGB eine unverzügliche Untersuchung bei Ablieferung verlangt. Zu berücksichtigen sind hierbei zahlreiche, von der Rechtsprechung entwickelte Grundsätze. Diese bestimmen beispielsweise, unter welchen Voraussetzungen eine Abnahme konkludent durch Nutzung des Gegenstandes oder der Software erfolgt, oder wann Mängel als bereits bei der Abnahme bekannt anzusehen sind. Bei der Feststellung von Mängeln ist auf die sorgfältige Dokumentation zu achten, um den Anforderungen an eine gegebenenfalls gerichtsverwertbare Beweisführung zu genügen.



Praxistipp: Verlust von Gewährleistungsansprüchen vermeiden.

Beachtet die IT-Abteilung die verschiedenen Anforderungen im Rahmen des Vertragsmanagements nicht, kann dies dazu führen, dass insbesondere Gewährleistungsansprüche nicht durchgesetzt werden können mit der Folge, dass das Unternehmen mangelhafte Gegenstände oder Software vollständig bezahlen muss oder die Kosten für die Mangelbeseitigung selbst zu tragen hat. Beides kann zu erheblichen wirtschaftlichen Nachteilen führen.

Führt eine Hardwarebeschaffung zu einem Ersatz alter Hardware, muss diese gegebenenfalls entsorgt werden. Hierbei wäre die – allerdings nicht bußgeldbewehrte – Pflicht gemäß § 9 Abs. 1 ElektroG (Elektro- und Elektronikgerätegesetz) zu berücksichtigen, Altgeräte einer getrennten Versorgung zuzuführen.

■ 13.8 Management der IT-Compliance

Durch die Fülle von Rechtsnormen und sonstigen Regelwerken sowie die heute fast durchgängige IT-Unterstützung aller Unternehmensprozesse sind Compliance-Anforderungen nicht mehr lediglich auf steuerliche oder datenschutzrechtliche Belange begrenzt. Vielmehr geht es darum, dass die gesamte geschäftliche Tätigkeit eines Unternehmens „compliant“ mit ver-

schiedensten Regelungen sein muss. Um den diversen Transparenz-, Prozess-, Nachweis- und Kontrollanforderungen nachzukommen, sind Maßnahmen zu ergreifen, die letztlich Auswirkungen auf jeden einzelnen Arbeitsplatz haben.

Hierbei gilt es, vor allem die Compliance-Anforderungen der verschiedenen Regelwerke aufeinander abzustimmen, um Doppelarbeit zu vermeiden. Insofern bilden

1. die Identifizierung von IT-Compliance-relevanten Regelwerken sowie die Ableitung und Dokumentation der Compliance-Anforderungen, die mit unterschiedlicher Priorität einzuhalten sind, den ersten und wichtigsten Aufgabenbereich eines Managements der IT-Compliance.

Weitere Aufgabenbereiche:

2. die Schaffung einer betrieblichen Organisation von Prozessen, Verfahrensregelungen, Delegationen und Kontrollen zur Überwachung der Einhaltung aller Anforderungen der IT-Compliance;
3. die Information aller in irgendeiner Form im Hinblick auf die bestehenden Verpflichtungen handelnden Betriebsangehörigen und gegebenenfalls entsprechend eingesetzter Dritter über die einzuhaltenden Regelungen;
4. die Dokumentation sowohl der Information als auch der Organisation und insbesondere deren Überwachung;
5. die Einrichtung eines Change-Managements zur Reaktion auf neue Entwicklungen der Anforderungen, z.B. innerhalb der aktuellen Rechtsprechung oder erkannter IT-Compliance-Schwachstellen und -Risiken.

Die ablauforganisatorische Gestaltung dieser Aufgaben führt zu einem allgemeinen IT-Compliance-Prozess, der den Kern eines Managementsystems für IT-Compliance bildet (siehe Abbildung 13.14).

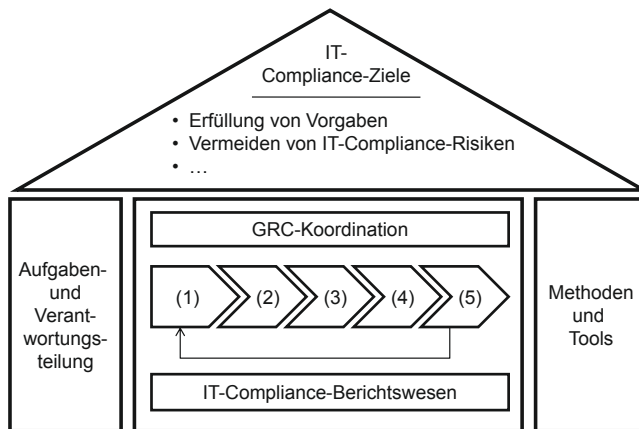


ABBILDUNG 13.14
Managementsystem für
IT-Compliance

Alle Compliance-Aktivitäten haben sich an den Zielen der IT-Compliance auszurichten, die sich zwar generell auf die Erfüllung von Vorgaben und das Vermeiden von Compliance-Risiken richten, aber hinsichtlich der relevanten Regelwerke sowie der weiteren Zielsetzungen unternehmensspezifisch zu konkretisieren sind. Hieraus kann ein Zielkatalog resultieren, der z.B. folgende Zielinhalte verfolgen kann:

- Senkung von Überwachungskosten
- Verbesserung der Auditierbarkeit
- Vermeidung von Betrugsrisiken
- Sicherung von Betriebsgeheimnissen
- Vermeidung von Risikoabschlägen
- Sicherung von IT-Vermögenswerten.

Maßnahmen zur Herstellung von IT-Compliance sind mit dem GRC-Management des Unternehmens zu koordinieren und durch ein Berichtswesen zu ergänzen, das die Unternehmensleitung bzw. entsprechende Steuerungsgremien über den Status der Zielerreichung, Compliance-Schwachstellen und -Risiken sowie wesentliche Projekte der IT-Compliance unterrichtet. Das Berichtswesen hängt wesentlich von der Ausgestaltung der IT-Compliance-Organisation ab. Im Einzelnen muss festgelegt werden, welche Berichte

- welchen Compliance-Bereich abdecken;
- welche Inhaltsstruktur aufweisen;
- von wem zu erstellen sind;
- welchen Berichtszeiträumen unterliegen;
- wie zu verdichten sind;
- an welchen Verteilerkreis zu adressieren sind;
- wie und wie lange aufzubewahren sind.

Zudem sind die IT-Compliance-Prozesse auf der Basis einer festgelegten und kommunizierten Aufgaben- und Verantwortungsteilung auszuführen und durch Methoden und Tools zu unterstützen. IT-Compliance ist ein relativ junges Gebiet des IT-Managements. Entsprechend befinden sich Methoden und Tools noch in einem frühen Entwicklungsstadium. Damit ist notwendig eine hohe Entwicklungsgeschwindigkeit mit zwischenzeitlich bestehenden konzeptionellen, methodischen und technischen Lücken verbunden. Dies muss bedacht werden, wenn die Nutzung von Methoden und Tools geplant wird.

Einen vollständigen Marktüberblick zu liefern, ist somit nicht möglich. Trotzdem soll durch exemplarische Nennung einiger am Markt verfügbarer Tools ein Eindruck vom aktuellen Angebot und dessen Leistungsumfang vermittelt werden. Selbstverständlich haben alle namhaften Softwarehersteller mittlerweile eine Compliance-Lösung im Angebot – zumeist als Teil eines GRC-Paketes –, die den Bereich der IT-Compliance integriert. Allen voran ist hier die SAP® AG zu nennen, die ihre Lösungen für Governance, Risk und Compliance als integriertes GRC-Anwendungsportfolio präsentieren, das sich auf Aktivitäten in den Bereichen der nachhaltigen Unternehmensführung, des Risikomanagements und der Einhaltung gesetzlicher Auflagen richtet. Die Lösung deckt zahlreiche GRC-Bereiche ab, z. B. Unternehmenskontrolle, Risikomanagement, Zugriffs- und Berechtigungssteuerung sowie Umwelt-, Gesundheits- und Arbeitsschutz. Zu den wesentlichen Funktionen gehören:

- Speicherung und Verwaltung von GRC-relevanten Informationen (Unternehmensregeln, interne Bestimmungen, Vorschriften, Richtlinien, Prozessabläufe, Risiko- und Kontrollbibliotheken etc.) in einem zentralen System
- Proaktive Identifizierung, Analyse und Überwachung potenzieller Gefahren und Initiierung entsprechender Reaktionen

- Automatische Kontrollen von Benutzerzugriffen und -berechtigungen
- Überwachung von Geschäftsprozessen zur Sicherstellung vorgegebener Abläufe und Optimierung der Ergebnisse
- straffes Management der Einhaltung von Vorschriften im Außenhandel und in den Bereichen Umwelt-, Gesundheits- und Arbeitsschutz

Kern der SAP-Lösung ist ein zentrales Repository, das alle GRC-relevanten Daten und Dokumente, z. B. Regelwerke, Richtlinien, Prozesse, Risiken, Kontrollen, Testpläne, Anwendungen, Systeme, Problemlösungsfälle oder Nachweise, verwaltet. Durch die Möglichkeit der Verknüpfung von Unternehmensrichtlinien und -verfahren mit behördlichen Auflagen wird eine konsistente und effektive Einhaltung externer wie interner Vorschriften und Regeln gewährleistet.

Ein weiterer, global tätiger Softwareanbieter ist die Firma Oracle®, die ebenfalls eine GRC-Plattform anbietet. Diese Plattform besteht aus den drei Ebenen Infrastruktur-Services, Anwendungen und Prozesse. Die Infrastruktur-Services beinhalten die Bereiche Identitäts- und Änderungsmanagement, Content Management, Datensicherheit und Datenaudit. Diese Services richten sich auf die unterschiedlichen Anwendungen, die von Oracle, aber auch von anderen Anbietern stammen können. Hierauf setzen die eigentlichen GRC-Prozesse auf: Risiko- und Compliance-Management, Richtlinien- und Controls-Management sowie branchenspezifische Compliance-Prozesse (z. B. Basel II). Der Schwerpunkt liegt auf einem Prozessmanagement mit automatisierten Kontrollen für alle betroffenen Anwendungen, Middleware und Datenbanken.

Die Lösungen der großen Softwarehersteller versuchen, das gesamte Spektrum von Governance, Risk und Compliance abzudecken. Eine eigenständige Compliance-Lösung gibt es dagegen eher selten. Dies ist historisch dadurch zu erklären, dass die jetzigen integrierten GRC-Pakete in der Regel aus früheren Risikomanagement-Lösungen stammen, die um Governance- und Compliance-Funktionalitäten erweitert wurden. Aus diesem Grunde finden sich auch noch zahlreiche Softwarelösungen, die zwar Compliance in ihrer Werbung versprechen, letztlich aber ausschließlich oder überwiegend Risikomanagement-Lösungen darstellen. Derartige Softwarelösungen stammen insbesondere von kleinen und mittleren Anbietern, die entsprechend den Mittelstand als Kunden adressieren.

GRC-Software muss wie jede andere Standard-Anwendungssoftware in einem systematischen, strukturierten Beschaffungsprozess ausgewählt werden. Vor allem umfassende Anforderungs- und Marktanalysen sind essenziell für die erfolgreiche Toolauswahl.



Praxistipp: Ziele und Prozesse der IT-Compliance zuerst klären.

Basierend auf den Zielen der IT-Compliance und einem klaren Prozessverständnis lassen sich die weiteren Elemente des Managementsystems für IT-Compliance leicht ableiten. Dies gilt insbesondere für die Aufgaben- und Verantwortungsteilung, das Berichtswesen und die einzusetzenden Methoden und Tools.

■ 13.9 Organisatorische Verankerung von IT-Compliance

Die Institutionalisierung von IT-Compliance richtet sich auf die Übertragung von Compliance-Aufgaben sowie eine entsprechende Zuweisung von Befugnissen und Verantwortung an alle Betroffenen. Es geht also nicht nur um die Etablierung einer Organisationseinheit mit der Bezeichnung „IT-Compliance“ bzw. der Einrichtung einer Position „IT-Compliance-Officer“ (ITCO). Grundlage für die aufbauorganisatorische Institutionalisierung der IT-Compliance ist die Frage, wie die Corporate Compliance im Unternehmen strukturiert ist, insbesondere ob hier eine zentrale oder eine dezentrale Ausrichtung dominiert. Größere, vor allem räumlich verteilt agierende Unternehmen werden nicht umhinkommen, eine dezentrale Zuordnung der Verantwortung für IT-Compliance vorzunehmen. Das Grundmodell der IT-Compliance-Organisation besteht dann zumindest aus drei Ebenen (nach [Bü10], S. 141 ff.):

- Ebene 1: Der Unternehmensleitung obliegt die Gesamtverantwortung für IT-Compliance (im Rahmen und als Teil der Verantwortung für Corporate Compliance).
- Ebene 2: Ein IT-Compliance-Officer nimmt per Delegation die zentrale Schnittstellen- und Steuerungsfunktion für IT-Compliance wahr.
- Ebene 3: Dezentrale IT-Compliance-Beauftragte nehmen in den einzelnen Unternehmensfunktionen bereichsbezogene IT-Compliance-Funktionen wahr.

In jedem Fall stellt die Unternehmensleitung auch für Compliance (inkl. IT-Compliance) die oberste Ebene dar. Bei ihr verbleibt die Gesamtverantwortung für die Initiierung, Konzeption, Implementierung, Überwachung und Weiterentwicklung des Compliance-Managementsystems. Immer mehr Unternehmen gehen dazu über, ein Compliance-Ressort in der Unternehmensleitung zu verankern, wobei das betreffende Mitglied der Unternehmensleitung dann von einem Corporate Compliance-Officer (COO) unterstützt wird. Ist ein solches Ressort in der Unternehmensleitung vorhanden, wäre auch hier die oberste Verantwortung für IT-Compliance zu verorten. Da aber letztlich allen Mitgliedern einer Unternehmensleitung eine Gesamtverantwortung zukommt, zeichnet auch das für die IT verantwortliche Mitglied der Unternehmensleitung (CIO) für IT-Compliance verantwortlich.

Die zweite Ebene der IT-Compliance-Organisation stellt der IT-Compliance-Officer dar. Für seine organisatorische Anbindung bieten sich grundsätzlich zwei Varianten an:

1. Zuordnung des IT-Compliance-Officer zum COO, wobei der ITCO in diesem Falle eher eine Linienstelle innerhalb des Compliance-Bereichs einnehmen wird.
2. Zuordnung des IT-Compliance-Officer zum Chief Information Officer (CIO), wobei die Position hier eher als Stabstelle ausgeprägt ist und die Compliance der IT-Funktion im Vordergrund stehen wird.

In der Praxis finden sich zudem Konstellationen, bei denen ein IT-Compliance-Officer eine dezentrale Compliance-Funktion in einem Konzernbereich wahrnimmt, mithin in der Fachfunktion angesiedelt ist und IT-Compliance in Zusammenarbeit mit einer zentralen Compliance-Funktion und/oder der IT-Funktion sicherstellt.

Da die Position eines IT-Compliance-Officer derzeit weder in der Theorie noch in der Praxis gefestigt ist, gibt es in Unternehmen eine große Spannbreite, die von fachlich eng fokussierten

IT-Spezialisten, die operativ tätig sind, bis hin zu einer im Unternehmensbereich Compliance für die IT verantwortlichen Führungspositionen reicht. Dies ist zu berücksichtigen, wenn im Folgenden versucht wird, das Aufgabenfeld eines IT-Compliance-Officer zu umreißen. Je nach Auslegung werden Teile des aufgezeigten Aufgabenspektrums relevant sein, andere hingegen entfallen.

Generelle Aufgaben des IT-Compliance-Officer bestehen darin, den COO bzw. den CIO in allen Compliance-relevanten Fragen zu beraten, die Gestaltung und Weiterentwicklung des Managementsystems für IT-Compliance zu konzipieren und die Umsetzung zu koordinieren. Im Rahmen des IT-Compliance-Managementsystems hat der IT-Compliance-Officer das Berichtswesen zu verantworten sowie die Koordination mit der Corporate Compliance sicherzustellen. Im Einzelnen kommen folgende Aufgaben für den IT-Compliance-Officer in Frage:

- Unterstützung der Unternehmensleitung (oder des CCO) und der IT-Leitung in allen IT-Compliance-relevanten Fragen
- Ansprechpartner für die IT-Mitarbeiter des Unternehmens vor allem bei Systementwicklung und -betrieb
- Ansprechpartner für externe Stellen, vor allem externe IT-Auditoren, IT-Berater
- Initiieren der Analyse des Regelungsbedarfs hinsichtlich IT-Compliance und Steuerung der Umsetzung in Richtlinien, Verfahrensanweisungen etc.
- Bestimmung fachbereichsübergreifender IT-Compliance-Risiken
- Einleitung fachbereichsübergreifender IT-Compliance-Maßnahmen und Überwachung ihrer Ausführung
- Realisierung von Synergien aus der Konsolidierung dezentraler IT-Compliance-Maßnahmen
- Konzeption und Weiterentwicklung des IT-Compliance-Managementsystems
- Koordination und Dokumentation der Umsetzung des IT-Compliance-Managementsystems
- Sicherstellen von Compliance-Information und -Kommunikation (IT-Compliance-Berichtswesen)
- Koordination mit IT-Risikomanagement und IT-Sicherheitsmanagement
- Steuerung der dezentralen IT-Compliance-Beauftragten
- Entgegennahme und Konsolidierung der Berichte seitens der dezentralen IT-Compliance-Beauftragten und Berichterstattung an den Corporate Compliance-Officer bzw. das IT-Compliance-Committee
- Initiierung und Steuerung von Konzeption und Betrieb eines Überwachungssystems zur Einhaltung der IT-Compliance-Anforderungen
- Mitwirkung an der Aufdeckung von Non-Compliance sowie Initiierung und Überwachung entsprechender Maßnahmen.

Stellenanzeigen kommen häufig mit kürzeren Aufgabenaufstellungen aus, wie das folgende Beispiel aus dem Jahr 2010 zeigt.

Beispiel:

Ein Finanzkonzern sucht einen IT-Compliance-Officer, der in einer der IT-Funktion zugeordneten Stabsabteilung folgende Aufgaben wahrnehmen soll:

- Unterstützung der IT-Compliance innerhalb des Konzerns

- Mitwirkung an der Weiterentwicklung des IT-Kontrollsystems
- Mitwirkung bei der Erstellung von Verfahrensanweisungen und der Qualitätssicherung von IT-Prozessen
- (Teil-)Projektleitung von IT-Compliance-Projekten
- Unterstützung bei der Betreuung von Prüfern (interne/externe Revision, Aufsichtsorganisationen etc.)
- Unterstützung bei der Beratung und Schulung von Mitarbeitern aus der IT und den Fachbereichen zum Thema IT-Compliance.

Dem IT-Compliance-Officer wird eher eine konzeptionelle, initiiierende, beratende und steuernde Rolle zukommen, sein Schwerpunkt wird weniger in der Durchführung liegen. Hierfür sind dem IT-Compliance-Officer dezentrale IT-Compliance-Beauftragte in der IT-Abteilung und in den Fachabteilungen zugeordnet, die jeweils spezifische Aufgaben innerhalb der IT-Compliance erfüllen, siehe Abbildung 13.15. Diese dezentralen Positionen stellen die dritte Ebene der IT-Compliance-Organisation dar. In größeren Unternehmen werden weitere Ebenen und auch eine regionale Dimension (z.B. Compliance-Verantwortliche in Landesgesellschaften) hinzukommen müssen.

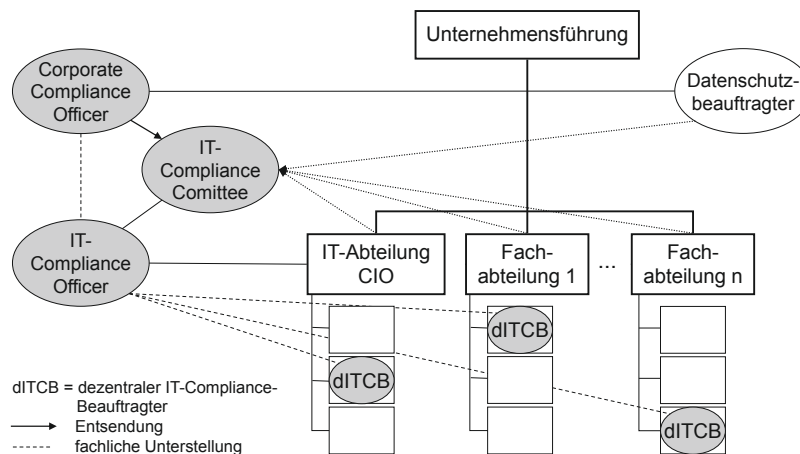


ABBILDUNG 13.15 Organisationsstruktur für IT-Compliance

Die Beziehung zwischen IT-Compliance-Officer und den dezentralen IT-Compliance-Beauftragten kann von einer begrenzten funktionalen Weisungsbefugnis bis zu einer vollständigen fachlichen Unterstellung reichen. Letztere Variante wird dann kaum in Betracht kommen, wenn Aufgaben der IT-Compliance von einem dezentralen Compliance-Beauftragten, der dem COO zugeordnet ist, wahrgenommen werden. Die Aufgaben der dezentralen IT-Compliance-Beauftragten sind:

- Identifizierung der für den jeweiligen Bereich relevanten Regelwerke und IT-Compliance-Vorgaben
- Bestimmung der fachbereichsbezogenen IT-Compliance-Risiken
- Einleitung der fachbereichsbezogenen IT-Compliance-Maßnahmen und Überwachung ihrer Ausführung

- Dokumentation und Berichterstattung an den IT-Compliance-Officer
- Zusammenarbeit mit dem IT-Compliance-Officer bei Vorliegen von Non-Compliance.

Je nach Größe und Gegenstand des Unternehmens kann es sinnvoll sein, das 3-Ebenen-Modell um ein IT-Compliance-Committee zu ergänzen, das aus dem CIO, dem Corporate Compliance-Officer, dem Datenschutzbeauftragten sowie Vertretern der Rechtsabteilung, der IT-Revision, der Personalabteilung und der Fachbereiche bestehen kann. Dieses Gremium bietet die Möglichkeit, weitere unternehmensinterne Zentral-Funktionen sowie die betroffenen Fachbereiche in die IT-Compliance-Organisation aktiv einzubinden. Eine organisatorische Alternative würde darin bestehen, die organisatorischen Schnittstellen im Einzelfall zu regeln.

Das IT-Compliance-Committee hat die Aufgabe, den IT-Compliance-Officer in seiner Funktion zu unterstützen, aber auch zu kontrollieren. Dieses Gremium wäre dann der Empfänger der vom ITCO erstellten IT-Compliance-Statusberichte. Die Unterstützung bezieht sich im Wesentlichen auf notwendige Abstimmungen in der Planungs- und Vorbereitungsphase von Compliance-Maßnahmen. Die Aufgaben des IT-Compliance-Committee sind im Einzelnen:

- übergreifende GRC-Koordination
- Koordination mit Corporate Compliance
- Risikobasierte Priorisierung von IT-Compliance-Maßnahmen
- Abstimmungen und Ressourcenbereitstellung in der Planungs- und Vorbereitungsphase von Compliance-Maßnahmen
- Unternehmensinterne Promotion für IT-Compliance, insbesondere in speziellen Bereichen, beispielsweise Datenschutz, Datensicherheit
- Kontrolle von IT-Compliance-Maßnahmen (vor allem in Folge von Compliance-Verstößen)
- Entgegennahme der IT-Compliance-Statusberichte



Praxistipp: IT-Compliance erfordert ein eigenes Organisationsprojekt

Die Organisation von IT-Compliance erfordert ein eigenes Organisationsprojekt, wie sich leicht anhand der Vielzahl der geschilderten Ansätze erkennen lässt. IT-Compliance lässt sich nicht „nebenbei“ mit der Zuweisung einiger Verantwortlichkeiten einrichten.

Die weitere Entwicklung der Organisation von IT-Compliance in einem Unternehmen wird wesentlich von der Integration der IT-Compliance in die Corporate Compliance und die Integration der Corporate Compliance in eine GRC-Organisation abhängen. Aufgrund der engen Verzahnung dürfte langfristig keine Alternative zu einer organisatorischen Zusammenführung bestehen. Dies bedeutet aber nicht, dass IT-Compliance als Teilbereich des IT-Managements seine Bedeutung verlieren wird.



Das Wichtigste – zusammengefasst:

- **Klären Sie Inhalt und Bedeutung von IT-Compliance für Ihr Unternehmen, insbesondere die Schnittstellen zur Corporate Governance und Compliance auf der einen, zu IT-Governance, IT-Risiko- und -Sicherheitsmanagement auf der anderen Seite!**

Im Rahmen des übergeordneten GRC-Konzeptes muss IT-Compliance mit den verschiedenen Managementbereichen strukturell, konzeptionell und methodisch abgestimmt werden. Die Hauptverantwortung kommt hierbei der Unternehmensleitung sowie dem für die IT-Funktion Verantwortlichen zu. Grundlegend bezeichnet IT-Compliance einen Zustand, in dem alle die IT des Unternehmens betreffenden, verbindlich vorgegebenen bzw. als verbindlich akzeptierten Vorgaben nachweislich eingehalten werden. Dies erfordert die Identifizierung relevanter Regelwerke und die Erfüllung der aus ihnen resultierenden Vorgaben im Rahmen eines IT-Compliance-Prozesses.

- **Klären Sie den Nutzen von IT-Compliance, um die Unterstützung von Top-Management und Fachabteilungen für IT-Compliance sicherzustellen!**

Neben der selbstverständlichen Pflicht zur Erfüllung gesetzlicher Vorschriften soll IT-Compliance ein Unternehmen vor allem vor wirtschaftlichen Nachteilen als Folge von Rechtsverletzungen bewahren. Es sollen insbesondere Schadensersatzpflichten, Strafen, Buß- und Zwangsgelder vermieden werden. Der weitere Nutzen von IT-Compliance richtet sich auf die Erhöhung des Wertbeitrags der IT, die Steigerung der Qualität von IT-Prozessen, die Erhöhung der IT-Sicherheit sowie die Reduzierung von IT-Kosten und IT-Risiken.

- **Richten Sie ein Managementsystem für IT-Compliance ein!**

Ein Managementsystem für IT-Compliance legt fest, aufgrund welcher IT-Compliance-Ziele und Verhaltensprinzipien sowie mit welchen Methoden und Tools das IT-Management die auf IT-Compliance gerichteten Aufgaben und Maßnahmen nachvollziehbar steuert (d. h. plant, einsetzt, durchführt, überwacht, prüft und verbessert). Hierbei ist auch zu klären, durch welche IT-Systeme IT-Compliance herbeigeführt werden soll. Hierfür sind z. B. Lösungen für Security- oder Content-Management, Archivierung, Verschlüsselung, Nutzer-, Zugangs- und Lizenzverwaltung aufeinander abgestimmt einzusetzen.

- **Organisieren Sie die Zusammenarbeit für IT-Compliance!**

Die IT-Abteilung und ihre Leitung haben den Großteil an Maßnahmen zur Erfüllung der IT-Compliance-Anforderungen zu planen und durchzuführen. Eine besondere Bedeutung kommt der Position des IT-Compliance-Officer zu. Dieser hat die Unternehmens- und IT-Leitung in allen IT-Compliance-relevanten Fragen zu beraten, die Gestaltung und Weiterentwicklung des Managementsystems für IT-Compliance zu konzipieren und die Umsetzung zu koordinieren. Aber auch die Fachabteilungen tragen eine Verantwortung bei der Erfüllung von IT-Compliance-Anforderungen – und zwar immer dann, wenn bereichsbezogene organisatorische oder personelle Compliance-Maßnahmen ergriffen und entsprechende IT-gestützte Kontrollen eingeführt werden.

■ 13.10 Literatur

- [AG08] Arnsberger, Malte; Grill, Markus: Lidl muss Millionen-Strafe zahlen, 11.09.2008, online verfügbar unter: <http://www.stern.de/wirtschaft/news/unternehmen/ueberwachungsskandal-lidl-muss-millionen-strafe-zahlen-638756.html> (Zugriff am 11.07.2011)
- [BF06] Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) [Bafin 2006]: Erläuterungen zu den Mindestanforderungen an das Risikomanagement (MaRisk), Fassung vom 04.05.2006, AT 7.2, online verfügbar unter: http://www.bundesbank.de/download/bankenaufsicht/pdf/marisk/060504_erl.pdf (Zugriff am 23.04.2011)
- [BKK10] BKK Gesundheit: Datensicherheit bei der BKK Gesundheit, online verfügbar unter: http://www.bkkgesundheit.de/gesundheitsbkk/Datensicherheit_bei_der_BKK_Gesundheit/n285/beitrag595/?archivenews=1 (Zugriff am 11.07.2011)
- [Bü10] Bürkle, Jürgen: Compliance-Beauftragte. In: Hauschka, Ch. E. (Hrsg.): Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen. 2. überarb. u. erw. Auflage, Beck, München, 2010, S. 136–162
- [DIN04] DIN Deutsches Institut für Normung e. V.: DIN EN 45020 – Normung und damit zusammenhängende Tätigkeiten – Allgemeine Begriffe (ISO/IEC Guide 2:2004), Juni 2004
- [DIN11] DIN Deutsches Institut für Normung e. V.: Jahresbericht 2010/2011, Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN, Berlin 2011, online verfügbar unter: http://www.nia.din.de/sixcms_upload/media/2397/Jahresbericht_2010_2011_Endfassung_2011_04_11.pdf (Zugriff am 22.04.2011)
- [Hau10] Hauschka, Christoph E.: § 1, Einführung. In: Hauschka, Ch. E. (Hrsg.): Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen. 2. überarb. u. erw. Auflage, Beck, München, 2010, S. 1–25
- Das mehr als 1100 Seiten umfassende, von Hauschka herausgegebene Sammelwerk hat sich in kurzer Zeit zum Standardwerk für die Corporate Compliance entwickelt, wobei die „Legal Compliance“ im Mittelpunkt steht. Hinsichtlich der IT-Compliance werden Datenschutz und IT-Sicherheit in eigenen Kapiteln abgehandelt. Außerdem findet sich ein Kapitel zu IT-gestützten Compliance-Lösungen, die das Interne Kontrollsystem unterstützen.
- [Hei08] Heise Online (Hg.): Fernsehmagazin: Datenpanne bei Einwohnermeldeämtern (Update), 23.06.2008, online verfügbar unter: <http://www.heise.de/newsticker/meldung/Fernsehmagazin-Datenpanne-bei-Einwohnermeldeaeamtern-Update-215737.html> (Zugriff am 11.07.2011)
- [ITGI05] IT Governance Institute (ITGI): COBIT 4.0, Deutsche Ausgabe, Rolling Meadows: ITGI 2005
- COBIT ist das führende Framework sowohl für die Implementierung eines IT-Kontrollsystems als auch für die normen- und standardkonforme Umsetzung von IT-Governance. COBIT enthält insofern auch Vorgaben für die IT-Compliance und kann als Basis für ein IT-Compliance-Managementsystem dienen.
- [JG07] Johannsen, Wolfgang; Goeken, Matthias: Referenzmodelle für IT-Governance – Strategische Effektivität und Effizienz mit COBIT, ITIL & Co. 2., akt. u. erw. Auflage, dpunkt.verlag, Heidelberg, 2011
- Das in einer aktuellen zweiten Auflage vorliegende Buch von Johannsen und Goeken enthält eine äußerst hilfreiche Beschreibung der wichtigsten Referenzmodelle, Normen und Standards für die IT-Governance. Die verschiedenen Regelwerke werden verglichen, woraus die Verfasser Hinweise für einen gemeinsamen Einsatz ableiten.
- [KD08] Klotz, Michael; Dorn, Dietrich-W.: IT-Compliance – Begriff, Umfang und relevante Regelwerke. In: HMD Praxis der Wirtschaftsinformatik, 2008, Jg. 45, Heft 263, S. 5–14
- [KD09] Klotz, Michael; Dorn, Dietrich-W.: IT-Compliance in KMU, in: Der Betriebswirt 2009, 50. Jg., Heft 1, S. 23–27 und: IT-Compliance in KMU (Teil 2), in: Der Betriebswirt 2009, 50. Jg., Heft 2, S. 17–20

- [K109a] Klotz, Michael: IT-Compliance – Ein Überblick, dpunkt-Verlag, Heidelberg 2009
- [K109b] Klotz, Michael: Facetten der IT-Compliance. In: IT-Service Management, 2009, 4. Jg., Heft 9, S. 5–8
- [KS11] Klotz, Michael; Sulk, Ingolf: Digitale Betriebsprüfung – Handlungsfelder und vorbereitende Datenanalyse. In: Der Betriebswirt, 2011, 52. Jg., Heft 1, S. 8–12
- [MK06] Michels, Thomas; Krzeminska, Anna: Sarbanes-Oxley Act und Six Sigma als Instrumente des Prozess-Controllings bei der AXA Konzern AG. In: v. Werder, A.; Stöber, H.; Grundeis, J. (Hrsg.): Organisations-Controlling – Konzepte und Praxisbeispiele. Gabler, Wiesbaden, 2006, S. 135–151
- [MM10] Manager Magazin (Hg.): Toyota zahlt Rekordstrafe in USA, 21.12.2010, online verfügbar unter: <http://www.manager-magazin.de/unternehmen/autoindustrie/0,2828,735853,00.html> (Zugriff am 11.07.2011)
- [RS09] Rath, Michael; Sponholz, Rainer: IT-Compliance – Erfolgreiches Management regulatorischer Anforderungen, Erich Schmidt Verlag, Berlin 2009
Das Buch von Rath und Sponholz ist die erste deutschsprachige Monographie zur IT-Compliance und bietet einen umfassenden Überblick. Neben dem rechtlichen Rahmen werden Management, Prozesse und Werkzeuge der IT-Compliance behandelt. Zahlreiche Übersichten und Verweise auf Studien und weitere Internet-Quellen ermöglichen eine Vertiefung der Thematik.
- [Sp09] Spiegel Online (Hg.): Ex-Chef Pierer zahlt Siemens fünf Millionen Euro, 02.12.2009, online verfügbar unter: <http://www.spiegel.de/wirtschaft/unternehmen/0,1518,664758,00.html> (Zugriff am 11.07.2011)
- [Sp10a] Spiegel Online (Hg.): Daimler kauft sich für 185 Millionen Dollar frei, 01.04.2010, online verfügbar unter: <http://www.spiegel.de/wirtschaft/unternehmen/0,1518,687097,00.html> (Zugriff am 11.07.2011)
- [Sp10b] Spiegel Online (Hg.): Stahl-Kartell muss halbe Milliarde Euro zahlen, 30.06.2010, online verfügbar unter: <http://www.spiegel.de/wirtschaft/unternehmen/0,1518,703834,00.html> (Zugriff am 11.07.2011)
- [St08] Stern.de (Hg.): 17 Millionen Kundendatensätze geklaut, 04.10.2008, online verfügbar unter: <http://www.stern.de/wirtschaft/news/unternehmen/t-mobile-17-millionen-kundendatensaetze-geklaut-641223.html> (Zugriff am 11.07.2011)
- [St09] Stern.de (Hg.): Bahn akzeptiert Millionenstrafe, 23.10.2009, online verfügbar unter: <http://www.stern.de/wirtschaft/news/unternehmen/datenaffaere-bahn-akzeptiert-millionenstrafe-1516469.html> (Zugriff am 11.07.2011)
- [St10] Stern.de (Hg.): Größte BKK wird erpresst, 11.02.2010, online verfügbar unter: <http://www.stern.de/wirtschaft/news/datendiebe-groesste-bkk-wird-erpresst-1542789.html> (Zugriff am 11.07.2011)

Rechtliche Rahmenbedingungen für das IT-Management

Werner Bachmann



Fragen, die in diesem Kapitel beantwortet werden:

- Welchen gesetzlichen Vorgaben muss das IT-Management gerecht werden, und welche Konsequenzen hat das für das IT-Management, wenn diese Vorgaben nicht beachtet werden?
- Welche Herausforderungen ergeben sich aus den wachsenden Anforderungen an die IT-Organisation bei der Sicherstellung von Corporate Compliance und Corporate Governance?
- Wie werden IT-Leistungen beschafft, und was sind die zentralen Anforderungen des Vergaberechts (etwa in öffentlichen Unternehmen)?
- Welche Bedeutung haben Allgemeine Geschäftsbedingungen und wie werden daraus belastbare Verträge?
- Welche Rechte habe ich als Kunde bei fehlerhaften Hardware-Lieferungen?
- Warum ist das Lizenzmodell bei der Softwarebeschaffung so wichtig, und wie erreiche ich eine auf mein Unternehmen zugeschnittene Lizenzierung?
- Welche Vertragsmodelle stehen für IT-Projekte zur Verfügung, und welches Modell ist das für mein Projekt passende?
- Welche rechtlichen Fragen sind bei Cloud Computing zu beachten?

Die Handlungsempfehlungen für das IT-Management, die Sie in diesem Handbuch bisher kennen gelernt haben, orientieren sich an dem, was Ihnen nach dem aktuellen Stand der Technik an Werkzeugen und Methoden an die Hand gegeben werden kann, um die Aufgaben einer IT-Organisation möglichst effizient und erfolgreich erfüllen zu können.

In diesem letzten Kapitel werden wir uns mit der Frage beschäftigen, welche wesentlichen rechtlichen Rahmenbedingungen Sie dabei zu beachten haben. Im Mittelpunkt stehen auch hier die „Werkzeuge“, also die rechtlichen Instrumente und Verfahren, die Sie kennen müssen, wenn Sie mit Aufgaben des IT-Management in Ihrem Unternehmen betraut sind. Hierzu gehört die Ausschreibung von Beschaffungsvorhaben, der Umgang mit Standardverträgen, die Software Lizenzierung und anderes mehr.

Bevor wir uns die „Toolbox“ des rechtlichen Instrumentariums näher ansehen, wenden wir uns dem übergeordneten Thema zu, welche rechtlichen Vorgaben für das IT-Management als Teil der Unternehmensorganisation insgesamt gelten und welche Konsequenzen es hat, wenn diese Vorgaben nicht beachtet werden. Für diese Fragestellung haben sich in jüngster Zeit die Begriffe „IT-Governance“ und „IT-Compliance“ eingebürgert. Mit ihnen beginnt deshalb der erste Teil dieses Kapitels.

■ 14.1 IT-Governance und IT-Compliance

14.1.1 Vorsorge gegen Gesetzesverstöße und Risikomanagement

Was sich hinter „Governance“ und „Compliance“ verbirgt, ist nicht leicht zu verstehen. Die lexikalischen Übersetzungen (Organisation und Kontrolle, Einhaltung geltender Gesetze) helfen im Grunde nicht weiter. IT-Management verlangt selbstverständlich eine gewisse Organisation, und Gesetze gelten natürlich im Rahmen ihres jeweiligen Anwendungsbereiches auch für die IT (zum Thema „Governance“ vgl. ausführlich Kapitel 10 in diesem Handbuch). Worum geht es bei IT-Compliance in der Sache?



IT-Compliance besteht aus drei Komponenten:

- Vorsorge gegen Gesetzesverstöße,
- Einrichtung eines Risikomanagementsystems,
- persönliche Haftung des Managements bei Verletzung der Compliance-Vorgaben.

Vorsorge gegen Gesetzesverstöße

Historischer Hintergrund der Compliance-Diskussion sind die in angelsächsischen Ländern entwickelten Strafzumessungsregelungen im Zusammenhang mit Unternehmensdelikten (typischerweise illegalen Preis- oder anderen Kartellabsprachen). Das United States Sentencing Guidelines Manual (<http://www.ussc.gov/guidelin.htm>), mit dessen Hilfe Bußgelder für solche Delikte festgelegt werden, sieht zwingend Strafmilderungen vor, wenn das betreffende Unternehmen nachweisen kann, dass es wirksame organisatorische Vorkehrungen zur Vorsorge und Aufdeckung gesetzeswidrigen Verhaltens getroffen hat, diese regelmäßig überprüft und fortentwickelt.



§ 8B2.1.

Effective Compliance and Ethics Program: (1) exercise due diligence to prevent and detect criminal conduct; and (2) otherwise promote an organizational culture that encourages ethical conduct and a commitment to **compliance** with the law. Such compliance and ethics program shall be reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct.

Vergleichbare Entwicklungen gab es in Deutschland im Bereich des Ordnungswidrigkeitenrechts. Nach § 130 OWiG kann mit Geldbuße belangt werden, wer als Inhaber eines Betriebs oder Unternehmens in vorsätzlicher oder fahrlässiger Weise Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in dem Unternehmen strafbewehrte Gesetzesverstöße zu verhindern. Anwendungsfälle hierfür waren in der Regel Produkthaftungsfälle (Körperverletzung durch fehlerhafte Produkte) und Verstöße gegen das Kartellgesetz. Die Gerichte haben aus Anlass solcher Fälle detaillierte und sehr strenge Anforderungen an die vom Manage-

ment zu treffenden Aufsichtsmaßnahmen entwickelt (beispielsweise Berichtspflicht der Mitarbeiter über jedweden Kontakt zu anderen Unternehmen als Vorsorgemaßnahme gegen Korruption)

Der Begriff Compliance hat schließlich auch Eingang in den deutschen Corporate Governance Kodex gefunden (<http://www.corporate-governance-code.de/ger/kodex/index.html>), dem Regelwerk für „gute“ Unternehmensführung im Sinne nachhaltigen, risiko- und wertorientierten, regelkonformen Managements. Unter Punkt 4.1.3 des Kodex heißt es:



Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance).

Börsennotierte Unternehmen sind verpflichtet, ihren Aktionären gegenüber jedes Jahr schriftlich zu erklären, ob sie sich diesem Corporate Governance Kodex unterwerfen (die so genannte „Entsprechenserklärung“, § 166 AktG).

Erster wesentlicher Bestandteil von Compliance ist damit die Pflicht eines Unternehmens,

- organisatorische und
- technische Maßnahmen

zu treffen, um Gesetzesverstöße zu vermeiden.

Die gesetzliche Verankerung von Compliance und Governance setzte in Deutschland Ende der 90er Jahre des letzten Jahrhunderts im Nachgang zu spektakulären Unternehmenszusammenbrüchen und Skandalen um Bilanzfälschungen ein. Der Gesetzgeber reagierte auf diese Vorfälle mit dem Gesetz über Kontrolle und Transparenz im Unternehmensbereich (KonTraG) von 1998. Die zentrale Vorschrift ist § 91 Abs. 2 AktG.



§ 91 Abs. 2 AktG

Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.

Die Unternehmen werden dazu verpflichtet, ein effizientes Risikofrüherkennungs- und Überwachungssystem für bestandsgefährdende Unternehmensrisiken einzurichten. Eine solche Gefahrenlage besteht dann, wenn nachteilige Entwicklungen im Hinblick auf die Vermögens- und Ertragslage eines Unternehmens eintreten, die das Risiko einer Insolvenz des Unternehmens entstehen lassen oder ein solches Risiko wesentlich erhöhen.

Welche Anforderungen an ein Compliance-System im Einzelnen zu stellen sind, darüber schweigt sich das Gesetz aus. Der Gesetzgeber hatte hier zunächst nur den Geschäftsprozess „Risikomanagement“ im Blick (vgl. hierzu ausführlich Kapitel 12 „IT-Risikomanagement“ dieses Handbuchs). Dieses System muss folgende Leistungsmerkmale aufweisen:

- Identifikation von Risiken,
- Risikoanalyse und Risikobewertung,

- Zuordnung von Aufgaben und Verantwortlichkeiten,
- Dokumentation der getroffenen Maßnahmen zur Bewältigung von Risiken und
- Risikokontrolle.

Im Hinblick auf die komplexen Organisationsstrukturen und Geschäftsprozesse in Unternehmen ist jedoch mit Händen zu greifen, dass der informationstechnologischen Infrastruktur in der Praxis eine entscheidende Rolle zukommen muss. Ohne Kommunikation und Dokumentation, Risikoanalyse und Risikokontrolle ist schlechterdings nicht vorstellbar, wie die frühzeitige Erkennung von Risiken für die finanzielle Stabilität eines Unternehmens umgesetzt werden könnte.



Risikomanagement als Kernaufgabe der IT

Für Unternehmen ab einer gewissen Größe ist die Unternehmens-IT das zentrale Mittel zur Umsetzung der gesetzlich geforderten Überwachungs- und Vorsorgesysteme für elementare Risiken. Das IT-Management muss darüber hinaus aber auch dafür Sorge tragen, dass die Compliance-Vorgaben in der IT-Organisation richtig umgesetzt werden. IT-Compliance gehört deshalb zu den Kernaufgaben des IT-Managements!

Kein Unternehmen ist wie das andere. Die gesetzlichen Strukturen geben deshalb mit den Formulierungen „geeignet“ und „angemessen“ hinreichenden Spielraum dafür, maßgeschneiderte Überwachungssysteme für die jeweilige Unternehmens- und Konzernsituation zu entwerfen. Wichtig ist nur, dass das Überwachungssystem effizient sein muss und dynamisch an die sich wandelnden Anforderungen und technischen Standards angepasst wird. Da der Gesetzgeber hinsichtlich der technischen Umsetzung keine Vorgaben macht, sind die Unternehmen auf die berechtigten Verkehrserwartungen und von Wissenschaft und Technik entwickelten anerkannten Standards für solche Überwachungssysteme verwiesen. Das Verbindungsstück zwischen den etablierten technischen Standards und Best Practices des IT-Managements, die in diesem Buch an anderer Stelle bereits vorgestellt wurden (siehe dazu die Kapitel 10 „IT-Governance“ und 13 „IT-Compliance“ dieses Handbuchs), stellen die Haftungsregelungen dar, mit denen Verstöße gegen Compliance-Vorgaben sanktioniert werden. Dieses Haftungssystem wird sogleich unten erläutert werden.

Geltung für alle Unternehmen

Für das IT-Management ist zu beachten, dass die Forderung nach einem unternehmensinternen System des Risikomanagements nicht auf Aktiengesellschaften beschränkt ist, an die sich die genannten rechtlichen Bestimmungen in erster Linie richten. In der Begründung des Gesetzentwurfs wird ausdrücklich darauf hingewiesen, dass die grundsätzliche Verpflichtung zur Einführung eines Risikomanagementsystems auch für alle anderen Unternehmensformen gelten soll (beispielsweise die GmbH, Genossenschaften u.a.), auch wenn die oben genannte Passage dort nicht ausdrücklich in den Gesetzeswortlaut aufgenommen worden ist. Aufgrund der prominenten Stellung der Regelung im Aktienrecht erwartet der Gesetzgeber ein „Ausstrahlen“ auf alle anderen Unternehmensformen.

14.1.2 Reporting

Über das Compliance-System einschließlich der IT-Risiken muss bei börsennotierten Unternehmen im **Lagebericht** der Gesellschaft berichtet werden, und zwar im Zusammenhang mit den Methoden und Zielen des Risikomanagements. Der Lagebericht ist Gegenstand der Prüfung durch den Abschlussprüfer, der von Gesetzes wegen die Eignung und Effizienz des Compliance-Systems beurteilen muss.



§ 317 Abs. 4 HGB

Bei einer börsennotierten Aktiengesellschaft ist außerdem im Rahmen der Prüfung zu beurteilen, ob der Vorstand die ihm nach § 91 Abs. 2 des Aktiengesetzes obliegenden Maßnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgabe erfüllen kann.

Die weiteren Einzelheiten für Inhalt und Umfang der Abschlussprüfung sind im Prüfungsstandard IDW PS 340 enthalten (www.idw.de).



Externe Prüfung des Risikomanagements durch den Wirtschaftsprüfer

Der Prüfungsbericht des Abschlussprüfers muss eine Bewertung des Risikomanagementsystems im Hinblick auf „existenzgefährdende“ Risiken enthalten. Hierzu gehört auch die Vorsorge für die Absicherung unternehmenskritischer IT-Prozesse und IT-Systeme.

14.1.3 Persönliche Haftung des Managements

Pflichtenstandard

Verstöße gegen Compliance-Vorgaben können zur persönlichen Verantwortung des IT-Managements führen, zivilrechtlich wie strafrechtlich.

Beispiele:

Aufgrund unzureichender externer Absicherung der Kundenportale kommt es zu wiederholten Angriffen auf die Kundendatenbanken eines Online-Service, von 24.000 Benutzerkonten werden Bankverbindungen und Kreditkarteninformationen gestohlen. In der Folgezeit kommt es zu einer Kündigungswelle von Kunden mit der Folge entsprechender Umsatzeinbrüche und massiven Verlusten beim Börsenkurs des Unternehmens.

Bei den in Deutschland zentral betriebenen SAP ERP-Systemen eines internationalen Medizingeräteherstellers werden für Test- und Produktivsysteme identische Administrationskonten verwendet (Kennung und PWD). Bei einer Routinewartungsmaßnahme (Update der Firmware) an den Serversystemen meldet sich der Servicetechniker versehentlich am Produktivsystem statt am Testsystem an und führt dort die Wartungsmaßnahme durch, was zu einem Systemstillstand führt. Trotz sofort eingeleiteter Recovery-Prozesse fällt das ERP-System für zwei Werktage aus, was zu einem entsprechenden weltweiten Betriebsstilland führt.

Vorstände und Geschäftsführer haften persönlich gegenüber ihren Unternehmen, wenn sie ihre Managementpflichten verletzen und dem Unternehmen dadurch ein Schaden entsteht.



§ 93 AktG

(1) Die Vorstandsmitglieder haben bei ihrer Geschäftsführung der Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Eine Pflichtverletzung liegt nicht vor, wenn das Vorstandsmitglied bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln.

(2) Vorstandsmitglieder, die ihre Pflichten verletzen, sind der Gesellschaft zum Ersatz des daraus entstehenden Schadens als Gesamtschuldner verpflichtet.

Die Beweislast dafür, dass das in Anspruch genommene Vorstandsmitglied sorgfältig und gewissenhaft gehandelt hat, liegt beim Vorstand (Beweislastumkehr). Mitglieder des Managements sehen sich deshalb immer stärker genötigt, Geschäftsentscheidungen und deren Grundlagen umfassend zu dokumentieren.

Neben der schadensersatzrechtlichen Verantwortung des IT-Managements gegenüber dem Unternehmen kann eine unmittelbare Haftpflicht gegenüber geschädigten Dritten bestehen, wenn das Leitungsorgan Organisationspflichten verletzt hat. Zu diesem Pflichtenkreis gehört der gesamte Bereich der IT-Compliance. Anspruchsgrundlage hierfür sind die allgemeinen Haftpflichttatbestände des Deliktsrechts und der Produkthaftung.



Non-Compliance bedeutet erhöhtes Haftungsrisiko für das IT-Management

Bei mangelhafter IT-Compliance des Unternehmens ergeben sich für die Unternehmensleitung persönliche Haftungsrisiken gegenüber dem Unternehmen, aber auch gegenüber geschädigten unternehmensfremden Personen!

Zu den grundlegenden Anforderungen an die IT-Sicherheit, die an anderer Stelle in diesem Buch dargestellt wurden (vgl. Kapitel 11 „IT-Security-Management“), gehört unzweifelhaft die Vorsorge gegen Datenverlust und das Vorhalten erprobter Verfahren für die Wiederherstellung der Systeme bei Ausfall der Energieversorgung.

Entscheidungsspielräume

Ganz so einfach macht uns der Gesetzgeber die Sache freilich nicht. Das Management eines Unternehmens muss ständig eine Vielzahl von Entscheidungen treffen, die notwendigerweise auf der Basis unzureichender Informationen getroffen werden müssen oder die in die Zukunft gerichtet und deshalb mit Unsicherheiten und dem Risiko des Scheiterns behaftet sind. Häufig lässt sich nicht genau auseinanderhalten, ob sich hier nur unternehmerisches Risiko verwirklicht oder ob Fehlentscheidungen der Entscheidungsträger für das negative Ergebnis maßgeblich sind. Eine strenge Verrechtlichung würde den Handlungsspielraum von Leitungsorganen so stark verringern, dass unternehmerisches Handeln gar nicht mehr möglich wäre. Den Organen von Gesellschaften wird deshalb ein Freiraum von Haftungsrisiken gewährt, solange

sich der Vorstand im Rahmen des unternehmerischen Risikos bewegt. Für diese Privilegierung hat sich der Begriff „Business Judgement Rule“ eingebürgert.

Zum Kern unternehmerischen Handelns gehören Entscheidungen auf der Basis unvollständiger Informationen. Das bewusste Eingehen geschäftlicher Risiken birgt deshalb die Gefahr von Fehlbeurteilungen und Fehleinschätzungen, mag das IT-Management auch noch so verantwortungsbewusst handeln. Bei „unternehmerischen“ Entscheidungen ist das Leitungsorgan deshalb ausdrücklich von Haftung frei.



Privilegierung der „Business Judgement Rule“

Das IT-Management haftet nicht bei unternehmerischen Entscheidungen, die sich im Nachhinein als riskant oder schadensträchtig erweisen.

Eine „unternehmerische“ Entscheidung liegt aber nicht mehr vor, wenn die Grenzen, in denen sich ein von Verantwortungsbewusstsein getragenes, ausschließlich am Unternehmenswohl orientiertes, auf sorgfältige Ermittlung der Entscheidungsgrundlage beruhendes unternehmerisches Handeln bewegen muss, deutlich überschritten sind, die Bereitschaft, unternehmerische Risiken einzugehen, in unverantwortlicher Weise überspannt worden ist oder das Verhalten des Vorstands aus anderen Gründen als pflichtwidrig gelten muss. Der Spielraum unternehmerischen Handelns ist dann überschritten, wenn aus der Sicht eines ordentlichen gewissenhaften Geschäftsführers das Risiko eines Schadens unabweisbar ist und keine vernünftigen wirtschaftlichen Gründe dafür sprechen, dies dennoch einzugehen.

Für die Frage der IT-Organisation und des IT-Managements bedeutet dies, dass Vorstand und CIO einen weiten Ermessensspielraum haben, in welcher Weise sie den gesetzlichen Anforderungen an ein Risikomanagementsystem nachkommen wollen. Es ist ihnen unbenommen, die Systeme nach den spezifischen Anforderungen ihrer Organisation und den verfügbaren finanziellen Mitteln zuzuschneiden. Die Grenze zur Haftung beginnt dort, wo grundlegende Anforderungen nicht mehr erfüllt werden. Diese elementaren Anforderungen bestimmen sich auf zweierlei Weise:

- Mindestanforderungen an die Leistungsmerkmale (siehe oben) müssen gegeben sein.
- Grundlegende Anforderungen der (weltweit) verfügbaren technischen Standards müssen gewahrt sein.

Bei einem komplexen Implementierungsvorhaben ist der zulässige Entscheidungsspielraum aber längst überschritten, wenn das Projektmanagement kein effizientes Projekt-Controlling vorsieht (in technischer Hinsicht: Quality Reviews, Quality Gates; in finanzieller Hinsicht: Zahlungsplan und Refinanzierung). Analoge Beispiele lassen sich für betriebliche Situationen oder Fragen der Sicherheit ohne weiteres bilden.

Bedeutung technischer Standards

Das Gesetz regelt die Sorgfaltspflichten des IT-Managements im Hinblick auf Compliance nur in sehr allgemeiner Weise. Zur Konkretisierung dieser Sorgfaltspflichten spielen technische Standards und Richtlinien eine wichtige Rolle. Regelwerke wie

- ISO 17799, 20000, 2700x, 9126
- BS 25999

- BSI Grundschutz Handbuch
- ITIL/COBIT/eTom
- Prince2, PMBok/PMI, DPGM
- GxP

sind keine Rechtsnormen und deshalb in der Regel auch nicht unmittelbar durchsetzbar.

Sie formulieren aber für ihren jeweiligen Bereich den Sorgfaltsmaßstab, der sich insoweit als Referenzstandard (Stand der Technik, Good Practice, Best Practice) herausgebildet hat. Wird aus der haftungsrechtlichen Perspektive gefragt, ob das IT-Management die gebotene Sorgfalt angewendet hat, dann muss bestimmt werden, was insofern die verkehrsüblichen Sorgfaltspflichten sind. Normen, Richtlinien und Standards sind gewissermaßen die erste Anlaufstelle für die Beantwortung dieser Fragen.

Wird ein anerkannter Standard nicht eingehalten, dann spricht der erste Anschein dafür, dass die im Verkehr erforderliche Sorgfalt nicht beachtet wurde. Umgekehrt kann der Nachweis einer Zertifizierung auf einen anerkannten Standard ausreichen, um darzulegen, dass vom IT-Management der gebotene Sorgfaltsmaßstab eingehalten wurde.



Technische Normen und Standards sind haftungsrelevant!

Technische Normen, Richtlinien und Standards bilden den Referenzstandard für die Sorgfaltspflichten des IT-Managements. Werden anerkannte Normen oder Standards nicht eingehalten, muss mit einem erhöhten Haftungsrisiko für die IT-Leitung gerechnet werden.

Delegation und Leitungsverantwortung

Die Leitungsorgane eines Unternehmens haften für Schäden, die auch nur von einem Vorstandsmitglied zu vertreten sind, immer insgesamt als Gesamtschuldner. Zwar kann über die Delegation von Zuständigkeiten innerhalb der Unternehmensleitung eine gewisse Aufteilung der Verantwortungsbereiche auf die jeweiligen Ressorts erreicht werden. Eine verbleibende Restverantwortung bleibt jedoch auch für die übrigen Mitglieder erhalten. Sie haben sich darüber zu informieren und auch zu kontrollieren, wie die entsprechenden Ressort-Aufgaben von dem zuständigen Vorstandsmitglied erfüllt werden. Liegt das IT-Management nach der internen Aufgabenverteilung allein beim IT-Vorstand/Technikvorstand/CIO, entbindet das die Vorstandskollegen nicht davon, bei konkreten Anhaltspunkten für mangelhaftes IT-Management zu intervenieren. Andernfalls verhalten sie sich selbst pflichtwidrig.

Innerhalb der IT-Struktur kann der IT-Vorstand Aufgaben an nachgeordnete Ebenen (vertikal) delegieren. Hierbei ist zu beachten, dass das IT-Management nicht nur Informations- und Überwachungspflichten hat, sondern auch für die Auswahl qualifizierter Funktionsträger verantwortlich ist. Aufsicht und Kontrolle über die nachgeordneten Stellen muss dauerhaft und gewissenhaft eingerichtet sein. Die Kontrolldichte muss deshalb relativ hoch sein. Das IT-Management kann nicht nach dem Vertrauensgrundsatz agieren, dass Kontroll- und Überwachungsmaßnahmen erst dann einsetzen müssen, wenn Anhaltspunkte für rechtswidriges Verhalten von Mitarbeitern oder externen Zulieferern vorliegen.



Delegation von Verantwortlichkeiten im IT-Management

Aufgaben können an nachgeordnete Ebenen (vertikal) delegiert werden. Dabei müssen Aufsicht und Kontrolle über die nachgeordneten Stellen so organisiert sein, dass nicht nur bei evidenten Pflichtverletzungen interveniert wird, sondern bereits präventiv Aufsicht und Kontrolle stattfinden muss.

Compliance und Outsourcing

Unternehmen haben beim Bezug von IT-Leistungen sehr unterschiedliche „Fertigungstiefen“. Nur in seltenen Fällen werden alle wesentlichen Leistungen (von der Infrastruktur über Systeme, Applikationen bis zum User Help Desk) selbst produziert. Typischerweise findet man Multi-Sourcing-Strategien, bei denen nur geschäftsprozessnahe und unternehmenskritische Leistungen inhouse selbst erbracht werden. Der Großteil der eher standardisierten IT-Leistungen wird von externen Dienstleistern bezogen.

Welche Auswirkungen hat der externe Bezug solcher Aufgaben auf Umfang und Inhalt der zu leistenden IT-Compliance? Die Antwort darauf ist vergleichsweise einfach: Die Auslagerung von wesentlichen IT-Funktionen lässt die Verantwortung des IT-Managements für den ordnungsgemäßen Betrieb der ausgelagerten Prozesse und Funktionen unberührt.

Dieser Grundsatz findet sich in zahlreichen Compliance-relevanten Regelungen formuliert. Ein viel zitiertes Beispiel ist die Auftragsdatenverarbeitung durch externe Dienstleister gemäß § 11 Bundesdatenschutzgesetz. Die Verantwortung für Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten bleibt beim auslagernden Unternehmen. Damit bleibt es auch bei der gegebenenfalls persönlichen Haftung des IT-Managements im Falle von Datenverlust oder missbräuchlicher Datennutzung.



§ 11 Abs. 1 BDSG

(...) Der Auftrag ist schriftlich zu erteilen, wobei die Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

Ähnliches gilt im Bereich der Finanzbuchhaltungssysteme aufgrund der Vorgaben der Grundsätze zur ordnungsgemäßen DV-gestützten Buchführung (GoBS).

Bei Banken, Finanzdienstleistern und Versicherungen ist bereits aufsichtsrechtlich festgelegt, dass die Unternehmen in besonderer Weise Risikomanagement betreiben müssen (§ 25 a Kreditwesengesetz; § 64 a Versicherungsaufsichtsgesetz; § 33 Abs. 1 Wertpapierhandelsgesetz). Für in den USA börsennotierte Unternehmen sind zusätzlich Art. 302 und 404 des Sarbanes Oxley Act (SOX) relevant.

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BAFIN) hat hierzu Mindestanforderungen an das Risikomanagement (MaRisk) formuliert, die der Auslagerung von IT-Strukturen und IT-Prozessen Rechnung tragen. Die MaRisk halten das auslagernde Unternehmen in vol-

lem Umfang in der Verantwortung für IT-Compliance und verlangen zugleich, dass gegenüber dem Outsourcing-Partner bestimmte Mindestanforderungen organisatorischer und technischer Art vertraglich verankert werden müssen.



AT 9 MaRisk (Rundschreiben 5/2007)

(...) Die Auslagerung darf nicht zu einer Delegation der Verantwortung der Geschäftsleitung an das Auslagerungsunternehmen führen. Die Leitungsaufgaben der Geschäftsleitung sind nicht auslagerbar. (...) Das Institut hat bei wesentlichen Auslagerungen im Fall der beabsichtigten Beendigung der Auslagerungsvereinbarung Vorkehrungen zu treffen, um die Kontinuität und Qualität der ausgelagerten Aktivitäten und Prozesse auch nach Beendigung zu gewährleisten. Bei wesentlichen Auslagerungen ist im Auslagerungsvertrag insbesondere Folgendes zu vereinbaren:

1. Spezifizierung und gegebenenfalls Abgrenzung der vom Auslagerungsunternehmen zu erbringenden Leistung,
2. Festlegung von Informations- und Prüfungsrechten der Internen Revision sowie externer Prüfer,
3. Sicherstellung der Informations- und Prüfungsrechte sowie der Kontrollmöglichkeiten der Bundesanstalt für Finanzdienstleistungsaufsicht,
4. soweit erforderlich Weisungsrechte,
5. Regelungen, die sicherstellen, dass datenschutzrechtliche Bestimmungen beachtet werden,
6. angemessene Kündigungsfristen,
7. Regelungen über die Möglichkeit und über die Modalitäten einer Weiterverlagerung, die sicherstellen, dass das Institut die bankaufsichtsrechtlichen Anforderungen weiterhin einhält,
8. Verpflichtung des Auslagerungsunternehmens, das Institut über Entwicklungen zu informieren, die die ordnungsgemäße Erledigung der ausgelagerten Aktivitäten und Prozesse beeinträchtigen können.



Outsourcing

Die Auslagerung von Funktionen befreit das IT-Management nicht von der Aufgabe des Risikomanagements! Je nach Wirtschaftssektor, in dem das auslagernde Unternehmen tätig ist, können erhebliche zusätzliche Anforderungen an die IT-Compliance aufgrund gesetzlicher oder aufsichtsrechtlicher Vorgaben entstehen. Besonderer Überprüfung bedarf der Bereich von Banken, Finanzdienstleistern und Versicherungen.

14.1.4 Strafrechtliche Verantwortung des Compliance Officer und anderer Funktionsträger mit besonderen Aufgaben

Aufgrund seiner im Arbeitsvertrag übernommenen Verpflichtung, wie sie sich aus der Stellenbeschreibung ergibt, kann sich der Compliance Officer strafbar machen, wenn er gegen Straftaten, die andere aus dem Unternehmen heraus begehen, nicht einschreitet. Er ist Garant, weil er den Schutz bestimmter Rechtsgüter übernommen hat, und kann auf diese Weise wegen Mittäterschaft bzw. Beihilfe zu einer entsprechenden Straftat belangt werden. In den Einzelheiten ist noch manches unsicher. Die Pflicht zur Erfolgsabwendung von Straftaten besteht nur im Rahmen des Möglichen und Zumutbaren. Ist der Compliance Officer nicht weisungsbefugt, wie häufig der Fall ist, kann er dem strafrechtlichen Risiko entgehen. Voraussetzung ist, dass er seiner Berichtspflicht umfassend genügt. Diese für den Compliance Officer von der Rechtsprechung entwickelten Grundsätze gelten im Übrigen auch für den Datenschutzbeauftragten!



Zuweisung von Aufgaben an Personen mit besonderen Compliance-Aufgaben („Compliance Officer“)

Die Bündelung von Compliance-Aufgaben in einer Person („Compliance Officer“) bedeutet für diese ein erhöhtes strafrechtliches Risiko. Werden aus dem Unternehmen heraus Straftaten begangen, kann der Compliance Officer unter Umständen wegen Beihilfe durch Unterlassen zur Verantwortung gezogen werden. Er ist Garant für die von ihm zu schützenden Rechtsgüter!

14.1.5 Unterstützung der Corporate Compliance durch die IT-Organisation

Die IT-Organisation muss nicht nur ihrerseits gesetzlichen Vorgaben entsprechen, sie ist zugleich eines der wichtigsten Instrumente im Unternehmen, um unternehmensweit Konformität und „Good Governance“ herzustellen und zu sichern.

IT-Richtlinien/Code of Conduct

Im Rahmen eines Datenschutz- und Datensicherheits-Konzepts mit dessen rechtlicher Absicherung durch Verhaltensrichtlinien für Mitarbeiter (Code of Conduct) gehören in diesen Bereich Betriebsvereinbarungen und arbeitsvertragliche Regelungen.

Datenschutz- und Datensicherheits-Konzepte müssen in regelmäßigen Abständen (mindestens einmal pro Jahr) auf ihre Einhaltung und Durchsetzung hin überprüft werden. Stehen die Richtlinien zur IT-Sicherheit nur auf dem Papier, ohne dass deren Einhaltung zumindest in Stichproben überprüft und gegen erkannte Verstöße vorgegangen wird, laufen sie Gefahr, von der Unternehmenspraxis verdrängt zu werden. Aufgrund „betrieblicher Übung“ können die im Unternehmen gelebten Praktiken, die im Widerspruch zu den Richtlinien stehen, diese verdrängen, wenn das IT-Management in Kenntnis der Verstöße über einen längeren Zeitraum (6–12 Monate) dagegen nicht einschreitet. Richtlinien ohne Kontrolle und Überwachung sind schon deshalb in der unternehmensinternen Praxis wertlos.

Ob und inwieweit Kontrollen der IT-Richtlinien durchsetzbar sind, hängt nicht zuletzt davon ab, ob im Unternehmen ein Betriebsrat bzw. Personalrat vorhanden ist. Die Kontrolle und Überwachung von IT-Richtlinien führt notwendigerweise dazu, dass auch die Tätigkeit der Mitarbeiter zum Gegenstand der Kontrolle wird. Eine solche bedarf aber immer (§ 87 Abs. 1 Nr. 1 Betriebsverfassungsgesetz) der Zustimmung der Mitarbeitervertretung. Es ist deshalb sinnvoll, IT-Richtlinien nach Möglichkeit durch entsprechende Betriebsvereinbarungen abzusichern. Inhalt der Betriebsvereinbarung muss dann auch sein, unter welchen Voraussetzungen und in welchem Verfahren Kontrollen der IT-Richtlinien durchgeführt werden können.

Whistleblower-Hotline

Durch den Sarbanes Oxley Act (SOX) wurden in den USA börsennotierte Unternehmen dazu verpflichtet, Anzeigesysteme einzurichten, bei denen Mitarbeiter im Schutz der Anonymität unternehmensinterne Unregelmäßigkeiten mitteilen können. Die Einrichtung solcher Whistleblower-Hotlines in börsennotierten Unternehmen ist inzwischen weit verbreitet. Ihre Einrichtung bedarf im Rahmen der betrieblichen Mitbestimmung der Zustimmung des Betriebsrates. Darüber hinaus sind eine Reihe von datenschutzrechtlichen Fragen zu beachten. Einzelheiten dazu finden Sie in der Stellungnahme 1/2006 der Article 29 Data Protection Working Party (www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_de.pdf).

Fraud Detection

Die Verpflichtung zu Risikoversorge und Risikomanagement verlangt auch die Einrichtung von Systemen zur Früherkennung von Wirtschaftsstraftaten zum Nachteil des Unternehmens (Fraud Prevention, Fraud Detection). Im Kern geht es um Dreierlei:

- Beabsichtigte falsche Angaben einschließlich absichtliches Weglassen von Beträgen oder Angaben im Zusammenhang mit Jahresabschluss und Rechnungslegung
- Missbrauch von Vermögensgegenständen oder Ressourcennutzung des Unternehmens durch Mitarbeiter für eigene oder fremde Zwecke
- Korruption: Nutzung von Informationsvorsprung oder Kompetenzen für Geschäftsabschlüsse, um sich oder Dritte zu bereichern

Hierzu sind in den letzten Jahren eine Reihe von Business Intelligence Systemen eingeführt worden, die technische Risikoversorge leisten sollen.

IT-Forensik/e-discovery

Die Umstellung von papierbasierten Dokumentationssystemen auf elektronische Aktenführung und Archivierung bringt mit sich, dass in Ermittlungs- und Gerichtsverfahren der Zugriff auf elektronische Dokumente eine immer größere Rolle spielt. Der Struktur nach geht es um zwei gegenläufige und nur schwer miteinander in Einklang zu bringende Tendenzen.

Die Bündelung der gesamten Unternehmenskommunikation auf einer technischen Plattform enthebt Ermittlungsbehörden von der mühevollen Arbeit, kartonweise Unternehmensakten beschlagnahmen und auswerten zu müssen. Kartellbehörden beschlagnahmen beispielsweise zum Nachweis unzulässiger Preisabsprachen gleich die gesamten E-Mail-Systeme und werten diese Software-gestützt aus. Das IT-Management muss sich deshalb darüber im Klaren sein,

dass nicht nur die Archivierung von Kommunikationsdaten Risiken vom Unternehmen fernhält, sondern auch das sichere Löschen von Daten, die für das Unternehmen bestandsgefährdend sein können.

Des Weiteren ist es Aufgabe des IT-Managements, diejenigen Informationen und Daten bereitzustellen, die für die gerichtliche Durchsetzung von Ansprüchen notwendig sind. Hierzu hat das Bundesamt für Sicherheit in der Informationstechnik inzwischen einen eigenen Leitfaden „IT-Forensik“ entwickelt. (https://www.bsi.bund.de/ContentBSI/Themen/Internet_Sicherheit/Uebersicht/ITRevision/IT-Forensik/it-forensik.html).

Drohen gerichtliche Verfahren gegen das eigene Unternehmen oder sind diese bereits anhängig, dann ist es Aufgabe des IT-Managements, sicherzustellen, dass alle relevanten Daten für die Dauer des Rechtsstreits gegen Veränderung oder Verlust gesichert werden. Der von der Partei selbst verursachte Datenverlust kann zu Sanktionen durch das Gericht führen, beispielsweise in Form von Geldstrafen bis hin zu Verlust des Prozesses wegen Beweislastumkehr.



IT-Forensik

Die Unterstützung des Unternehmens bei gerichtlichen Auseinandersetzungen durch Bereitstellung und Sicherung von Informationen ist eine Aufgabe mit wachsender Bedeutung, weil die papierbasierte Dokumentation von Unternehmensvorgängen abnimmt.

GoBS, GDPDU, e-Invoicing

Die Konformität der Buchhaltungssysteme mit den etablierten GoBS- und GDPDU-Standards ist inzwischen alltägliche Praxis geworden, ebenso die Vorbereitung der Finanzsysteme für die digitale Steuerprüfung. Besondere Beachtung verdienen die im Zusammenhang mit der Umstellung auf elektronische Rechnungen im B2B-Verkehr entstehenden Probleme. Nach § 14 Abs. 3 UStG erfordert die Abzugsfähigkeit der Vorsteuer ein digitales Rechnungsdokument, das mit einer qualifizierten elektronischen Signatur versehen ist. Dieses digitale Rechnungsdokument hat in der Praxis aber nur geringe Verbreitung gefunden. Die hohen technischen Hürden einer qualifizierten elektronischen Signatur haben viele Projekte zum Scheitern gebracht, weil die erhofften Effizienzgewinne angesichts des Aufwandes nicht eingetreten sind. Zudem wurde die deutsche elektronische Rechnung im grenzüberschreitenden Verkehr kaum akzeptiert.

Der europäische Gesetzgeber hat deshalb interveniert und die Umsatzsteuerrichtlinie 2010 dahingehend erweitert, dass die **Echtheit der Herkunft** der Rechnung, die **Unversehrtheit ihres Inhalts** und die **Lesbarkeit der Rechnung** auch auf andere Weise als durch eine qualifizierte elektronische Signatur mit Anbieterkennung hergestellt werden kann. Den Unternehmen ist nunmehr freigestellt, diese drei Anforderungen durch ein nicht näher spezifiziertes „innerbetriebliches Kontrollverfahren“ sicherzustellen (Steuervereinfachungsgesetz 2011, Inkrafttreten 1. Juli 2011. Aufgabe des IT-Managements ist es künftig, die technische Basis für ein solches innerbetriebliches Kontrollverfahren zu schaffen.

**e-Invoicing**

Ab dem 1. Juli 2011 können elektronische Rechnungen auch ohne qualifizierte Signatur mit Anbieterkennung für den Vorsteuerabzug eingesetzt werden. Erforderlich ist ein „internes Kontrollsystem“, das Echtheit der Herkunft der Rechnung, Unversehrtheit ihres Inhalts und Lesbarkeit der Rechnung sicherstellt.

■ 14.2 IT-Beschaffung

Die Investitionszyklen für IT-Systeme und Applikationen spiegeln die Dynamik der Anforderungen wider, die aus den Geschäftsprozessen heraus oder aufgrund externer Compliance-Vorgaben an solche Investitionsgüter gestellt werden. Es kommt hinzu, dass es nicht bei einer einmaligen Investition in IT bleibt, sondern dass die einmal beschafften Systeme kontinuierlich betreut und gewartet werden müssen.

Im Hinblick auf die rechtlichen Rahmenbedingungen für IT-Beschaffungen stellt dieser Abschnitt folgende Gebiete vor: zunächst wird das förmliche Vergabeverfahren vorgestellt, wie es im öffentlich-rechtlichen Sektor zwingend vorgegeben ist.

Im Bereich der privatwirtschaftlichen Beschaffung hat das IT-Management typischerweise mit Standardverträgen zu tun. Welche Besonderheiten dabei zu beachten sind, wird im Anschluss erläutert. Schließlich endet der Abschnitt mit Rechtsfragen, die vor allem bei der Beschaffung von Hardware immer wieder auftreten, nämlich Einstandsverpflichtung für die vertragsgemäße Beschaffenheit der Ware und die Rechte des Käufers bei auftretenden Mängeln.

14.2.1 Ausschreibung von Beschaffungsvorhaben

IT-Beschaffungen im öffentlichen Sektor unterliegen bestimmten förmlichen Beschaffungsregelungen. Die wichtigste Frage für das IT-Management – und natürlich auch für die ein Angebot unterbreitenden Lieferanten (!) – ist zunächst die, ob die konkrete Beschaffungsmaßnahme dem förmlichen Ausschreibungsverfahren des Vergaberechts unterliegt.

Europäische Vorgaben

Das Vergaberecht ist durch und durch von europäischen Vorgaben geprägt. Das liegt ganz wesentlich daran, dass für das Funktionieren eines einheitlichen Binnenmarkts das Investitionsvolumen des öffentlichen Sektors eine wichtige Größe darstellt. Ein grenzüberschreitender, europaweiter Binnenmarkt kann kaum funktionieren, wenn diese Investitionsbereiche national abgeschottet sind, sei es aufgrund expliziter rechtlicher Vorgaben oder de facto aufgrund unverhohlener Präferenzen für lokale Anbieter.

Bei http://ec.europa.eu/internal_market/publicprocurement/legislation_de.htm finden Sie eine Zusammenstellung der einschlägigen europäischen Richtlinien.

In der Umsetzung dieser europarechtlichen Vorgaben hat der deutsche Gesetzgeber die Regelungen in den §§ 97ff. des Gesetzes gegen Wettbewerbsbeschränkungen (GWB), der Vergabeverordnung und den Verdingungsordnungen geschaffen beziehungsweise modifiziert.



§ 97 GWB

- (1) Öffentliche Auftraggeber beschaffen Waren, Bau- und Dienstleistungen nach Maßgabe der folgenden Vorschriften im Wettbewerb und im Wege transparenter Vergabeverfahren.
- (2) Die Teilnehmer an einem Vergabeverfahren sind gleich zu behandeln, es sei denn, eine Benachteiligung ist auf Grund dieses Gesetzes ausdrücklich geboten oder gestattet.
- (3) Mittelständische Interessen sind vornehmlich durch Teilung der Aufträge in Fach- und Teillöse angemessen zu berücksichtigen.
- (4) Aufträge werden an fachkundige, leistungsfähige und zuverlässige Unternehmen vergeben; andere oder weitergehende Anforderungen dürfen an Auftragnehmer nur gestellt werden, wenn dies durch Bundes- oder Landesgesetz vorgesehen ist.
- (5) Der Zuschlag wird auf das wirtschaftlichste Angebot erteilt. [...].

Öffentliche und nicht-öffentliche Auftraggeber

Dass staatliche Gliederungen (Bund, Land, Kommune) öffentliche Auftraggeber sind, ist evident. Schwierig ist die Beurteilung von Organisationen und Unternehmen in der Grauzone zwischen öffentlichem Bereich und Privatwirtschaft. Die Rechtsform ist dafür grundsätzlich nicht entscheidend, und zwar schon deshalb nicht, weil die Organisationsformen europaweit zu verschieden sind. Entscheidend ist vielmehr, ob die jeweilige Einrichtung aufgrund ihrer Aufgaben, ihrer Finanzierung und ihrer Leitungskontrolle als Bestandteil des staatlichen Sektors behandelt werden muss („funktionaler Auftraggeber“).

Beispiele:

- Das von kommunalen Gebietskörperschaften gegründete Gemeinschaftsunternehmen, das für diese Kommunen IT-Leistungen erbringen soll (RZ GmbH) und in privatwirtschaftlicher Form organisiert ist, gehört zum öffentlichen Sektor, weil die Gesellschafter des Unternehmens dem öffentlichen Sektor angehören (öffentlich-rechtliche Körperschaften).
- Kirchliche Einrichtungen sind aufgrund der Staatskirchenverfassung (Konkordatsverträge) nicht Teil staatlicher Organisation oder Finanzierung, deshalb unterliegen ihre Vorhaben nicht dem Vergaberecht.

Zur Verfügung stehende Verfahrensarten

Bei öffentlichen Auftraggebern sowie bei der Verwendung von Fördermitteln der öffentlichen Hand im Rahmen einer Beschaffung sieht der Gesetzgeber vor, dass für die Beschaffungen nur eine beschränkte Zahl von Verfahrensarten zur Verfügung steht (Numerus Clausus). Es sind dies das offene Verfahren, das nicht-offene Verfahren, der wettbewerbliche Dialog und das Verhandlungsverfahren (§ 101 GWB). Die Verfahrensarten lassen sich wie folgt skizzieren:

- *Offene Verfahren* richten sich an einen offenen Teilnehmerkreis von Anbietern. Das ausgeschriebene Projekt ist vollständig spezifiziert. Verhandlungen oder Nachverhandlungen von

Angeboten mit den einzelnen Bietern finden nicht statt, lediglich Antworten auf Nachfragen von Bietern sind erlaubt.

- Das *nicht-offene Verfahren* unterscheidet sich vom offenen nur dadurch, dass der Teilnehmerkreis durch einen vorgeschalteten Teilnahmewettbewerb von vornherein wesentlich beschränkt wird (mindestens fünf Anbieter).
- Beim *wettbewerblichen Dialog* steht die Spezifikation des Projekts zu Beginn der Ausschreibung noch nicht fest. Deshalb wird zunächst ein Teilnahmewettbewerb durchgeführt, und in der zweiten Phase (Dialogphase) dann mit einem beschränkten Teilnehmerkreis die Spezifikation erarbeitet. In einem dritten Schritt geben diese Teilnehmer verbindliche Angebote ab.
- Das *Verhandlungsverfahren* ist ein weitgehend formloses Verfahren mit einem beschränkten Teilnehmerkreis (mindestens drei). Ob nacheinander oder parallel verhandelt wird, steht dem öffentlichen Auftraggeber grundsätzlich frei, in jedem Fall aber muss transparent und fair verhandelt werden.

Die verschiedenen Verfahrensarten empfehlen sich für folgende Situationen:

- Das *offene Verfahren* sollte zur Anwendung kommen, wenn Leistung und Umfang vollständig definiert sind.
- Das *nicht-offene Verfahren* eignet sich, wenn nur wenige Unternehmen in der Lage sind, die Leistung zu erbringen, die Kosten der offenen Ausschreibungen nicht im Verhältnis zum Wert der Leistung stehen, oder eine offene Ausschreibung gescheitert oder unzweckmäßig ist.
- Der *wettbewerbliche Dialog* ist prädestiniert für Situationen, in denen Leistungen und Funktionsumfang nicht oder nicht vollständig im Voraus definiert werden können. Dies wird insbesondere dann der Fall sein, wenn die technologische Kompetenz des Auftraggebers nicht ausreicht, eine dem Stand der Technik entsprechende Lösung umfassend zu planen. Beispielhaft seien besonders komplexe Aufträge oder Vorhaben mit komplexer Finanzierung genannt, deren rechtliche und finanzielle Konstruktionen im Voraus nicht beschrieben werden können.
- Das *Verhandlungsverfahren* sollte gewählt werden, wenn Leistungen und Funktionsumfang nicht vollständig im Voraus definiert werden können, offene oder nicht-offene Verfahren zuvor gescheitert sind, eine vorherige globale Preisgestaltung im Angebot nicht möglich ist (Komplexität des Gegenstands, große Zahl von Leistungsvarianten), die Leistung nur von einem Unternehmen erbracht werden kann, es sich um ein Forschungs- und Entwicklungsvorhaben handelt, die Vergabe besonders dringlich ist oder Zusatzleistungen zu einem bereits vergebenen Auftrag vergeben werden, die technisch zusammengehören.



Was nicht im Gesetz steht:

- Das Vergaberecht versucht, mit formalen Mitteln (Verfahrensregeln) eine inhaltlich gute Entscheidung (Zuschlag dem wirtschaftlichsten Angebot) im Beschaffungsprozess herbeizuführen. Das konnte nicht funktionieren, die Praxis hat aber damit leben gelernt.
- Die offenen Verfahren taugen nur für Produkte, die vollständig spezifiziert werden können und allein über den Preis eingekauft werden. Das funktioniert für Krankenhausbetten genauso wie für aktive Netzwerkkomponenten und CT-Scanner.

- Mit den Eignungskriterien lässt sich das Feld der Bieter so einschränken, dass der präferierte Anbieter in jedem Fall im Wettbewerb ist.
- Vergleichsweise unangreifbar sind Auswahlentscheidungen, die nicht einer subjektiven Bewertung durch die Vergabestelle folgen, sondern auf Eigenauskünfte des Bieters setzen: Der Bieter füllt das Leistungsverzeichnis aus und erklärt, ob er die Anforderungen ganz oder teilweise oder überhaupt nicht erfüllt. Entsprechend diesem Eintrag wird eine bestimmte Punktezahl vergeben, aus der sich dann ein rechnerisches Gesamtergebnis ableiten lässt (Bewertungsmatrix).
Ob das Leistungsverzeichnis für das Projekt sachlich richtig ist und die Bewertung zutreffend, könnte nur ein Sachverständiger beurteilen. Die Überprüfung durch die Vergabekammer ist aber ein summarisches Verfahren, bei dem Sachverständige nicht hinzugezogen werden. Das Ergebnis hängt also mehr oder weniger von der Unverfahrenheit des Anbieters ab! Fühlt er sich gerade „fully compliant“ im Hinblick auf die „requirements“, muss ihm die Vergabestelle die maximale Punktzahl geben. Selbst wenn nach der Leistung in vergleichbaren Projekten evident ist, dass der Anbieter die Leistung keinesfalls erbringen wird!
- In den offenen Verfahren darf mit dem Bieter nicht verhandelt werden. Zulässig sind allein sogenannte Aufklärungsgespräche. Die Praxis verhandelt gleichwohl, muss es aber kaschieren. Da der Anbieter sein Gebot nicht mehr ändern darf (der Preis steht fest), wird im Gewand der Präzisierung der Leistung verhandelt.
- Ein belastbarer Vertrag kommt in den offenen Verfahren nie zustande. Die von der Vergabestelle vorgegebenen Dokumente (Vertragsentwürfe, ergänzende Vergabebedingungen etc.) sind vertragsrechtlich nur einseitige allgemeine Geschäftsbedingungen, die der Inhaltskontrolle unterliegen – selbst wenn der Bieter diese Dokumente in seinem Angebot pauschal „anerkennen“ sollte. Das Verhandlungsverbot ist ein schwerer Konstruktionsfehler der offenen Verfahren.
- Komplexere und dynamische IT-Projekte können sinnvoll nur im Verhandlungsverfahren oder wettbewerblichen Dialog ausgeschrieben werden.

14.2.2 Voraussetzungen für die Ausschreibungspflicht

Die Ausschreibungspflicht von Beschaffungsmaßnahmen ist nach folgendem Schema zu prüfen, wobei *alle* Voraussetzungen gegeben sein müssen:

- Voraussetzung 1: *Nur öffentliche Auftraggeber* müssen Aufträge ausschreiben.
Öffentliche Auftraggeber sind
 - Gebietskörperschaften (Bund, Land, Kommunen)
 - Öffentliche Unternehmen („funktionale Auftraggeber“)
 - Verbände der beiden vorgenannten Institutionen
 - Private Unternehmen der Bereiche Wasser, Energie, Verkehr und Telekommunikation
 - Private Unternehmen bei öffentlich geförderten Projekten
 - Private Baukonzessionäre

- Voraussetzung 2: Nur *öffentliche Aufträge* müssen ausgeschrieben werden.
Der öffentliche Auftrag ist ein
 - entgeltlicher Vertrag (auch Änderung, Verlängerung, Nichtkündigung)
 - zwischen öffentlichen Auftraggebern und Unternehmen
 - zur Beschaffung von Leistungen am Markt.
- Voraussetzung 3: Auszuschreiben ist, wenn die *Schwellenwerte* für europaweite Ausschreibung erreicht sind:
 - (IT) Liefer- und Dienstleistungsaufträge ab 193.000 €

Wie wird dieser Schwellenwert berechnet?

- Schätzung des Gesamtauftragswerts ohne Umsatzsteuer.
- Bei Laufzeitverträgen ist die Gesamtvergütung über die Vertragsdauer maßgeblich.
- Bei unbefristeten Verträgen ist eine Laufzeit von 48 Monaten anzunehmen.
- Rahmenvereinbarungen werden nach dem Gesamtwert aller erwarteten Lieferungen berechnet.



Beachten Sie:

Öffentliche Aufträge müssen auf dem Vergabeportal der Europäischen Union veröffentlicht werden: <http://ted.europa.eu>.

Über http://simap.europa.eu/buyer/forms-standard_de.html können Sie die Formulare für die Veröffentlichung beziehen.

14.2.3 Weitere Fragestellungen

Muss ich die EVB-IT verwenden?

Die Koordinierungsstelle des Bundes, der BDI und die Bitkom haben eine Reihe von überwiegend gemeinsam verabschiedeten Musterverträgen ausgehandelt, die „Ergänzenden Vertragsbedingungen für die Beschaffung von IT-Leistungen“ (EVB-IT):

- EVB-IT System
- EVB-IT Systemlieferung
- EVB-IT Kauf
- EVB-IT Dienstleistung
- EVB-IT Überlassung Typ A
- EVB-IT Überlassung Typ B
- EVB-IT Instandhaltung
- EVB-IT Pflege S

Die EVB-IT finden Sie unter <http://www.kbst.bund.de/zumDownload>.

In der Qualität unterscheiden sich die EVB-IT kaum von anderen Musterverträgen, die am Markt verfügbar sind. Sie teilen deren Vorteile, indem sie ein Grundgerüst für eine Leistungsbeschreibung und eine vertragliche Regelung bieten, und alle Nachteile, weil sie den Beson-

derheiten eines Vorhabens nie Rechnung tragen können. Das IT-Management ist gut beraten, solchen Standardverträgen nicht blind zu vertrauen. Sie sollten deshalb nur als „Checkliste“ verstanden werden. In den für die IT kritischen Bereichen Lizenzmodell, Projektsteuerung und Risikomanagement sind die EVB völlig unzureichend. Sie sollten deshalb allenfalls für sehr einfache Projekte mit geringer Kritikalität verwendet werden.

Anhand der konkreten Anforderung, die das IT-Management an den Beschaffungsgegenstand und die Unterstützung von Lieferant und Hersteller im Falle von Mängeln hat, muss dann sehr sorgfältig geprüft werden, ob und inwieweit Ergänzungen oder Änderungen an diesem Standardverträgen vorgenommen werden müssen. Wenn das IT-Management seine Anforderungen erstellt, dann sollte dabei der gesamte Lebenszyklus und voraussehbare Einsatzzwecke und Betriebssituationen über diesen gesamten Zeitraum betrachtet werden.



Wofür sich die EVB-IT eignen

EVB-IT sind Standarddokumente, die für komplexere oder dynamische IT-Projekte vollkommen ungeeignet sind. Sie taugen lediglich für einfache Beschaffungsvorgänge.

Es wäre fahrlässig und mit der gebotenen Risikovorsorge durch das IT-Management unvereinbar, gewissermaßen „blind“ auf die EVB-IT Formulare zu vertrauen.

Schließlich ein Letztes: Entgegen ihrem hoheitlichen „Anstrich“ sind die EVB-IT von Rechts wegen nur AGB. Sie sind deshalb im Grunde nur Konditionenempfehlungen. Ob sie im Streitfall vor Gericht Bestand haben können, muss der „AGB-Test“ erweisen (Einzelheiten dazu finden Sie in Abschnitt 14.3).

Öffentliche Auftraggeber sind aus haushaltsrechtlichen Gründen (verabschiedete Haushaltsrichtlinien) gehalten, die EVB-IT anzuwenden. Ihre Anwendung ist aber nicht zwingend vorgeschrieben. Beispielsweise dürfen Sie andere Entwürfe benutzen, wenn nur ein Bieter in Betracht kommt und dieser nicht bereit ist, auf der Basis der EVB-IT zu verhandeln, oder wenn die Beschaffung durch Anwendung der EVB-IT unwirtschaftlich wäre.

Als Anbieter in einem Ausschreibungsverfahren müssen Sie die EVB-IT beachten, wenn es sich um ein offenes Verfahren handelt, weil sie hier keine Änderungen an den Ausschreibungsunterlagen vornehmen dürfen (sonst droht der Ausschluss vom Vergabeverfahren). Im Verhandlungsverfahren hingegen können Sie Änderungen gegenüber den EVB-IT oder Ihre eigenen Musterdokumente vorschlagen.

Wie verhandle ich ein ausgeschriebenes Projekt?

Das Verhandlungsverfahren ist formfrei, aber nicht rechtsfrei. Die Mindestzahl der Verhandlungspartner ist vorgegeben (drei). In der Reihenfolge der Verhandlung ist der Auftraggeber grundsätzlich frei, er kann die Verhandlungen parallel oder sequenziell führen. Es ist ebenfalls möglich, zunächst mit einem „Preferred Bidder“ zu verhandeln. Endverhandelt werden muss das Vorhaben, sofern es überhaupt mehr als ein geeignetes Unternehmen gibt, aber mit mindestens zweien (§ 3 a Nr. 7 Abs. 2 S. 2 VOL/A).

Ein Verhandlungsverfahren ist deshalb außerordentlich aufwändig und langwierig. Es verlangt eine sehr sorgfältige Dokumentation des jeweiligen Verhandlungsstandes und der im Verhandlungsprozess getroffenen Entscheidungen in der Vergabeakte.

Wie wähle ich den richtigen Anbieter aus?

Als Auftraggeber müssen Sie zwei Auswahlentscheidungen treffen:

- Sie müssen unternehmensbezogen entscheiden, ob der Anbieter die für das Vorhaben erforderliche Eignung besitzt (Fachkunde, wirtschaftliche Leistungsfähigkeit, Zuverlässigkeit). Die Eignungskriterien machen Sie in der Bekanntmachung über das Vorhaben öffentlich.
- Die zweite Entscheidung ist die über das wirtschaftlichste Angebot, dem der Zuschlag erteilt wird.



§ 25 VOL/A Wertung der Angebote

[...]

3. Der Zuschlag ist auf das unter Berücksichtigung aller Umstände wirtschaftlichste Angebot zu erteilen. Der niedrigste Angebotspreis allein ist nicht entscheidend.

In die Bewertung der Angebote dürfen nur diejenigen Faktoren einfließen, die zuvor in der Ausschreibung als Zuschlagskriterien offen gelegt worden sind. Eine nachträgliche Änderung dieser Kriterien hat deshalb zwingend eine neue Ausschreibung zur Folge.



Praxistipp:

Es empfiehlt sich, eine vollständige Bewertungsmatrix für die Angebote zu erstellen. Ein anschauliches Beispiel enthält die Unterlage für die Ausschreibung und Bewertung von IT-Leistungen (UfAB Version V). Die Unterlage für die Ausschreibung und Bewertung von IT-Leistungen (UfAB) finden Sie unter <http://www.kbst.bund.de/> zum Download.

Wie muss ich Streitfälle eskalieren, und welcher Rechtsschutz steht im Vergabeverfahren zur Verfügung?

Fehler des Vergabeverfahrens sind vom Bieter unverzüglich gegenüber dem Auftraggeber zu rügen, sonst kann er sich im Nachprüfungsverfahren nicht mehr darauf berufen (§ 107 Abs. 3 GWB). Des Weiteren muss das Überprüfungsverfahren eingeleitet sein, bevor der Auftraggeber den Zuschlag erteilt hat (§ 114 Abs. 1 GWB). Schließlich muss der Bieter bei der Vergabekammer einen schriftlichen Nachprüfungsantrag stellen (§ 108 GWB). Er muss dabei darlegen, dass er Interesse am Auftrag hat, in seinen Rechten verletzt wurde und durch die behauptete Verletzung der vergaberechtlichen Bestimmungen ein Schaden entstanden ist oder zu entstehen droht (§ 107 Abs. 2 GWB).



Als Anbieter sollten Sie auf Folgendes achten:

Die formalen Anforderungen an ein Angebot sind peinlich genau zu beachten (Formen, Fristen, verlangte Dokumente und Erklärungen).

Erkannte Mängel des Vergabeverfahrens müssen Sie rechtzeitig – spätestens innerhalb von 14 Tagen – rügen, sonst können Sie sich später darauf nicht mehr

berufen. Sie dürfen daher keine Scheu haben, die Kommunikation mit dem Auftraggeber durch Rügen „atmosphärisch“ zu belasten, wenn Sie Ihre Rechte wahren wollen.

Wird die Auftragsvergabe im Amtsblatt der EU bekanntgemacht, haben Sie nur 30 Tage Frist, um ein Nachprüfungsverfahren einzuleiten (§ 101 b GWB)!

Der Bieter kann nach § 126 GWB unter bestimmten Voraussetzungen Schadensersatzansprüche geltend machen, wenn bieterschützende Verfahrensregelungen vom Auftraggeber verletzt wurden und der Bieter eine „echte Chance“ auf Erteilung des Auftrags hatte.

Daneben stehen dem Bieter auch die allgemeinen Schadensersatztatbestände aus Verletzung vorvertraglicher Pflichten offen (Ersatz des Vertrauensschadens).

**Beachten Sie:**

Der einzig praktisch wirksame Rechtsbehelf im Vergaberecht ist die Nachprüfung durch die Vergabekammer. Auf den Schadensersatzanspruch zu vertrauen („dulde und liquidiere“) ist gefährlich, weil die „echte Chance“ auf Erteilung des Auftrags schwer nachweisbar ist und Ihnen bei unterlassenen Rügen der Einwand des Mitverschuldens entgegengehalten werden kann!

■ 14.3 Allgemeine Geschäftsbedingungen

Produkte und Dienstleistungen werden in der Regel auf der Basis von Verträgen beschafft, die Allgemeine Geschäftsbedingungen enthalten. Der Umgang mit sich widersprechenden oder voneinander abweichenden Formularen im Rahmen der Vertragsverhandlungen ist Kernbestandteil des Vertragsmanagements. Wessen Vorlage „gewinnt“ und worauf beim Verhandeln auf der Basis vorformulierter Vertragsdokumente zu achten ist, lernen Sie in diesem Abschnitt kennen.

14.3.1 Grundlagen

Verträge, welche die Parteien auf der Grundlage von vorformulierten Vertragsbedingungen verhandeln und abschließen, gliedern sich aus der gesetzgeberischen Perspektive immer in zwei Teile: der eine Teil sind die von den Parteien im einzelnen ausgehandelten Regelungen (die „Individualvereinbarung“), der andere die Allgemeinen Geschäftsbedingungen (AGB), welche eine Partei der anderen vorlegt, ohne dass hierüber im Einzelnen verhandelt worden ist. Da sich nahezu jeder Vertragstext dafür eignet, bei mehreren Vertragsabschlüssen verwendet zu werden, ist ein Vertragsentwurf einer Partei im Grundsatz immer eine AGB, und zwar auch dann, wenn er nur einmal verwendet wird!



§ 305 BGB

(1) Allgemeine Geschäftsbedingungen sind alle für eine Vielzahl von Verträgen vorformulierten Vertragsbedingungen, die eine Vertragspartei (Verwender) der anderen Vertragspartei bei Abschluss eines Vertrags stellt. Gleichgültig ist, ob die Bestimmungen einen äußerlich gesonderten Bestandteil des Vertrags bilden oder in die Vertragsurkunde selbst aufgenommen werden, welchen Umfang sie haben, in welcher Schriftart sie verfasst sind und welche Form der Vertrag hat. Allgemeine Geschäftsbedingungen liegen nicht vor, soweit die Vertragsbedingungen zwischen den Vertragsparteien im Einzelnen ausgehandelt sind.

Ob sich Individualvereinbarung und AGB in einem Dokument (dem Vertragsdokument) oder in zwei Dokumenten befinden (beispielsweise Bestellformular mit separatem Dokument „Allgemeine Einkaufsbedingungen“), ist nicht entscheidend. Eine Individualvereinbarung liegt nur vor, wenn die folgende *Kontrollfrage* mit ja beantwortet werden kann:

„Hat der Verwender der Klausel – also der, der sie in die Vertragsverhandlungen eingeführt hat – deren Inhalt in den Vertragsverhandlungen ernsthaft zur Disposition gestellt und der anderen Seite Gestaltungsfreiheit zur Wahrung von deren eigenen Interessen eingeräumt?“

Das gesetzliche Leitbild vom Verhandeln eines Vertrages ist formalistisch. Nicht der Vertrag als Ganzes muss von den Parteien als aus ihrer Sicht ausgewogen akzeptiert werden, sondern jede einzelne Klausel – und bei umfangreichen Klauseln jeder einzelne Absatz – zur Disposition gestellt und eigens akzeptiert werden.

Mit dem realen Verhandlungsprozess hat dies in der Regel wenig zu tun. Jede Partei wird für sich im Verhandlungsprozess ein Raster zugrundelegen, das die für sie entscheidenden Punkte identifiziert und nach Prioritäten gliedert. Die Einigung kommt dadurch zustande, dass man sich durch Nachgeben an der einen Stelle die Zustimmung der anderen Seite bei einer anderen Klausel regelrecht „erkauft“. Dieses „Feilschen“ kreuz und quer über den gesamten Vertrag hinweg ist aber kein Aushandeln im strengen Sinne der oben dargestellten gesetzlichen Vorschriften.

Die Hürden zu einer Individualvereinbarung sind hoch. Die betreffende Klausel muss im Einzelnen erörtert worden sein und daraufhin die Klausel entweder geändert oder von der anderen Seite ausdrücklich akzeptiert worden sein. Das bloße Erörtern genügt ebenso wenig wie das bloße Vorlesen oder eine Multiple-Choice-Option durch Ankreuzen unterschiedlicher vorformulierter Klauseln. Der Erfordernis des Aushandelns im Einzelnen kann man natürlich auch nicht dadurch Rechnung tragen, dass mittels einer vorformulierten Klausel unterstellt wird, eine Individualabrede liege vor (Getreu dem Motto: Diese AGB sind Individualabreden).



Beachten Sie:

Wenn Sie Klauseln gerichtsfest machen wollen, dann müssen Sie das „Aushandeln“ dieser Klausel beweisen können. Das geht entweder über die Vorlage der verschiedenen Vertragsentwürfe, aus denen sich die Änderungen (im Änderungsmodus!) durch die Parteien ergeben, oder Sie müssen ein Verhandlungsprotokoll vorlegen können. Daraus muss sich ergeben, dass die andere Seite die Möglichkeit hatte, Änderungen vorzuschlagen, aber diese Möglichkeit „eingetauscht“ hat, um beispielsweise einen günstigeren Preis zu erzielen.

Verwenden beide Parteien bei Vertragsabschluss vorformulierte Vertragsbedingungen (beispielsweise Einkaufsbedingungen, Lieferbedingungen, etc.), dann ist Folgendes zu prüfen:

- *Einbeziehung in den Vertrag:* Sind die Allgemeinen Geschäftsbedingungen (AGB) beider Parteien Bestandteil der Vertragsdokumente (Angebot bzw. Auftragsbestätigung) oder verweisen die Vertragsdokumente zumindest darauf (beispielsweise auf eine Internetadresse, bei der die Allgemeinen Geschäftsbedingungen abgerufen werden können)?
 - Wenn nein, dann sind keine oder nur die AGB einer Partei Vertragsbestandteil geworden, letztere müssen dann daraufhin geprüft werden, ob sie den „AGB-Test“ bestehen (Weicht die Klausel von der gesetzlichen Regelung ab und stellt sie eine unangemessene Benachteiligung der anderen Partei dar?).
 - Wenn ja, dann folgt als nächster Prüfungsschritt die
- *Delta-Analyse Stufe I:* Widersprechen sich die allgemeinen Geschäftsbedingungen insgesamt, d.h. verwenden beide Parteien eine so genannte globale Widerspruchs- oder Abwehrklausel („Für den Vertragsinhalt gelten ausschließlich unsere AGB, andere Bedingungen werden nicht Vertragsinhalt, auch wenn wir ihnen nicht ausdrücklich widersprechen.“)?
 - Wenn nein, dann geht es weiter mit der Delta-Analyse Stufe II.
 - Wenn ja, dann heben sich die AGB insgesamt gegenseitig auf, es gilt stattdessen die gesetzliche Regelung.
 - Wenn nur eine Seite eine globale Widerspruchs- oder Abwehrklausel enthält, werden die AGB der anderen Seite nicht Vertragsbestandteil.
- *Delta-Analyse Stufe II:* Widersprechen sich nur einzelne Klauseln (ohne globale Widerspruchs- oder Abwehrklausel), dann heben sich die betreffenden Klauseln gegenseitig auf, es gilt für die jeweilige Sachfrage die gesetzliche Regelung.
- *Delta-Analyse Stufe III:* Sind die Klauseln inhaltlich verschieden, ohne sich direkt zu widersprechen, bilden sie insgesamt den „Vertrag“. Die Wirksamkeit jeder einzelnen Klausel hängt dann davon ab, ob sie den inhaltlichen „AGB-Test“ bestehen. (Weicht die Klausel von der gesetzlichen Regelung ab und stellt sie eine unangemessene Benachteiligung der anderen Partei dar?)

14.3.2 Weitere Fragestellungen

Welche Folgen hat es, wenn sich die Parteien nicht einigen können?

Die Individualvereinbarung enthält aus der Sicht der Parteien die wichtigen Teile des Vertrages. Hier finden sich die kommerziellen Kernbestandteile der Transaktion (beispielsweise die Festlegung von Ware, Menge und Preis). Können sich die Parteien bei den Kernbestandteilen nicht einigen, dann heißt das aus rechtlicher Sicht „No Deal“. Der Vertrag kommt mangels Einigung nicht zustande.

Im Bereich der AGB sind widersprechende Klauselinhalte hingegen kein Grund, eine vertragliche Bindung der Parteien abzulehnen. Wenn sich die Parteien über die aus ihrer Sicht wesentlichen Fragen des Vertrages haben einigen können, dann soll der Vertrag nicht an Divergenzen über „Nebensächlichkeiten“ scheitern.

Wie soll mit divergierenden AGBs verfahren werden, wenn gleichwohl ein Vertrag zustande kommen soll? Die von deutschen Gerichten erarbeitete Lösung läuft auf einen Kompromiss hinaus: den Kern der vertraglichen Vereinbarung bildet die Individualvereinbarung. Die sich widersprechenden Klauseln gelten als nicht geschrieben, an deren Stelle treten die für die jeweiligen Sachfragen geltenden gesetzlichen Regelungen. Ergänzend gelten diejenigen Klauseln in den AGB, bei denen sich die Parteien nicht unmittelbar widersprechen (also bei den „zusätzlichen“ oder „ergänzenden“ Klauseln).

Tabelle 14.1 zeigt Beispiele für Regelungen, die sich widersprechen.

TABELLE 14.1 Beispiele sich widersprechender Regelungen

Auftraggeber	Auftragnehmer	Gesetzliche Regelung
„Verbindlicher Liefertermin [DATUM]“	„Lieferung baldmöglich“	Lieferung hat unverzüglich nach Vertragsschluss zu erfolgen.
„Lieferant garantiert die Einhaltung der vereinbarten Spezifikation.“	„Gelieferte Ware funktioniert entsprechend der veröffentlichten Dokumentation ohne jede Garantie für den Verwendungszweck des Bestellers.“	Ware muss der vereinbarten Beschaffenheit entsprechen, für den bekannten Verwendungszweck taugen oder zumindest die marktübliche Produktqualität aufweisen.
„Lieferant haftet bei Vorsatz und grober Fahrlässigkeit unbeschränkt, im übrigen beschränkt auf den bei Vertragsabschluss vorhersehbaren Schaden.“	Lieferant haftet bei Vorsatz und grober Fahrlässigkeit unbeschränkt, im Übrigen insgesamt für alle Schadensfälle beschränkt auf den 1,5-fachen Auftragswert.“	Unbegrenzte Haftung

Mit diesem abgestuften Kompromiss wollte sich die Rechtspraxis aber nicht zufrieden geben. Die Klauselschneiderei hat deshalb sog. globale „Abwehrklauseln“ oder „Widerspruchsklauseln“ hervorgebracht, mit denen die Parteien jeweils zum Ausdruck bringen, dass der Vertrag „ausschließlich“ zu den eigenen Geschäftsbedingungen zustande kommt. Verwendet wird beispielsweise auch: „Anderslautende Bedingungen – soweit sie nicht in dieser gesamten Bestellung festgelegt sind – gelten nicht.“ Solange nur eine Seite so verfährt, hat das auch Erfolg. Da sich diese Aufrüstung der Formulare aber in Windeseile verbreitet hat, neutralisieren sie sich im Ergebnis. Über den Bereich der Individualvereinbarung hinaus gelten dann die gesetzlichen Bestimmungen.

Welchen inhaltlichen Anforderungen müssen AGB genügen?

Im Bereich der Individualabrede genießen die Parteien Vertragsfreiheit. Schranken bilden hier nur die allgemeinen Gesetze (gesetzliches Verbot, Sittenwidrigkeit).

Im Bereich der AGB ist die Vertragsfreiheit hingegen drastisch eingeschränkt. Die zentrale Regelung für die inhaltliche Kontrolle von allgemeinen Geschäftsbedingungen findet sich in § 307 BGB. Entscheidend ist das Abweichen der vorgeschlagenen Klausel von den „wesentlichen Grundgedanken der gesetzlichen Regelung“.



§ 307 BGB

(1) Bestimmungen in Allgemeinen Geschäftsbedingungen sind unwirksam, wenn sie den Vertragspartner des Verwenders entgegen den Geboten von Treu und Glauben unangemessen benachteiligen. Eine unangemessene Benachteiligung kann sich auch daraus ergeben, dass die Bestimmung nicht klar und verständlich ist.

(2) Eine unangemessene Benachteiligung ist im Zweifel anzunehmen, wenn eine Bestimmung

1. mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht zu vereinbaren ist oder

2. wesentliche Rechte oder Pflichten, die sich aus der Natur des Vertrags ergeben, so einschränkt, dass die Erreichung des Vertragszwecks gefährdet ist.

Für Verbraucherverträge (B2C) sind diese Anforderungen in den Katalogen unzulässiger Klauseln von § 308 und § 309 BGB näher aufgefächert.

Aufgrund dieses engmaschigen Netzes von Klauselverboten ist es gegenüber Verbrauchern, d.h. solchen Personen, die ein Rechtsgeschäft weder im Rahmen ihrer gewerblichen noch ihrer selbstständigen Tätigkeit abschließen (so die Definition in § 13 BGB), ohne Aussicht auf Erfolg, mit dem Mittel der AGB von gesetzlichen Regelungen der einzelnen Vertragstypen (Kauf, Dienstleistung, Miete etc.) abweichen zu wollen.

Im unternehmerischen Bereich (B2B), wo sich auf beiden Seiten versierte Vertragspartner gegenüberstehen, sollte man meinen, dass der Gesetzgeber eine größere Bewegungsfreiheit gestattet. § 307 BGB bietet mit der Formulierung, dass die betreffende Klausel die andere Seite „entgegen den Geboten von Treu und Glauben unangemessen benachteiligen“ müsse, ein entsprechend bewegliches Stellglied für eine flexiblere Bewertung. Die einschlägigen Gerichtsentscheidungen stellen indes lapidar fest, dass die Verbotstatbestände der § 308 und § 309 auch für Verträge zwischen Unternehmern gelten beziehungsweise für Verträge zwischen Unternehmern dieselben Wertungen zugrunde zu legen seien. § 308 und § 309 werden also lediglich als Konkretisierungen des allgemeinen Standards von § 307 verstanden.



Beachten Sie:

Die Klauselverbote von § 308 und § 309 gelten zwar formal nur für B2C-Verträge, die Gerichte wenden diese Bestimmungen jedoch grundsätzlich auch für B2B-Verträge an.

Für den B2C-Bereich kann man den zulässigen AGB-Inhalt in dem Satz zusammenfassen „Es gilt das Gesetz“. Alles was von den gesetzlichen Vorgaben des jeweiligen Vertragstyps (Werkvertrag, Kaufvertrag etc.) abweicht, ist unwirksam. Sinnvoll und wirksam sind hier nur Klauseln für die Beschreibung des Geschäftsprozesses (Präzisieren des Pflichtenprogramms, Kommunikation, Reporting, Eskalation). Im B2B-Bereich gestattet die Kontrolle Allgemeiner Geschäftsbedingungen nur unwesentlich mehr, im Wesentlichen die Anpassung des Vertrages an die sich zwischen Vertragsabschluss und Lieferung ändernden Marktbedingungen (beispielsweise durch Preisgleitklauseln). Diese Kontrolldichte einseitiger Vertragsgestaltungen ist weltweit einzigartig. Ausländische Vertragspartner versuchen deshalb die Anwendung des deutschen Vertragsrechts nach Möglichkeit zu vermeiden!

Verweisen beide Parteien bei den Vertragsverhandlungen auf ihre jeweiligen Klauselwerke, dann scheitert ein Vertragsabschluss nicht, wenn sich die Parteien zumindest auf den Kernbestandteile einer Vereinbarung einigen können. Die sich widersprechenden Klauseln in den AGB heben sich gegenseitig auf, an ihre Stelle tritt die gesetzliche Regelung.

Wie gehe ich mit englischsprachigen Formularen um?

Auf dem Markt für IT-Güter und -Dienstleistungen haben Unternehmen aus dem angloamerikanischen Raum nach wie vor eine dominierende Stellung. Das IT-Management wird deshalb bei Beschaffungsvorgängen nicht selten mit Standardverträgen in englischer Sprache konfrontiert werden. Aber auch deutsche Unternehmen, die sich in besonderer Weise ihren Ambitionen verpflichtet fühlen, ein „global player“ zu sein, verwenden gegenüber ihren deutschen Kunden englischsprachige Vertragsdokumente.

Das kann zu Verhandlungssituation führen, die an Absurdität grenzen, wenn beispielsweise zwei deutsche Verhandlungsteams radebrechend auf der Basis englischsprachiger Vertragstexte Einvernehmen herstellen wollen. Der Umgang mit englischsprachigen Verträgen ist deshalb so schwierig, weil sich rechtliche Konzepte nur mit Einschränkungen übersetzen lassen. Die über Jahrhunderte getrennt verlaufenden Entwicklung rechtlicher Konzepte zwischen dem europäischen Kontinent und dem angloamerikanischen Raum sind dafür die tiefere Ursache. Dabei sind die Unterschiede umso größer, je allgemeiner die Begriffe und Konzepte werden. Spezialgesetzliche Fragen der Geräte-Sicherheit beispielsweise sind deshalb wesentlich „verlustfreier“ zu übertragen als allgemeine vertragsrechtliche Fragen wie Verantwortung und Delegation, Haftung und dergleichen.

Ob die Parteien unter „termination for cause“ das Gleiche verstehen wie unter „Kündigung aus wichtigem Grund“, muss deshalb sehr sorgfältig geprüft werden. „Express and implied warranties“ sind in der Konzeption durchaus verschieden von Beschaffungsgarantien und Nacherfüllungsansprüchen beim Vorliegen von Mängeln; „indirect and consequential damages“ können gänzlich andere Schadenstypen meinen als der Begriff „Folgeschaden“. Wesentliche Unterschiede gibt es auch im Bereich des Urheberrechtsschutzes für Software.

Diese konzeptionellen Unterschiede machen Vertragsabschlüsse in einem anderen rechtlichen „Kulturraum“ in besonderem Maße riskant und fehlerträchtig.

Das IT-Management sollte deshalb, wenn sich ein Vertragsabschluss in englischer Sprache nicht vermeiden lässt, folgende Sicherheitsvorkehrungen beachten:

- Der Vertrag sollte als anwendbares Recht immer deutsches Recht vorsehen.
- Sachkundige (interne oder externe) Rechtsberatung muss hinzugezogen werden, weil die rechtlichen Risiken für das IT-Management schlechterdings nicht übersehbar sind.



Fazit:

Verweisen beide Parteien bei den Vertragsverhandlungen auf ihre jeweiligen Klauselwerke, dann scheitert ein Vertragsabschluss nicht, wenn sich die Parteien zumindest auf den Kernbestandteil einer Vereinbarung einigen können. Die sich widersprechenden Klauseln in den AGB heben sich gegenseitig auf, an deren Stelle tritt die gesetzliche Regelung.

Soweit sich die AGB nicht widersprechen, sondern sich jeweils ergänzen, können sie Vertragsbestandteil werden und unterliegen dann der inhaltlichen Kontrolle des AGB-Rechts. Klauseln sind danach nur zulässig, wenn sie keine Abweichung vom gesetzlichen Vertragstyp darstellen oder nur unwesentlich abweichen, so dass sie keine unangemessene Benachteiligung der anderen Seite darstellen.

■ 14.4 Mängel und Garantie beim Hardwarekauf

14.4.1 Rechte bei Mängeln

In diesem und den folgenden Abschnitten beziehen wir uns auf den Händlervertrag (nur Vertrieb der Ware), den Integrator-Vertrag (Kauf mit Montageverpflichtung) und den Vertriebsvertrag des Herstellers, der die Ware selber herstellt bzw. assembliert (Werklieferungsvertrag). Dreh- und Angelpunkt ist der Begriff des Mangels.



§ 433 BGB

(1) Durch den Kaufvertrag wird der Verkäufer einer Sache verpflichtet, dem Käufer die Sache zu übergeben und das Eigentum an der Sache zu verschaffen. Der Verkäufer hat dem Käufer die Sache frei von Sach- und Rechtsmängeln zu verschaffen.

(2) Der Käufer ist verpflichtet, dem Verkäufer den vereinbarten Kaufpreis zu zahlen und die gekaufte Sache abzunehmen.

Den Referenzstandard für die Mangelfreiheit bildet in erster Linie die Vereinbarung der Vertragsparteien. Fehlt eine solche Vereinbarung, kommt es auf den „nach dem Vertrag“ vorausgesetzten Verwendungszweck an. Das Gesetz zwingt damit zur Offenlegung der Verwendungsrisiken schon bei Vertragsabschluss. Hilfsweise muss die Ware diejenigen Eigenschaften ausweisen, die für solche Produkte berechtigterweise erwartet werden dürfen. Das ist weniger als „Stand der Technik“, aber immerhin noch Konformität mit etablierten Standards, die beispielsweise durch das BSI gesetzt werden.



Beachten Sie:

Werbeaussagen des Herstellers sind nach deutschem Kaufrecht verbindliche Beschaffenheitszusagen, für die der Händler (!) einzustehen hat.

14.4.2 Vorgehen in der Praxis

Nachfolgend finden Sie einige Empfehlungen für ein sachgerechtes Verhalten in den möglichen Praxissituationen:

- Überprüfen Sie die gelieferte Ware bereits bei der Anlieferung (Identität, sichtbare Beschädigungen, Vollständigkeit), führen Sie möglichst zeitnah erste Funktionstests durch, spätestens bei „Go-Live“ muss ein umfassender Test durchlaufen sein. Melden Sie dem Lieferanten aufgetretene Mängel spätestens innerhalb von fünf Werktagen. Der Mängelbericht muss so detailliert sein, dass der Lieferant Ansatzpunkte für Analyse und Fehlerbehebung hat.
- Mangel bedeutet nicht „Defekt“, sondern Abweichen von der vereinbarten, hilfsweise nach dem Vertragszweck vorausgesetzten oder hilfsweise nach der marktüblichen Spezifikation.
- Setzen Sie dem Lieferanten eine Frist zur „Nacherfüllung“, d. h. zu Reparatur oder Ersatzlieferung. Die Frist muss angemessen lang sein, in der Regel genügen 14 Tage bis vier Wochen.
- Verstreicht die Frist zur Nacherfüllung erfolglos, können Sie
 - am Vertrag festhalten, aber den Kaufpreis mindern (beziehungsweise zu viel gezahlten Kaufpreis zurückfordern) und Schadensersatz verlangen:
 - Ersatz von Mehraufwand (intern/extern)
 - Ersatz vergeblicher Investitionen
 - Ersatz entgangenen Gewinns
 - oder
 - vom Vertrag zurücktreten (Rückgabe von Geld und Waren) und Schadensersatz verlangen:
 - Ersatz von Mehraufwand (intern/extern)
 - Ersatz vergeblicher Investitionen
 - Ersatz entgangenen Gewinns
 - Ersatz der Mehrkosten eines alternativen Produkts

14.4.3 Weitere Fragestellungen

Welche Verpflichtungen zur Untersuchung und Rüge habe ich?

Die Verpflichtung zu unverzüglicher Untersuchung und unverzüglicher Anzeige von Mängeln gilt grundsätzlich für alle kommerziellen Kaufverträge (B2B). Es empfiehlt sich, Untersuchungsverfahren und Untersuchungsfristen vertraglich zu regeln.

Was mache ich, wenn es Streit darüber gibt, ob die Ware vertragsgemäß ist?

Ist zwischen den Parteien umstritten, ob die gelieferte Ware vertragsgemäß ist, kann es sich empfehlen, die Mangelhaftigkeit durch einen gerichtlich bestellten Sachverständigen schon vor Prozessbeginn in einem selbständigen Beweisverfahren feststellen zu lassen. Die Zivilpro-

zessordnung (ZPO) verlangt hierfür in § 485 ZPO die Zustimmung des Gegners. Wird diese verweigert, dann kann der Kläger das selbständige Beweisverfahren anstrengen, wenn die Beweiserhebung durch Verlust der Beweismittel gefährdet ist oder ein berechtigtes Interesse an der Feststellung u. a. des Zustandes einer Sache, der Ursache eines Sachschadens oder eines Sachmangels, dem Aufwand für die Beseitigung eines Personen- oder Sachschadens oder eines Sachmangels besteht.

Wähle ich ein staatliches Gericht oder ein Schiedsgericht?

Die staatlichen Gerichte sind für ihre Sachkunde bei der Beurteilung von komplexen IT-Sachverhalten nicht gerade berühmt. Das liegt unter anderem daran, dass größere IT-Vorhaben so gut wie nie vor staatliche Gerichte kommen. Weder Anbieter noch Auftraggeber haben ein sonderliches Interesse daran, die Einzelheiten gescheiterter Projekte vor aller Öffentlichkeit und damit auch vor ihren Wettbewerbern auszubreiten.

Bei größeren Vorhaben oder solchen, die bei ihrem Scheitern eine hohe Presseresonanz erfahren würden, empfiehlt sich daher, Streitigkeiten nicht vor staatlichen Gerichten, sondern vor einem Schiedsgericht auszutragen. Hierzu bedarf es nicht mehr, als dass die Parteien in ihrem Vertrag eine so genannte Schiedsklausel aufnehmen.



Beispiel:

„Alle Streitigkeiten, die sich im Zusammenhang mit dem Vertrag (... Bezeichnung des Vertrages ...) oder über seine Gültigkeit ergeben, werden nach der Schiedsgerichtsordnung der Deutschen Institution für Schiedsgerichtsbarkeit e. V. (DIS) unter Ausschluss des ordentlichen Rechtsweges endgültig entschieden.“

Es gibt eine Vielzahl von Schiedsordnungen, die sich bewährt haben, insbesondere die des Schiedsgerichts der Internationalen Handelskammer (Paris). Die Wahl eines bestimmten (ständigen) Schiedsgerichts ist nicht erforderlich, in der Regel genügt ein Ad-hoc-Schiedsgericht: Jede Partei ernennt einen Schiedsrichter, diese wiederum den Vorsitzenden.

Schiedsgerichte sind in der Regel teurer als staatliche Gerichte, sie gelangen aber wesentlich schneller zu einer verbindlichen Endentscheidung.



Fazit:

Die Aufhebung und Rückabwicklung des Kaufvertrages lässt das Gesetz nur zu, wenn der Vertrag im Wesentlichen gescheitert ist. Deshalb muss dem Lieferanten eine Frist zur Nacherfüllung gesetzt werden. Erst wenn diese erfolglos verstrichen ist, ist der Weg zur Minderung oder zu Rückabwicklung eröffnet.

■ 14.5 Software-Lizenzierung

Die Lizenzierung von Software spielt bei der Beschaffung von IT-Leistungen eine wichtige Rolle. Die Besonderheit von Software besteht darin, dass sie ein immaterielles Wirtschaftsgut ist. Der Datenträger ist völlig irrelevant. Die Berechtigungen an diesem Wirtschaftsgut, die Sie erwerben oder nutzen können, unterscheiden sich von denen, die bei Hardware in Betracht kommen, in grundlegender Weise. Der Grund für diese eigentums- und besitzrechtlichen Anomalien bei Software liegt darin, dass der berühmte Federstrich des Gesetzgebers Software der Kategorie „urheberrechtlich geschützter Werke“ zugewiesen hat. Die sich daraus ergebenden rechtlichen Konsequenzen lernen Sie in diesem Abschnitt kennen; weitere Details zu dem Thema liefert Kapitel 8 „Herausforderung Lizenzmanagement – vom Risiko zum Wert“ in diesem Handbuch.

14.5.1 Grundlagen

Software wird nach geltendem Recht behandelt wie Werke der Literatur, der Wissenschaft und der Kunst. Der Softwareentwickler ist Urheber eines Werkes und kann Zeit seines Lebens (und seine Erben 70 Jahre nach seinem Tode) Schutz vor unzulässiger Nutzung der Software beanspruchen. Die Urheberschaft (des Künstlers!) kann nicht übertragen werden, lediglich die wirtschaftlichen Verwertungsrechte (Nutzungsrechte) am Werk.

Diese Gleichstellung von „Oracle 10“ mit „Buddenbrooks“ ist einigermaßen erstaunlich, weil technische Texte (Werke) es in der Regel nicht schaffen, die für urheberrechtlichen Schutz erforderliche Originalität („Schöpfungshöhe“) nachzuweisen. Der urheberrechtliche Schutz von Software beruht letztendlich auf Vorgaben des europäischen Rechts und entspricht im Übrigen auch der inzwischen weltweiten Schutzpraxis für Software.



§ 69 a UrhG

- (1) Computerprogramme im Sinne dieses Gesetzes sind Programme in jeder Gestalt, einschließlich des Entwurfsmaterials.
- (2) Der gewährte Schutz gilt für alle Ausdrucksformen eines Computerprogramms. Ideen und Grundsätze, die einem Element eines Computerprogramms zugrunde liegen, einschließlich der den Schnittstellen zugrundeliegenden Ideen und Grundsätze, sind nicht geschützt.
- [...]
- (4) Auf Computerprogramme finden die für Sprachwerke geltenden Bestimmungen Anwendung, soweit in diesem Abschnitt nichts anderes bestimmt ist.

Die Angemessenheit der Regelung kann man mit Fug und Recht anzweifeln. Die Innovationszyklen der Software-Industrie liegen typischerweise unterhalb eines Zeitraums von 10 Jahren. Die urheberrechtliche Schutzfrist von mindestens 70 Jahren ist deshalb nicht sinnvoll. Die patentrechtlichen Schutzfristen von 10 bis 15 Jahren wären wesentlich sinnvoller.

Das Urheberrecht bietet auch keinen angemessenen Schutz. Es schützt im Kern nur gegen zeichenidentischen Nachbau („Plagiat“), die dem Quelltext zugrundeliegenden Technologien, Architekturen und Funktionsprinzipien werden grundsätzlich nicht geschützt (so die Inkassoentscheidung, BGHZ 94, S. 276–277). Darin liegt aber in der Regel der eigentliche Wert der Software. Der auf den Schutz der technischen Ingenieurleistung zugeschnittene Patentschutz würde insoweit besser passen.

Der urheberrechtliche Schutz zeichnet sich dadurch aus, dass er sofort zur Verfügung steht und nichts kostet (im Gegensatz zu den langwierigen und kostenträchtigen Anmeldeprozeduren im Patentrecht) und bis zu einem gewissen Grade auch effizient ist (im Gegensatz zum Designschutz, der nur das Screen-Design vor Nachahmung bewahrt).

14.5.2 Das sollten Sie beachten

Für den Abschluss eines Software-Überlassungsvertrages sollten Sie Schritt für Schritt die folgenden Fragen prüfen und beantworten:

- Was wird lizenziert? Listen Sie die Software(module) genau auf.
 - Ausführbarer Code, Quellcode
 - Anwender- und Entwicklerdokumentation
- Welche Rechte werden Ihnen eingeräumt?
 - Nutzen
 - Vervielfältigen
 - Bearbeiten
 - Verbreiten (nur bei Vertriebsvertrags)
 - Übersetzen (bei Portierung auf andere Systeme)
 - Öffentlich Zugänglichmachen (bei Softwareverteilung über Download)
- Für welchen Zeitraum?
 - Zeitlich unbeschränkt
 - Zeitlich beschränkt
- Stehen Ihnen diese Rechte exklusiv zu?

Das ist nur bei einer Auftragsentwicklung erforderlich, sonst genügt auch eine nicht-ausschließliche Einräumung.
- Sind diese Rechte übertragbar (z. B. an Konzernunternehmen)?
- Dürfen Sie Unterlizenzen erteilen (z. B. an Konzernunternehmen)?
- Definieren Sie das Lizenzmodell. Dafür gibt es verschiedene Möglichkeiten:
 - Unbeschränkte unternehmensweite Nutzung
 - Beschränkte Nutzung per User, Concurrent User, Seat
 - Beschränkte Nutzung pro Produktivsystem, Server, Instanz
- Für welche Nutzungsarten dürfen Sie die Software einsetzen?
 - Eigene, gegenwärtige und künftige Geschäftszwecke
 - Für Geschäftszwecke von Konzernunternehmen

- Nutzung durch Sie für die Erbringung von Leistungen an Dritte (z.B. Konzernunternehmen)
- Nutzung durch Dritte für Ihre Zwecke (z.B. Outsourcer/Outtasker)
- Nutzung an beliebigen Standorten
- Nutzung der Software auf allen vom Lizenzgeber unterstützten Hardware-Plattformen und deren Betriebssystemumgebung(en). Bei Wechsel der Plattformen (z.B. HP zu Sun) entstehen keine zusätzlichen Lizenzkosten.
- Ist im Lieferumfang Fremdsoftware (beispielsweise Middleware, Datenbank) enthalten, für die besondere Regelungen gelten?
- Erhält man die Quellcode-Lizenz für den Fall, dass der Lizenzgeber Mängel der Software in vertragswidriger Weise nicht behebt?
- Berücksichtigt der Lizenzvertrag die Hinterlegung des Quellcodes bei der Hinterlegungsstelle (Escrow-Agent) für den Fall gescheiterter Mängelbehebung und Insolvenz des Lizenzgebers? Wer trägt die Kosten der Hinterlegung?
- Welche Aufzeichnungspflichten bestehen und welches Prüfungsrecht (Audit) wird eingeräumt? Hier gilt es das Verfahren festzulegen, mit dem die Einhaltung der Lizenzbedingungen geprüft wird. Dies beinhaltet:
 - Technische Aspekte: Wie lassen sich beispielsweise Key Files auslesen?
 - Administrative Aspekte: Z.B. welche Aufzeichnung der Einsatzbedingungen müssen vorliegen?
 - Organisatorische Aspekte: Wie und wie oft findet die Überprüfung statt? Wie lange vorher ist sie anzukündigen? Welcher Zugang zu Dokumenten und Systemen muss gewährleistet werden?
- Wie wird die Software geliefert? In welcher Form bzw. auf welchen Datenträger, z.B. DVD oder CD-Rom? Wird sie zusätzlich zum Download bereitgestellt?

14.5.3 Weitere Fragestellungen

Welche Rechte muss ich mir im Lizenzvertrag einräumen lassen?

Weil sie ein immaterielles Wirtschaftsgut ist, kann man an der Software selbst weder Eigentum erwerben (d.h. sie kaufen) noch sich den Besitz auf Zeit einräumen lassen (d.h. mieten, leasen). Man kann sich lediglich die Nutzung von Verwertungsrechten an der Software für bestimmte Nutzungsarten dauerhaft oder für eine bestimmte Zeit einräumen lassen. Welche Verwertungsrechte es an Software gibt, bestimmt ein urheberrechtlich vorgegebener Kanon. Er enthält das Recht

- zur Vervielfältigung (als Kopien auf Datenträger wie im flüchtigen Arbeitsspeicher),
- zur Bearbeitung (Übersetzen, Bearbeiten, Arrangieren, Verbinden und andere Umarbeitungen),
- zur Verbreitung eines körperlichen Vervielfältigungsstücks (Datenträger)
- zur öffentlichen Wiedergabe (Push-Dienst),
- zur öffentlichen Zugänglichmachung (Bereitstellung zum Download, Pull-Dienst).

**Praxistipp:**

In Vertragsformularen findet sich häufig die Formulierung, dem Lizenznehmer werden „alle erforderlichen Nutzungsrechte“ eingeräumt. Das klingt bestechend, weil man sich damit scheinbar die Mühe sparen kann, Nutzungsrechte und Nutzungsarten im Einzelnen festlegen zu müssen. Da Zweifel bei der Rechteeinräumung immer zu Lasten des Lizenznehmers gehen – er unter Umständen also teuer nachlizenzieren muss –, sind solche „catch all“-Formulierungen keine sinnvolle „Abkürzung“, sondern der direkte Weg in die vollständige Rechtsunsicherheit. Wenn sich eine solche allgemeine Formulierung aus verhandlungstaktischen Gründen nicht vermeiden lässt, dann muss der Vertrag genauestens aufzeigen (etwa in der Präambel oder in einer Anlage zum Vertrag), für welche Verwendungszwecke die Software künftig eingesetzt werden soll.

Muss ich mir Änderungsrechte einräumen lassen?

Softwareprodukte, die „Out-of-the-Box“ bereits lauffähig sind und volle Funktionalität haben, gibt es im Grunde nur im Consumer-Bereich. Für den kommerziellen Einsatz entwickelte Produkte (wie ERP, CRM, CAM etc.) sind in diesem Zustand in der Regel nicht einsatzfähig. Es bedarf vielmehr einer Anpassung an die Bedürfnisse des jeweiligen Kunden und seiner IT-Architektur. Hierfür haben sich in der Praxis Begriffe wie Parametrisierung, Konfiguration, Customizing, Erweiterung, User Exit-Programmierung u. a. eingebürgert.

Von der Konfiguration des Softwareprodukts durch vordefinierte Anpassungsmöglichkeiten im Setup-Routinen oder entsprechenden Optionen abgesehen, erfordert jede der dargestellten Anpassungen und Erweiterungen der Software ein entsprechendes Bearbeitungsrecht. Deshalb sollte die Frage der Änderbarkeit der Software in den Vertragsverhandlungen explizit zur Sprache gebracht und entsprechend geregelt werden.

**Praxistipp:**

Mit dem Recht zur Anpassung der Software an die Kundenbedürfnisse geht häufig die Frage einher, ob der Softwarehersteller solche vom Kunden beauftragten spezifischen Routinen „an sich ziehen kann“. Der Hersteller weiß in der Regel alles über die Softwaretechnik, aber nichts über die spezifischen Kundenprozesse. Er hat deshalb durchaus ein massives Interesse daran, das spezifische Prozesswissen des Kunden für die Weiterentwicklung seines Produkts nutzen zu können. Dem Hersteller kann daher ein einfaches Nutzungsrecht an solchen Entwicklungen eingeräumt werden, aber nur gegen entsprechende Rückvergütung!

**Beachten Sie:**

Wenn Sie die Software ändern bzw. erweitern und der Hersteller diese Änderungen nicht in seinen Standard übernimmt, laufen Sie Gefahr, bei jedem Patch oder Upgrade/Update diese Änderungen erneut einspielen zu müssen.

Wann muss ich mir Rechte am Quellcode einräumen lassen?

In Lizenzverträgen finden sich häufig Formulierungen, dass der Quellcode und/oder der Objektcode zur Nutzung überlassen werden. Dahinter steht das den Juristen bekannte, aber veraltete Modell der kompilierten Software. Sie besteht aus Sicht des Urheberrechts aus zwei getrennten „Werken“, dem Quellcode und dem Objektcode. Will ich Software ändern können, dann nützt mir eine entsprechende Rechteeinräumung am Objektcode wenig, erforderlich ist die entsprechende Überlassung und Rechteeinräumung der Quelltexte. Es kommt freilich auf die spezifische Software an. Kompilierte Software ist nicht mehr die Regel. Häufig werden scriptbasierte Programmiersprachen eingesetzt, deren generierter Softwarecode zugleich „Machine-readable“ und „Human-readable“ ist. In solchen Fällen liegt nur ein „Werk“ vor, nämlich der zugleich „ausführbare“ wie „editierbare“ Code. Hier wäre es sinnlos, Rechteeinräumung für Quellcode einerseits und Objektcode andererseits zu verhandeln, weil das eine mit dem anderen identisch ist.



Praxistipp:

In der Regel genügt der Zugang auf den editierbaren Code nicht für eine zielgerichtete Anpassung des Produkts. Sie müssen darüber hinaus auch die Designspezifikation und die Entwicklerdokumentation überlassen bekommen.

Sollte ich auf einer Softwarehinterlegung bestehen?

Die Hinterlegung von Software – auch Software Escrow genannt – ist ein dreiseitiger Vertrag zwischen Lizenzgeber, Lizenznehmer und einer Hinterlegungsstelle. Darin verpflichtet sich der Lizenzgeber, der Hinterlegungsstelle den aktuellen (und künftigen) ausführbaren wie editierbaren Code einschließlich Dokumentation zur Verfügung zu stellen. Die Hinterlegungsstelle verwahrt die Software und verpflichtet sich die Software bei Eintritt bestimmter Voraussetzungen an den Lizenznehmer herauszugeben. Die Hinterlegungsstelle kann darüber hinaus noch weitere Dienstleistungen erbringen, die je nach Produkt und Lieferstufen- bzw. Updatezyklus sinnvoll sein können. Solche Dienstleistungen können die Prüfung der hinterlegten Gegenstände auf Vollständigkeit (insbesondere der Dokumentation) und die Prüfung der Funktionsfähigkeit der Software umfassen (lässt sich aus dem überlassenen Quellencode tatsächlich lauffähiger Code generieren?).

Diese Freigabesituationen sind typischerweise die Insolvenz des Lizenzgebers, die Abkündigung des Produkts und des Produktsupports sowie die gescheiterte Beseitigung von gravierenden Mängeln. Bei Lizenzgebern, deren wirtschaftliche Stabilität fraglich ist, sollte man auf eine Softwarehinterlegung keinesfalls verzichten. Im Falle des Zusammenbruchs des Lizenzgebers gibt es häufig keine andere Möglichkeit, um das Produkt weiterhin sinnvoll einsetzen und warten zu können.

Ob die Softwarehinterlegung im Insolvenzfall tatsächlich zu der erwünschten Freigabe führt, ist aus rechtlichen Gründen nicht sicher. Es gibt insoweit keine verlässliche Gesetzeslage. Aufgrund der Besonderheiten eines Software-Lizenzvertrages ist nämlich nicht sicher, ob nicht der Insolvenzverwalter des Lizenzgebers berechtigt sein kann, den Hinterlegungsvertrag anzufechten. Dieses Risiko soll im Zuge einer geplanten Novelle des Insolvenzrechts ausgeräumt werden, derzeit besteht diese Unsicherheit jedoch noch.

Darf ich darauf vertrauen, dass der Lizenzgeber berechtigt ist, mir die entsprechenden Nutzungsrechte einzuräumen?

Nutzungsrechte an Software können nicht im guten Glauben an die Rechtsinhaberschaft oder Verfügungsbefugnis des Lizenzgebers erworben werden. Sofern der Lizenzgeber seinerseits die Software ganz oder teilweise von Dritten lizenziert hat, können nur diejenigen Rechte weitergeben, die ihm tatsächlich zustehen. Erweist sich die „Lizenzkette“ im Nachhinein als brüchig, weil der Lizenzgeber seinerseits nicht mehr oder nicht ausreichend lizenziert ist, bricht die Rechteeinräumung zusammen. Eine wirksame Absicherung dagegen gibt es nicht. Als „zweitbeste“ Lösung müssen Sie im Vertrag vorsehen, dass in allen Fällen, in denen Dritte an Sie herantreten und Ansprüche auf die Software aus „älterem“ oder „besserem“ Recht geltend machen, der Lizenzgeber Sie sofort dagegen verteidigen muss. Er sollte verpflichtet werden, auf „erstes Anfordern“, d. h. ohne dass zuvor noch eine Prüfung erfolgen muss, ob diese Ansprüche zu Recht geltend gemacht werden, die Verteidigung gegen solche Ansprüche zu übernehmen und – für den Fall, dass solche Ansprüche nicht abzuwehren sind – von solchen Ansprüchen Dritter freistellen muss.

Die Möglichkeit, dass dritte Personen Ansprüche auf die Software erheben, besteht über den gesamten Lebenszyklus der Software hinweg. Bei der Vertragsgestaltung muss deshalb darauf geachtet werden, dass keine Ausschlussfristen oder Verjährungsfristen vereinbart werden, die den Rückgriff auf den Lizenzgeber verhindern könnten.

Kann gebrauchte Software gefahrlos eingesetzt werden?

Es gibt inzwischen einen regen Sekundärmarkt für Software-Applikationen für Unternehmen. Dafür sind nicht zuletzt Unternehmensinsolvenzen oder Reorganisationen von Unternehmen verantwortlich, in deren Zuge überflüssig gewordene Softwareprodukte einer Zweitverwertung zugeführt werden. Auf den Markt gelangen nicht nur vollständige Lizenzpakete, die obsolet geworden waren, sondern auch Teile davon in Form nicht genutzter Lizenzvolumina (typischerweise bei user/subscriber/seat Lizenzierung).

Solange und soweit der „Verkäufer“ der Software von seinem Lizenzgeber die Berechtigung erhalten hat, diese entgeltlich weiterzugeben, ist der Einsatz von Gebrauchtsoftware unproblematisch. Die Befugnis zur Weitergabe wird der Lizenzgeber aber nur in den seltensten Fällen im Vorhinein erteilen. Die gebräuchlichen Software-Lizenzverträge schließen die Befugnis zur Weitergabe grundsätzlich aus oder machen sie von einer besonderen Zustimmung im Einzelfall abhängig. Erfolgt die Weitergabe ohne solche Zustimmung, dann handelt der Verkäufer der Gebrauchtsoftware seinem Lizenzgeber gegenüber vertragswidrig. Er macht sich aufgrund dieses Vertragsbruches schadensersatzpflichtig und muss etwa im Falle der unzulässigen Abspaltung von Lizenzen die Kündigung des gesamten Lizenzvertrages befürchten.

Für den Käufer sind die Konsequenzen nicht weniger unangenehm. Er geht das Risiko ein, dass ihm der Lizenzgeber der Software deren Nutzung jederzeit untersagen kann. Im Bereich unternehmenskritischer Anwendungen (beispielsweise Datenbanken) wäre eine solche Nutzungsuntersagung, die der Lizenzgeber im Wege der einstweiligen Verfügung ohne weiteres gerichtlich durchsetzen könnte, gleichbedeutend mit erzwungenem Betriebsstillstand. Da die Gerichte in solchen Fällen bisher überwiegend lizenzgeberfreundlich entschieden haben, sollte Gebrauchtsoftware nur mit ausdrücklicher vorheriger Zustimmung des Softwareherstellers erworben und eingesetzt werden.

**Fazit:**

Der zentrale Gesichtspunkt bei Lizenz-Verträgen muss aufgrund der urheberrechtlichen Besonderheiten sein, dass schon bei Vertragsabschluss die Einsatzbedingungen und der Nutzungszweck für die gesamte wirtschaftliche Lebensdauer bedacht und entsprechend im Vertrag verankert werden. Jede Unklarheit führt im Zweifel zu fehlenden Nutzungsrechten, die später teuer nachlizenzieren werden müssen.

■ 14.6 Das Lizenzaudit

Ihr Software-Hersteller möchte bei Ihnen ein Lizenzaudit durchführen. Ihr erster Gedanke: Was darf er? Was muss ich befürchten? Was muss ich ihm offenlegen?

Art und Umfang der eingeräumten Nutzungsrechte sind die wesentlichen preisbildenden Faktoren des Produkts Software. Die Hersteller haben deshalb ein verständliches Interesse daran, dass die Nutzung beim Lizenznehmer den eingeräumten Lizenzumfang nicht überschreitet. Im Geschäftsmodell der Software-Hersteller spielen die Lizenzgebühren für Software eine ganz wichtige Rolle. Wer Software lizenziert, benötigt auch Dienstleistungen für die Implementierung und er wird für die voraussichtliche Dauer der Nutzung einen Wartungsvertrag mit dem Hersteller schließen, um das Produkt auf den aktuellen Stand zu halten. An den Lizenzumsätzen lässt sich deshalb der künftige wirtschaftliche Erfolg des Softwareunternehmens ablesen. Ergibt ein Audit Ihre Unterlizenzierung, dann meldet sich deshalb nicht die Rechtsabteilung bei Ihnen, sondern der Vertrieb!

Die Überprüfung ordnungsgemäßer Lizenzierung haben Softwarehersteller häufig auf externe Dienstleister verlagert, das gibt dem Ganzen einen neutralen, geradezu offiziellen Anstrich. Was müssen Sie tun, wenn Ihr Telefon klingelt und Ihnen ein Audit angekündigt wird?

Die Nutzung von nicht ausreichend lizenzierter Software ist strafrechtlich verboten,¹ die entsprechende Nutzung der Software kann im Wege der einstweiligen Verfügung untersagt² werden, sie berechtigt den Software-Hersteller, Schadensersatz zu verlangen (mindestens in Höhe der üblichen Lizenzgebühren).

Die Ansprüche auf Unterlassung und Schadensersatz setzen voraus, dass der Lizenzgeber die Verletzung der Lizenzbedingungen nachweisen kann. Wenn er dies nachweisen kann, kann, dann stehen ihm zur Vorbereitung von bezifferten Schadensersatzansprüchen auch Ansprüche auf Auskunft und Rechnungslegung (Nachweis lizenzgemäßer Nutzung) gegen den Lizenznehmer zu. Er kann sich des Weiteren von ihm genau zu bezeichnende Datenträger und Systeme zur Besichtigung vorlegen lassen. Eine gewisse Verschärfung zu Gunsten des Lizenzgebers ist seit kurzem dadurch eintreten, dass mit dem seit 1. 1. 2009 geltenden Tatbestand des § 101a UrhG schon bei „hinreichend wahrscheinlicher“ Verletzung von Urheberrechten

¹ § 106 UrhG.

² § 97 UrhG.

Auskunft und Vorlagepflichten des Lizenznehmers und aller anderen „Verletzer“ erzwungen werden können.

Schwieriger ist die Situation für den Lizenzgeber, wenn er den Bruch des Lizenzvertrages nur vermuten kann oder er über Art und Umfang der konkreten Nutzung seiner Software beim Lizenznehmer keine Kenntnis hat. Von Gesetzes wegen steht ihm weder ein Überprüfungsrecht zu, noch darf er gar ohne oder gegen den Willen des Lizenznehmers dessen Betriebsgelände betreten, Mitarbeiter des Lizenznehmers befragen und Durchsuchungen vornehmen. Auch die vorgenannten Auskunft- und Besichtigungsrechte stehen ihm nicht zur Verfügung, wenn es um „Fishing Expeditions“ geht.

Selbst eine Strafanzeige hätte wenig Aussicht auf Erfolg, weil auch die Staatsanwaltschaft Ermittlungsverfahren nur einleiten würde, wenn der Anfangsverdacht strafbaren Handel gegeben ist.

**Beachten Sie:**

- Informieren Sie bei Eingang der Auditankündigung sofort die Rechtsabteilung. Führen Sie keine Gespräche oder Maßnahmen ohne vorherige Freigabe durch die Rechtsabteilung.
- Prüfen Sie den Lizenzvertrag daraufhin, ob dem Software-Hersteller ein Auditrecht eingeräumt ist:
 - Besteht eine Auditklausel, wird das weitere Vorgehen durch diese Klausel bestimmt (Ankündigungsfrist, Inhalt der vorzulegenden Dokumente, Besichtigungsrecht).
 - Ohne Auditklausel steht dem Lizenzgeber kein Auditrecht zu. Er darf sich lediglich Dokumente und Softwaredatenträger vorlegen lassen.

**Fazit:**

Software-Audit ist ein Thema für Rechtsabteilung und Lizenzmanagement. Es darf nicht der IT oder der Betriebsmannschaft überlassen werden. Im Falle einer angekündigten Überprüfung dürfen ohne eine entsprechende rechtliche Freigabe keine Informationen übermittelt oder der Fernzugriff auf die Produkktivsysteme eröffnet werden.

■ 14.7 Externe Software-Entwicklung

Für die Vertragsgestaltung für IT-Dienstleistungen haben sich Bezeichnungen wie „Consulting-Leistungen“, „Professional Services“, „Systems Integration“ etc. eingebürgert. Diese Terminologie ist zum Teil der Internationalität dieser Branche geschuldet, zum Teil aber auch nur Marketinggeklingel. Welche rechtlichen Grundstrukturen sich dahinter verbergen, erfahren Sie in diesem Abschnitt.

Dienstvertrag, Werkvertrag

Die gesetzliche „Folie“, vor der Verträge über IT-Dienstleistungen und zu verhandeln sind, sieht zwei relevante Vertragstypen vor, den Dienstvertrag und den Werkvertrag. Tabelle 14.2 beschreibt die wesentlichen Unterschiede.

TABELLE 14.2 Unterschiede zwischen Dienst- und Werkvertrag

	Dienstvertrag	Werkvertrag
Erfolgsverantwortung	Nein	Ja
Weisungsabhängig	Ja	Nein
Abnahmeverfahren für Leistungen	Nein	Ja
Leistungen sind persönlich zu erbringen	Ja	Nein

Welchem Vertragstyp die entsprechenden Consulting-Leistungen zuzuordnen sind, hängt von den vereinbarten Pflichtenprogrammen ab. Die Bezeichnung des Vertrages ist demgegenüber irrelevant.

Bei einem Entwicklungsauftrag sollten Sie sich in möglichst umfassender Weise Nutzungs- und Verwertungsrechte an der Software übertragen lassen („ausschließliche Rechte“). Der Entwickler wird bestrebt sein, Routinen und Know-how für andere Kunden einsetzen zu dürfen. Gegen eine solche „Rücklizenzierung“ an den Entwickler ist im Grundsatz nichts einzuwenden, es sollte freilich bei den kommerziellen Regelungen angemessen berücksichtigt werden. Sofern die Entwicklung Schlüsseltechnologien betrifft, sollte im Vertrag über eine entsprechende Wettbewerbsklausel gesichert werden, dass Code und Know-how erst nach einer angemessenen Wartezeit („Cool-Down-Periode“) an Ihre Wettbewerber lizenziert werden dürfen. Die Nutzungsrechte und Nutzungsarten müssen im Einzelnen benannt sein, siehe Abschnitt 14.5 zur Software-Lizenzierung.

Das sollten Sie beachten

Bevor Sie einen Vertrag über Consulting-Leistungen oder Professional Services abschließen, sollten Sie Folgendes prüfen:

- Was ist der genaue Leistungsumfang (bzw. Funktionsumfang)?
- Hat der Dienstleister eine Erfolgsverpflichtung (Test: Wer trägt die Folgen, wenn der Leistungserfolg nicht erreicht wird, obwohl beide Parteien keine Fehler gemacht haben)?
- Wer hat die Planungsverantwortung, wer wirkt an der Planung nur mit?
- Wer führt das Projekt und ist für das Projektmanagement verantwortlich?
- Ist der eingeräumte Lizenzumfang an den vom Dienstleister zu liefernden Arbeitsergebnissen ausreichend?
- Ist der Dienstleister berechtigt, Subunternehmer einzusetzen oder muss er die Leistungen mit eigenem Personal erbringen?
- Haben Sie die wirtschaftliche Stabilität des Dienstleisters geprüft? Ist eine Absicherung für den Insolvenzfall erforderlich (Software Escrow)?
- Darf der Dienstleister die Arbeitsergebnisse und das dabei entwickelte Know-how für andere Kunden weiterverwenden?

**Fazit:**

Consulting-Verträge gehen in der Regel davon aus, dass Planung und Projektsteuerung Sache des Auftraggebers sind. Dieser Bereich bedarf daher bei der Vertragsgestaltung besonderer Sorgfalt. Darüber hinaus ist die Rechteeinräumung an den Arbeitsergebnissen an die geplanten Einsatzbedingungen und Verwendungsweisen genauestens anzupassen.

■ 14.8 Software aus der Eigenentwicklung

Wenn ein Mitarbeiter Software für sein Unternehmen entwickelt hat, stellt sich die Frage: Wem gehört diese? Wer darf sie nutzen? Man spricht von „Work made for hire“.

Die im angelsächsischen Rechtskreis geltende Doktrin, wonach die Rechte an der für den Auftraggeber entwickelten Software immer dem Auftraggeber zustehen, gilt im deutschen Recht nur sehr eingeschränkt. Nach § 69b UrhG entwickelt nur derjenige Auftragnehmer für den Auftraggeber, der dies im Rahmen seiner vertraglich vereinbarten Tätigkeitsbeschreibung tut.

**§ 69b UrhG**

- (1) Wird ein Computerprogramm von einem Arbeitnehmer in Wahrnehmung seiner Aufgaben oder nach den Anweisungen seines Arbeitgebers geschaffen, so ist ausschließlich der Arbeitgeber zur Ausübung aller vermögensrechtlichen Befugnisse an dem Computerprogramm berechtigt, sofern nichts anderes vereinbart ist.
- (2) Absatz 1 ist auf Dienstverhältnisse entsprechend anzuwenden.

Der angestellte Softwareentwickler ist also von der Verwertung der von ihm selbst geschaffenen Software ausgeschlossen. Gehört die Programmierung von Software nicht zur „Job Description“, dann entwickelt der Arbeitnehmer oder Beamte die Software immer nur für sich, selbst wenn er dies innerhalb der Dienstzeit tut und dafür auch Arbeitsmittel oder Kenntnisse aus dem Unternehmen verwendet.

**Beachten Sie:**

Verträge mit freien Mitarbeitern müssen immer eine umfassende Rechteeinräumung an den Auftraggeber enthalten.

Das sollten Sie beachten

- Alle Nutzungs- und Verwertungsrechte an Software, die ein Arbeitnehmer oder Beamter im Rahmen seiner arbeitsrechtlichen oder dienstrechtlichen Verpflichtungen erstellt, stehen dem Arbeitgeber zu; es entscheidet die „Job Description“.

- Alle Nutzungs- und Verwertungsrechte an Software, die
 - freie Mitarbeiter erstellen oder
 - fest angestellte Arbeitnehmer oder Beamte erstellen, zu deren Aufgaben die Softwareentwicklung nicht gehört,

stehen dem jeweiligen Softwareentwickler zu. Will der Arbeitgeber sie nutzen, muss er einen Lizenzvertrag mit dem Softwareentwickler abschließen.

**Fazit:**

Nur der angestellte Softwareentwickler, zu dessen Aufgaben es gehört, Programme zu schreiben, entwickelt für seinen Arbeitgeber.

■ 14.9 Verträge in der Vorbereitung eines IT-Projekts

IT-Projekte gehören zu den Vorhaben, bei denen das Risiko eines Scheiterns besonders groß ist (Ausführliche Informationen zu IT-Projekten bzw. zum IT-Projektmanagement finden Sie in Kapitel 5 dieses Handbuchs). Auftraggeber und Auftragnehmer haben zu Beginn oft nur unscharfe Vorstellungen davon, wie das endgültige Produkt, speziell die zu entwickelnde Software, beschaffen sein muss. Die Vertragsparteien müssen Zeit und Geld (beispielsweise in Hardware) investieren, ohne zu wissen, ob sich das Vorhaben realisieren und der endgültige Vertrag geschlossen wird. Um sich dennoch eine rechtliche Sicherheit zu verschaffen, zeichnen beide Parteien zur Vorbereitung des Projekts und begleitend zu den Vertragsverhandlungen häufig Dokumente, die mit Bezeichnungen wie „Letter of Intent“, „Letter of Agreement“, „Agreement in Principle“, „Memorandum of Intent“, „Memorandum of Understanding“, „Non Disclosure Agreement“, „Vorvertrag“ oder „Option“ überschrieben sind. Was es damit auf sich hat und wie Sie die vorvertragliche Phase eines Projekts absichern müssen, das behandelt dieser Abschnitt.

Absicherung der vorvertraglichen Phase eines Projekts

Die Vorbereitung und Vertragsverhandlungen von IT-Projekten nehmen in der Regel mehrere Wochen bis Monate Zeit in Anspruch. In diesem Zeitraum müssen die Parteien sich gegenseitig Informationen zur Verfügung stellen, Planungsleistungen erbringen, gegebenenfalls Pilot-systeme aufbauen und dergleichen. Ob es einen Vertragsschluss jemals geben wird, ist zu diesem Zeitpunkt noch alles andere als sicher. Um in dieser Phase der Unsicherheit überhaupt effizient zusammenarbeiten zu können, benötigen beide Parteien eine berechenbare Verhandlungsgrundlage. Sie wird typischerweise durch die o.g. vorvertraglichen Erklärungen oder Vereinbarungen geschaffen.

Letter of ... und Memorandum of ...

Die Erscheinungsformen „*Letter of Intent*“ und „*Letter of Agreement*“ sind in ihrer historischen Genese im anglo-amerikanischen Recht einseitige Erklärungen eines Anbieters, mit dem er die Ernsthaftigkeit seiner Absichten dokumentiert, ohne jedoch an sein Angebot oder den Abschluss eines Vertrages gebunden zu sein. Bei „*Agreement in Principle*“, „*Memorandum of Intent*“ und „*Memorandum of Understanding*“ legen die Parteien im Einvernehmen wesentliche Punkte fest, die die Geschäftsgrundlage für den beabsichtigten und noch zu verhandelnden Vertrag festlegen. Sie können bei Abschluss des Hauptvertrags zu dessen Auslegung herangezogen werden.

In der Rechtspraxis werden die Begriffe im Wesentlichen synonym und vollständig losgelöst von der Verwendungsweise in ihrem jeweiligen Heimatrecht verwendet. Es sind von beiden (!) Parteien unterschriebene Vereinbarungen über die Art und Weise der Vertragsverhandlungen und die Behandlung vorvertraglicher Leistungen. Wichtig ist, dass sie beiden Parteien ohne weiteres den jederzeitigen Abbruch der Verhandlungen erlauben („No Binding Clause“). Die Parteien unterwerfen sich einer ernsthaften Verpflichtung zu Verhandlungen, versprechen sich jedoch keinen Vertragsabschluss (nur „Duty to negotiate“, keine „Duty to agree“).

Ohne eine entsprechende Absicherung bleibt unsicher, wie mit Vorinvestitionen der Verhandlungspartner im Falle des Abbruchs der Verhandlungen zu verfahren ist. Überdies kann der Abbruch der Vertragsverhandlungen gegenüber der anderen Seite schadensersatzpflichtig machen (Ersatz des Vertrauensschadens).

Geheimhaltungserklärung

Das *Non Disclosure Agreement* ist eine isolierte Geheimhaltungsvereinbarung, mit deren Hilfe das gegenseitig offen gelegte Know-how und die ausgetauschten Dokumente vor unzulässiger Weitergabe an Dritte geschützt werden.

Vorvertrag, Option

Im Gegensatz zu den Absichtserklärungen verpflichtet der Vorvertrag zum Abschluss eines Hauptvertrags. Typischerweise sind Vorverträge nicht so umfassend oder vollständig wie der vorgesehene Hauptvertrag. Er muss jedoch die Kernelemente der Vereinbarung (Leistung, Vergütung) enthalten.

Option meint das Recht, das einer Vertragspartei eingeräumt wird, einseitig durch eine entsprechende Erklärung ein Vertragsverhältnis zu begründen oder zu verlängern. Der Optionsvertrag muss deshalb schon in umfassender Weise das Vertragsverhältnis regeln. Das Optionsrecht ist in der Regel befristet oder an den Eintritt eines bestimmten Ereignisses geknüpft.



Praxistipp:

Die Vereinbarung über die vorvertragliche Phase und die Vertragsverhandlungen sollte folgende Elemente enthalten:

- Verpflichtung zur ernsthaften Verhandlung über das vorgelegte Angebot, aber keine Verpflichtung zum Abschluss eines entsprechenden Vertrages. Die Parteien sind frei, die Verhandlungen jederzeit und ohne Angabe von Gründen abbrechen.

- Exklusivität der Verhandlungen (keine parallelen Verhandlungen mit Wettbewerbern über den gleichen Gegenstand).
- Rechteeinräumung an Arbeitsergebnissen. Entscheiden, ob die Arbeitsergebnisse auch nach Abbruch der Vertragsverhandlungen für eine ggf. neue Ausschreibung des Projekts verwendet werden dürfen.
- Beauftragung bzw. Übernahme von bestimmten Vorleistungen sowie Vergütungsregelungen hierfür.
- Geheimhaltungsvereinbarung.
- Haftungsvereinbarungen, typischerweise Haftungsausschlüsse für einfache Fahrlässigkeit.
- Rechtswahl und Gerichtsstandvereinbarung.

**Fazit:**

Die vertragliche Absicherung der Verhandlungsphase eines Projekts ist aufgrund der bestehenden Schadensersatzrisiken unerlässlich. Wie die Vereinbarung bezeichnet wird, ist nebensächlich. Entscheidend sind vielmehr die Möglichkeit der freien Abstandnahme vom Verhandlungsprozess, die Geheimhaltungsvereinbarung und dass Sie regeln, wie Vorinvestitionen behandelt werden.

■ 14.10 Verträge für schlüsselfertige IT-Systeme

Projekte zum Erstellen von IT-Systemen sind besonders komplexe Vorhaben. Sie teilen das Schicksal der Anlagebauverträge in den „alten Industrien“, dass die gesetzlichen Regelungen für solche Vorhaben völlig unzureichend sind. Die klassischen Konzepte des Werkvertrages, wie sie im bürgerlichen Gesetzbuch niedergelegt werden, sind auf einfache Austauschverträge hin entwickelt (zugespißt formuliert: auf das Fertigen eines Maßanzuges) und seit dem Inkrafttreten dieser Regelungen vor mehr als 100 Jahren auch nicht mehr wesentlich erweitert worden. Die Eigentümlichkeiten komplexer IT-Projekte (Dauer des Projekts, Notwendigkeit kooperativer Zusammenarbeit der Beteiligten auf ein gemeinsames Projektziel hin, vielfältige Abhängigkeiten der Leistung untereinander und von Mitwirkung des Auftraggebers, Dynamik der Anforderungen, Steuerung und Controlling, differenzierte Ergebnisverantwortung) sind in den gesetzlichen Bestimmungen noch nicht einmal in den Grundsätzen berücksichtigt.

Für das IT-Management wäre deshalb der Rückgriff auf die unzureichenden gesetzlichen Bestimmungen der sichere Weg in ein unkontrollierbares Projekt. Es führt deshalb kein Weg daran vorbei, für solche Vorhaben eigene Vertragswerke zu erarbeiten. Was dabei zu beachten ist, beleuchtet dieser Abschnitt.

14.10.1 Grundlagen

Werkvertrag, Werklieferungsvertrag

Die rechtliche Zuordnung von IT-Projekten zu den gesetzlichen Vertragstypen ist unsicher, wenn zentraler Bestandteil des Projekts die Systemintegration mit ihren unterschiedlichen Facetten der Änderung und Anpassung von Software ist. Auslöser für die Unsicherheiten bei der Zuordnung ist der misslungene, im Zuge der Schuldrechtsreform geänderte § 651 BGB.



§ 651 BGB

Auf einen Vertrag, der die Lieferung herzustellender oder zu erzeugender beweglicher Sachen zum Gegenstand hat, finden die Vorschriften über den Kauf Anwendung. [...].

Er unterwirft die Lieferung „herzustellender beweglicher Sachen“ den kaufrechtlichen Bestimmungen. Dies hätte zur Folge, dass insbesondere die Abnahmeregelungen des Werkvertragsrechts nicht zur Anwendung kommen. Die Kommentarliteratur versuchte, mit einer Dreiteilung zu helfen: Standardsoftware, die entweder nur damit versiert oder individuell angepasst und erweitert wird, soll über § 651 BGB den kaufrechtlichen Regelungen unterliegen; die kunden-spezifische Individualsoftware hingegen dem Werkvertragsrecht. Es ist derzeit nicht vorhersehbar, wie Gerichte bei Streitfällen aus Anlass komplexer IT-Projekte verfahren und welche gesetzlichen Regelungen sie zur Anwendung bringen werden. Aufgrund dieser Unsicherheit müssen die Parteien im Projektvertrag alle relevanten Sachfragen selbst behandeln und festlegen, welche Rechtsbehelfe im Falle nicht vertragsgemäßer Erfüllung zur Anwendung kommen sollen.

Generalunternehmerschaft

IT-Projekte vereinen häufig eine Vielzahl von Leistungserbringern. Software und Infrastrukturkomponenten werden von jeweils verschiedenen Zulieferern bezogen, die Produktivumgebung wird von einem RZ-Betreiber (Data Center-Betreiber) betrieben, die Softwareentwicklung und -anpassung obliegt wiederum einem Systemhaus auf seiner eigenen Entwicklungsumgebung. Viele Projekte erreichen den angestrebten Erfolg gerade deshalb nicht, weil zwar jede Zuliefererleistung für sich genommen die vereinbarten Ergebnisse zeitigt, beim Zusammenspiel aller Teilleistungen es aber zu unüberwindbaren Problemen kommt.

Deswegen ist eine der ganz wesentlichen planerischen Aufgaben, die in einem Projekt erledigt werden müssen, die übergreifende Planung und Koordinierung aller Teilprojekte durch das Projektmanagement (im Sinne eines Multiprojektmanagement). Vertraglich muss diese Sachfrage zwingend geregelt werden. Sie wird es häufig in der Weise, dass einer der Auftragnehmer die Generalunternehmerschaft für das Gesamtprojekt übernimmt. Der Auftragnehmer schließt nur einen Vertrag, und zwar mit dem Generalunternehmer. Dieser wiederum beauftragt alle Subunternehmer.

Der Vorteil einer einheitlichen Koordination des Gesamtprojekts durch den Generalunternehmer hat ihren Preis, weil Projektmanagement und Risikorückstellung in die kommerzielle Bewertung einfließen müssen. Zudem ist mit Aufschlägen für das „Handling“ der Subunternehmer zu rechnen.

Dem Vorteil der einheitlichen Koordination und Verantwortung stehen weitere gewisse Nachteile gegenüber. Ob der Generalunternehmer tatsächlich über das ausreichende Know-how

verfügt, die Zulieferer in geeigneter Weise zu steuern, ist häufig fraglich. In der Regel schließen die Generalunternehmer ihre Subunternehmerverträge erst dann, wenn der Projektvertrag unterschriftsreif ist. Der Generalunternehmer will sich verständlicherweise gegenüber seinen Subunternehmern nicht binden, bevor klar ist, welchen Verpflichtungen er gegenüber dem Auftraggeber unterliegt. Die nachgelagerte Verhandlung der Subunternehmerverträge bringt es aber mit sich, dass in die Verhandlung des Projektvertrages die besondere Expertise der Zulieferer/Subunternehmer nicht einfließen kann.

14.10.2 Vorgehen in der Praxis

- Benennen Sie die Projektziele ausdrücklich im Vertrag (Inhalt, Zeit, Kostenziele, Einsparungen).
- Legen Sie den Projektumfang fest und achten Sie dabei auf folgende Aspekte:
 - Auftragnehmer ist Generalunternehmer (Planung, Koordinierung, Projektmanagement, übergreifende Erfolgsverantwortung für alle Teilprojekte und Schnittstellen, Steuerung der Subunternehmer).
 - Migration der Altdaten (Datenübernahme, Datenbereinigung).
 - Spezifikationsdokumente und Projektplan müssen bei Vertragsabschluss vorliegen und als Anlagen beigelegt werden.
- Legen Sie die (Erfolgs-)Verantwortung des Auftragnehmers fest.
- Falls Hardware oder Software vom Auftraggeber beschafft werden, muss der Auftragnehmer entsprechende Beschaffungsempfehlungen (Sizing!) abgeben.
- Sorgen Sie für eine genaue und abschließende (!) Festlegung der Beistellungs- und Mitwirkungspflichten des Auftraggebers. Alle übrigen für den Erfolg des Projekts erforderlichen Leistungen sind vom Auftragnehmer zu erbringen.
- Der Projektvertrag gilt auch für vorvertragliche Leistungen und regelt wie Leistungen in der Pilotphase, das Pre-Sales Invest, vergütet werden. Oft vereinbaren die Vertragsparteien, dass bei Projektdurchführung bereits erbrachte Zahlungen auf die Vergütung angerechnet werden.
- Legen Sie die Projektorganisation fest: Dokumentation des Projekts, Meetingstruktur, Monitoring, Reporting, Ansprechpartner.
- Legen Sie das Eskalationsverfahren fest.
- Treffen Sie Regelungen für den Einsatz von Subunternehmern. Dazu können gehören:
 - Keine Delegation von zentralen Aufgaben (Projektplanung, Projektmanagement, Qualitätssicherung, Zugriff auf Produktivsysteme).
 - Delegation mit vorheriger Anzeige und Widerspruchsmöglichkeit für andere Tätigkeiten
- Projektleistungen werden grundsätzlich durch eigene, fest angestellte Mitarbeiter des Auftragnehmers erbracht. Folgendes sollten Sie darüber festhalten:
 - Zuweisung von namentlich benanntem Schlüsselpersonal
 - Sicherung des Know-how-Transfers bei Personalwechsel
 - Ablösung und Ersatz von Personal auf Anforderung des Auftraggebers bei berechtigtem Interesse

- Der Auftraggeber sollte direkten Durchgriff auf Subunternehmer erhalten.
- Regeln Sie die Rechteeinräumung an Arbeitsergebnissen.
- Legen Sie verbindliche Termine (Meilensteine) fest. Bei Überschreiten der Termine sollten Sie Vertragsstrafenregelungen vorsehen.
- Bestimmen Sie die Vergütungsmodelle. Dies beinhaltet:
 - Festpreis, aufwandsbezogene Vergütung mit/ohne Zielbudget (ggf. mit Bonus/Malus bei Unterschreiten/Überschreiten des Zielbudgets)
 - Anwendbare Vergütung für Zusatzleistungen (Change Request)
 - Controlling, Zahlungsplan
- Legen Sie das Abnahmeverfahren fest:
 - Welche Leistungen unterliegen Abnahmetests? (Gibt es ein einheitliches Abnahmeverfahren am Schluss oder sind Teilabnahmen möglich? Diese sollten unter dem Vorbehalt der Mangelfreiheit bei nachfolgenden Abnahmen stehen.)
 - Was müssen die beiden Seiten bei der Endabnahme zur Abnahme bereitstellen? Welche Dokumentation gilt es vorzulegen? Auch sollte geregelt werden, welche Abnahmetests und Anforderungen (z. B. Prio 1 und Prio 2) fehlerfrei zu bestehen sind.



Praxistipp:

Vereinbaren Sie einen Abnahmebetrieb unter Produktivbedingungen für einen Zeitraum von mindestens einem Monat.

- Alle übrigen Leistungen werden „freigegeben“. Das bedeutet, dass nicht eine Billigung als vertragsgemäß erfolgt, sondern der Funktionsumfangexplizit bestätigt wird. Spätere Abweichungen unterliegen dann dem Change-Request-Verfahren).
- Legen Sie Verfahren zu Datenschutz und Datensicherheit fest, wenn der Auftragnehmer Zugriff auf die Echtzeiten des Auftraggebers erhält (insbesondere Verpflichtung der Mitarbeiter auf Datengeheimnis). Dazu zählen:
 - Weisungsstruktur für Datenverarbeitung im Auftrag festlegen
 - Sicherung der Daten gegen Missbrauch (Weitergabe an Dritte, Zugänglichmachen für Dritte) mit Vertragsstrafenregelung
- Vereinbaren Sie einen Servicelevel für die Mängelbeseitigung nach der Abnahme.
- Arbeitsergebnisse müssen frei von Rechten Dritter sein (Verpflichtung zur unverzüglichen Freistellung auf erstes Anfordern, falls Dritte an den Arbeitsergebnissen Rechte geltend machen).
- Legen Sie die Vergütung des Auftragnehmers fest, wenn das Projekt, durch Sie als Auftragnehmer gekündigt wird. Diese sogenannte Run-Down-Kompensation könnte beispielsweise beinhalten, dass erbrachte Leistungen vergütet, nicht mehr zu erbringende Projektleistungen nicht vergütet werden.
- Sehen Sie Haftungsregelungen mit angemessener Haftungsbegrenzung vor. Dabei müssen zwingend ersatzfähig sein:
 - Interner und externer Mehraufwand

- Aufgrund der Vertragsverletzung wertlos gewordene Investitionen (frustrierte Aufwendungen) und
- Mehrkosten eines Deckungsgeschäfts.
- Lassen Sie den Auftragnehmer eine Haftpflichtversicherung mit angemessener Deckung nachweisen (mindestens über die vertragliche Haftungssumme).
- Regeln Sie Geheimhaltung und Vertraulichkeit.
- Einseitige Leistungsverweigerungsrechte des Auftragnehmers sollten ausgeschlossen werden. Der Auftragnehmer sollte nur mit Zustimmung des Auftraggebers oder aufgrund gerichtlicher Entscheidung Zurückbehaltungsrechte geltend machen oder die Einrede des nichterfüllten Vertrages erheben dürfen.
- Legen Sie Change-Request-Verfahren fest. Wichtig ist dabei, dass der Auftragnehmer innerhalb einer kurzen Frist (zwei Wochen) eine erste Einschätzung von Kosten und Risiken vorlegen muss, auf deren Basis dann das weitere Vorgehen entschieden werden kann.
- Legen Sie das Auditrecht des Auftraggebers fest.

**Praxistipp:**

Vereinbaren Sie, dass der Auftraggeber das Audit durch einen Dritten durchführen lassen kann. Das belastet die Beziehung zwischen Auftraggeber und Auftragnehmer weniger stark.

- Rechtswahl: Bei internationalen Vertragsverhältnissen müssen zwingend das anwendbare Recht und die Vertragssprache (!) bestimmt werden.
- Bestimmen Sie das zuständige Gericht beziehungsweise weisen Sie Streitigkeiten über eine Schiedsklausel einem Schiedsgericht zu.

**Fazit:**

Bei Projektverträgen genügt es nicht, nur die technischen Aspekte von Planung, Durchführung und Management des Vorhabens zu regeln. Aufgrund der bestehenden rechtlichen Unsicherheiten sind auch in umfassender Weise die Rechtsbehelfe bei vertragswidriger Leistung in den Vertrag aufzunehmen.

14.11 Verträge über Cloud Services

Mit der weltweiten Verfügbarkeit von kostengünstigen Breitbandnetzen sind in den letzten Jahren neue Servicemodelle entstanden, die das traditionelle „on premises“-Betriebsmodell für IT-Systeme ergänzen. Es gibt dafür eine Reihe von wirtschaftlichen Faktoren, die den Markt für solche Dienstleistungen befördern, z. B. entstehen **Skaleneffekte** bei gemeinsam genutzten Infrastrukturen: Die Investitionen in dem Stand der Technik entsprechende Rechen-

zentren (Tier-3+, Tier-4) sind nämlich im Allgemeinen hoch, ebenso die Energiekosten für den laufenden Betrieb (vor allem die Umwandlung von **CAPEX in OPEX**). Die Verlagerung von IT-Services in die „Cloud“ bindet jedoch kein langfristiges Kapital und entlastet die Bilanz. Ein weiterer Vorteil liegt in der drastischen Verkürzung der Einführungszeiten für neue Prozessunterstützung (kürzere Time-to-Market).

Zu diesen ökonomischen Faktoren gibt es eine eingehende Untersuchung der Europäischen Kommission (The Future of Cloud Computing: Opportunities for European Cloud Computing beyond 2010; <http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf>).

Was unter „Cloud Computing“ zu verstehen ist, ist im Einzelnen umstritten. Eine ganz brauchbare Definition stammt von Gartner: „A style of computing where scalable and elastic IT capabilities are provided as a service to multiple customers using Internet technologies“. Die definitorischen Schwierigkeiten rühren daher, dass eine Reihe von etablierten Anbietern versuchen, ihren traditionellen Rechenzentrumsleistungen einen neuen Anstrich zu geben, hinter Cloud Computing oftmals also nur Marketingtrends stehen. Zum Teil liegt es aber auch daran, dass eingeführte Geschäftsmodelle wie multi-tenant Software as a Service oder nutzerabhängige Plattformleistungen (z. B. utility computing von Sun Microsystems) evolutionär weiterentwickelt werden und sich so nicht mit einer längerfristigen allgemeingültigen Definition fassen lassen. Ein weiterer Aspekt, der die Entstehung von Cloud Computing befördert hat, ist der Trend zur Standardisierung von Schnittstellen über Internettechnologien (gewissermaßen in Nachfolge von proprietären Schnittstellen/Middleware/SOA). Solche Systeme sind offenbar besser geeignet für das modulare Hinzufügen oder Wegnehmen von einzelnen Services.

Bis zum Erscheinen der Auflage dieses Werkes (Stand Mai 2011) beschränken sich die Cloud Computing Produkte mehr oder weniger auf periphere Systeme und Kommunikationsdienste.

Beispiele:

- 37signals: Basecamp
- Akamai: Hosting
- Amazon: webservices
- Dropbox: File Hosting und Backup
- GoGrid: GoGrid application hosting and storage
- Google: Google Apps Premier
- IBM: Smart Business Cloud application hosting and storage
- Iron Mountain. LiveVault data archiving
- Joyent: Joyent Cloud application hosting
- Microsoft: Azure/Office 365
- Nirvanix Storage Delivery Network
- Salesforce: CRM

Kernsysteme von Unternehmen (Finanzen/Controlling, ERP/PPS) werden, soweit ersichtlich, bisher nicht angeboten.

Bei Vertragsverhandlungen mit Anbietern von Cloud Services sollten Sie auf folgende Aspekte unbedingt achten:

Anwendbares Recht und Gerichtsbarkeit

Die meisten der oben genannten Anbieter haben ihren Sitz außerhalb der Europäischen Union. Ist der Anbieter nicht bereit, deutsches Recht und deutsche Gerichtsbarkeit zu akzeptieren, dann sollte der Rechtsstreit zumindest im Wege eines Schiedsverfahrens durchgeführt werden. Da es außerhalb der Europäischen Union keine etablierten Verfahren zur wechselseitigen Anerkennung von Gerichtsurteilen gibt, sind Schiedsurteile die einzige Möglichkeit, Entscheidungen innerhalb kurzer Frist mit einem überschaubaren finanziellen Aufwand grenzüberschreitend durchzusetzen.

Migrationsunterstützung

Die Laufzeiten der Verträge für Cloud Services sind typischerweise 3–5 Jahre. Das Versprechen der hohen Flexibilität bedingt geradezu, dass der Kunde „nach Bedarf“ den Anbieter wechseln kann. Hier ergeben sich aber genau dieselben Migrationsprobleme wie in jedem Outsourcing-Projekt: Wie lässt sich das beispielsweise bei Salesforce abonnierte CRM migrieren? Sofern es sich nicht um virtualisierte Systeme auf marktüblichen Plattformen handelt, die „en bloc“ verschoben werden können, bleibt nur der mühsame Weg der Datenextraktion mit anschließendem Neuaufbau von Systemen und Datenmodell. Die Standardverträge der Anbieter sehen keine Karenzperiode nach Vertragsende vor, die für eine Migration der Systeme zur Verfügung steht. Sofern hier keine abweichende Vereinbarung getroffen wird, muss der Kunde seine Systeme während der Laufzeit des Vertrages migrieren!

Lizenzmodell

Besonderes Augenmerk, wie bei jedem IT-Projekt, gilt dem Lizenzmodell. Die eingeräumten Nutzungsrechte müssen genau der Geschäftsprozessstruktur entsprechen, und zwar einschließlich des Sourcing Modells: Übertragbarkeit im Konzern, Nutzung durch externe Dienstleister/Outtasker sowie Nutzung für Third Party Services im Konzern.

Datenschutz und Datensicherheit

Die technische Datensicherheit stellt in der Regel bei den oben genannten Anbietern kein Problem dar. Kaum eines der kundeneigenen Rechenzentren wird den Sicherheitsstandards genügen, die dort typischerweise eingesetzt werden (Tier-4). Sehr viel schwieriger ist die Datenkontrolle zu bewerkstelligen. Die Anbieter versuchen aus naheliegenden Gründen, ihre häufig weltweiten Kapazitäten gleichmäßig auszunutzen und diese betrieblichen Anforderungen den Kundensystemen/Kundendaten entsprechend zu verschieben. Aus Kundensicht ist dies aus mehreren Gründen nicht akzeptabel: Die europäischen Rahmenregelungen zu Datenschutz zwingen dazu, dass zwischen Datenverarbeitung auf europäischem Boden und in anderen Regionen unterschieden wird. Bei Letzterem müssen entsprechende besondere Vereinbarungen vorliegen (sog. Safe Harbour Verträge). Darüber hinaus ist zu beachten, dass der Zugriff von öffentlichen Stellen und Ermittlungsbehörden weltweit dem Standard entspricht, der in der Europäischen Union üblich ist. Deshalb sollte darauf gedrungen werden, dass die Daten physikalisch in Rechenzentren auf europäischem Boden verbleiben.

Service Level Agreement

Die Anbieter sind in der Regel sehr zurückhaltend, kundenspezifische Qualitätszusagen an ihren Service zu machen, denn das läuft den angestrebten Effizienzgewinnen, eine Plattform für eine Vielzahl von Kunden nutzen zu können, zuwider. Manche Anbieter, wie z. B. Sales-

force, verwenden ein Zweiklassensystem: Den Standardkunden gegenüber verpflichtet sich der Anbieter, nur Leistungen nach „bestem Bemühen“ zu erbringen. VIP-Kunden können hingegen auf dezidierte Quality-of-Service-Zusagen vertrauen. Aus Kundensicht muss zumindest bei auftretenden Fehlern/Incidents ein abgestimmtes Verfahren vereinbart werden, wie schnell auftretende Probleme analysiert, vorläufige Lösungen bereitgestellt und endgültige Fehlerbehebung erreicht werden. Ohne eine solche Zusage ist das Service Management nicht in der Lage, die eigene IT-Organisation wie auch das Unternehmen im Gesamten zu steuern. Die Fachabteilungen müssen wissen, welche Systeme betroffen sind, ob Umgehungen zur Verfügung stehen und wann mit einem Wiederanlaufen der Systeme gerechnet werden kann. Das Service Level Agreement sollte des Weiteren Regelungen zu Monitoring und Reporting der Systemverfügbarkeit und Performanz enthalten. Die Sanktionen sind typischerweise zweistufig: Hält sich die Abweichung von den vereinbarten Service-Parametern in Grenzen, verringert sich die Vergütung; bei Überschreiten der kritischen Schwelle sollten Vertragsstrafen und Kündigungsrechte vereinbart werden.

Haftung/Gewährleistung

Die Standardverträge von Anbietern sehen überwiegend einen vollständigen Haftungsausschluss vor. Sofern der Vertrag nicht deutschem Recht unterliegt, ist dies im Zweifel rechtsverbindlich. Deshalb muss in jedem Fall bei einer Abwahl deutschen Rechts eine ausreichende Haftungsregelung getroffen werden.



Das Wichtigste – zusammengefasst

- **IT-Management ist permanentes Compliance-Management!**

Der Weg von der Leitung einer internen Technikabteilung zum Management unternehmensweiter Unterstützung von Geschäftsprozessen ist längst durchschritten. IT-Compliance ist deshalb eine Kernanforderung, die das IT-Management erfüllen muss. IT-Compliance ist keine Angelegenheit für Zertifikate und Urkunden, sondern eine Quality-of-Service-Anforderung, die beständig umgesetzt werden muss!

- **Beachten Sie, dass sich Beschaffungsprozesse öffentlicher Unternehmen vorwiegend auf die Ausschreibung konzentrieren – und dies zu Unrecht!**

Auch bei IT-Projekten im öffentlichen Sektor muss der Projekterfolg als Umsetzung in Zeit, Qualität und Budget im Vordergrund stehen. Projektsteuerung, Risikomanagement und deren vertragliche Abbildung sind deshalb von überragender Bedeutung. Die Ausschreibung, so formalistisch und schwerfällig sie auch sein mag, ist nur die Vorphase zum Vertrag!

- **Standardverträge im Verhältnis B2C kann man auf die Klausel reduzieren: „es gilt das Gesetz“, was die Möglichkeit zu einseitiger Vertragsgestaltung minimiert; im B2B-Verhältnis ist diese Möglichkeit nur unwesentlich größer!**

Das deutsche Vertragsrecht lässt einseitige Vertragsgestaltung durch Standardverträge kaum zu. Wenn Sie Regelungen für eine Vielzahl von Geschäftsvorfällen belastbar vereinbaren wollen, dann sollten Sie zu Rahmenvereinbarungen greifen. Diese müssen im Einzelnen verhandelt werden, sind dann aber auch belastbar.

▪ **Jede Beschaffung von Software muss ein dediziertes Lizenzmodell vorsehen!**

Aufgrund der Eigentümlichkeiten des Urheberrechts gehen alle Lücken und Unklarheiten bei der Lizenzierung zu Lasten und zu Kosten des Lizenznehmers. Deshalb sollten Sie vor der Beschaffung die möglichen Einsatzbedingungen und Verwendungsweisen der Software über den gesamten wirtschaftlichen Lebenszyklus festlegen und dies im Lizenzvertrag verankern.

▪ **Kein IT-Projekt ohne Projektvertrag!**

Die gesetzlichen Auffangregelungen sind so spärlich, dass es im Konfliktfall einer Lotterie gleichkommt, herauszufinden, wer welche Pflichten hatte und wer welche Ansprüche. Wichtig sind dabei nicht die nahliegenden Dinge (wann verjähren Rechte bei Mängeln und wie hoch ist die Haftungssumme), sondern Projektsteuerung, Projektcontrolling und Risikomanagement!

▪ **Keine Angst vor Cloud Computing!**

Aus rechtlicher Sicht werden hier nur bestehende Geschäftsmodelle evolutionär weiterentwickelt. Wie bei jedem Projekt geht es auch hier im Kern um Projektsetup und Migration, Quality of Service und Absicherung. Besondere Schwierigkeiten bereiten die Datenschutz- und Datensicherheitsfragen, deshalb sollten die Daten immer auf europäischem Boden bleiben.

■ 14.12 Literatur

- [Ba03] *Bayreuther, F.*: Zum Verhältnis zwischen Arbeit-, Urheber- und Arbeitnehmererfindungsrecht, GRUR 2003, S. 570
- [Brä04] *Bräutigam, P.* (Hrsg.): IT Outsourcing. 2. Auflage, Erich Schmidt Verlag Berlin, 2009
- [Bri09] *Brisch, K.* (Hrsg.): IT Compliance, Schriftlicher Management Lehrgang, Euro Forum Verlag 2009
- [Ha07] *Hauschka, C.*: Corporate Compliance, 2. Aufl., C. H. Beck, München 2010
- [He07] *Heussen, B.* (Hrsg.): Handbuch Vertragsverhandlung und Vertragsmanagement, 3. Aufl., O. Schmidt, Köln 2007
- [KH08] *Kilian, W; Heussen, B.*: Computerrechts-Handbuch, 26. Aufl., C. H. Beck, München 2008
- [LM08] *Lehmann, M., Meents, J. G.* (Hrsg.): Informationstechnologierecht, Luchterhand 2008
- [Mo06] *Moos, F.*: Software-Lizenz-Audits, Computer und Recht 2006, S. 797
- [Re07] *Redeker, H.*: IT-Recht. 4. Aufl. C. H. Beck, München 2007
- [Schn09] *Schneider, J.*: Handbuch des EDV-Rechts, 4. Aufl., O. Schmidt, Köln 2009
- [Schu06] *Schumacher, V.*: Service Level Agreements: Schwerpunkt bei IT- und Telekommunikationsverträgen. In: Multimedia und Recht 2006, 12
- Simitis, S.: Bundesdatenschutzgesetz, 7. Aufl., Nomos, Baden-Baden 2011
- [We08] *Westphalen, F. Graf von* (Hrsg.): Vertragsrecht und AGB Klauselwerke, C. H. Beck, München 2011

Die Autoren



Werner Bachmann

ist Rechtsanwalt und Partner einer großen deutschen Wirtschaftskanzlei. Der Schwerpunkt seiner Beratungstätigkeit sind die Planung, Ausschreibung, Verhandlung und Durchführung von Projekten der Informationstechnologie und der Telekommunikation. Er ist Dozent am Institut für Informationstechnologien im Gesundheitswesen.

Werner Bachmann hat das Kapitel 14 „*Rechtliche Rahmenbedingungen für das IT-Management*“ verfasst.



Dipl.-Kfm., MBA Robert Bergmann

ist kfm. Geschäftsführer der international tätigen EFR GmbH mit Sitz in München, einem Dienstleister im Bereich Energiemanagement und Smart Metering. Davor arbeitete er für die N-ERGIE Aktiengesellschaft in Nürnberg, wo er zuletzt Leiter des Zentralbereichs Zentrale IT-Steuerung war.

Robert Bergmann hat zusammen mit Ernst Tiemeyer das Kapitel 10 „*IT-Governance*“ verfasst.



Torsten Groll

Inhaber und Geschäftsführer der 1993 gegründeten CTC Computer Training & Consulting verfügt über mehr als 25 Jahre Erfahrung als IT-Berater, Trainer und Dozent. Der Schwerpunkt seiner Beratertätigkeit sind das Softwareasset- und Lizenzmanagement und dessen Verzahnung mit den Geschäftsprozessen im Unternehmen. Er gibt seine Erfahrungen in zahlreichen Seminaren und Webinaren weiter und ist Autor erfolgreicher Bücher und Fachartikel.

Torsten Groll hat das Kapitel 8 „*Herausforderung Lizenzmanagement*“ verfasst.



Prof. Dr. Michael Klotz

ist seit 1999 Professor für Betriebswirtschaftslehre, insb. Informationsmanagement, Organisation und Datenverarbeitung an der FH Stralsund. In 2008 gründete er das „Stralsund Information Management Team“ (SIMAT), in dem Forschung und Projekte im Bereich des Informationsmanagements und der IT-Governance gebündelt sind. Er ist Regionalverantwortlicher (Mecklenburg-Vorpommern) der gfo Gesellschaft für Organisation e.V. und Wissenschaftlicher Beirat des ISACA Germany Chapter sowie in dieser Funktion Mitherausgeber der Zeitschrift „IT-Governance“.

Michael Klotz hat das Kapitel 13 „*IT-Compliance*“ verfasst.



Dipl.-Kfm. Dietmar Kopperger

ist Leiter des Competence Center Softwaremanagement des Fraunhofer-Instituts für Arbeitswirtschaft und Organisation IAO in Stuttgart.

Dietmar Kopperger hat zusammen mit Anette Weisbecker und Jörg Kunsmann das Kapitel 4 „*IT-Servicemanagement*“ verfasst.



Prof. Dr. Helmut Krcmar

ist Inhaber des Lehrstuhls für Wirtschaftsinformatik an der TU München. Seine Forschungsinteressen umfassen Informations- und Wissensmanagement, IT-basierte Dienstleistungen, IS, eGovernment sowie verteilte und mobile Arbeits- und Lernprozesse. Er ist Gründer der Beratungsgesellschaft ITM und Mitgründer mehrerer Spin-offs aus dem universitären Umfeld.

Helmut Krcmar hat zusammen mit Andreas Schwertsik das Kapitel 7 „*IT-Controlling*“ verfasst.



Dipl.-Ing. Jörg Kunsmann

ist Senior Managing Consultant bei IBM Global Business Service im Bereich Public Sector und eHealth.

Jörg Kunsmann hat zusammen mit Anette Weisbecker und Dietmar Kopperger das Kapitel 4 „*IT-Servicemanagement*“ verfasst.



DI. Andreas Nehfort

ist Gründer und Geschäftsführer der Nehfort IT-Consulting KG. Zu seinen Schwerpunkten als Berater, Trainer und Assessor zählen Vorgehensmodelle in der Software Entwicklung, Prozessreifegradmodelle für Software und Systems Engineering, CMMI und SPiCE/ISO 15504, IT Service Management mit ITIL und ISO 20000, Anforderungsanalyse und Requirementsmanagement und IT-Projektmanagement.

Andreas Nehfort hat das Kapitel 9 „*Qualitätsmanagement für IT-Lösungen*“ verfasst.



Dipl.-Inform. Klaus Schmidt

unterstützt als Inhaber des Innomenta Security Consultings Unternehmen bei Aufbau und Optimierung des Managements der Informationssicherheit. Neben der Beratung erlangte er die Zertifizierungen zum CISM und ISO27001-Trainer, nahm einen Lehrauftrag an der Hochschule Fulda wahr, bildet Security Manager aus und ist regelmäßiger Referent von Seminaren im Themengebiet Informationssicherheit.

Klaus Schmidt hat die Kapitel 11 „*IT-Security-Management*“ und Kapitel 12 „*IT-Risikomanagement*“ verfasst.

**Dipl.-Kfm. Andreas Roland Schwertsik**

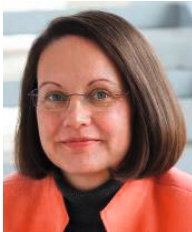
ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Wirtschaftsinformatik an der TU München bei Professor Krcmar.

Andreas Schwertsik hat zusammen mit Helmut Krcmar das Kapitel 7 „*IT-Controlling*“ verfasst.

**Dipl.-Hdl. Ernst Tiemeyer**

ist seit mehr als 20 Jahren in leitenden Projektfunktionen sowie als IT-Consultant und im Bildungsbereich bzw. Managementtraining tätig. Schwerpunktmäßig befasst er sich in der Praxis mit Projektmanagement, strategischem IT-Management, IT-Architekturmanagement, IT-Governance, IT-Controlling sowie prozessorientierten IT-Anwendungen (Business-IT-Lösungen).

Ernst Tiemeyer ist der Herausgeber dieses Handbuchs und hat die Kapitel 1 „*IT-Management – Herausforderungen und Rollenverständnis*“, Kapitel 3 „*Enterprise Architecture Management (EAM)*“, Kapitel 5 „*IT-Projektmanagement*“ und Kapitel 6 „*Organisation und Führung im IT-Bereich*“ sowie zusammen mit Walter Wintersteiger Kapitel 2 „*IT-Strategien entwickeln und umsetzen*“ und mit Robert Bergmann Kapitel 10 „*IT-Governance*“ verfasst.

**Priv.-Doz. Dr.-Ing. habil. Anette Weisbecker**

ist Institutsdirektorin am Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO in Stuttgart und Leiterin des Geschäftsfelds Informations- und Kommunikationstechnik.

Anette Weisbecker hat zusammen mit Jörg Kunsmann und Dietmar Kopperger das Kapitel 4 „*IT-Servicemanagement*“ verfasst.

**Dr. Walter Wintersteiger**

ist Unternehmensberater für Management & Informatik, Lektor an Universitäten und Fachschulen, Ehrenpräsident der Österreichischen Vereinigung für Softwarequalitätsmanagement (STEV), Dornbirn

Walter Wintersteiger hat zusammen mit Ernst Tiemeyer das Kapitel 2 „*IT-Strategien entwickeln und umsetzen*“ verfasst.

Index

A

ABC-Technik 215, 219
Abgabenordnung 612, 614, 619, 621
Abhängigkeitsanalyse 559
Abnahmeregung 683
Abnahmeverfahren 685
Abschlussphase 333
– eines Projektes 286
Abteilungen 6, 302
Abweichungsanalysen 275
AGB 661
agile Prozesse 439
Allgemeine Geschäftsbedingungen 661
Amortisationsrechnung 221
Analyse 109
analytische Qualitätsmaßnahmen 442
Änderungsprozess 158
Anforderungsdefinition 281
Anforderungsentwickler 425
Anforderungsmanagement 303
Anforderungsprozess 383
Angriffspfad 553
Antragsverfahren 212
Anwender 16
Anwendungsarchitektur 24
Anwendungsmanagement 30
Applikationskonsolidierung 123
Arbeitnehmervertretung 242
Arbeitspakete 244, 248
Arbeitspaket-Beschreibung 248
Architekturanalyse 559
Architekturprinzipien 108
Architekturteam 107
Argumentebilanz 221
Audit *siehe* Lizenzaudit
Aufgabendelegation 324
Auftraggeber 234, 238
– nicht-öffentliche 655
– öffentliche 655
Auftrittswahrscheinlichkeit 567
Aufwandsschätzung 216, 248
Auslastungsdiagramme 285
Ausschreibung 654, 657
Ausschreibungspflicht 657
Authentifizierung 597
Authentizität 533

Autorisierung 597
Availability Management 149, 161

B

Balanced Scorecard 4, 76, 189, 572
Balkendiagramm 253
Basel II 612, 632
BDSG *siehe* Bundesdatenschutzgesetz
Bedrohung 554
– akute 555
– potenzielle 554
Bedrohungsanalyse 561
Belastungsausgleich 258, 285
Benchmark 359
Benchmarking 359
Berichtsarten 26
Berichtsplan 245
Berichtswesen 189, 349, 358
Beschaffungsprozess 383
Bestands-Controlling 353
Bestellungsprozess 383
Betriebsrat 627, 628
Betriebsverfassungsgesetz 612, 627
Bewertungskriterien für IT-Projekte 218
BGB-InfoV 612, 624
Blog 626
BPO (Business-Process-Outsourcing) 314
Brauchbarkeit 422
Bruchfaktor 431
BSI-Standards 530
Budgetierung 208, 350
Bundesdatenschutzgesetz 510, 593, 597, 608, 609, 612, 623, 649
Bürgerliches Gesetzbuch 612, 624, 629
Business-Architekt 114
Business Engineering 48
Business Impact Analyse *siehe* Geschäftseinflussanalyse
Business-Process-Outsourcing (BPO) 314
Business Services 314
Business Software Alliance 375

C

Capability Maturity Model (CMM) 316
Capability Maturity Model Integration (CMMI) 454
Capacity Management 149, 162
Central Information Officer (CIO) 304
CERT *siehe* Computer Emergency Response Team
Change Control Board 276
Change Management 149, 157, 217
Charging 182
Chief Information Officer 588, 604, 608, 633, 636
CIO (Chief Information Officer) 304
Claim-Management 275
Client-Server-Architektur-Varianten 101
Cloud Computing 687
Cloud Services 686
CMM (Capability Maturity Model) 316
CMMI (Capability Maturity Model Integration) 454, 495, 600, 604, 615
COBIT 147, 494, 585, 600, 615
Code of Conduct 651
Combined Code 509
Compliance 585, 642
Compliance Officer 651
Computer Emergency Response Team 561
Configuration Management 149, 156
Conjoint-Analyse 264
Controllingbereiche 345
Corporate Compliance 586, 590, 591, 595, 596, 610, 633, 634, 636
Corporate Compliance-Officer 633, 634, 636
Corporate Governance 590, 598
COSO 508

D

Data-Mining 105
Data-Warehouse 623

Daten 585, 591, 605, 609, 620, 627
 Datenarchitektur 24, 66, 104
 Datenklassifizierung 597
 Datenkonsolidierung 123, 130
 Datenschutz 594, 603, 606, 609, 623, 636
 – und Datensicherheit 688
 Datenschutzbeauftragter 591, 609, 636
 Datensicherheit 609, 632, 636
 Datensicherung 597, 613
 Datenverschlüsselung 597
 Delegieren 322
 Deliverables 217
 Delta-Analyse 663
 Deming-Cycle 426
 Demotivation 323
 Design 109
 Deutscher Corporate Governance Kodex 590
 Dienstleister 10
 Dienstleistungsorientierung 301
 Dienstvertrag 678
 Dilemma, sequenzielles 415
 DMAIC-Zyklus 368
 Dokumentenmanagement 598, 621, 622
 Domänen 108
 Domänenarchitektur 108
 Domänenteam 108
 Dreischichtenarchitektur 109

E

E-Commerce 623, 624
 Economies of Scale 367
 e-discovery 652
 Eigenpersonal 256
 Einführung, Ablauf 174
 Einkommensteuergesetz 612, 621
 Eintrittswahrscheinlichkeit 562, 568
 e-Invoicing 653
 Einzelkosten 259, 260
 E-Mail 598, 618, 621, 627, 628
 Endzeitpunkt 251
 Entdeckungswahrscheinlichkeit 567
 Enterprise Architecture Management 606
 Entscheidungsprobleme 3
 Entscheidungsprozess 3
 Entsorgungsprozess 384
 Entwicklung
 – iterative 416
 – sequenzielle 414
 Erfahrungsdatenbank 349

Erfolgsfaktorenanalyse 13
 Ergebnisabweichungen 272
 Ergebniskennzahlen 5
 Error Control 156
 8. EU-Richtlinie 612
 EuroSOX 509
 EVB-IT 658
 externe IT-Projekte 210
 externe Qualitätsmerkmale 451

F

Failure Mode and Effects Analysis *siehe* FMEA
 Feedback-Memo 319
 Fehlerkosten 443
 Fertigstellungsgrad 271
 Fertigstellungswert 272
 Financial Management for IT Services 149
 Finanzierungsfrage 222
 FMEA 567
 Formierungsphase 333
 Fortschrittskontrolle 271
 FP (Freie Pufferzeit) 255
 Framework 25, 91, 92, 300
 Fraud Detection 652
 Freie Pufferzeit (FP) 255
 Fremdpersonal 256
 Führung 27, 320
 Führungsaufgaben 322
 Führungsfunktionen 304
 Führungsinstrumente 328
 Führungskraft 296
 Führungsstile 325
 Funktion „Service Desk“ 149

G

Garantie 667
 GDPdU 613, 620
 Geheimhaltungsvereinbarung 681
 Gemeinkosten 260
 Generalunternehmerschaft 683
 Generischer Sicherheitsstandard 538
 Gesamte Pufferzeit (GP) 255
 Geschäftsarchitektur 24
 Geschäftseinflussanalyse 558
 Geschäftsprozess 6, 50, 303, 593, 596, 601, 632
 Geschäftsprozessmanagement 598, 608, 609
 Gesetz gegen den unlauteren Wettbewerb 613, 624
 GoBS 613, 620
 GP (Gesamte Pufferzeit) 255
 Grundschatzkataloge 530, 593, 607, 614

H

Handelsgesetzbuch 612, 620, 621, 629
 Handlungsportfolios 219
 Hard Factors 192
 Hardware-Konsolidierung 123
 Help-Desk 308
 Hinweisgebersystem 594
 House of IT-Compliance 611

I

Identitätsmanagement 598
 IDW Prüfungsstandard 616
 Implementierung 109
 Incident Management 154
 Individualvereinbarung 662
 Informationsbedarf 317
 Information Security Circle 527
 Information Security Policy 538
 Informationsmanagement 302, 339
 Informationssicherheitshandbuch 530
 Informationssicherheits-Standards 560
 Informationssystem 49
 Informationsverarbeitungsprozess 3
 Infrastruktur-Controlling 351
 Innovationsperspektive 4
 Installationsprozess 384
 Instanz 302
 Integrität 533
 interne IT-Projekte 210
 internes Kontrollsystem 588, 595, 599, 606
 interne Qualitätsmerkmale 451
 Investition 654
 Investitionsrechnung 221
 investment 340
 ISACA 600, 607
 ISO 616
 ISO 1926 450
 ISO 2700x 529
 ISO 9001 449
 ISO 25000 451
 ISO/IEC 2700x 607, 615
 ISO/IEC 15504 Part 1–7
 – Information Technology – Process Assessment 456
 ISO/IEC 20000 615, 617, 618
 ISO/IEC 27001 592, 609
 ISO/IEC 27002 593, 600
 ISO/IEC 27005 607
 IST-Aufnahme 558
 IT-Abteilung 295
 IT-Anwendungen 599, 609
 IT-Applikations-Architektur 65
 IT-Architekt 114, 306

IT-Architekturen 24, 85
 IT-Architekturmanagement, Rollen-konzept 114
 IT-Architekturteams 115
 IT-Auditor 605, 634
 IT-Balanced Scorecard 355
 IT-Beschaffung 307
 IT-Betrieb 85, 307
 IT-Budget 28
 IT-Compliance *siehe* Compliance
 IT-Compliance-Committee 634, 636
 IT-Compliance-Officer 608, 633
 IT-Compliance-Organisation 631, 633, 635
 IT-Compliance-Risiken 599, 606, 630, 634
 IT-Controller 29
 IT-Controlling 305, 340
 IT-Dienstleister 27
 iterative Entwicklung 416
 IT-Forensik 652
 IT-Führung 296
 IT-Governance 8, 147, 490, 494, 585, 599, 600, 605
 IT-Grundschutz 530
 IT-Informationssysteme 141
 IT-Infrastruktur 85, 594, 596, 600, 607, 609, 615
 IT-Infrastrukturprojekte 232
 IT-Kennzahlen 318
 IT-Konsolidierungsprojekt 123, 131, 135
 IT-Kontrollen 608, 609
 IT-Kontrollsystem 599, 602, 609, 635
 IT-Koordination 307
 IT-Koordinatoren 307
 IT-Kosten 607
 IT-Leistungsprozesse 10
 IT-Leiter 304
 IT-Leitung 304
 IT-Lieferant 16
 IT-Normen 593, 595, 600, 607, 611, 615
 IT-Notfallmanagement 528
 IT-Organisation 20, 69
 IT-Personal 18
 IT-Planung 305
 IT-Portfolios 346
 IT-Projekt 609, 680
 IT-Projektcontrolling 26
 – Tools 26
 IT-Projekte 26
 – Bewertungskriterien 218
 – externe 210
 – interne 210
 IT-Projektleiter 234

IT-Projektleitung 310
 IT-Projektmanagement 208
 IT-Projekttypen 208
 IT-Prozesse 68, 300, 601, 603, 606, 609, 618, 635
 IT-Prozessunterstützung 141
 IT-Qualitätsmanagement 306
 IT-Quality-Manager 30
 IT-Recht 35
 IT-Ressourcen 141
 IT-Revision 608, 636
 IT-Richtlinien 593, 604, 611, 615, 618, 634, 651
 IT-Risiko 599, 602, 607
 IT-Risikoanalyse 557
 – umfassende 558
 – verkürzte 557
 – vollständige 558
 IT-Risikomanagement 547, 595, 599, 602, 607, 608, 634
 IT Risk Landscape 572
 IT Risk Scorecard 572
 IT-Security Auditing 541
 IT-Security-Management 501
 IT-Security Policy 537
 IT-Security Reporting 524
 IT-Service CMM 146
 IT Service Continuity Management 149
 IT-Service-Delivery 301
 IT-Servicemanagement 24, 139, 617, 618
 – in der Praxis 181
 IT-Service-Prozesse 301
 IT-Servicequalität 143
 IT-Services 25, 141, 366
 IT-Service-Supports 301
 IT-Sicherheit 595, 598, 602, 607, 615, 618
 IT-Sicherheitskriterien 531
 IT-Sicherheitsmanagement 592, 607, 608, 634
 IT-Sicherheitsrelevanz 503
 IT-Sicherheitsstandards 528
 IT-Standards 593, 595, 599, 600, 606, 607, 611
 IT-Strategie 22, 44
 IT-Strategieorientierung 88
 IT-Strategie-Projekt 50
 IT-Verträge 595, 609, 615
 IT-Verwaltung 310
 IT, Wirksamkeit 18
 ITIL 148, 600, 608, 609, 615, 617

K

Kann-Services 186
 Kapazitätsabstimmungen 283
 Kapazitätsmanagement 162

Kapazitätsplanung 257, 285
 KEF (kritische Erfolgsfaktoren) 170
 Kennzahlen 189, 317
 Kennzahlendefinition 358
 Kennzahlensystem 191, 355
 Kick-off-Meeting 225, 226
 Kirchliche Einrichtungen,
 Konfessionelle Krankenhäuser 655
 Klauselverbot *siehe* AGB
 Kompletteinführung 172
 Konflikte 331
 Konfliktmanagement 331
 Konfliktphase 333
 Konformität 534
 konstruktive Qualitätsmaßnahmen 441
 KonTraG 506, 608
 Kontrollgrößen 268
 Kontrollverfahren 268
 Kontrollzeitpunkte 268
 Konvergenz 127
 Koordinieren 322
 Koordinierungsausschuss 218
 Körperschaftsteuergesetz 613, 621
 Kosten, qualitätsbezogene 409
 Kostenarten 217
 Kostenartenrechnung 363
 Kostenaspekt 215
 Kostencontrolling in Projekten 273
 Kostenerfassung 271
 Kosten-Nutzen-Analyse 350
 Kostenplanung 216
 Kostenstellenrechnung 363
 Kostenträgerrechnung 364
 Kosten- und Finanzplan 245
 Kostenverrechnung, direkte 183
 Kostenverschwendungen in der IT 28
 kritischer Pfad 253
 Kundenperspektive 4

L

Lagebericht 645
 Legal IT-Compliance 585, 612, 619
 Leistungsphase 333
 Leistungsspezifikation 361
 Leistungsverrechnung 182, 363
 Leitbilder 4
 Lenken 322
 Lenkungsausschuss 234
 Letter of Agreement 681
 Letter of Intent 680, 681
 Lieferorganisation 302
 Lieferungsprozess 383
 Lizenzaudit 676

Lizenzierung 670
 Lizenzmodell 688
 Lizenzschein 374
 Lizenzvertrag 672

M

Machbarkeitsstudie 212
 Machtpromoter 239
 MaComp 590
 Malware 598
 Managementaufgaben 7
 Managementfunktionen 7
 Management-Information 489
 Management-Memo 319
 Managementprozess 2
 Managementtätigkeit 2
 Mangel 667
 Mangelfreiheit 667
 MaRisk 614, 649
 Marketing 307
 Marketingmaßnahmen 278
 Marketing-Mix 277
 Materialkosten 260
 Maturity Level 455
 Meilensteine 231, 233, 253
 Meilenstein-Sitzung 290
 Meilenstein-Trendanalyse 273
 Memorandum of Understanding 681
 Mengenmanagement 307
 Mentor 241
 Migrationsplan 108
 Migrationsunterstützung 688
 Mitarbeitergespräch 330
 Motivation 323
 Motivieren 322
 Multiprojektmanagement 241, 280
 Multiprojektplanung 259, 284
 Multi-Tier-Entwicklung 109
 mündliche Reviews 445
 Muss-Projekte 283
 Musterverträge 658

N

Nachfrageorganisation 302
 Nachvollziehbarkeit 534
 Networking 38
 Netzplantechnik 254
 Netzwerkkonsolidierung 127
 Netzwerkprojekte 232
 Netzwerkservice 308
 Non-Compliance 586, 591, 603, 634, 636
 Non Disclosure Agreement 681
 Normen 585, 589, 592, 616, 627
 Normenreihe ISO 9000 448
 Normierungsphase 333

Nutzenaspekte 215
 Nutzungsrecht 374, 672, 675

O

OLA (Operational Level Agreement) 160
 OLAP 105
 One Page Management (OPM) 319
 Operating-Level-Agreement 602
 Operatives IT-Controlling 345
 OPM (One Page Management) 319
 Organisation 27, 296
 Organisationskultur 240
 Organisationsplan 245
 Organisationsprobleme 334
 organisatorische Qualitätsmaßnahmen 441
 Outsourcing 312
 Outsourcing-Partner 314

P

Patentrecht 670
 PDCA-Zyklus 580
 Penetration Test 560
 performance 340
 Personalauswahl 322
 Personalbemessung 311
 Personalentwicklung 3, 322, 324
 Personalkapazität 258
 Personalkosten 259
 Personalverwaltung 310
 Personentage 249
 Phasengliederung 231
 Plan-Ist-Vergleiche 272
 Planoptimierung 284
 Planungsmethodik 254
 Portfolio-Controlling 347
 Portfoliotechnik 219
 Priorisierungsverfahren 218
 Prioritäten 38
 Problem Control 156
 Problem-Management 149, 155
 Process Assessments 457
 Produktabnahmebericht 287
 Produkt-Controlling 350
 Produktfortschrittskontrolle 271
 Produktlebenszyklus 350
 Produktplanung 246
 Produktspezifischer Sicherheitsstandard 540
 Produkt-Strukturplanung 246
 Produktübergabe 287
 Professional Services 313
 Project Closing 286
 Project Office (Projektbüro) 234, 241
 Project-Services 313
 Projekte
 – Kostencontrolling 273
 – Strategierelevanz 214
 Projektablaufplan 244, 250
 Projektanbahnung 287
 Projektabschlussanalyse 288
 Projekt-Abschlussbericht 289
 Projekt-Abschlussitzung 287
 Projektantrag 213, 214
 Projektarbeit 207
 Projektaufbauorganisation 234
 Projektauftrag 213, 223
 Projekt-Auftraggeber 238
 Projektbeirat 234
 Projektberichterstattung 274
 Projekt-Berichtswesen 217
 Projektbeteiligte 234
 Projektbüro (Project Office) 241
 Projektcontroller 242
 Projekt-Controlling 241, 347
 Projektdatenbanken 347
 Projektdokumentation 289
 Projektende 207
 Projekterfahrungen 290
 Projektfortschrittskontrolle 26, 271
 Projekt-Gesamtdokumentation 289
 Projektgruppe 234
 Projektkostenarten 259
 Projekt-Kostenplanung 259
 Projektleitung 235
 Projektleitungsausschuss 240
 Projektmanagement 310
 Projektmanagementaufgaben 223
 Projektmanagementprogramme 266
 Projektmanagement-Software 278
 Projektmarketing 184, 228, 277
 Projektmarketingprozess 278
 Projektmentor 174
 Projektmitarbeiter 234
 Projektorganisation 173, 234
 Projektphasen 216, 232
 Projektplanung 246
 Projektportfolio 73, 285
 Projekt-Portfoliomanagement 280, 310
 Projekt-QS-Plan (Projekt-Qualitätsplan) 262
 Projekt-Qualitätsmanagement 241
 Projekt-Qualitätsplan (Projekt-QS-Plan) 262
 Projekt-Qualitätsplanung 261
 Projektreporting 274
 Projektressourcen 256
 Projektrisiken 212

Projekt-Risikoplanung 264
 Projektrollen 234
 Projektskizze 213
 Projektstart 225
 Projektstatus-Daten 269
 Projektsteuerung 267
 Projektstrukturplan (PSP) 244, 246
 Projektteam 173, 236
 Projektterminpläne 251
 Projekttypen 209
 Projektüberwachung 268
 Projektumfeldanalyse 225
 Projektumsetzung 217
 Projektvisionen 225, 226
 Projektvorschlag 213
 Projektzeitplan 216
 Projektziele 225, 231
 Prozess (Verwendung und Betrieb) 384
 – agiler 439
 Prozess-Architekturen 103
 Prozesskonsolidierung 124
 Prozesskostenrechnung 364
 Prozessmanagement 6
 Prozessmanager 308
 Prozessmodell 106
 Prozessorientierung 300
 Prozessqualität 434
 Prozessreifegrad-Modelle 436
 PSP (Projektstrukturplan) 244

Q

QFD-Workshops 264
 Q-Policy 107
 QS-Beauftragter 242, 262
 QS-Plan (Qualitätssicherungsplan) 245
 Qualität 407
 Qualität der Lösung
 – äußere Qualität 428
 – innere Qualität 428
 Qualitätsbezogene Kosten 409
 Qualitätsmanagement 30, 217, 403, 405, 406, 410
 Qualitätsmaßnahmen
 – analytische 442
 – konstruktive 441
 – organisatorische 441
 Qualitätsplanung 262
 Qualitätspolitik 450
 Qualitätssicherungsplan (QS-Plan) 245
 Qualitätsverbesserung 409
 Qualitätsziele 450
 Quality-in-Use 452

R

Rahmenbedingungen 213
 Rahmenverträge 307
 Rahmenwerke 300
 Rangfolgeverfahren 219
 Rechtsberatung 666
 Refactoring 418
 Referenz-Prozessmodelle 458
 Regelprozesse 209
 Release Management 149, 158
 Reporting 286, 317, 318, 645
 Requirements Provider 424
 Ressourcenbedarfsplan 256
 Ressourceneinsatzplan 256
 Ressourceneinsatzplanung 258
 Ressourcenkapazitätsplanung 257
 Ressourcenmanagement 256
 Ressourcenpläne 244
 Restrisiko 577
 Restrisikodeklaration 577
 Return on Investment 489
 Review 272, 273, 444
 – mündliches 445
 – schriftliches 445
 Risiko 548
 Risikoabwälzung 577
 Risikoakzeptanz 574
 Risikoanalyse 265
 Risikoarten 217
 Risikobehandlung 265
 Risikobewältigung 575
 Risikodokumentation 568
 Risikoeliminierung 576
 Risikoentscheidung 573
 Risikoformel 562, 566
 Risikofrüherkennung 580
 Risikograd 220
 Risikokorridor 578
 Risikolagebericht 573
 Risikomanagement 189, 217, 264, 375
 Risikomatrix 568
 Risikoplan 245
 Risikoprioritätsziffer 567, 568
 Risikoprofil 570
 Risikoszenario 555, 563
 – Best-Case-Szenario 564
 – Worst-Case-Szenario 564
 Risikotragfähigkeit 574
 Risikovermeidung 575
 Risikoverminderung 576
 Risikovorsorge 265
 Risk IT Framework 607
 ROI 28
 Rollen 303
 Rollenkonflikte 334
 Rollenkonzept 113, 236
 RPZ *siehe* Risikoprioritätsziffer

S

Sachfortschritte 271
 Sachfortschrittsabweichungen 272
 Sachfortschrittskontrolle 271
 Sachmittel 297
 Sarbanes Oxley Act 508, 599
 Scale-Up 125
 Schadenshöhe 563, 566, 568
 Schätzklausur 260
 Schichtenmodell 92
 Schiedsgericht 669
 schriftliche Reviews 445
 Schutzbedarfsanalyse 523
 Schwachstelle 552
 Schwachstellenanalyse 560
 Schwerpunkt-Memo 319
 SCMM *siehe* Security Capability Maturity Model
 Scorecards 286
 Security Capability Maturity Model 525
 Security Landscape 527
 Security Policy Management 540
 Security Service Level Agreement 544
 sequenzielles Dilemma 415
 sequenzielle Entwicklung 414
 Server, Kapazitätsoptimierung 125
 Serverkonsolidierung 125
 Service Delivery 149
 Service Delivery-Prozesse 159, 164
 Service Desk 153, 308
 Serviceelemente 366
 Servicekataloge 366
 Servicekultur 178
 Service-Level-Agreement 170, 360, 602, 611, 618, 688
 – ergebnisbezogene 362
 – potenzialbezogene 362
 – prozessbezogene 362
 Service Level Management 149, 160
 Servicemodule 366
 Service-Prozessverantwortliche 308
 Service Support 149, 153
 Shared Service Center 368
 Sicherheitsarchitektur 67
 Sicherheitsklassen 535
 Sicherheitsorganisation 514
 Sicherheitsrelevantes Ereignis 555
 Sicherheitsstrategien 536
 Single-Tier-Entwicklung 109
 Six-Sigma 368

SLA (Service Level Agreements) 160
 Soft Factors 192
 Software-Einführungsprojekte 232
 Software-Entwicklung 677
 Software-Entwicklungsprojekte 232
 Software-Ingenieur 115
 Software-Konsolidierung 128
 Software-Lizenzierung *siehe* Lizenzierung
 Software- und Netzwerkdienste, Standardisierung 123
 Soll-Ist-Vergleich 268, 279
 Soll-Projekte 284
 Speicherkonsolidierung 126
 Speichermanagement 126
 SSLA *siehe* Security Service Level Agreement
 Stakeholderanalyse 228
 Stakeholdermanagement 228
 Standards 586, 589, 592, 609, 616
 – Festlegung 129
 Standard-IT-Projekte 284
 Standardisierung 87, 88
 Standish Group, Chaos Report 404
 Start-up-Workshop 225, 226
 Startveranstaltungen 225
 Startzeitpunkt 251
 Statusabgleich 269
 Statuserfassung 269
 Statusmeldung 270
 Stellen 310
 Stellenaufgaben 310
 Stellenbemessung 311
 Stellenbeschreibung 310
 Stellenbildung 303, 310
 Stelleninhaber 310
 Steuervereinfachungsgesetz 2011 653
 Storage-Konsolidierung 126
 Strategic Alignment 24, 88
 Strategie 42
 Strategierelevanz 214
 strategische Grundsätze 62
 Strategisches IT-Controlling 344
 Systementwicklungsprozess 108
 Systemintegration 109
 Systemmanagement 598

T

TCO-Verfahren 316
 Teamarbeit 208
 Teambildung 208, 236, 237, 332
 Teamentwicklung 332
 Teamklima 335
 Teamkultur 335
 Teammanagement 332
 Technologie-Architektur 24, 67
 Technologiemanagement 3
 Teilkostenrechnung 364
 Teilpläne 244
 Telekommunikationsgesetz 613, 628
 Telemediengesetz 613, 623
 Terminabweichungen 272
 Terminliste 252
 Terminplan 244
 Terminplanungsmethoden 256
 Termin-Trendanalyse 273
 Test 109
 Teufelsquadrat 431
 Tools für IT-Projektcontrolling 26
 Total-Cost-of-Ownership 192, 316

U

UfAB 660
 Umlageverfahren 182
 Unternehmensarchitektur 24
 Unternehmensführung 16, 239
 Unternehmensleitbild 43
 Unternehmensprozesse 6
 Unternehmensstrategie 13, 44
 Unternehmensziele 4
 Urheberrecht 670, 674
 Urheberrechtsgesetz 613, 625, 626

V

Verbindlichkeit 534
 Verdingungsordnungen 655
 Verfahren
 – nicht offenes 656
 – offenes 655
 Verfahrensarten 655
 Verfügbarkeit 532
 Verfügbarkeitsmanagement 161
 Vergaberecht 654
 Vergabeverfahren 660
 Vergabeverordnung 655
 Vergütungsmodelle 685
 Verhaltenskodex 594, 611
 Verhandlungsverfahren 656

Verrechnungspreis
 – Art 186
 – Grundlagen und Einführung 184
 – kostenorientierte 184
 Vertrag 682
 Vertragsbedingungen 663
 Vertragsfreiheit 664
 Vertragsmanagement 307
 Vertraulichkeit 533
 Vertrieb 307
 Verwaltung der IT 310
 Visionen 38
 Vision-Map 227
 V-Modell 414
 §25 VOL/A 660
 Vollkostenrechnung 259, 364
 Vorgangsliste 250, 251
 Vorgehensmodell 216, 420
 Vorstudie 212
 Vorvertrag 681
 Vulnerability Scanning 560

W

Wartbarkeit 422
 Werklieferungsvertrag 667, 683
 Werkvertrag 678, 683
 Wertbeitrag der IT 599, 606
 wettbewerblicher Dialog 656
 Wettbewerbsvorteil 489
 Whistleblower-Hotline 652
 Wirksamkeit 220
 – der IT 18
 Wirtschaftlichkeit 11, 220
 Wirtschaftlichkeitsbetrachtung 350
 Wirtschaftlichkeitsbeurteilung 221
 Wirtschaftlichkeitsüberlegungen 215
 Wirtschaftsprüfer 600, 605, 608, 612
 Wissensmanagement 290

Z

Zeitschätzwert 248
 Zielanalyse 108
 Zielarchitektur 24, 88
 Zielgrößen 224
 Zielsystem 231
 Zielvereinbarungen 328
 Zivilprozessordnung 613, 622
 Zugriffskontrolle 597

Alles für IT-Projektmanager



Tiemeyer (Hrsg.)

Handbuch IT-Projektmanagement

Vorgehensmodelle, Managementinstrumente, Good Practices

714 Seiten.

ISBN 978-3-446-42192-9

Die deutliche Mehrheit der IT-Projekte sprengt nach wie vor den Kosten- oder Zeitrahmen oder wird abgebrochen. Wer seine IT-Projekte erfolgreich abschließen will, muss ein breites Praxiswissen haben. Das reicht von Kenntnissen darüber, wie Projekte geplant, beantragt und gestartet werden, über die Fähigkeit, Teams zu bilden und zu führen bis hin zu komplexen Management-Aufgaben wie Risikomanagement, Stakeholdermanagement, Qualitätsmanagement, Projekt-Marketing und mehr.

In diesem Handbuch haben 16 in der Wirtschaft und an Hochschulen tätige Autoren ihre vielfältigen Erfahrungen zusammengefasst. Sie geben Ihnen einen vertieften Einblick in die für die Projektarbeit notwendigen Methoden, Instrumente und Führungstechniken. Egal, mit welcher Art von IT-Projekt Sie sich befassen, mit diesem Handbuch können Sie sich alle wesentlichen Teilgebiete und Prozesse im IT-Projektmanagement gezielt erschließen. Die zahlreichen Tipps und Beispiele aus der Praxis versetzen Sie in die Lage, IT-Projekte erfolgreich zu starten, zu leiten und zu steuern.

Mehr Informationen zu diesem Buch und zu unserem Programm unter **www.hanser.de/computer**

Enterprise Architecture Management im Griff.



Hanschke
**Strategisches Management
der IT-Landschaft**

Ein praktischer Leitfaden für das
Enterprise Architecture Management
470 Seiten.

ISBN 978-3-446-42257-5

Die IT spielt für den Erfolg eines Unternehmens eine ganz entscheidende Rolle. Nur wenn die IT-Landschaft an den Business-Zielen ausgerichtet ist, kann ein Unternehmen erfolgreich im Markt agieren und auf die großen Herausforderungen wie Globalisierung, Fusionen und immer kürzere Innovationszyklen rasch und flexibel genug reagieren.

In diesem Buch erfahren Sie, wie Sie als IT-Manager oder CIO Ihre IT-System-Landschaft am Business ausrichten und erfolgreich planen und steuern. Die relevanten Kernaufgaben dabei sind das IT-Bebauungsmanagement und das technische Architekturmanagement.

Die praktischen Anleitungen und Best Practices versetzen Sie in die Lage, Ihrem Unternehmen eine IT-Unterstützung für das Business zu marktgerechten Preisen anzubieten, die flexibel auf Veränderungen reagieren kann.

Mehr Informationen zu diesem Buch und zu unserem Programm
unter www.hanser.de/computer

HANDBUCH IT-MANAGEMENT //

- Lernen Sie die Methoden und Techniken für erfolgreiches IT-Management kennen
- Aktuelles Wissen und praktische Tipps, die Sie in Ihrem Berufsalltag umsetzen können
- Profiwissen für erfahrene und werdende IT-Manager
- Von 13 Experten aus Unternehmenspraxis, Consulting-Firmen und Hochschulen
- Neu in der 4. Auflage: Kapitel zu IT-Compliance sowie IT-Lizenzmanagement

Informationstechnik (IT) hat inzwischen so gut wie alle Geschäftsbereiche durchdrungen. Die IT ist zum unverzichtbaren Enabler von Geschäftsprozessen geworden. So ist erfolgreiches IT-Management inzwischen einer der wichtigsten Erfolgsfaktoren für jedes Unternehmen und deshalb nehmen IT-Manager in Unternehmen eine ganz zentrale Rolle ein.

Damit Sie als IT-Manager für die Praxis gerüstet sind, stellt dieses Handbuch umfassendes, aktuelles und unverzichtbares Wissen aus allen Bereichen des IT-Managements zur Verfügung. Die Autoren vermitteln Ihnen die Fähigkeit zur Entwicklung von IT-Strategien und zur Planung von IT-Architekturen sowie fundiertes Wissen zu Managementthemen und Führungsaufgaben. Sie erhalten einen Überblick über wichtige Handlungsfelder der IT und Unterstützung bei der Nutzung bewährter Methoden und Instrumente im IT-Management.

Neu in der 4. Auflage: Die Kapitel »IT-Compliance« und »IT-Lizenzmanagement« machen Sie mit der Einhaltung aller wichtigen Richtlinien vertraut und geben Ihnen wertvolle Tipps für den effizienten – und damit kostengünstigeren – Umgang mit Software.

»Die Autoren verstehen es, ihre jeweiligen Spezialgebiete umfassend und präzise darzustellen. In der Regel ergänzen sie theoretische Ausführungen durch konkrete Hinweise aus der Praxis. So vermittelt das Handbuch solides Fachwissen über das ganze Spektrum des IT-Managements.« c't

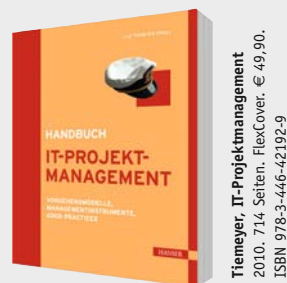
MIT BEITRÄGEN VON //

Werner Bachmann · Robert Bergmann · Torsten Groll · Michael Klotz · Dietmar Kopperger · Helmut Krcmar · Jörg Kunsmann · Andreas Nehfort · Klaus Schmidt · Andreas Roland Schwertsik · Ernst Tiemeyer · Anette Weisbecker · Walter Wintersteiger

AUS DEM INHALT //

- IT-Strategien
- Enterprise Architecture Management
- IT-Servicemanagement
- IT-Projektmanagement
- Organisation und Führung im IT-Bereich
- IT-Controlling
- IT-Lizenzmanagement
- IT-Qualitätsmanagement
- IT-Governance
- IT-Security-Management
- IT-Risikomanagement
- IT-Compliance
- Rechtliche Rahmenbedingungen für das IT-Management

UNSER BUCHTIPP FÜR SIE //



Tiemeyer, IT-Projektmanagement
2010. 714 Seiten. FlexCover. € 49,90.
ISBN 978-3-446-42192-9

HANSEN

