Manuela Reiss
Georg Reiss

Praxisbuch IT-Dokumentation

Betriebshandbuch, Systemdokumentation und Notfallhandbuch im Griff

ADDISON-WESLEY

CD

Praxisbuch IT-Dokumentation

Praxisbuch IT-Dokumentation

Manuela Reiss
Georg Reiss

ADDISON-WESLEY
An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

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.

10 9 8 7 6 5 4 3 2 1

11 10 09

ISBN: 978-3-8273-2681-2

ein Imprint der Pearson Education Deutschland GmbH,
Martin-Kollar-Straße 10–12, D-81829 München/Germany

Fachlektorat und Korrektorat: René Wiegand, info@wiegand-dokumentation.de
Lektorat: Sylvia Hasselbach, shasselbach@pearson.de
Herstellung: Philipp Burkart, pburkart@pearson.de
Satz: Andreas Franke, SatzWERK, Siegen, www.satz-werk.com
Druck und Verarbeitung: Kösel, Krugzell (www.KoeselBuch.de)
Printed in Germany

Inhaltsverzeichnis

V

Vorwort

Das IT-Projekt ist erfolgreich abgeschlossen, die Abnahmen sind gegengezeichnet, die Geschäftsleitung hat den Produktivstart zustimmend zur Kenntnis genommen, und die in das Projekt eingebundenen Mitarbeiter können sich wieder vollständig dem Betriebsalltag widmen. Dann meint noch jemand, dass man ein Betriebshandbuch erstellen müsse – der guten Ordnung halber.

Aber warum um alles in der Welt braucht man jetzt noch ein Betriebshandbuch? Die Administratoren und die Key-User waren selbstverständlich im Projekt beteiligt und wenden die neuen Prozesse direkt in der Praxis an, und die Standard-Benutzer sind natürlich alle geschult. Außerdem ist das Projekt-Budget sowieso schon überschritten und der vorgesehene Anteil für die Erstellung einer Betriebsdokumentation bereits für die verlängerten Integrationstests verbraucht. Eine gesetzliche Verpflichtung für die Erstellung einer Betriebsdokumentation gibt es ebenfalls nicht, also könne man doch auch die Projektdokumentation verwenden.

Die Auffassung, die Projektdokumentation „tue es doch auch", ist jedoch ein Irrglaube. Aus nachvollziehbaren Gründen weicht die Projektdokumentation deutlich von einer Dokumentation des Betriebs ab.

Während im Projekt die wesentlichen Aufgaben in der Planung, Entwicklung, Testen und schließlich in der Implementierung liegen, ist der Betrieb durch die routinemäßige Anwendung, deren Kontrolle und gegebenenfalls die Anpassung

und Optimierung sowie die Störungsbeseitigung geprägt. Nicht nur ablauforganisatorisch, sondern auch aufbauorganisatorisch bestehen wesentliche Unterschiede zwischen Projekten und dem Betrieb. So gibt es nicht ohne Grund eine dezidierte Projektorganisation, in der zum einen unternehmensinterne Mitarbeiter häufig eine andere Rolle haben als im Regelbetrieb, und zum anderen in der Regel externe Beratungskräfte beschäftigt sind, die für den nötigen Know-how-Transfer sorgen sollen. So stellt das Projekt eine vom Betrieb abweichende Sondersituation dar.

Aber spätestens, wenn der IT-Betrieb einer Qualitätsüberprüfung unterzogen werden soll oder eine Zertifizierung anstrebt, wird die Erstellung einer Betriebsdokumentation eine unabdingbare Voraussetzung für einen erfolgreichen Abschluss. Aber auch rechtliche Regularien stellen bereits überraschend hohe Anforderungen an die Dokumentation.

Welche Anforderungen muss eine IT-Betriebsdokumentation erfüllen? Eine klare und eindeutig abgegrenzte Anforderungsbeschreibung gibt es weder in den Gesetzen, Richtlinien und Normen noch in den internationalen Vorgehensmodellen für den IT-Bereich. Daher werden in Kapitel 1, „Anforderungen an die IT-Dokumentation", die wesentlichen rechtlichen Ansätze vorgestellt und auf die IT-Dokumentation übertragen. Weiter werden die wesentlichen internationalen Vorgehensmodelle wie COBIT und ITIL beleuchtet und Anforderungen für die IT-Dokumentation abgeleitet. Auch der revisorische Ansatz auf Basis der international und national gültigen Richtlinien wird dargelegt, da Revisionssicherheit und Compliance Schlagworte mit einer immer höheren Bedeutung sind.

Was ist überhaupt ein Betriebshandbuch? Genauso wenig wie es konkrete Anforderungen an die Betriebsdokumentation gibt, so wenig sind die Begriffe normiert. In Kapitel 2, „Bausteine einer IT-Dokumentation", erfolgt deshalb sowohl eine logische als auch eine inhaltliche Abgrenzung der wesentlichen Schlüsselbegriffe in diesem Buch, wie beispielsweise Projekt, Betrieb und Betriebshandbuch.

Was muss im IT-Betrieb alles dokumentiert werden? Sicherlich ist es nicht sinnvoll, jeden kleinen Ablaufschritt zu dokumentieren. Auch hier gilt der Wirtschaftlichkeitsgrundsatz, wonach das Ergebnis in einem angemessenen Verhältnis zum Aufwand stehen sollte. In Kapitel 4, „Dokumentation des IT-Betriebs" wird daher eine auf die wesentlichen IT-Prozesse bezogene Übersicht über die erforderlichen Dokumente gegeben und – abgeleitet aus den Anforderungen – der Inhalt dieser Dokumente beschrieben. Der prozessorientierte Ansatz bei der IT-Dokumentation ergibt sich daraus, dass nahezu alle Qualitätsaudits und Zertifizierungen die Prozessbewertung in den Vordergrund stellen. Somit muss ebenfalls die *Betriebsdokumentation* prozessorientiert sein. Trotzdem muss es zusätzlich auch eine Systemdokumentation der eingesetzten Hard- und Softwaresysteme geben, die als Bestandsnachweis fungiert und auf die in den *Prozessbeschreibungen* bei Bedarf verwiesen wird.

Und was ist im Notfall? Einen Sonderfall des Betriebs stellt der Notfall dar, da hier die gewohnten Regelabläufe in der Regel nicht mehr funktionieren und die Verfügbarkeit der IT-Systeme zumindest stark eingeschränkt oder gar nicht gegeben

ist. Da der Notfall auch bedrohend für das Unternehmen sein kann, ist eine zielgerichtete Dokumentation der durchzuführenden Notfallmaßnahmen und der dafür notwendigen Organisationsstrukturen in Gestalt eines Notfallhandbuches dringend geboten. Was bei der Notfalldokumentation zu beachten ist und welche Dokumente im Rahmen der *Notfallvorsorge* bzw. der *Notfallbewältigung* benötigt werden, ist Schwerpunkt von Kapitel 5, „Dokumentation für den Notfall".

Gibt es noch etwas zu dokumentieren? Nicht nur der IT-Betrieb und der Notfall sind zu dokumentieren. Auch im Rahmen von Projekten, sei es zur Einführung neuer Verfahren oder IT-Systeme oder der Optimierung des IT-Betriebe, sind Planung, Durchführung, Tests und Implementierung bedarfsgerecht zu dokumentieren. Wie eine Projektdokumentation sinnvoll in die IT-Dokumentation eingebunden werden kann, wird in Kapitel 6, „Dokumentation von IT-Projekten" erläutert.

Wie wird das alles aufeinander abgestimmt? Es ist leicht nachvollziehbar, dass die Dokumente der zuvor angesprochenen Bereiche nicht isoliert erstellt werden können. Viele haben einen mehr oder weniger direkten Bezug zueinander. Es müssen also Regelungen getroffen werden, die das Zusammenspiel der Dokumente untereinander sicherstellen. Hierzu werden in Kapitel 3 die sog. Rahmendokumente beschrieben, die eine Klammer für die anderen Dokumente darstellen. In den Rahmendokumenten werden allgemeingültige Vorgaben, wie z. B. Namenskonventionen oder Dokumentationsrichtlinien beschrieben, die für alle bzw. eine Gruppe von Dokumenten Gültigkeit haben. Ohne diese Rahmenvorgaben funktioniert eine IT-Dokumentation höchstens stark eingeschränkt und kann ihre eigentlichen Vorteile wie die Grundlage zur Prozessoptimierung und zur schnellen Nachvollziehbarkeit nicht entfalten.

Wie können Dokumente optimiert erstellt und verwaltet werden? In Kapitel 7, „Dokumente erstellen und verwalten in der Praxis", steht nicht mehr die Frage im Vordergrund „Was ist zu dokumentieren?", sondern die Frage „Wie erstelle ich ein Dokument?" bzw. „Welche Punkte müssen beachtet werden, um anforderungsgerechte Dokumente zu erstellen?".

Gute Dokumente können nicht ohne die Einbindung in ein Regelwerk entstehen. Gerade in komplexen IT-Bereichen nimmt die Betriebsdokumentation einen erheblichen Umfang an Dokumenten an. In diesem Kapitel werden zunächst Vorschläge für eine einheitliche Dokumentenstruktur zusammengestellt. Einen weiteren Schwerpunkt des Kapitels bilden die Erläuterungen zur Erstellung einer Dokumentationsrichtlinie. Eine solche Dokumentationsrichtlinie darf nicht nur Vorgaben für die Einzeldokumente enthalten, sondern muss auch die Verwaltung und Speicherung der Gesamtdokumentation regeln. Je mehr Dokumente aber entstehen, desto wichtiger ist es, diese so abzulegen, dass alle schnell gefunden werden können und jeder auf die von ihm benötigten Dokumente Zugriff hat. Auch hierzu möchte das Kapitel Anregungen liefern.

Dokumentationsrichtlinien allein reichen aber nicht. In der Praxis werden konkrete Hilfen wie Dokumentvorlagen und Anleitungen für den Einsatz benötigt. Dabei ist es unter Beachtung einiger wichtiger Punkte durchaus auch für weni-

ger Geübte möglich, anforderungsgerechte Dokumente zu erstellen. Diese Hilfestellungen bietet das Kapitel und liefert unter anderem konkrete Hinweise für die Arbeit mit Microsoft Word.

Die Erstellung eines Dokuments darf aber nicht nur aus formaler Sicht betrachtet werden. Viele Fehler passieren im organisatorischen Bereich. Wurden beispielsweise bei der Informationssammlung wichtige Vorläuferdokumente übersehen und daher nicht berücksichtigt, kann auch ein perfektes formales Dokument die inhaltlichen Mängel nicht mehr ausgleichen. Kapitel 7 bietet deshalb auch Hilfen und Anregungen zur Optimierung der Vorgehensweise bei der Erstellung von Dokumenten, beispielsweise durch Einsatz von Mind Maps.

Welche Tools unterstützen die IT-Dokumentation? Je umfangreicher die Anzahl an Dokumenten und je größer die Komplexität der Abhängigkeiten ist, desto stärker ist das Erfordernis nach einer zentralen IT-gestützen Datenhaltung und Tool-Unterstützung bei der Dokumentation.

So werden begleitend in den Kapiteln Frontend-Tools wie MindManager, DocuSnap und SemTalk als auch die SharePoint Services von Microsoft als Dokumentations- und Datenhaltungstools vorgestellt. Entsprechend der hohen Marktverbreitung haben wir uns auf Windows-Tools konzentriert. Funktional gleichartige Software ist selbstverständlich auch in einer Unix-basierten Systemumgebung zu finden.

Gibt es Musterdokumente? Nachdem die formalen Anforderungen, der Aufbau und die wesentlichen Inhalte der Dokumente in den ersten sieben Kapiteln herausgearbeitet wurden, werden in Kapitel 8 Praxishilfen in Form von Beispielen, Mustern und Checklisten angeboten. Die Vorlagen haben bereits einen relativ hohen Detaillierungsgrad und können angepasst werden. Sie liegen auf der beigefügten Buch-CD im originalen Word-Format vor. Weiter befindet sich auf der CD die komplette Mind Map aller im Buch in den einzelnen Kapiteln dargestellten Mind Maps. Hieraus kann bei Bedarf mit wenig Aufwand eine Blaupause für eine komplette IT-Dokumentation erstellt werden.

Darüber hinaus liefert die Tabelle *Literatur und Links* in Anhang B eine Reihe von Verweisen auf nützliche Internetseiten und weiterführende Bücher. Im Buch stehen die dazugehörenden Literaturverweise in eckigen Klammern.

Fazit: Abgeleitet aus den Erfordernissen der Gesetze Normen und Standards sowie den methodischen Ansätzen der Vorgehensmodelle entwickeln und beschreiben wir für die Bereiche Betrieb, Projekt und Notfall die wesentlichen Bausteine einer anforderungsgerechten IT-Dokumentation. Eine angemessene IT-Dokumentation sollte diese drei Bereiche umfassen. In welchem Umfang und Detaillierungsgrad diese realisiert wird, hängt wesentlich von der Unternehmensgröße und der Komplexität der IT-Anwendungen ab. Insofern stellen die dargestellten Teile einer IT-Dokumentation ein Angebot dar, aus dem für jedes Unternehmen gesondert das Portfolio an Dokumentationsbestandteilen festgelegt werden muss.

Insgesamt bietet das Buch ein Angebot an alle Entscheider und an alle in den IT-Bereichen zuständigen Mitarbeiter, die eine IT-Dokumentation erstellen wollen oder müssen. Die Umsetzung der in dem vorliegenden Buch beschriebenen Dokumentationsbausteine im eigenen Unternehmen bietet eine gute Voraussetzung, den zunehmenden rechtlichen und den immer wichtigeren Anforderungen aus Zertifizierungsprogrammen gewachsen zu sein.

Über die Autoren

Manuela Reiss ist seit mehr als 16 Jahren selbstständig tätig als Beraterin, Trainerin und Fachbuchautorin im Microsoft Windows-Umfeld. Ihr Fachwissen hat sie sich in zahlreichen Zertifizierungsprogrammen vor allem bei Microsoft erworben. So ist sie u.a. Microsoft Certified Systems Engineer (MCSE) für mehrere Versionen von Windows-Serversystemen. Darüber hinaus verfügt Sie über langjährige praktische Erfahrungen, die sie in zahlreichen Projekteinsätzen in den Bereichen Administration und Support, schwerpunktmäßig im Banken- und Telekommunikationsumfeld sowie in der öffentlichen Verwaltung erworben hat.

In den vergangenen Jahren hat sie sich im Rahmen der Beratertätigkeit verstärkt auf die Bereiche Konzeption und Dokumentation spezialisiert und deckt damit das breite Spektrum von der theoretischen Konzeptionierung über eine prozessorientierte Planung bis hin zur praktischen Umsetzung ab. Als zertifizierte Projektmanagement-Fachfrau (GPM) unterstützt sie Firmen im Bereich Projektmanagement und bei der Implementierung von IT-Prozessen sowie bei allen Fragen rund um das Thema Dokumentation.

Daneben hat sie sich als Fachbuchautorin einen Namen gemacht und an mehreren Fachbüchern für den Verlag Addison-Wesley mitgearbeitet. Außerdem ist sie seit vielen Jahren als Herausgeberin für den WEKA-Verlag tätig. Ihre fachlichen Schwerpunkte liegen hierbei vor allem in der Administration und Migration heterogener Windows-Netzwerke, sowie im Bereich Troubleshooting von Windows Server- und Client-Systemen.

Georg Reiss ist Dipl. Kaufmann und stellvertretender Bereichsleiter der internen Revision in einem großen Konzern der öffentlichen Verkehrs- und Energieversorgung. In seiner mehr als 15-jährigen Berufspraxis hat er als IT-Revisor die unterschiedlichen Aspekte der IT-Infrastruktur sowohl von der administrativen als auch von der rechtlichen, organisatorischen und wirtschaftlichen Seite analysiert und bewertet. Die Nachvollziehbarkeit von Prozessen und somit auch die Qualität der Dokumentation ist dabei einer seiner Kernanforderungen. Als Revisor ist er in der Lage IT-Themen neutral zu analysieren und ausgewogen zu beurteilen.

1 Anforderungen an die IT-Dokumentation

Die Erstellung und Pflege einer Dokumentation ist nicht nur bei der Ersterstellung, sondern auch bei der permanenten Pflege eine Aufgabe, die nicht unwesentliche Personalressourcen und Arbeitsmittel erfordert und somit entsprechende Kosten verursacht. Damit ein Unternehmen diesen Aufwand betreibt, muss es entweder den Vorteil für seine Organisation oder die Notwendigkeit hierzu erkennen.

Einen allgemein gültigen Standard, was in eine IT-Dokumentation aufzunehmen ist, oder gar ein gesondertes Dokumentationsgesetz gibt es nicht. In der Praxis gibt es vielmehr unterschiedliche Motivationen für die Erstellung und Vorhaltung einer Dokumentation, die deren Inhalt und Aufbau prägen.

Warum überhaupt dokumentieren?

In einer von Personalabbau, Effizienzsteigerung und Kosteneinsparung geprägten Zeit ist die Realisierung einer effektiven und schlanken Organisation eine wesentliche Motivation für die Vorhaltung einer Dokumentation. Prozesse lassen sich nur optimieren, sofern sie dokumentiert sind. Undokumentierte Prozesse stehen unter dem Risiko, dass die agierenden Personen ihre Aufgaben nach eigenem Gutdünken variieren und damit heute so und morgen so agieren. Hierdurch wird neben anderen Faktoren die Messbarkeit des Erfolgs stark erschwert oder sogar verhindert.

Modelle

Zur Optimierung der IT-Organisation, also der Aufbau- und Ablauforganisation, haben sich verschiedene Modelle wie ITIL oder COBIT durchgesetzt. Sie stellen in der Regel ein Baukastensystem (Framework) zur Verfügung, in dem die IT-Organisation segmentiert wird und deren Hauptprozesse entsprechend der Ausrichtung der Modelle beschrieben sind. Die IT-Modelle stellen somit ein internes Gestaltungswerkzeug dar. Diese Modelle werden in Abschnitt 1.3 näher erläutert.

Da die IT-Modelle nach innen gerichtete Werkzeuge darstellen, besteht eine weitere Motivation für die Vorhaltung einer Dokumentation in der außenwirksamen Präsentation der IT-Organisation. Es entsteht ein immer größerer Druck, den Kunden und potenziellen Kunden deutlich zu machen bzw. nachzuweisen, dass die eigene IT-Organisation am besten geeignet ist, den Kundenanforderungen zu entsprechen.

Normen und Standards

Der Nachweis dieser Eignung wird mittels Zertifizierungsverfahren, zum Beispiel nach ISO 9000 oder nach BSI-Grundschutz, durchgeführt. Entsprechend der kundenorientierten Ausrichtung steht bei diesen Zertifizierungen weniger die Effizienz, sondern mehr das Qualitätsmanagement der zu prüfenden Organisation im Vordergrund. Demzufolge sind die zu zertifizierenden Arbeitsabläufe auch nicht so feinteilig zu dokumentieren wie bei einem Modell zur Prozessoptimierung. Da diese Regelwerke und die darauf basierenden Zertifizierungen allgemein anerkannt sind, werden sie auch als *Normen* oder *Standards* bezeichnet.

Zusätzlich gibt es Standards, die sozusagen eine interne Zertifizierung zum Ergebnis haben. Wesentlich in diesem Zusammenhang sind die Prüfungsstandards des Instituts der Wirtschaftsprüfer (IDW), insbesondere der Standard IDW 330 für die Beurteilung des IT-Betriebs. Weiter wichtig sind die Prüfungsstandards des Deutschen Instituts für Interne Revision (DIIR), nach denen die meisten Revisionsorgansisationen in Deutschland auch die IT prüfen. Die für die IT wesentlichen Standards werden in Abschnitt 1.2 beschrieben.

Gesetzliche Regelungen

Entgegen der landläufigen Meinung gerade auch vieler erfahrener IT-Administratoren gibt es eine Reihe von gesetzlichen Regelungen, aus denen sich direkt oder indirekt Anforderungen an die IT-Dokumentation ergeben. So stellen bereits die IT-bezogenen *Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS)* oder dass *Bundesdatenschutzgesetz (BDSG)* konkrete Anforderungen, aus denen sich entsprechende IT-Dokumente ableiten lassen.

Mit dem amerikanischen Sarbanes-Oxley Act (SOX) und dem europäischen Pendant „8. EU-Richtlinie“ (Euro-SOX) wurden in den letzten Jahren Regelungen mit Gesetzeskraft verabschiedet, die einen erheblichen Einfluss auf die vorzuhaltende IT-Dokumentation haben. Wenn auch die meisten gesetzlichen Regelungen von kaufmännischen Grundsätzen, wie dem Gläubigerschutz getrieben sind, so haben sie dennoch für die IT eine direkte Bedeutung, da die kaufmännischen Kernprozesse wie Buchhaltung und Einkauf in aller Regel IT-gestützt ablaufen (z. B. die ERP-Anwendung SAP). Einen Überblick über die für die IT-Dokumentation relevanten gesetzlichen Regelungen finden Sie in Abschnitt 1.1.

Aus den Ausführungen lassen sich drei Anforderungsgruppen für die IT-Dokumentation ableiten:

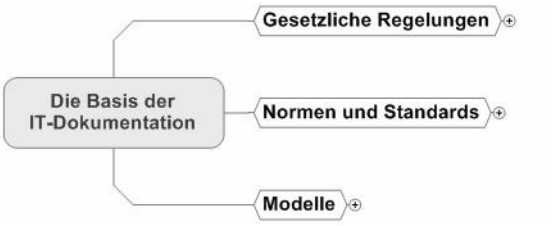


Abbildung 1.1: Anforderungen an die IT-Dokumentation kommen aus verschiedenen Bereichen.

Empfehlungen für die Dokumentation

Da es, wie gesagt, keinen allgemein gültigen Standard oder gar ein Gesetz für die IT-Dokumentation gibt, ist es erforderlich, entsprechend den Erfordernissen der eigenen IT-Organisation und insbesondere auch der strategischen Unternehmensausrichtung Anforderungen an die IT-Dokumentation zu formulieren. In Abschnitt 1.4 werden – abgeleitet aus den Gesetzen, Standards und Modellen – Anforderungen an eine IT-Dokumentation beschrieben, die den gesetzlichen Vorgaben entsprechen und die wesentlichen Grundlagen für eine Prozessoptimierung sowie für eine eventuell angestrebte Zertifizierung darstellen.

cd-rom

Auf der beigefügten CD-ROM befindet sich eine mit MindManager erstellte Datei, die alle im Folgenden vorgestellten Gesetze, Standards und Modelle grafisch in einer Übersicht darstellt und eine Betrachtung der einzelnen Bereiche in einer Zusammenschau ermöglicht. Mit dem ebenfalls beigefügten MindManager Viewer kann diese Datei angesehen werden. Außerdem ist es möglich, Zweige zu öffnen, zu schließen und in sie hineinzuzoomen.

1.1 Gesetzliche Regelungen

Da es kein Gesetz gibt, das die Anforderungen an die IT-Dokumentation umfassend und eindeutig regelt, werden die für die IT-Dokumentation wesentlichen Gesetze in vier Gruppen zusammengefasst und erläutert.

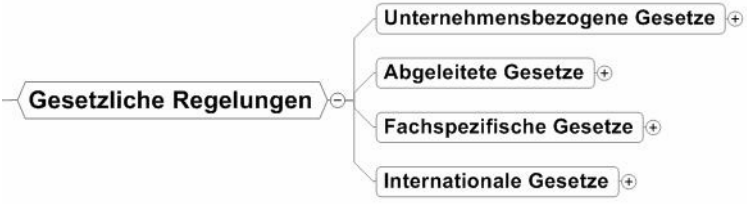


Abbildung 1.2: Unterteilung der Gesetze in Gruppen

Zunächst wird auf die für ein Unternehmen allgemein wichtigen Gesetze wie das *Aktiengesetz*, das *Handelsgesetzbuch* sowie die *Abgabenordnung* eingegangen. Sie bilden die gesellschaftsrechtliche Klammer und haben einen mehr oder weniger großen Einfluss auf die IT-Dokumentation.

Aus den genannten Gesetzen sind dann weitere Regelungen und Auslegungen entstanden, die ebenfalls Gesetzescharakter haben. Zu nennen sind hier insbesondere die *GoBS* und *KonTraG*, die eine die Gesetze präzisierende Regelungssammlung darstellen.

Außerdem gibt es fachspezifische Gesetze wie das *Bundesdatenschutzgesetz (BDSG)* und die *Mindestanforderungen an das Risikomanagement* (*MaRisk*), die für Kreditinstitute und vergleichbare Finanzdienstleister verbindlich sind. Da auch viele mittelständische Unternehmen Konzernstrukturen haben und ein explizites Konzernfinanzierungsmanagement (Treasury) betreiben, verankern sie die MaRisk in ihrem Unternehmensregelwerk. In diesen gesetzlichen Regelungen sind bereits konkrete Anforderungen an die IT-Dokumentation normiert.

Schließlich wird auf die internationalen Gesetze wie *SOX* und die *8. EU-Richtlinie* eingegangen, die eine umfassende Rückwirkung auf die IT-Dokumentation haben. Das amerikanische SOX ist deshalb auch für deutsche Unternehmen relevant, weil sich die Anwendbarkeit von SOX auf alle Unternehmen erstreckt, die entweder an einer amerikanischen Börse notiert sind oder als ein Tochterunternehmen eines amerikanischen Unternehmens agieren.

1.1.1 Unternehmensbezogene Gesetze

Bei den unternehmensbezogenen Gesetzen sind aus Sicht der IT-Dokumentation im Wesentlichen drei Gesetze wichtig:

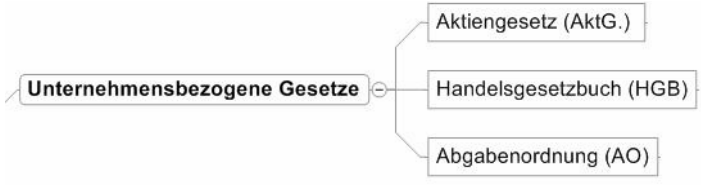


Abbildung 1.3: Wichtige Gesetze für Unternehmen

1.1.1.1 Aktiengesetz

Das Aktiengesetz beschreibt die gesetzlichen Anforderungen an eine Aktiengesellschaft und regelt unter anderem die Aufgaben der Organe der Aktiengesellschaft.

Danach haben die Vorstandsmitglieder bei ihrer Geschäftsführung „*die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden*“ (§ 93 AktG Satz 1). Weiter hat der Vorstand geeignete Maßnahmen zu treffen. „*Insbesondere ist ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden*“ (§ 91 AktG Satz 2).

Während Ersteres bereits auf eine ordnungsgemäße und damit nachvollziehbare Geschäftsführung hinweist, ist die zweite Forderung eine klare Aufforderung, ein geeignetes Risikomanagementsystem einzurichten. Diese zweite Forderung ist erst 1998 in das Gesetz mit aufgenommen worden und bildet die Basis für das *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)*, das in Abschnitt 1.1.2 beschrieben wird [GESETZE].

1.1.1.2 Handelsgesetzbuch (HGB)

Während das Aktiengesetz die Aktiengesellschaft zum Gegenstand hat, regelt das Handelsgesetzbuch (HGB) die Rechtsverhältnisse der Kaufleute, also im Wesentlichen der handelnden Personen. Es bildet einen wesentlichen Teil des Handelsrechtes in Deutschland [GESETZE].

Im Dritten Buch des HGB sind die Vorschriften für das Führen der Handelsbücher enthalten. So ist in § 238 Abs. 1 geregelt, dass die Buchführung so beschaffen sein muss, *„dass sie einem sachverständigen Dritten innerhalb angemessener Zeit einen Überblick über die Geschäftsvorfälle und über die Lage des Unternehmens vermitteln kann. Die Geschäftsvorfälle müssen sich in ihrer Entstehung und Abwicklung verfolgen lassen."* Gemäß § 239 Abs. 2 müssen die Eintragungen in Büchern und die sonst erforderlichen Aufzeichnungen *„vollständig, richtig, zeitgerecht und geordnet vorgenommen werden"*. Und in Abs. 4 ist festgelegt, dass *„die Handelsbücher und die sonst erforderlichen Aufzeichnungen auch in der geordneten Ablage von Belegen bestehen oder auf Datenträgern geführt werden können, soweit diese Formen der Buchführung einschließlich des dabei angewandten Verfahrens den Grundsätzen ordnungsmäßiger Buchführung entsprechen. Bei der Führung der Handelsbücher und der sonst erforderlichen Aufzeichnungen auf Datenträgern muss insbesondere sichergestellt sein, dass die Daten während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb einer angemessenen Frist lesbar gemacht werden können"*.

Diese zuvor genannten Absätze sind der Kern der Grundsätze ordnungsgemäßer Buchführung (GoB), die wiederum die Basis für die *Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS)* darstellen. Diese werden in Abschnitt 1.1.2 beschrieben. Wichtig ist in diesem Zusammenhang der Hinweis, dass die Zulässigkeit der Speicherung auf Datenträger davon abhängig gemacht wird, dass auch das dabei angewandte Verfahren den Grundsätzen ordnungsmäßiger Buchführung entsprechen muss. Hier ist bereits ein sehr direkter Bezug zur IT und damit der IT-Dokumentation gegeben.

Aufbewahrungsfristen

Auch im Zusammenhang mit den Festlegungen zur Aufbewahrung von Unterlagen in § 257 wird ein Bezug zur IT hergestellt. So ist nach Abs. 1 jeder Kaufmann verpflichtet, Unterlagen wie zum Beispiel Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Lageberichte, Konzernabschlüsse, Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen geordnet aufzubewahren, und zwar dies für zehn Jahre (Abs. 4). Hieraus kann abgeleitet werden, dass damit auch die Verfahrensdokumentation gemeint ist.

Die Art der Aufbewahrung regelt § 257 Abs. 3 derart, dass mit Ausnahme der Eröffnungsbilanzen, Jahresabschlüsse und Konzernabschlüsse die in Abs. 1 aufgeführten Unterlagen

> *„auch als Wiedergabe auf einem Bildträger oder auf anderen Datenträgern aufbewahrt werden können, wenn dies den Grundsätzen ordnungsmäßiger Buchführung entspricht und sichergestellt ist, dass die Wiedergabe oder die Daten*
>
> 1. *mit den empfangenen Handelsbriefen und den Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden,*
> 2. *während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können."*

1.1.1.3 Abgabenordnung (AO)

In diesem Zusammenhang lohnt auch ein Blick in die Abgabenordnung (AO). In ihr sind die grundlegenden Regelungen enthalten, wie die Steuern zu erheben sind. Hier sind in Anlehnung an das HGB auch Anforderungen an das Führen der Bücher sowie weiterer steuerlich relevanter Unterlagen beschrieben [GESETZE].

Kernsatz der ordnungsgemäßen Buchführung

Im vierten Teil der AO, in dem es um die Durchführung der Besteuerung geht, konkretisieren die Paragrafen 145 bis 147 die Anforderungen an die Buchführung und an die Aufzeichnungen. Danach muss gemäß § 145 Abs. 1 *„die Buchführung so beschaffen sein, dass sie einem sachverständigen Dritten innerhalb angemessener Zeit einen Überblick über die Geschäftsvorfälle und über die Lage des Unternehmens vermitteln kann"*. Dies ist einer der Kernsätze der GoB sowie auch die Basis jeder Ordnungsmäßigkeitsprüfung einer Revision.

Die weiteren Anforderungen entsprechen weitgehend denen aus dem HGB. Es gibt jedoch in der AO eine kleine Ergänzung zum HGB, die für die IT von erheblicher Relevanz ist. In § 147 Abs. 1 sind zunächst gleichlautend zum § 257 Abs. 1 die aufzuhebenden Unterlagen genannt. Zusätzlich werden in der AO aber noch Unterlagen dazu gezählt, wenn diese für die *„Besteuerung von Bedeutung"* sind. Im Rahmen wirtschaftlicher Aktivitäten sind aber fast alle Geschäftsvorfälle von steuerlicher Relevanz. Somit können die Anforderungen auf weite Bereiche des IT-Betriebs Anwendung finden.

Fazit

Insgesamt lässt sich festhalten, dass bereits die grundlegenden Gesetze für die Wirtschaftsunternehmen eine Grundhaltung normiert haben, die in Richtung einer nachvollziehbaren Dokumentation der Geschäftsvorfälle und Geschäftsabläufe abzielen.

1.1.2 Abgeleitete Gesetze

Ausgehend von den im vorhergehenden Abschnitt beschriebenen Gesetzen sind im Laufe der Zeit Konkretisierungen dieser Gesetze zu speziellen Aspekten hinzugekommen.

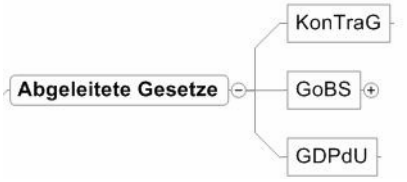


Abbildung 1.4: Konkretisierungen unternehmensbezogener Gesetze

1.1.2.1 KonTraG

Ausgehend von den zunehmenden Korruptions- und Bilanzskandalen der 80er- und 90er- Jahre des letzten Jahrhunderts wurde 1998 das *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)* verabschiedet. Seine Anwendung erstreckt sich über die Aktiengesellschaft hinaus auch auf GmbH-Gesellschaften. Ziel dieses Gesetzes ist die Stärkung und Verbesserung der Unternehmensführung und Unternehmenskontrolle. Das KonTraG präzisiert dabei die entsprechenden Festlegungen im Aktiengesetz und im Handelsgesetzbuch [KONTRAG].

Zu diesem Zweck ist in das Aktiengesetz in § 91 der Absatz 2 neu aufgenommen worden, wonach der Vorstand verpflichtet wird, geeignete Maßnahmen zu treffen. Insbesondere ist *„ein Überwachungssystem einzurichten, damit Entwicklungen, die den Fortbestand der Gesellschaft gefährden, frühzeitig erkannt werden"*.

Einrichtung einer internen Revision

Die Forderung, ein Überwachungssystem einzurichten, wird allgemein so interpretiert, dass damit die Vorhaltung einer angemessenen Revision festgelegt wird. Durch die vom Wirtschaftsbetrieb unabhängige, weil nicht in Linienaufgaben eingebundene Organisation, ist die Revision das geeignete Instrument zur Realisierung eines Überwachungssystems.

Wenn aber die Revision als zentraler Bestandteil der Überwachung festgeschrieben ist, dann gehört der IT-Betrieb zu einem wesentlichen Teil zur Revisionstätigkeit. Nicht umsonst gibt es in der Regel gesonderte IT-Revisoren.

Hervorgehoben wird die Betonung der internen Überwachung durch die Aufnahme eines weiteren Absatzes (Nr. 4) in § 317 des HGB, wonach im Rahmen der Jahresabschlussprüfung zu beurteilen ist, *„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 Aufgaben erfüllen kann"*.

Mit dem § 91 Abs. 2 AktG ist also nicht nur die Vorhaltung einer Revision gefordert, sondern auch, ob diese ihre Aufgaben erfüllen kann. Der Jahresabschlussprüfer hat also zu beurteilen, ob eine im Verhältnis zu den Unternehmensrisiken angemessene Revision existiert. In diesem Zusammenhang wird ebenfalls regelmäßig kontrolliert, wie viel und welche IT-Prüfungen im Berichtsjahr durchgeführt wurden.

1.1.2.2 GoBS

Während das KonTraG aus dem AktG und dem HGB abgeleitet grundlegende Anforderungen an die Unternehmensüberwachung stellt, beschreiben die 1995 veröffentlichten *Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS)* in Präzisierung des HGB und der Abgabenordnung die organisatorischen und technischen Anforderungen an die IT-gestützte Buchführung [GESETZE].

Unternehmensleitung ist verantwortlich

Es wirkt zunächst trivial, dass für die Einhaltung der GoBS der Buchführungspflichtige, also die Unternehmensleitung, verantwortlich ist. Wesentlich in diesem Zusammenhang ist jedoch, dass die Unternehmensleitung ebenfalls für die Einhaltung der GoBS verantwortlich ist, falls die DV-Buchführung von Fremdfirmen durchgeführt wird. Das berührt selbstverständlich nicht die Rechte des Auftraggebers (Buchführungspflichtige) gegenüber dem Auftragnehmer (Fremdfirma) bei einer mangelhaften Auftragserfüllung.

Aus Sicht der IT sind insbesondere die *Kapitel 4, Internes Kontrollsystem (IKS),* und *Kapitel 6, Dokumentation und Prüfbarkeit,* von Bedeutung.

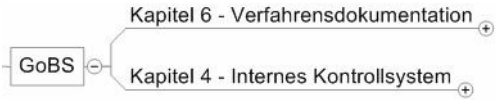


Abbildung 1.5: Wichtige Kapitel der GoBS

In Ergänzung zu § 145 Abs. 1, wonach die Buchführung so beschaffen sein muss, dass sie einem sachverständigen Dritten innerhalb angemessener Zeit einen Überblick über die Geschäftsvorfälle und über die Lage des Unternehmens vermitteln kann, ist in Kapitel 6 der GoBS darüber hinaus festgelegt, dass diese auch prüfbar sein müssen und sich diese Prüfbarkeit auch auf die Abrechnungsverfahren erstreckt. Weiter muss sich gemäß Kapitel 6 aus der Dokumentation ergeben, *„dass das Verfahren entsprechend seiner Beschreibung durchgeführt worden ist"*.

Verfahrensdokumentation

Nach Kapitel 6.1 der GoBS ist eine Verfahrensdokumentation erforderlich, aus der *„Inhalt, Aufbau und Ablauf des Abrechnungsverfahrens vollständig ersichtlich"* sind. Weiter richtet sich der Umfang der erforderlichen Verfahrensdokumentation *„nach der Komplexität der DV-Buchführung (zum Beispiel Anzahl und Größe der Programme, Struktur ihrer Verbindungen untereinander, Nutzung von Tabellen)"*.

„Die Anforderungen an die Verfahrensdokumentation sind unabhängig von der Größe/Kapazität der genutzten DV-Anlage (Hardware) zu stellen, das heißt, sowohl bei Großrechnersystemen als auch bei PC-Systemen ist für eine entsprechende Verfahrensdokumentation zu sorgen."

Die Verfahrensdokumentation muss nach Kapitel 6.2 insbesondere folgende Bereiche beinhalten:

- *„eine Beschreibung der sachlogischen Lösung*
- *die Beschreibung der programmtechnischen Lösung*
- *eine Beschreibung, wie die Programm-Identität gewährt wird*
- *eine Beschreibung, wie die lntegrität von Daten gewahrt wird*
- *Arbeitsanweisungen für den Anwender"*

Die Beschreibung eines jeden der vorgenannten Bereiche muss den Umfang und die Wirkungsweise des internen Kontrollsystems erkennbar machen.

In Kapitel 6.2.1 werden die Inhalte der sachlogischen Beschreibung aus der Sicht des Anwenders wie folgt aufgeführt. Diese sind:

- *„Generelle Aufgabenstellung*
- *Beschreibung der Anwenderoberflächen für die Ein- und Ausgabe einschließlich der manuellen Arbeiten*
- *Beschreibung der Datenbestände*
- *Beschreibung von Verarbeitungsregeln*
- *Beschreibung des Datenaustausches (Datenträgeraustausch/Datentransfer)*
- *Beschreibung der maschinellen und manuellen Kontrollen*
- *Beschreibung der Fehlermeldungen und der sich aus den Fehlern ergebenden Maßnahmen*
- *Schlüsselverzeichnisse*
- *Schnittstellen zu anderen Systemen"*

Anforderungen an die Dokumentation

In Abschnitt 6.2.2 werden die Anforderungen an die Dokumentation der programmtechnischen Lösung dargestellt. Danach ist zu dokumentieren, wo und wie die sachlogischen Forderungen in Programmen umgesetzt sind.

„Tabellen, über die die Funktionen der Programme beeinflusst werden können, sind wie Programme zu behandeln. Programmänderungen sind in der Verfahrensdokumentation auszuweisen. Soweit die Programmänderungen nicht automatisch dokumentiert werden, muss durch zusätzliche organisatorische Maßnahmen gewährleistet werden, dass sowohl der Alt- als auch der Neuzustand eines geänderten Programms nachweisbar sind. Änderungen von Tabellen mit Programmfunktion sind in der Weise zu dokumentieren, dass für die Dauer der Aufbewahrungsfrist der jeweilige Inhalt einer Tabelle festgestellt werden kann."

Insbesondere in Kapitel 6.2.2 werden sehr hohe Anforderungen an die IT-Dokumentation gestellt. So dürfte es aus systemtechnischen Gründen in vielen Fällen wohl unmöglich sein, den jeweils gültigen Änderungsstand von Tabellen zu jedem Zeitpunkt der letzten zehn Jahre festzuhalten.

In Kapitel 6.2.5 ist geregelt, *„dass Arbeitsanweisungen, die für den Anwender zur sachgerechten Erledigung und Durchführung seiner Aufgaben vorhanden sein müssen, ebenfalls zur Verfahrensdokumentation gehören und schriftlich zu fixieren sind. Das ist insbesondere die Beschreibung der im Verfahren vorgesehenen manuellen Kontrollen und Abstimmungen. Die Schnittstellen zu vor- und nachgelagerten Systemen sind hierbei zu berücksichtigen."*

Internes Kontrollsystem

In Kapitel 4 der GoBS werden die Anforderungen an das Interne Kontrollsystem (IKS) definiert, wobei das IKS als *„die Gesamtheit aller aufeinander abgestimmten und miteinander verbundenen Kontrollen, Maßnahmen und Regelungen*" verstanden wird. Das IKS hat nach Kapitel 4.1 die folgenden Aufgaben zu erfüllen:

- *„Sicherung und Schutz des vorhandenen Vermögens und vorhandener Informationen vor Verlusten aller Art;*
- *Bereitstellung vollständiger, genauer und aussagefähiger sowie zeitnaher Aufzeichnungen;*
- *Förderung der betrieblichen Effizienz durch Auswertung und Kontrolle der Aufzeichnungen;*
- *Unterstützung der Befolgung der vorgeschriebenen Geschäftspolitik."*

Insbesondere die zweite und dritte Aufgabe haben direkten Einfluss auf die IT-Dokumentation.

Prüfung des IKS

Die Bedeutung des IKS für die GoBS wird dadurch verstärkt, dass laut Kapitel 4.3 zum Nachweis der Ordnungsmäßigkeit einer DV-Buchführung das IKS beurteilt werden muss.

> *„Dabei reichen wegen komplexen Abläufe und Strukturen beim Buchführungspflichtigen einzelne, voneinander isolierte Kontrollmaßnahmen keinesfalls aus. Vielmehr bedarf es einer planvollen und lückenlosen Vorgehensweise, um ein effizientes Kontrollsystem im Unternehmen zu installieren."*

Die Prüfung des IKS muss nach Kapitel 4.4 folgende Prüfpunkte enthalten:

- Abgestimmte manuelle und maschinelle Kontrollen der Systeme
- Eindeutige Regelungen der Zuständigkeiten und Verantwortlichkeiten der betrieblichen Funktionen
- Buchungsrelevante Arbeitsabläufe müssen definiert und in ihrer Reihenfolge festgelegt sein.

- Ausgeführte manuelle und maschinelle Kontrollen wie Abstimmungskontrollen, Plausibilitätskontrollen und Freigabeverfahren müssen dokumentiert werden.
- Im Rahmen eines funktionsfähigen IKS muss auch die Programmidentität sichergestellt werden. Es muss periodenbezogen geprüft werden, ob die eingesetzte DV-Buchführung auch tatsächlich dem dokumentierten System entspricht.

Sicherstellung der Programmintegrität

Zur Sicherstellung der Programmintegrität sind entsprechend den Unternehmensanforderungen Richtlinien für die folgenden Aufgaben erforderlich:

- *„Programmierung*
- *Programmtests*
- *Programmfreigaben*
- *Programmänderungen*
- *Änderungen von Stamm- und Tabellendaten*
- *Zugriffs- und Zugangsverfahren*
- *den ordnungsgemäßen Einsatz von Datenbanken, Betriebssystemen und Netzwerken*
- *Einsatz von Testdatenbeständen /-sytemen*
- *Programmeinsatzkontrollen“*

Auch muss die jeweils aktuelle Programmversion feststellbar sein und dokumentiert werden.

Fazit

Insgesamt beschreibt die GoBS einen umfangreichen Forderungskatalog an die IT-Dokumentation, der noch um weitere Kapitel wie die Datensicherheit und die Wiedergabe der auf Datenträgern geführten Unterlagen ergänzt wird. Dass die GoBS auch heute noch von großer Bedeutung ist, lässt sich aus der Tatsache ableiten, dass sie derzeit überarbeitet wird.

1.1.2.3 GDPdU

Im Zusammenhang mit der GoBS sind auch die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), die auch wie die GoBS eine Präzisierung der Abgabenordnung darstellen und seit 2002 Anwendung finden, für die IT-Dokumentation wichtig [GDPDU].

In Kapitel I GDPdU wird auf den § 147 Abs. 6 AO Bezug genommen, wonach *„der Finanzbehörde das Recht eingeräumt ist, die mit Hilfe eines Datenverarbeitungssystems erstellte Buchführung des Steuerpflichtigen per Datenzugriff zu prüfen. Diese neue Prüfungsmethode tritt neben die Möglichkeit der herkömmlichen Prüfung. Das Recht auf Datenzugriff steht der Finanzbehörde nur im Rahmen steuerlicher Außenprüfungen zu.“*

Vorhaltung steuerlich relevanter Daten

Weiter wird in Kapitel I.1 GDPdU ausgeführt, dass sich der digitale Zugriff nur auf steuerlich relevante Daten, also im Wesentlichen auf Daten der Finanz- und Anlagenbuchhaltung bezieht. Im weiteren Verlauf wird jedoch ergänzt, dass, soweit sich auch in anderen Bereichen des Datenverarbeitungssystems steuerlich relevante Daten befinden, diese durch den Steuerpflichtigen nach Maßgabe seiner steuerlichen Aufzeichnungs- und Aufbewahrungspflichten zu qualifizieren und für den Datenzugriff in geeigneter Weise vorzuhalten sind.

Wie bereits zuvor dargelegt, kann diese Ausweitung dazu führen, dass ein großer Teil der Geschäftsvorfälle steuerlich relevant sein kann. Das letzte Wort hat hier das Finanzamt.

Sofern Dokumente elektronisch unter Zuhilfenahme einer elektronischen Signatur zu Abrechnungszwecken verarbeitet und dabei gegebenenfalls verschlüsselt werden, muss nach Kapitel II.1 der GDPdU der Originalzustand der übermittelten Dokumente jederzeit überprüfbar sein. Dies setzt neben einer Reihe anderer Tatbestände voraus, dass die Übertragungs-, Archivierungs- und Konvertierungssysteme den Anforderungen der GoBS, insbesondere an die Dokumentation, an das interne Kontrollsystem, an das Sicherungskonzept sowie an die Aufbewahrung entsprechen.

Fazit

Die Verankerung der GoBS in der GDPdU macht deutlich, dass der Umfang der Dokumentationspflichten zunimmt.

1.1.3 Fachspezifische Gesetze

Von den allgemeinen unternehmensbezogenen Gesetzen sowie den daraus abgeleiteten gesetzlichen Regelungen können Gesetze mit fachspezifischer Ausrichtung unterschieden werden. Aus Sicht der IT-Dokumentation sind hier das Bundesdatenschutzgesetz und MaRisk zu nennen.

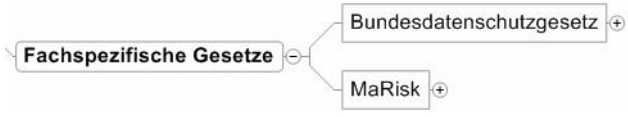


Abbildung 1.6: Gesetze mit fachspezifischer Ausrichtung

1.1.3.1 Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz (BDSG) ist ausgerichtet auf den Schutz der Privatsphäre und regelt sowohl für öffentliche (unter anderem Kommunen, Ämter und staatliche Unternehmen) als auch für nichtöffentliche Stellen (unter anderem natürliche und juristische Personen und Gesellschaften) den Umgang mit personenbezogenen Daten. Es ist eine Reaktion des Gesetzgebers auf das Volkszählungsurteils von 1983, wonach die bisher vorhandenen Datenschutzgesetze nicht den verfassungsrechtlichen Anforderungen genügten. Nachdem daraufhin bereits einige Bundesländer eigene Landesdatenschutzgesetze verabschiedet hatten, trat das Bundesdatenschutzgesetz 1990 in Kraft. Es liegt derzeit in der Fassung von 2006 vor [BDSG].

Das BDSG ist in fünf Abschnitte unterteilt, wobei im Abschnitt 1 die allgemeinen Bestimmungen enthalten sind. Für den IT-Betrieb wichtig ist Abschnitt 3, in dem die Verarbeitung personenbezogener Daten geregelt ist.

Nach § 3, Abs. 1 sind personenbezogene Daten *„Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person"*. Von besonderem Interesse dabei sind Einzelangaben, aus deren Kombination oder Auswertung sich eine Person ableiten, also bestimmen, lässt. Also beispielsweise die Adresse in Kombination mit der Telefonnummer. Besonders schutzwürdig sind Daten zur rassischen und ethnischen Herkunft, politische Meinungen sowie religiöse und philosophische Überzeugungen und Angaben zur Gewerkschaftszugehörigkeit, zur Gesundheit und zum Sexualleben.

Die automatisierte Nutzung wird in § 3, Abs. 2 beschrieben als Erhebung, Verarbeitung und Nutzung der Daten. Danach teilt sich die Verarbeitung auf in Speichern, Verändern, Übermitteln, Sperren und Löschen.

Das BDSG ist ein Verbotsgesetz, das die Erhebung, Verarbeitung und Nutzung personenbezogener Daten grundsätzlich untersagt. Sie sind nur dann zulässig, wenn dieses oder andere Gesetze es erlaubt oder der Betroffene eingewilligt hat. Die Einwilligung hat in der Regel schriftlich zu erfolgen und hat zur Voraussetzung, dass sie aus freier Entscheidung und in Kenntnis des Zwecks und der Folgen der Verarbeitung gefallen ist (§ 4a Abs. 1).

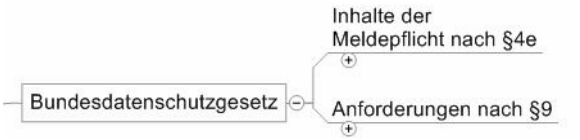


Abbildung 1.7: Relevante Paragraphen des Bundesdatenschutzgesetzes

DV-Verfahren sind zu melden

Eine wesentliche Bestimmung des BDSG ist die der Meldepflicht nach § 4d, wonach Verfahren automatisierter Verarbeitungen vor ihrer Inbetriebnahme der zuständigen Aufsichtsbehörde bzw. dem betrieblichen Datenschutzbeauftragten zu melden sind. Eine Produktivsetzung einer Verarbeitung personenbezogener Daten, etwa eines Kundenmanagementsystems, ist danach nicht zulässig und kann gerichtlich untersagt werden.

Der Inhalt der Meldepflicht sieht gemäß § 4e Abs. 1 neun Bestandteile vor. Unter anderem die Zweckbestimmung sowie eine Beschreibung der zu erhebenden Daten, der betroffenen Personengruppen und Empfänger der Daten. Das bedeutet, dass diese Festlegungen vor der Inbetriebnahme feststehen müssen. Eine diesbezügliche Veränderung, etwa das Verändern oder Ausweiten des Zweckes während der Produktivphase, ist nicht zulässig.

Aus dem § 4g Abs. 2 Satz 1 leitet sich das Erfordernis zur Aufstellung eines Verfahrensverzeichnisses ab, in dem alle meldepflichtigen Verfahren zu dokumentieren sind. Dieses Verzeichnis hat die verantwortliche Stelle zu führen und dem Datenschutzbeauftragten zur Verfügung zu stellen. Eine nähere Beschreibung des Verfahrensverzeichnis finden Sie in Abschnitt 3.2.6 .

Dokumentation bereits vor der Inbetriebnahme

Diese Bestimmungen führen zu hohen Anforderungen an die Dokumentation von IT-Projekten. Es muss also vor der Implementierung eines Verfahrens, in dem personenbezogene Daten verarbeitet werden sollen, exakt festgelegt und damit dokumentiert sein, welche Daten von wem und für wen zu welchem Zweck erhoben, verarbeitet und genutzt werden sollen. Es genügt nicht, nur das Verfahren mitzuteilen. Das Unternehmen hat nach § 9 des BDSG technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes – insbesondere die in der Anlage des Gesetzes genannten Anforderungen – zu gewährleisten. Die in der Anlage des Gesetzes genannten Anforderungen beschreiben Maßnahmen

- zur Zutrittskontrolle,
- zur Zugangskontrolle,
- zur Zugriffskontrolle,
- zur Weitergabekontrolle,
- zur Eingabekontrolle,
- zur Auftragskontrolle und
- zur Verfügbarkeitskontrolle.

Diese Anforderungen nach § 9 sowie der Anlage des BDSG stehen unter dem Vorbehalt, dass die Maßnahmen im Verhältnis zum angestrebten Schutzzweck angemessen sein müssen.

Nach § 4f Abs. 1 hat auch jede nichtöffentliche Stelle, die personenbezogene Daten erhebt, verarbeitet oder nutzt, einen Datenschutzbeauftragten zu bestellen, sofern mehr als vier Personen damit beschäftigt sind. Kleinstbetriebe sind also von dieser Vorschrift ausgenommen. Sofern der Betrieb jedoch geschäftsmäßig personenbezogene Daten zum Zwecke der Übermittlung erhebt, gilt diese Einschränkung jedoch nicht mehr.

Dem Datenschutzbeauftragten ist nach § 4g Abs. 2 eine Übersicht über die in § 4e beschriebenen Verfahren zur Verfügung zu stellen. Nach Abs. 1 des Paragraphen ist er rechtzeitig, also vor der Einführung, zu unterrichten. Weiter hat er die ordnungsgemäße Verwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen.

Für die entsprechende IT-Dokumentation zur Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten hat dies zur Folge, dass sie bereits vor der Implementierung vorliegen und in die Überwachung durch den Datenschutzbeauftragten mit einbezogen werden muss. Dieser beurteilt damit auch die Ordnungsmäßigkeit der IT-Dokumentation im Sinne des Gesetzes.

1.1.3.2 MaRisk

Während im KonTraG allgemeine Regelungen zur risikoorientierten Unternehmensführung und Überwachung enthalten sind, richten sich die *Mindestanforderungen an das Risikomanagementsystem (MaRisk)* an Unternehmen der Kreditwirtschaft sowie Finanzdienstleister [MARISK].

Ziel der MaRisk ist, Missständen im Kredit- und Finanzdienstleistungswesen entgegenzuwirken, welche die Sicherheit der den Instituten anvertrauten Vermögenswerte gefährden, die ordnungsgemäße Durchführung der Bankgeschäfte oder Finanzdienstleistungen beeinträchtigen oder erhebliche Nachteile für die Gesamtwirtschaft herbeiführen können.

Wie bereits gesagt, verankern viele Unternehmen, die ein explizites konzerninternes Finanzmanagement betreiben, die MaRisk in ihrem Unternehmensregelwerk. Somit haben die MaRisk für eine Reihe deutscher Unternehmen eine direkte Bedeutung.

Wichtig für die IT-Dokumentation sind die Anforderungen hinsichtlich der Aufbau- und Ablauforgansiation und deren Dokumentation sowie die Anforderungen an die Prüfaktivitäten der internen Revision, die im Kreditwesen ohnehin obligatorisch ist.

Grundsätzlich sind gemäß Kapitel 4.3.1 des Allgemeinen Teils (AT) die „*Prozesse sowie die damit verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen sowie Kommunikationswege klar zu definieren und aufeinander abzustimmen. Das gilt auch bezüglich der Schnittstellen zu wesentlichen Auslagerungen.*“ Weiter wird in AT 5 festgelegt, „*dass die Geschäftsaktivitäten auf der Grundlage von Organisationsrichtlinien betrieben werden (zum Beispiel Handbücher, Arbeitsanweisungen oder Arbeitsablaufbeschreibungen). Die Organisationsrichtlinien müssen schriftlich fixiert und den betroffenen Mitarbeitern in geeigneter Weise bekannt gemacht werden. Es ist sicherzustellen, dass sie den Mitarbeitern in der jeweils aktuellen Fassung zur Verfügung stehen. Die Richtlinien sind außerdem bei Änderungen der Aktivitäten und Prozesse zeitnah anzupassen.*“

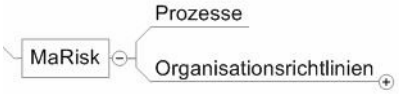


Abbildung 1.8: Anforderungen an Prozesse und Richtlinien

Die Organisationsrichtlinien müssen gemäß AT 5 folgende Regelungen enthalten:

- *„Regelungen für die Aufbau- und Ablauforganisation sowie zur Aufgabenzuweisung, Kompetenzordnung und den Verantwortlichkeiten,*
- *Regelungen hinsichtlich der Ausgestaltung der Risikosteuerungs- und Risikocontrollingprozesse,*
- *Regelungen zur internen Revision,*

- *Regelungen, die die Einhaltung gesetzlicher Bestimmungen sowie sonstiger Vorgaben (z. B. Datenschutz oder Compliance) gewährleisten sowie*
- *Regelungen zu Verfahrensweisen bei wesentlichen Auslagerungen."*

Zudem muss die Ausgestaltung der Organisationsrichtlinien eine Sachprüfung der internen Revision ermöglichen.

Die Pflicht zur Dokumentation ergibt sich aus AT 6, wonach Geschäfts-, Kontroll- und Überwachungsunterlagen systematisch und für sachkundige Dritte nachvollziehbar abzufassen sind.

Forderung nach einem Notfallkonzept

In Bezug auf die IT-Organisation und IT-Dokumentation wird in AT 7.2 ausdrücklich ein Notfallhandbuch gefordert, das Geschäftsfortführungs- sowie Wiederanlaufpläne umfasst. Die Geschäftsfortführungspläne müssen gewährleisten, dass im Notfall zeitnah Ersatzlösungen zur Verfügung stehen. Die Wiederanlaufpläne müssen außerdem innerhalb eines angemessenen Zeitraums die Rückkehr zum Normalbetrieb ermöglichen. Die im Notfall zu verwendenden Kommunikationswege sind festzulegen. Das Notfallhandbuch muss den beteiligten Mitarbeitern zur Verfügung stehen.

Auch hinsichtlich der Prüfungsaktivitäten der internen Revision werden in der MaRisk klare Vorgaben gemacht. So wird im Besonderen Teil (BT) 2.1 ausgeführt, *„dass sich die Prüfungstätigkeit der internen Revision auf der Grundlage eines risikoorientierten Prüfungsansatzes grundsätzlich auf alle Aktivitäten und Prozesse des Instituts erstreckt"*. Damit werden die IT-Prozesse ebenfalls zum Prüfungsgegenstand.

Weiter sind gemäß BT 2.3 die Aktivitäten und Prozesse des Instituts, auch wenn diese ausgelagert sind, in angemessenen Abständen, grundsätzlich innerhalb von drei Jahren, zu prüfen. Wenn besondere Risiken bestehen, ist jährlich zu prüfen. Da die Kernprozesse der IT gerade im Kreditgeschäft ein hohes Risiko darstellen, sind diese und ihre zugrunde liegende Dokumentation jährlich zu prüfen.

Die interne Revision hat aber nicht nur eine Prüfungspflicht, sondern nach BT 2.5 auch eine Überwachungspflicht, was die Beseitigung der festgestellten Mängel angeht. Hat die Beseitigung nicht stattgefunden, wird hierüber zunächst der Fachvorgesetzte und gegebenenfalls in einem nächsten Schritt die Geschäftsleitung unterrichtet.

Fazit

Der IT-Bereich hat also nicht nur umfangreiche Dokumentationspflichten bezüglich der eingesetzten Technik sowie der Aufbau- und Ablauforganisation. Er hat ebenfalls auch die Umsetzung der Empfehlungen der internen Revision zu dokumentieren.

1.1.4 Internationale Gesetze

Neben nationalen Gesetzen bekommen auch internationale Gesetze eine zunehmende Bedeutung für die IT-Abteilungen und damit auch für die IT-Dokumentation. Wesentliche Gesetze in diesem Zusammenhang stellen der amerikanische Sarbanes-Oxley Act sowie die 8. EU Richtlinie dar.

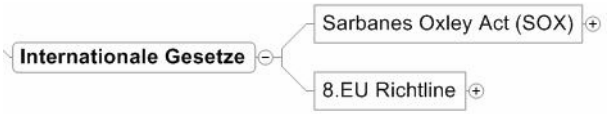


Abbildung 1.9: Relevante Internationale Gesetze

1.1.4.1 Sarbanes-Oxley Act (SOX)

Unter dem Eindruck der Aufsehen erregenden Bilanzskandale in Amerika wurde mit dem *Sarbanes-Oxley Act (SOX)* 2002 ein US-amerikanisches Bundesgesetz verabschiedet, das die Wiederherstellung des Vertrauens der Öffentlichkeit in die Finanzberichte der Unternehmen durch Anforderungen an die Offenlegung und Genauigkeit von veröffentlichten finanzwirtschaftlichen Informationen zum Ziel hat [SOX].

Die Gültigkeit dieses Gesetzes erstreckt sich auch auf deutsche Unternehmen, sofern sie an einer amerikanischen Börse gelistet sind oder sich im überwiegenden Besitz einer amerikanischen Muttergesellschaft befinden.

Dieses Gesetz besteht aus elf Hauptsektionen, wobei für die IT die *Section 404* von besonderer Bedeutung ist. In der Section 404 „Management Assessment Of Internal Controls", wird das Prüfungserfordernis externer Prüfer für das interne Kontrollsystem normiert. Dabei wird jedoch nicht präzisiert, welche internen Kontrollen genügen, um eine uneingeschränkte Bescheinigung für deren Effizienz zu erhalten.

Anforderungen aus der Prüfungspraxis

In der Prüfungspraxis haben sich unter anderem die folgenden Anforderungen herauskristallisiert:

- Die Systemdokumentation muss aktuell sein und dem tatsächlichen Verfahren entsprechen.
- Die manuellen Prozesse und insbesondere die manuellen Kontrollen müssen dokumentiert werden.
- Die im Unternehmen selbst entwickelten Anwendungen müssen gegen den Zugriff Unbefugter geschützt werden und müssen einer geregelten Datensicherung unterliegen.
- Die Benutzerkonten ausgeschiedener Mitarbeiter oder nicht aktiver Berater müssen gesperrt werden.
- Benutzern dürfen nur diejenigen Berechtigungen erhalten, die sie wirklich brauchen. Besonders kritisch sind in diesem Zusammenhang die „Super-User"-Berechtigungen.
- Es ist sicherzustellen, dass Mitarbeiter im Entwicklungsbereich über keine Berechtigungen im Produktivbereich verfügen dürfen.
- Die Betriebssysteme und Datenbanken, auf denen große Anwendungen (wie beispielsweise SAP) aufsetzen, sind genauso zu schützen wie die Anwendungssysteme selbst.

Fazit

Die Brisanz der Section 404 liegt darin, dass die Einhaltung der Sicherheitsregelungen und die Effizienz des internen Kontrollsystems im Einzelnen nachgewiesen werden muss – und dies jährlich. Das revisionstypische Bewertungsstereotyp *Es haben sich keine Anhaltspunkte ergeben, dass …* reicht hier nicht aus. Daher steht die Section 404 in dem Ruf extrem personal und ressourcenaufwendig zu sein. Aus Sicht der IT-Dokumentation stellt sich damit jährlich die gleiche große Herausforderung der Nachweispflicht.

1.1.4.2 8. EU-Richtlinie

Aber nicht nur in Amerika haben Bundesgesetze eine immer stärkere Bedeutung für die IT. Auch in der EU sind mit der „Richtlinie über die Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen" aus dem Jahr 2006 Regelungen geschaffen worden, die eine Auswirkung auf die IT-Dokumentation entfalten. In journalistischer Vereinfachung wird diese sogenannte 8. EU-Richtlinie als *Euro-SOX* bezeichnet, da sie eine ähnliche Auswirkung auf die Überwachungs- und Nachweispflichten der Unternehmen hat [ASPRÜF].

Tatsächlich stellt diese Richtlinie aber eine Harmonisierung und Konkretisierung bereits bestehender EU-Richtlinien aus den Jahren 1978 bis 1984 dar und ist nicht wie SOX direkt an die Unternehmen, sondern an die Mitgliedsstaaten der EU gerichtet. Erfasst werden auch nur Unternehmen von öffentlichem Interesse, wobei jeder Mitgliedsstaat eine eingeschränkte Entscheidungsfreiheit hat.

Prüfungsausschuss ist erforderlich

Für die IT ist insbesondere der Artikel 41 der Richtlinie entscheidend, wonach jedes von der Richtlinie erfasstes Unternehmen einen Prüfungsausschuss zu bilden hat, unabhängig von den sonstigen Überwachungsorganen, wie zum Beispiel einer internen Revision. Der Prüfungsausschuss hat nach Artikel 41 Abs. 2 unter anderem folgende Aufgaben:

- Überwachung des Rechnungslegungsprozesses
- Überwachung der Wirksamkeit des internen Kontrollsystems, gegebenenfalls des internen Revisionssystems, und des Risikomanagementsystems des Unternehmens
- Überwachung der Abschlussprüfung des Jahresabschlusses
- Empfehlungen über den zu beauftragenden Abschlussprüfer abzugeben

Fazit

Auch wenn sich aus Artikel 41 nicht ableiten lässt, welche Anforderungen an die Prozesse und an das interne Kontrollsystem gestellt werden, so verbirgt sich hinter den Begriffen „Überwachung" und „Wirksamkeit" die Grundforderung nach einer aussagefähigen Dokumentation.

1.2 Normen und Standards

Während Gesetze und daraus abgeleitete Rechtsnormen verbindlichen Charakter haben, entfalten Standards ihre Wirkung durch nationale oder internationale Anerkennung. Entweder durch öffentlich legitimierte Organisationen wie bei den ISO-Normen und dem IT-Grundschutz oder durch Grundsätze berufsständischer Verbände wie bei den Prüfungsrichtlinien der IDW oder dem DIIR.

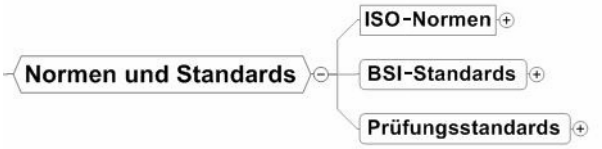


Abbildung 1.10: Relevante Nomen und Standards

1.2.1 Wichtige Normen und Standards im Überblick

Entsprechend dem Deutschen Institut für Normung e. V. (DIN) gibt es auch ein internationales Pendant – die *International Organization for Standardization (ISO)*. Sie ist ein Zusammenschluss internationaler Organisationen und entwickelt und veröffentlicht, mit wenigen Ausnahmen (z. B. IEC), für alle Bereiche der Wirtschaft Normen. Da derzeit ca. 150 Länder der ISO angehören gelten die von ihr veröffentlichten Standards nahezu weltweit. Zertifizierungen nach den ISO-Normen sind in der Regel drei Jahre gültig und beinhalten einen jährlichen unternehmensinternen Auditprozess [ISOLIST].

Unterschiedliche Begriffe für ISO-Normen

Da diese ISO-Normen vom DIN als deutsche Norm übernommen werden, findet man häufig die Bezeichnung *DIN ISO* oder *DIN EN ISO*, sofern es auch noch eine entsprechende *Europäische Norm (EN)* gibt. Bei der weiteren Beschreibung werden der Übersichtlichkeit halber die ISO-Bezeichnungen verwendet.

Eine der bekanntesten ISO-Normen für die Unternehmensorganisation ist die ISO 9000 sowie die damit in Zusammenhang stehenden Normen ISO 9001, ISO 9004 und ISO 9011. Hierin sind Grundsätze für Maßnahmen zum Qualitätsmanagement enthalten. Da diese allgemeine managementbezogene Normen darstellen, können sie für jedes Unternehmen für eine Zertifizierung herangezogen werden. Gerade für kleinere und mittlere Unternehmen kann das Vorweisen eines derartigen Zertifikats überhaupt erst den Zugang zum Anbietermarkt bedeuten. Nämlich dann, wenn der Auftraggeber vom potenziellen Auftragnehmer beispielsweise eine Zertifizierung nach ISO 9000 verlangt.

Weitere – insbesondere für die IT wichtige – Normen sind:

- ISO 20000 – IT-Servicemanagement
- ISO 27001 – IT-Sicherheitsverfahren – Informationssicherheitsmanagementsysteme (Anforderungen)

Aufgaben des BSI

Auf nationaler Ebene stellt das *Bundesamt für Sicherheit in der Informationstechnik (BSI)* eine durch ein entsprechendes Bundesgesetz (BSIG von 1990) legitimierte Organisation dar, die in erster Linie für die Verwaltungen in Bund, Ländern und Gemeinden zuständig ist, sich aber auch an private Nutzer und Hersteller richtet. Nach § 3 des BSIG hat das BSI unter anderem folgende Aufgaben:

- *„Untersuchung von Sicherheitsrisiken bei der Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen – insbesondere von informationstechnischen Verfahren und Geräten für die Sicherheit in der Informationstechnik"*
- *„Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten"*
- *„Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten und Erteilung von Sicherheitszertifikaten"*
- *„Unterstützung der für Sicherheit in der Informationstechnik zuständigen Stellen des Bundes, insbesondere soweit sie Beratungs- oder Kontrollaufgaben wahrnehmen; dies gilt vorrangig für den Bundesbeauftragten für den Datenschutz, dessen Unterstützung im Rahmen der Unabhängigkeit erfolgt, die ihm bei der Erfüllung seiner Aufgaben nach dem Bundesdatenschutzgesetz zusteht"*
- *„Beratung der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen"* [BSIG]

BSI-Standards

Für die IT von Bedeutung ist das BSI-Regelwerk zum IT-Grundschutz, das den Unternehmen Methoden an die Hand gibt, dem Stand der Technik entsprechende IT-Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Dieses seit den 90er-Jahren des letzten Jahrhunderts bestehenden Regelwerkes ist seit 2005 in *IT-Grundschutz-Kataloge* umbenannt und eine bausteinartige Umsetzung der neuen *BSI-Standards 100-1 bis 100-4*. In diese BSI-Standards sind bereits auch Kernelemente der ISO 27001 mit eingeflossen.

Während die ISO- und BSI-Standards für die Unternehmen durch ihre Zertifizierbarkeit eine besondere Bedeutung für die Außendarstellung haben, sind die Prüfungsstandards der Jahresabschlussprüfer sowie der internen Revision nach innen gerichtete Regularien.

Wie bereits in Abschnitt 1.1.1 verdeutlicht wurde, bekommen die Prüfungsorganisationen eine immer größere Bedeutung für die Unternehmensüberwachung, die ja eine Kernaufgabe jeder Unternehmensleitung darstellt. Gesetze wie das KonTraG, SOX und die 8. EU-Richtlinie schreiben das Prüfungserfordernis fest.

Prüfungsstandards

Die berufsständischen Organisationen *Institut der Wirtschaftsprüfer in Deutschland e. V. (IDW)* sowie das *Deutsche Institut für Interne Revision e. V. (DIIR)* haben jeweils eigene Prüfungsstandards herausgegeben. Dabei hat das DIIR bei seinen drei Prüfungsstandards eher allgemeine Beschreibungen der Revisionstätigkeit vorgenommen, während das IDW zu einzelnen Prüfansätzen spezialisierte Prüfungsleitlinien veröffentlicht hat. Den Standards beider Organisationen gemein ist jedoch, dass sie für ihre Mitgliedsunternehmen verbindlich sind und insofern Normencharakter annehmen.

Für die IT sind insbesondere die Prüfungsstandards *IDW PS 330 – Abschlussprüfung bei Einsatz von Informationstechnologie* und *IDW PS 880 – Erteilung und Verwendung von Softwarebescheinigungen* von Bedeutung. In Vorbereitung ist der *IDW PS 850*, der die *Projektbegleitende Prüfung bei Einsatz von Informationstechnologie* beschreibt.

Vom DIIR ist insbesondere der Revisionsstandard *Nr. 2* relevant, da dort die Anforderungen der Prüfung des Risikomanagements beschrieben werden. Dieser eher allgemein gehaltene Ansatz ergibt sich direkt aus dem KonTraG und hat für die IT im Hinblick auf die Organisation und Dokumentation des internen Kontrollsystems entsprechende Bedeutung.

Sonderrolle TÜVIT

Eine Sonderrolle nimmt die *TÜV Informationstechnik GmbH (TÜVIT)* als Unternehmen der *Unternehmensgruppe TÜV Nord* ein. Sie ist zum einen bei nationalen und internationalen Organisationen akkreditiert und kann somit Zertifikate nach ISO- oder BSI-Standard vergeben und bietet zum anderen in Kooperation mit IT-Herstellern eigene Zertifizierungsdienstleistungen an, so beispielsweise mit Microsoft oder der Deutsche Telekom.

1.2.2 ISO-Normen

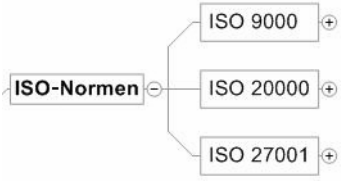


Abbildung 1.11: Für die IT-Dokumentation wichtige ISO-Normen

1.2.2.1 ISO 9000

Die ISO 9000-Normenreihe wurde aus einer Reihe von Vorgängernormen entwickelt und 1994 veröffentlicht. Im Zuge der Weiterentwicklung wurde der ursprünglich funktionsorientierte Ansatz in einen prozessorientierten Ansatz, der auf dem Deming-Kreis beruht, verändert. Gleichzeitig wurden Teile der Normenreihe zusammengefasst und einheitliche Begriffsdefinitionen ergänzt. Derzeit hat die 9000er-Normenreihe folgende Struktur, wobei die zweite Zahl jeweils das Jahr angibt: [ISO9000]

Abbildung 1.12: 9000er Normenreihe

ISO 9001:2000

Die Grundlage für die Zertifizierung der Unternehmen stellt die ISO 9001:2000 dar, die die Anforderungen an ein Qualitätsmanagementsystem festlegt. Die Norm ist in acht Kapitel unterteilt, wobei die ersten drei Kapitel allgemeine Aussagen enthalten. Die Kapitel 4 bis 8 haben folgenden Inhalt:

- Kapitel 1–3: Vorwort und allgemeine Hinweise
- Kapitel 4: Qualitätsmanagement-System
- Kapitel 5: Verantwortung der Leitung
- Kapitel 6: Management von Ressourcen
- Kapitel 7: Produktrealisierung
- Kapitel 8: Messung, Analyse und Verbesserung

Während die Kapitel 4–7 die Anforderungen an das Management allgemein und an die Kundenorientierung beschreiben, wird mit Kapitel 8 die Anlehnung an den Deming-Kreis deutlich. Hier wird der kontinuierliche Änderungsprozess dargestellt, der im Deming-Kreis mit den Prozessteilen *Plan*, *Do*, *Check* und *Act* dargestellt ist.

Sechs Verfahren sind zu dokumentieren

Grundsätzlich fordert die ISO 9001 die Dokumentation mindestens der folgenden sechs Verfahren:

- Lenkung der Dokumente
- Lenkung der Qualitätsaufzeichnungen
- Durchführung der internen Audits
- Lenkung fehlerhafter Produkte
- Korrekturmaßnahmen
- Vorbeugungsmaßnahmen

Für die IT-Dokumentation ist insbesondere das Kapitel 4 von Bedeutung, da hier die Dokumentationsanforderungen beschrieben werden. Diese sind zwar nicht speziell auf die IT ausgerichtet. Wenn aber ein Unternehmen seine IT-Abteilung nach ISO 9001 zertifizieren möchte, so sind die Anforderungen nach Kapitel 4.2 direkt auf die IT anzuwenden.

Für die Dokumentation gelten folgende Anforderungsbereiche:

- Es muss ein Qualitätsmanagement-Handbuch erstellt werden, das neben der Darstellung der unternehmensbezogenen Qualitätspolitik alle für die Produkterstellung und deren Absatz erforderlichen Verfahren beschreibt. Dazu gehört ebenfalls eine Beschreibung der Wechselwirkungen mit anderen Prozessen (z. B. eine Schnittstellenbeschreibung).
- Weiter ist die Lenkung von Dokumenten zu beschreiben. Wichtig sind in diesem Zusammenhang unter anderem der Nachweis der jeweils gültigen Fassung, die Kennzeichnung von Änderungen an den Dokumenten und deren lesbare Bereitstellung. Ein operatives Ziel der Lenkung von Dokumenten ist zu vermeiden, dass veraltete Versionsstände verwendet werden. Zu der Beschreibung gehören auch Festlegungen zu Aufbewahrungsfristen sowie zur Archivierung.

1.2.2.2 ISO 20000

Die ISO 20000 ist eine speziell auf das IT-Servicemanagement ausgerichtete Norm und wurde im Jahr 2005 auf der Basis der gleichnamigen britischen Norm BS 15000 veröffentlicht. Wie die ISO 9000ff ist sie prozessorientiert ausgerichtet, beschreibt aber weniger das produktbezogene Qualitätsmanagement im Allgemeinen, sondern das IT-Servicemanagement im Besonderen. Die prozessorientierten Festlegungen orientieren sich an den Prozessbeschreibungen gemäß ITIL, stellen dabei aber teilweise noch eine Ergänzung dazu dar [ISO20000].

Im Gegensatz zu ITIL zertifizierbar

Es besteht aber ein wesentlicher formaler Unterschied zu ITIL. Im Gegensatz zu ITIL, das keinen Standard darstellt, sind die Prozesse des IT-Servicemanagements nach ISO 20000 international anerkannt zertifizierbar.

Die ISO 20000-Norm ist in zwei Hauptteile unterteilt, nämlich in „Service Management: Specification“ (Part 1) und „Service Management: Code of Practice“ (Part 2). Dabei stellt Part 1 die zwingend erforderlichen Anforderungen dar („must have“) während Part 2 weitere optionale Anforderungen beschreibt („shoud have“).

Die Struktur von Part 1 ISO 20000 teilt sich auf in die folgenden zehn Kapitel:

1. Scope
2. Terms and Definitions
3. Management system
4. Planning and Implementing Service management
5. Planning and Implementing new or changed Services
6. Service Delivery Processes, Service Level Management
   Service Reporting, Capacity Management
   Service Continuity and Availability Management
   Information Security Management
   Budgeting and Accounting for IT Services

7. Relationship Processes
   Business Relationship Management
   Supplier Management
8. Resolution Processes
   Incident Management
   Problem Management
9. Release Process
10. Control Processes
    Configuration Management
    Change Management

Die Prozessausrichtung wird anhand der Kapitelstruktur besonders augenfällig. Während die ISO 9001 die Dokumentationsanforderungen stark betont, sind in der ISO 20000 die Dokumentationserfordernisse implizit Voraussetzung, um die Prozesse nachvollziehbar und prüfbar zu machen. In Kapitel 3 der ISO 20000, Management System, werden allgemeine Anforderungen an die Dokumentation formuliert.

1.2.2.3 ISO 27001

Ebenfalls im Jahr 2005 wurde die ISO 27001 veröffentlicht, die wie die ISO 9001 zu einer Normenfamilie gehört (ISO 27000 bis ISO 27006). Sie wurde aus dem britischen Standard BS 7799-2 abgeleitet und beschreibt die Anforderungen an das Informationssicherheitsmanagement. Ihre vollständige Bezeichnung lautet: *Information technology – Security techniques - Information security management systems – Requirements* [ISO27001].

IT-Sicherheitsmanagement im Focus

Während die ISO 20000 das IT-Servicemanagement und damit die Kundenorientierung zum Inhalt hat, liegt der Focus bei der ISO 27001 auf dem IT-Sicherheitsmanagement. Sie hat damit eine ähnliche Ausrichtung wie die Normenreihe des deutschen BSI, die im nachfolgenden Kapitel beschrieben wird.

Hervorzuheben ist in diesem Zusammenhang, dass die Norm nicht auf die IT-Abteilung ausgerichtet ist, sondern die Informationssicherheit in allen Wertschöpfungsstufen eines Unternehmens adressiert. Sie hat also die IT-bezogene Informationssicherheit in allen Unternehmensbereichen zum Gegenstand. An die Dokumentation werden unter anderem folgende Anforderungen gestellt, die in dem Zertifizierungsprozess zu überprüfen und zu bewerten sind:

- Aufstellung der eingesetzten IT-Systeme (z. B. Server, Clients, Netzkomponenten)
- Aufstellung der eingesetzten Anwendungen, wobei eine Zuordnung zu den verwendeten Systemen möglich sein muss
- Netzplan aller Systemkomponenten
- Risikobeschreibung der eingesetzten Systeme und Anwendungen

- Festlegung des Schutzbedarfes der eingesetzten Systeme und Anwendungen

Bei der Prüfung der Dokumentation werden unter anderem die Vollständigkeit, Nachvollziehbarkeit, Plausibilität und die Aktualität der Dokumente bewertet. Weiter wird überprüft und bewertet, inwiefern die Dokumentation die tatsächlichen Gegebenheiten widerspiegelt.

1.2.3 BSI-Standards

Wie bereits zu Beginn des Abschnitts 1.2 dargelegt, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemäß dem BSI-Gesetz unter anderem die Aufgabe, Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten zu entwickeln.

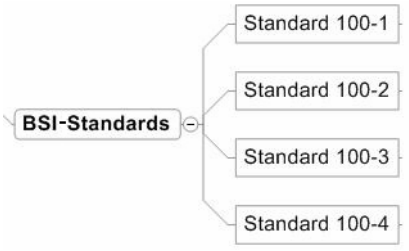


Abbildung 1.13: BSI-Standards

Im Jahr 1995 hat das BSI das erste Grundschutzhandbuch herausgegeben, das sich als eine Referenz für die IT-Sicherheit verstanden hat und Vorgehensweisen zur Erstellung von IT-Sicherheitskonzepten enthielt. Es setzte sich damals aus 18 Grundschutzbausteinen und 200 Maßnahmen zur Erlangung des Grundschutzes zusammen. Während der Weiterentwicklung bis 2004 wuchs das „Handbuch", das sich zwischenzeitlich auf mehrere Ordner erstreckte, auf 58 Grundschutzbausteine mit über 700 Maßnahmen an.

Reaktion auf ISO 27001

Mit der Veröffentlichung der ISO-Norm 27001 hat das BSI das Handbuch zugunsten einer Zweiteilung des IT-Grundschutzes aufgegeben. Zum einen hat das BSI die Standards 100-1 bis 100-3 entwickelt und als Handbuch herausgegeben (der Standard 100-4 liegt derzeit als Entwurf vor), in dem die grundsätzlichen Anforderungen beschrieben sind. Zum anderen wurden aus den Bausteinen und Maßnahmen die IT-Grundschutz-Kataloge in Form einer Loseblattsammlung erstellt. Standards und Kataloge bilden dabei eine inhaltliche Einheit, wobei die Standards die Klammer um die Grundschutz-Kataloge bilden [BSISTAND].

Die BSI-Standards bilden die ISO 27001 vollständig ab und integrieren zusätzlich weitere Teile der 27000er-Normenfamilie. Das BSI verfolgt damit das Ziel, eine noch umfassendere Behandlung der Themen, ein einfacheres Verständnis für die Themenstellungen sowie eine leichtere Lesbarkeit zu erreichen. Im Folgenden werden die BSI-Standards kurz vorgestellt. Die vollständige Dokumentation ist kostenfrei auf den Webservern des BSI im PDF-Format verfügbar.

1.2.3.1 Standard 100-1

Managementsystem für Informationssicherheit - ISMS

Der Standard beschreibt den Aufbau von Managementsystemen für Informationssicherheit (*Information Security Management System, ISMS*) und beinhaltet dabei alle für die Zielerreichung erforderlichen Regelungen. Neben den beiden einleitenden Kapiteln enthält der Standard 100-1 die folgenden Kapitel:

- Kapitel 1–2: Vorwort und allgemeine Hinweise
- Kapitel 3: ISMS-Definition und Prozessbeschreibung
- Kapitel 4: Management-Prinzipien
- Kapitel 5: Ressourcen für Informationssicherheit
- Kapitel 6: Einbindung der Mitarbeiter in den Sicherheitsprozess
- Kapitel 7: Der Informationssicherheitsprozess
- Kapitel 8: Sicherheitskonzept
- Kapitel 9: Das ISMS des BSI: IT-Grundschutz

Während in den Kapiteln 3 bis 7 allgemeine Anforderungen an das ISMS beschrieben werden, ist in Kapitel 8 die Notwendigkeit, ein Sicherheitskonzept zu erstellen, dargelegt. Da auch die BSI-Normen den Deming-Kreis als Basis haben, wird das Sicherheitskonzept in seinem Lebenszyklus mit den folgenden Abschnitten dargestellt:

- Plan: Planung und Konzeption des Sicherheitskonzepts
- Do: Umsetzung des Sicherheitskonzepts
- Check: Überwachung und Erfolgskontrolle
- Act: Optimierung und Verbesserung

Das Sicherheitskonzept muss Aussagen zu folgenden Themen machen:

- Methoden der Risikobewertung
- Klassifikation der Risiken bzw. Schäden
- Risikobewertung
- Strategie zur Behandlung von Risiken
- Beschreibung der Sicherheitsmaßnahmen

Im Rahmen der Überwachung und Erfolgskontrolle sind entsprechende Managementberichte zu erstellen, die zum einen die Aktivitäten dokumentieren und zum anderen die Basis für die Optimierung bilden.

1.2.3.2 Standard 100-2

Dieser Standard beschreibt im Wesentlichen die Initiierung des Sicherheitsprozesses und die Umsetzung der Sicherheitskonzeption. Dabei wird bei der Maßnahmenauswahl explizit auf die gesonderten Grundschutz-Kataloge verwiesen. Die Grundschutz-Kataloge sind zur besseren Erweiterbarkeit modular aufgebaut und enthalten die folgenden Teile:

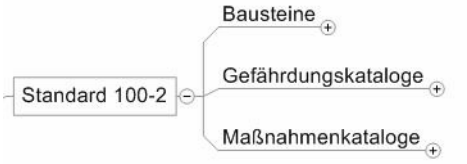


Abbildung 1.14: Aufbau der Grundschutz-Kataloge

Struktur der Grundschutz-Kataloge

Bausteine

- B 1: Übergreifende Aspekte
- B 2: Infrastruktur
- B 3: IT-Systeme
- B 4: Netze
- B 5: Anwendungen

Gefährdungskataloge

- G 1: Höhere Gewalt
- G 2: Organisatorische Mängel
- G 3: Menschliche Fehlhandlungen
- G 4: Technisches Versagen
- G 5: Vorsätzliche Handlungen

Maßnahmenkataloge

- M 1: Infrastruktur
- M 2: Organisation
- M 3: Personal
- M 4: Hard- und Software
- M 5: Kommunikation
- M 6: Notfallvorsorge

Dabei wird so vorgegangen, dass für jeden in Frage kommenden Baustein die individuellen Gefährdungen anhand der Gefährdungskataloge identifiziert werden. Hiermit soll nach den Angaben des BSI ein verringerter Analyseaufwand bei typischen Anwendungsfällen erforderlich sein und somit kostengünstig ein angemessenes Sicherheitsniveau bei durchschnittlichem Schutzbedarf erreicht werden.

Ebenfalls ist in diesem Standard die Zertifizierung nach ISO 27001 beschrieben, für die das BSI zugelassen ist.

1.2.3.3 Standard 100-3

Sofern ein Unternehmen bereits eine IT-Grundschutzanalyse durchgeführt hat, liefert das BSI mit diesem Standard darüber hinaus die Möglichkeit einer weitergehenden Risikoanalyse für den IT-Bereich. Diese zusätzliche Risikoanalyse bietet sich an bei einem erhöhten Schutzbedarf, beispielsweise beim Thema Vertraulichkeit oder bei Anwendungsfällen, die in den Grundschutz-Katalogen nicht ausreichend beschrieben sind.

Im Rahmen des Sicherheitsprozesses würde sich nach der Standard-Sicherheitsüberprüfung die ergänzende Sicherheitsanalyse anschließen, bevor die Realisierung der Sicherheitsmaßnahmen vorgenommen wird.

1.2.3.4 Standard 100-4

In diesem noch nicht offiziell vorliegendem Standard (Version 0.7 vom Februar 2008) werden die Anforderungen an das Notfallmanagement beschrieben. Ähnlich wie der Standard 100-3 stellt auch dieser Standard eine Ergänzung des Standards 100-2 dar, um gezielt auf die Besonderheiten des Notfallmanagements eingehen zu können. Das grundsätzliche Erfordernis zur Einrichtung eines Notfallmanagements leitet sich bereits aus den allgemeinen Anforderungen an das Sicherheitsmanagement, wie sie im Standard 100-1 beschrieben werden, ab.

Notfalldokumentation

In der Entwurfsfassung wird die Notwendigkeit zur Erstellung eines Notfallhandbuches festgelegt. In diesem Zusammenhang werden unter anderem folgende Dokumente gefordert:

- Leitlinie zum Notfallmanagement
- Bericht der Business Impact-Analyse
- Bericht der Risikoanalyse
- Notfallvorsorgekonzept
- Notfallhandbuch inkl. Geschäftsfortführungsplänen
- Melde- und Eskalationswege
- Übungskonzept, Übungspläne und Übungsanlagen

Gemäß dem Standard sind Aktualität und regelmäßige Überarbeitung der Dokumente besonders wichtig. Weiter werden zusätzliche Angaben spezifiziert, die in den Dokumenten enthalten sein sollen:

- Eindeutige Bezeichnung (aussagekräftiger Titel)
- Ersteller / Autor
- Versionsnummer
- Letzte Überarbeitung, nächste geplante Überarbeitung
- Freigegeben am/durch
- Klassifizierung (z. B. Vertraulichkeit)
- Verteilerkreis
- Aufbewahrungszeitraum

Inhalt Notfallkonzept

Entsprechend dem Sicherheitskonzept ist ein Notfallkonzept (Leitlinie) zu erstellen, das u. a. folgende Themen beinhalten soll:

- Definition eines Notfallmanagements
- Stellenwert des Notfallmanagements und dessen Bedeutung für die Institution
- relevante Gesetze, Richtlinien und Vorschriften
- Geltungsbereich mit Angaben zu Grenzen und Ausschlüssen
- Kernaussagen der Notfallstrategie
- Struktur der Aufbauorganisation und deren wichtigsten Rollen

Auch der Aufbau eines Notfallhandbuches ist in dem Standard beschrieben. Sofern dieser Standard mit diesen Inhalten veröffentlicht wird, bildet er eine umfassende Grundlage für den Aufbau und die Dokumentation eines Notfallmanagements.

1.2.4 Prüfungsstandards

Das Erfordernis zur Prüfung der Geschäfte eines Unternehmens ergibt sich aus der nationalen und internationalen Rechtslage. Die Prüfung des Jahresabschlusses durch eine Wirtschaftsprüfungsgesellschaft hat dabei die breiteste Gesetzesbasis, nämlich das Aktiengesetz, die 8. EU-Richtlinie und eventuell SOX. Die Prüfung durch die interne Revision ergibt sich aus dem KonTraG sowie gegebenenfalls durch die MaRisk. Die Prüfungspflichten des ab 2009 zu bildenden Prüfungsausschuss wiederum basieren auf entsprechenden Festlegungen der 8. EU-Richtlinie und gegebenenfalls SOX.

Im Gegensatz zu dem Prüfungsausschuss, für den es noch keine ausformulierten Prüfungsstandards gibt, haben die berufsständischen Organisationen für die Wirtschaftsprüfer (IDW) und für die interne Revision (DIIR) konkrete Prüfungsstandards erlassen, die im Laufe der Zeit weiterentwickelt und ergänzt werden.

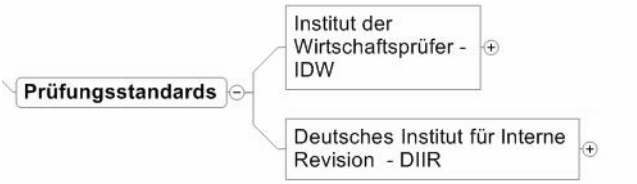


Abbildung 1.15: Berufsständische Prüfungsstandards

1.2.4.1 Institut der Wirtschaftsprüfer in Deutschland (IDW)

Bei den Prüfungsstandards (PS) des Instituts der Wirtschaftsprüfer in Deutschland e. V. (IDW) ist für die IT im Wesentlichen der *PS 330 - Abschlussprüfung bei Einsatz von IT* von Bedeutung. Dieser stellt eine Umsetzung des internationalen Prüfungsstandards ISA 401 dar. Danach hat der Abschlussprüfer das IT-gestützte Rechnungslegungssystem dahingehend zu beurteilen, ob die gesetzlichen und im Fachausschuss Informationstechnologie des IDW formulierten Anforderungen an die Ordnungsmäßigkeit und die Sicherheit (FAIT 1) erfüllt werden. Damit werden die GoBS als rechtliche Basis für den Prüfungsstandard herangezogen und entsprechend bei der Abschlussprüfung berücksichtigt. Daneben sind die beiden Prüfungsstandards 850 und 880 für den IT-Bereich relevant.

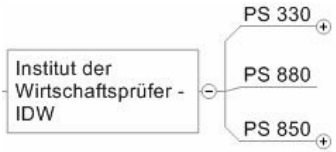


Abbildung 1.16: IT-relevante Prüfungsstandards

PS 330

Die im Rahmen des PS 330 durchgeführten IT-Systemprüfungen haben folgende Struktur: [PS330]

- Aufnahme des IT-Systems
- IT-Umfeld und IT-Organisation
- IT-Infrastruktur
- IT-Anwendungen
- IT-Geschäftsprozesse
- Aufbauprüfung (Beurteilung der Angemessenheit)
- Funktionsprüfung (Prüfung und Beurteilung der Wirksamkeit)

Aus der Struktur wird erkennbar, dass es sich dabei weniger um einen prozessorientierten, sondern eher um einen funktionsbezogenen Prüfungsansatz handelt. In jedem Fall aber wird die den zu prüfenden Objekten zugrunde liegende Dokumentation mit einbezogen. Ein eventueller Dokumentationsmangel, sei es wegen fehlender oder unvollständiger Unterlagen, führt gegebenenfalls zu einer entsprechenden Feststellung im Abschlussbericht.

Auch wenn gemäß den gesetzlichen Anforderungen nur die rechnungslegungsrelevanten Prozesse und Systeme geprüft werden, ist doch ein großer Teil der IT davon betroffen. So werden zum Beispiel die Sicherheits- und Kontrollstrukturen nicht nur im Hinblick auf die Anwendungssysteme, sondern auch im Hinblick auf die Datenbank- und Systembasis geprüft.

PS 880

Während die Prüfungen nach dem PS 330 auf implementierte Anwendungen und Systeme ausgerichtet sind, stellt der *PS 880 - Erteilung und Verwendung von Softwarebescheinigungen*, einen Prüfungsstandard dar, der die Anwendungen (Softwareprodukte) vor der Implementierung prüft. Ein derartiges Prüftestat bescheinigt dem Unternehmen, dass seine entwickelte Software den Grundsätzen ordnungsgemäßer DV-gestützter Buchführungssysteme entspricht.

PS 850

In Zukunft wird auch der Prüfungsstandard *PS 850 - Projektbegleitende Prüfung bei Einsatz von Informationstechnologie* bedeutend. Derzeit liegt der Standard im Entwurf vom September 2007 vor und beschreibt auf Basis der Ordnungsmäßigkeitsanforderungen des PS 330 die Prüfungsanforderungen zu den Projektphasen [PS850]

- Planung,
- Entwicklung bei Individualsoftware,
- Test,
- Datenmigration,
- Produktivsetzung.

Entsprechend der umfassenden Bedeutung des Projektbegriffs werden durch den Prüfungsstandard die Planung, Einführung sowie die Änderung von IT-Systemen im Rahmen eines Projekts erfasst.

1.2.4.2 Deutsches Institut für Interne Revision e. V. (DIIR)

Im Gegensatz zu den Prüfungsstandards des IDW, die auf die rechnungslegungsrelevanten Anwendungen und Verfahren ausgerichtet sind, decken die Revisionsstandards des Deutschen Instituts für Interne Revision e. V. (DIIR) die gesamte Breite der Unternehmensprozesse als Prüfungsgegenstand ab [DIIR].

Ebenfalls im Gegensatz zu den auf den Jahresabschluss ausgerichteten Prüfungshandlungen der Abschlussprüfer sind die Prüfungsaktivitäten der Konzernrevision in erster Linie nicht anlassbezogen, sondern stellen eine permanente Überwachung der Aufbau- und Ablauforganisation des Unternehmens dar. Die interne Revision ist Teil des internen Überwachungssystems, das die Geschäftsleitung gemäß § 91 AktG (und damit gemäß KonTraG) einzurichten hat.

Drei Revisionsstandards

Während die Prüfungsstandards des IDW konkrete Prüfungsfelder und -themen zum Gegenstand haben, beschreiben die Revisionsstandards des DIIR die grundsätzliche Arbeitsweise und die qualitativen Anforderungen an die Revisionsausübung. Das DIIR hat drei Standards herausgegeben, die sich inhaltlich an die Standards des amerikanischen *The Institute of Internal Auditors (IIA)* anlehnen.

- Revisionsstandard Nr. 1:
  Zusammenarbeit von interner Revision und Abschlussprüfer
- Revisionsstandard Nr. 2:
  Prüfung des Risikomanagements durch die interne Revision
- Revisionsstandard Nr. 3:
  Qualitätsmanagement in der Internen Revision

Kriterien Revisionsstandard 1

Gemäß dem Revisionsstandard Nr. 1 werden die Prüfungen der internen Revision nach folgenden Kriterien durchgeführt:

- Risiken
- Ordnungsmäßigkeit
- Sicherheit
- Wirtschaftlichkeit
- Zukunftssicherung
- Zweckmäßigkeit

Zusätzlich zu den Revisionsstandards hat das DIIR eine Sammlung von „Praktischen Ratschlägen" veröffentlicht, die eine Übernahme der „Practice Advisories" des IIA darstellen.

Mit den Standards deckt die interne Revision nicht nur inhaltlich ein breiteres Prüfungsfeld ab als der Abschlussprüfer, der sich bei seiner Abschlussprüfung auf rechnungslegungsrelevante Daten und Verfahren konzentriert. Auch die Kriterien, nach denen geprüft wird, sind bei der internen Revision breiter als bei einem Abschlussprüfer, der im Wesentlichen die Ordnungsmäßigkeit sowie die Übereinstimmung mit Gesetzen und unternehmensbezogenen Regelungen wie dem Gesellschaftsvertrag überprüft.

Revisionsstandard 2

Der Prüfung des Risikomanagements wird eine besondere Bedeutung im Rahmen der Revisionsaufgaben eingeräumt, was in dem Revisionsstandard Nr. 2 zum Ausdruck kommt. Hier werden wesentliche Prüfungsansätze beschrieben, die auch bei der Prüfung von IT-Verfahren angewandt werden.

Ein zentraler Prüfungsgegenstand dabei sind die Organisationsgrundlagen wie Richtlinien, Handbücher und Arbeitsanweisungen, in denen die organisatorischen Regelungen zur Planung Steuerung und Kontrolle der Prozesse als Sollvorgaben beschrieben sind. Zu prüfen sind aber nicht nur die Sollvorgaben selbst, sondern insbesondere auch, ob die tatsächlichen Abläufe, also die Ist-Abläufe, den Sollvorgaben entsprechen. Insgesamt hat die Interne Revision zu bewerten, ob die geprüften Organisationseinheiten oder Prozesse die genannten Prüfungskriterien erfüllen. Sie hat gegebenenfalls Empfehlungen zur Zielerreichung zu unterbreiten. In den „Praktischen Ratschlägen" sind die Anforderungen an die Prüfungstätigkeiten konkretisiert.

1.3 Modelle

Wie in der Einleitung bereits ausgeführt, dienen die Modelle zur Ausrichtung und Optimierung der IT-Organisation einer definierten Struktur bzw. Vorgehensweise. Sofern eine Entscheidung zur Ausrichtung der IT-Organisation an ein Modell getroffen wird, hängt die Wahl des Modells von dem unternehmenseigenem Bedürfnis ab.

Für den IT-Bereich spielen derzeit die beiden Modelle *IT Infrastructure Library* und *COBIT (Control Objectives for Information and Related Technology)* die Hauptrolle. Die Bedeutung beider Modelle wird auch dadurch deutlich, dass ITIL vor allem auch in ISO bzw. BSI und COBIT in SOX verankert sind. Beide Modelle werden im Folgenden näher vorgestellt:

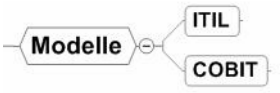


Abbildung 1.17: IT-relevante Modell

Das insbesondere in Europa bekanntere Modell ist ITIL. Es stellt den Servicegedanken in den Vordergrund und richtet die IT-Prozesse dementsprechend serviceorientiert aus.

In Amerika haben die beiden Modelle *COBIT (Control Objectives for Information and Related Technology)* und *COSO (The Committee of Sponsoring Organizations of the Treadway Commission)* weite Verbreitung gefunden, wobei COBIT eine Weiterentwicklung von COSO darstellt. Diese Modelle stellen den Compliance-Ansatz in den Vordergrund. Indem diese Modelle angewandt werden, soll die IT-Organisation rechtskonform ausgerichtet werden. Eine besondere Bedeutung haben die beiden Modelle durch das amerikanische Gesetz *Sarbanes-Oxley Act (SOX)* erhalten, in dessen Auslegung die Anwendung eines Compliance-orientierten Modells wie COSO empfohlen wird. Da COBIT auf COSO aufbaut, werden beide Modelle als Grundvoraussetzungen angesehen, wenn es darum geht, die SOX-Anforderungen zu erfüllen.

Welche Bedeutung diese inzwischen in der IT anerkannten Modelle erlangt haben, mag der Umstand belegen, dass sie in Gesetzen und Normen verankert sind. Während COSO und COBIT durch SOX eine wesentliche Bedeutung erlangen, ist ITIL inzwischen im noch relativ neuen ISO-Standard 20000 aus dem Jahr 2005 verankert.

hinweis

Da die einzelnen Modelle in der IT-Literatur ausführlich beschrieben werden, soll an dieser Stelle ein kurzer Überblick über die Modelle ITIL und COBIT reichen. Bei Bedarf wird an anderen Stellen des Buches auf die Modelle näher eingegangen.

1.3.1 ITIL

ITIL ist das Modell für eine serviceorientierte IT-Organisation. Es wurde von der britischen Regierung in der Version 2 im Jahr 2001 veröffentlicht und ist in dem britischen Standard (BS) 15000 als zertifizierbare Norm enthalten. Der BS 15000 wiederum wurde in dem ISO-Standard 20000 überführt, womit es für ITIL indirekt ebenfalls einen international anerkannten Standard gibt. Auch Microsoft hat bei seinem Model *Microsoft Operations Framework (MOF)* ITIL zugrunde gelegt [ITIL].

Das ITIL-Framework ist in neun Bücher aufgeteilt, von denen sich zwei, nämlich *Service-Support* und *Service-Delivery*, als wesentlicher Kern im IT-Bereich durchgesetzt haben.

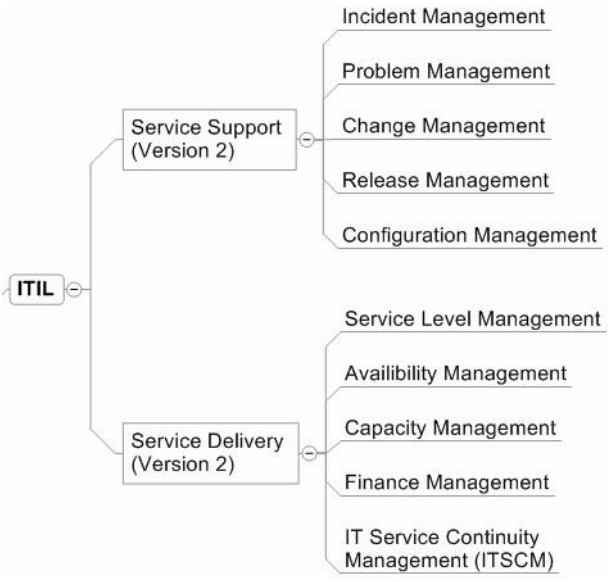


Abbildung 1.18: Komponenten des IT-Servicemanagements bei ITIL V2

Service Support

Dem Service Support, der für den (störungsfreien) Regelbetrieb sowie für die Sicherstellung der Leistungsfähigkeit (wichtig für die Erfüllung von SLAs) verantwortlich ist, werden die folgenden Aufgaben zugeordnet:

- Das *Incident Management* hat zwei Hauptaufgaben: Zum einen behandelt es Störungsmeldungen (Incidents) und sorgt für deren Beseitigung, entweder selbst (First-Level-Support) oder per definierter Eskalation. Zum anderen nimmt es Vorschläge zur Verbesserung der Servicequalität (Service Requests) auf und behandelt sie wie Störungsmeldungen. Der aufbauorganisatorische Dreh- und Angelpunkt ist der Service-Desk, das den alleinigen Kontakt (Single Point of Contact) mit dem Kunden herstellt.

- Das *Problem Management* nimmt die Informationen aus dem Incident Management auf und realisiert die Fehler- bzw. Problembehebung, soweit dies nicht bereits durch das Incident Management erfolgen konnte. Eine weitere Aufgabe ist die Überwachung des Betriebes im Hinblick auf eine vorausschauende Problemvermeidung.
- Die Verarbeitung von Änderungsanforderungen wird im Rahmen des *Change Managements* vorgenommen. Dabei hat das Change Management zunächst die Aufgabe, die Notwendigkeit und die wirtschaftliche Durchführbarkeit der Anforderung zu untersuchen und zu bewerten. Die Entscheidung, ob eine Veränderung vorgenommen wird, trifft bei kleineren oder Standardänderungen, für die es einen definierten Change-Prozess gibt, der Change-Manager. Bei umfangreicheren oder risikoreicheren Veränderungen muss das zentrale Gremium (Change Advisory Board) entscheiden. Die Realisierung der Änderungsanforderung und die Erfolgskontrolle wird ebenfalls vom Change Management vorgenommen.
- Das *Release Management* ist in Zusammenarbeit mit dem Change Management für die Planung, Durchführung und Überwachung insbesondere bei umfangreichen Änderungen an der Hard- und Software zuständig. Dem Release Managemnt kommt hier die wichtige Aufgabe der vollständigen Dokumentation sowohl des Bestandes als auch der Veränderungen der Hard- und Software zu.
- Das *Configuration Management* bildet die gesamte IT-Infrastruktur in einem logischen Modell ab und bildet somit den Kernbereich der Datenvorhaltung im Rahmen des IT-Servicemanagements. Auf diese zentrale Datenbasis gemäß ITIL *Configuration Management Database (CMDB)* greifen alle Prozesse des Service-Supports zu. Auch wenn von ITIL keine (technischen) Vorgaben über die Realisierung dieser CMDB gemacht werden, so ist es doch nachvollziehbar, dass wegen der erheblichen Komplexität heutiger IT-Umgebungen hierfür nur ein leistungsfähiges Datenbanksystem in Frage kommen kann.

Service Delivery

Während der Service Support die betrieblichen Strukturen des Service Managements beschreibt, umfasst das Service Delivery die verwaltungsbezogenen Managementprozesse. Sie sind u. a. zuständig für die Ausgestaltung der Kundenbeziehungen, aber auch für die Planung und Steuerung der Support-Prozesse. Nach ITIL werden dem Service Delivery die folgenden Aufgaben zugeordnet:

- Das *Service Level Management* legt Art, Umfang und Qualität der Dienstleistungen für den Kunden fest. Auf der einen Seite verhandelt das Service Level Management mit den Kunden (beispielsweise die Vereinbarung von SLAs) und auf der anderen Seite koordiniert es die internen Servicemanagement-Prozesse. Ihren Niederschlag finden die vereinbarten Services im sogenannten Service-Katalog, der den Charakter eines Lastenheftes annimmt. Die einzelnen Kataloge können in der CMDB abgelegt sein.

- Das *Availibility Management* ist für die Einhaltung der vereinbarten Services verantwortlich. Hierzu werden einerseits Bedarfsprognosen erstellt und andererseits auf der Basis von Überwachungsmaßnahmen Vorschläge zur Optimierung der Leistungsfähigkeit erarbeitet. Hier werden u. a. interne Richtlinien erstellt und unterstützende Maßnahmen durchgeführt. Ein wichtiges (Dokumentations-)Instrument stellt der Verfügbarkeitsplan dar, in dem die technischen, personellen und auch finanziellen Aspekte berücksichtigt werden.
- Während das Availability Management für die Sicherstellung der Leistungsfähigkeit des Service Managements zuständig ist, ist das *Capacity Management* darauf ausgerichtet, wirtschaftliche und technisch erforderliche Lösungen zu erarbeiten, damit im Falle einer schnellen Marktveränderung nicht überhastet und damit unüberlegt reagiert wird. Somit ist das Availability Management für die proaktive Steuerung der Serviceangebote zuständig. Die Planung des optimalen Einsatzes der Ressourcen, also auch des Personals, ist eine zentrale Aufgabe. Die Datenhaltung und Datenverarbeitung findet in einer eigenständigen Datenbank, der Capacity Management Database, statt. Diese wird teilweise mit Ist-Daten aus der CMDB gefüllt und enthält Szenarien und strategische Daten für künftige Serviceangebote.
- Das *Finance Management* (for IT-Services) ist zuständig für alle Fragen zum externen und internen Rechnungswesen sowie der Budgetierung. Dabei ermittelt das Finance Management nicht nur die Daten, sondern ist auch an der Preisgestaltung für die angebotenen Dienstleistungen mit zuständig. Es liefert zudem wirtschaftliche Entscheidungsgrundlagen für die Managementebene hat die Aufgabe, für ein angemessenes Kostenbewusstsein im Unternehmen zu sorgen.
- Das *IT Service Continuity Management (ITSCM)* ist dafür verantwortlich, dass in einer Notfallsituation der Betrieb, also die Leistungserbringung, aufrechterhalten bleibt oder entsprechend wieder hergestellt wird. Im Katastrophenfall kann das ITSCM die Überlebensfähigkeit des Unternehmens sicherstellen. Hierzu erstellt es Risikoanalysen und für die zu definierenden Notfallsituationen spezifische Notfallpläne.

ITIL Version 3

Auch wenn ITIL 2005 in den ISO-Standard 20000 Eingang gefunden hat, so ist es doch grundlegend in Richtung Service Lifecycle weiterentwickelt worden und liegt seit 2007 in der Version 3 (ITIL V3) vor. Das Ziel von ITIL V3 ist eine noch stärkere Kundenorientierung durch weiter optimierte IT-Prozesse [ITILB].

Auch das ITIL-Framework selbst ist, obwohl weitere Prozesse hinzugekommen sind, gestrafft worden und enthält nunmehr die folgenden fünf Bücher:

- *Service Strategy*
  (Kombination von IT- und Unternehmensstrategie)
- *Service Design*
  (Entwicklung von Kundenlösungen und Gestaltung von Prozessen)

- *Service Transition*
  (Planung und Einführung neuer bzw. geänderter Prozesse)
- *Service Operation*
  (Der eigentliche Servicebetrieb inkl. Kundenschnittstelle)
- *Continual Service Improvement*
  (Permanente Serviceverbesserung mit siebenstufigem Prozess)

Weitere Informationen zum Thema ITIL finden Sie in 978-3-8273-2599-0, ITIL V3 Basis-Zertifizierung, das ebenfalls im Verlag Addison-Wesley erschienen ist.

1.3.2 COBIT

COBIT (Control Objectives for Information and Related Technology) wurde 1995 vom Internationalen Verband der IT-Prüfer (Information Systems Audit and Control Association, ISACA) als Grundlage für IT-Prüfungen ve/röffentlicht. Es wurde aus COSO entwickelt, dass ebenfalls ein Modell zur Compliance-orientierten Managementstruktur des gesamten Unternehmens darstellt. COBIT ist ein auf die Informationstechnologie ausgerichtetes Steuerungsmodell und liegt derzeit in der Version 4 vor, die aus den folgenden vier Büchern besteht: [COBIT]

- Core Content
- IT Assurance Guide
- Implementation Guide
- Control Practices

Im Core Content werden 34 Prozesse beschrieben, denen mehr als 200 sogenannte „Control Objectives" (Steuerungsvorgaben) zugeordnet sind. Somit werden für die einzelnen Prozesse zu erreichende Ziele festgelegt. Den Prozessen werden weitere beschreibende Größen zugeordnet, die im Folgenden genannt werden:

- Prozessbeschreibung
- Prozessziel
- Wesentliche Aktivitäten
- Wesentliche Messgrößen
- Control Objectives
- Management Guidelines
  - mit den Prozesses-Inputs und Prozesses-Outputs
  - mit der RACI-Matrix (für Aufgaben und Zuständigkeiten)
  - Mess- und Zielgrößen zur Prozessbeurteilung
- Reifegradmodell – angelehnt an CMMI

Die 34 Prozesse sind – dem Deming-Kreis entsprechend – in vier sogenannte Domänen aufgeteilt und haben folgende Bezeichnungen:

- PO – Planning and Organisation
- AI – Acquisition and Implementation
- DS – Delivery and Support
- M – Monitoring

Im IT Assurance Guide sind konkrete Prüfleitfäden zu den Prozessen und Objectives enthalten. In den Control Practices (Steuerungsleitfaden) sind für die Objectives Maßnahmen enthalten, wie diese erreicht werden können. Der „Implementation Guide" (Umsetzungsleitfaden) enthält Methoden und Maßnahmen für das Unternehmensmanagement, wie eine IT-Governance zu implementieren ist.

1.4 Fazit

Es gibt also keinen allgemein gültigen Standard oder gar ein Gesetz, der bzw. das festlegt, wie eine IT-Dokumentation auszusehen hat. Eindeutig aber ist, dass eine IT-Dokumentation zu erstellen ist. Was lässt sich für diese aber konkret aus den betrachten Gesetzen, Normen und Modellen ableiten?

Verfahrensdokumentation erforderlich

Betrachtet man zunächst die unternehmensbezogenen Gesetze, so ergeben sich bereits aus den Ausführungen des Handelsgesetzbuches Ansätze, nach denen eine Verfahrensdokumentation zu pflegen ist. Auch die Abgabenordnung enthält Forderungen, die in Richtung einer nachvollziehbaren Dokumentation der Geschäftsvorfälle und Geschäftsabläufe abzielen.

Konkreter werden bereits die GoBS. In den „Grundsätzen ordnungsgemäßer DV-gestützter Buchführungssysteme" wird eine Verfahrensdokumentation gefordert, aus der Inhalt, Aufbau und Ablauf des Abrechnungsverfahrens vollständig ersichtlich sein müssen. Die Anforderungen an die Verfahrensdokumentation sind unabhängig von der Größe der genutzten DV-Anlage (Hardware) und gelten sowohl für Großrechnersysteme als auch für PC-Systeme. Betrachtet man die vorgestellten Anforderungen der GoBS genauer, so wird deutlich, dass diese sogar sehr hoch sind. So ist beispielsweise der Änderungsstand von Tabellen zu jedem Zeitpunkt der letzten zehn Jahre festzuhalten. Weiter fordert die GoBS, dass Arbeitsanweisungen, für die Anwender zur sachgerechten Erledigung und Durchführung ihrer Aufgaben erstellt werden müssen. Es ist also noch nicht einmal erforderlich, Qualitätsmanagementstandards wie ISO 9000 bzw. 20000 oder abgeleitete Gesetze wie KontraG heranzuziehen, um die Notwendigkeit für eine Verfahrensdokumentation abzuleiten.

Als ein erster und wesentlicher Baustein einer IT-Dokumentation ist demzufolge eine prozessorientierte Betriebsdokumentation zu erstellen und zu pflegen. Wie das Kapitel weiter gezeigt hat, sind an diese Dokumentation zusätzliche Anforderungen zu stellen, wie sie sich beispielsweise aus dem Datenschutzgesetz ableiten lassen.

Daneben wird aus den allgemeinen Bilanzierungserfordernissen heraus eine Bestandsdokumentation benötigt. So ist beispielsweise sowohl für Hard- als auch für Software ein Anlagenverzeichnis zu führen. Somit ist die wesentliche Basis für eine Systemdokumentation bereits gegeben.

Sicherheit hat einen hohen Stellenwert

Neben den Anforderungen an das Qualitätsmanagement rückt die Sicherheit der IT immer stärker in den Fokus. Die Sicherheit der betrieblichen IT ist Gegenstand diverser Prüfungen. Zu nennen ist hier vor allem die ISO 27001 (sie beschreibt die Anforderungen an das Informationssicherheitsmanagement), die die Grundlage der Prüfungen des BSI darstellt. Und auch bei den auf den Jahresabschluss ausgerichteten Prüfungshandlungen der Abschlussprüfer sowie bei den Prüfungsaktivitäten der internen Revision ist die IT-Sicherheit ein wichtiger Gegenstand. Hierbei wird das IT-Sicherheitsmanagement als Teil des Risikomanagements des Unternehmens geprüft und bewertet. Das Unternehmen ist dabei selbst verantwortlich für eine hohe IT-Sicherheit – unabhängig davon, ob sie die IT selbst betreibt oder ausgelagert hat.

Vor allem aber ist die IT-Sicherheit die Grundlage für eine störungsfreie Geschäftstätigkeit: Sie gewährleistet, dass erforderliche Daten tatsächlich verfügbar sind, dass schützenswerte Daten vertraulich bleiben und dass ein Unternehmen mit unverfälschten und zuverlässigen Daten arbeiten kann. An die Sicherheit von Finanzdienstleister werden zusätzliche hohe gesetzliche und aufsichtsrechtliche Anforderungen gestellt. So haben diese bereits heute die MaRisk zu erfüllen. Und diese fordert in Bezug auf die IT-Organisation und IT-Dokumentation ausdrücklich ein Notfallhandbuch, das Geschäftsfortführungs- sowie Wiederanlaufpläne umfasst.

Notfallhandbuch erforderlich

Als ein weiterer wichtiger Baustein der IT-Dokumentation ist demzufolge ein Notfallhandbuch zu erstellen, das in das Sicherheits- und Risikomanagement des Unternehmens eingebunden ist.

2 Bausteine einer IT-Dokumentation

Erstellen Sie dann mal das Betriebshandbuch für das neue System! Diesen Satz hat wohl schon so mancher Administrator gehört und sich gefragt, was eigentlich genau ein Betriebshandbuch ist. Gehört die Beschreibung einer Installation ebenfalls in das Betriebshandbuch? Und was ist mit den Prozessbeschreibungen?

Das nachfolgende Kapitel entwickelt, ausgehend von einem prozessorientierten Unternehmensansatz, die Strukturierung für eine *IT-Dokumentation*. Die herausgearbeiteten Bestandteile werden anschließend im Überblick und als Vorbereitung auf die Hauptkapitel erläutert.

2.1 Die Rolle der IT in einem prozessorientierten Unternehmen

In der Einleitung wurde darauf hingewiesen, dass im Folgenden von einem prozessorientierten Unternehmensansatz ausgegangen wird. Was ist darunter zu verstehen?

Lange Zeit war die vorherrschende Organisationsform von Unternehmen funktionsorientiert. Diese funktionsorientierte Form ist geprägt durch vertikale Hierarchien, eine aufbauorganisatorische Struktur und eine starke Trennung zwischen Fach- und Ressourcenverantwortung.

Was heißt prozessorientiert?

Bei einer prozessorientierten Ausrichtung stehen die Geschäftsprozesse im Mittelpunkt der betrieblichen Organisation. Die Arbeitsabläufe erfolgen nicht mehr anhand der typischen vertikal ausgerichteten Hierarchien. Vielmehr stehen idealtypischerweise die Kunden, Mitarbeiter und Prozesse im Mittelpunkt. Alle Tätigkeiten, die das Unternehmen durchführt, werden in Prozessen dargestellt.

Ein *Prozess* ist hierbei als eine Kette aufeinander aufbauender, funktionsübergreifender Arbeitsschritte bzw. Aktivitäten zu betrachten, durch die ein klar definierter Input in einen definierten (materiellen oder immateriellen) Output umgewandelt wird. Er beginnt mit einem definierten Auslöser und endet mit einem definierten Ergebnis. Alle Prozesse sind jeweils einem Prozessverantwortlichen unterstellt. Dieser ist für die Ergebnisse verantwortlich und übernimmt die Koordination innerhalb der Prozesse und zwischen diesen. Die Mitarbeiter werden dabei bestimmten Prozessteams zugeordnet, die einen Prozess vom Anfang bis zum Ende betreuen. Dadurch entstehen flache Hierarchien mit kurzen Informationswegen. Im Idealfall werden die Selbstorganisationsfähigkeiten der Teams gestärkt.

beispiel

Ein kleines Beispiel aus dem IT-Bereich soll dies verdeutlichen: Beim funktionsorientierten Ansatz gibt es einen Administrator für die Benutzerverwaltung und einen für das Mailsystem. Außerdem gibt es noch eine Organisationseinheit, die für die Clientrechner zuständig ist. Kommt nun ein neuer Mitarbeiter in das Unternehmen, werden in vollkommen separaten Arbeitsschritten durch unterschiedliche Personen mit dementsprechend eingeschränkten Befugnissen ein neues Benutzerkonto, ein Postfach und ein Arbeitsplatzrechner für den neuen Mitarbeiter eingerichtet. Es ist leicht vorstellbar, dass es hierbei zu Kommunikationsproblemen und Schwierigkeiten bei der Abgrenzung der Verantwortung kommen kann.

Beim prozessorientierten Ansatz hingegen gibt es einen Prozess „Neuer Mitarbeiter". Dieser benötigt einen Arbeitsplatz mit Tisch und Stuhl, einen Rechner, ein Benutzerkonto, ein Postfach und diverse Zugriffe. Alle diese Tätigkeiten werden als eine Abfolge von Tätigkeiten betrachtet, die von einer (einzigen) Person verantwortet und koordiniert werden. Alle Informationen bleiben in einer Hand, die Abstimmungsprozesse werden somit reduziert.

Unterteilung in Prozessgruppen

Typischerweise werden die Unternehmensprozesse in Prozessgruppen unterteilt. Die Geschäftsprozesse können gemäß der Qualitätsmanagementnorm der Normenreihe ISO 9000 in drei Gruppen unterteilt werden:

- *Managementprozesse* steuern das Unternehmen. Sie legen die Unternehmensziele fest, definieren und bewerten die damit verbundenen Risiken und überwachen die Zielerreichung,

- Der wertschöpfende Betriebsablauf eines Unternehmens besteht aus *Kernprozessen* und *Nebengeschäftsprozessen*, die sich aus dem Unternehmenszweck ergeben (hierbei kann es sich sowohl um Produktions- als auch um Dienstleistungsprozesse handeln). Beispielsweise ist der Verkauf von Reisen für ein Reisebüro unzweifelhaft ein Kernprozess. Zusätzlich betreiben viele Unternehmen Nebengeschäfte, die jedoch keine Kernprozesse darstellen. Für das im Beispiel gewählte Reisebüro ist der Verkauf von Eintrittskarten für Veranstaltungen ein Nebengeschäft. Beiden gemeinsam ist der wertschöpfende Charakter der Prozesse.
- Daneben gibt es sogenannte *Serviceprozesse* (auch als *Unterstützungsprozesse* bezeichnet), die ausschließlich darauf ausgerichtet sind, die Kernprozesse des Unternehmens zu unterstützen, indem sie betriebliche Ressourcen bereitstellen und diese verwalten. Diese Prozesse erzeugen keinen direkten Kundennutzen. Zu den Serviceprozessen zählen beispielsweise das interne und externe Rechnungswesen, das Personalwesen und die IT.

Serviceprozesse nur selten dokumentiert

Historisch bedingt sind die genannten drei Prozessbereiche häufig sehr unterschiedlich gut dokumentiert Während viele technische Abläufe innerhalb der Kernprozesse sehr gut beschrieben sind, wurde für die meisten Serviceprozesse eine Dokumentation häufig als nicht erforderlich angesehen. So gibt es wohl kaum eine technische Anlage, für die nicht in irgendeiner Form eine Betriebsanleitung vorliegt. Aber erst mit der immer stärkeren Marktdurchdringung der SAP-Software wurden auch die kaufmännischen Prozesse häufiger dokumentiert.

Gesamtheitliche IT-Dokumentation fehlt häufig

Ähnlich verhält es sich mit den IT-Aufgaben. Hier gab und gibt es viele Insellösungen, die bereits sehr gut dokumentiert sind – insbesondere im Mainframe-Bereich. Außerdem ist diese Dokumentation in aller Regel an den Systemen und nicht an den Prozessen ausgerichtet. Eine gesamtheitliche Dokumentation der IT-Prozesse oder gar die Einbindung der IT-Dokumentation in die Strukturen einer Unternehmensdokumentation ist bisher aber eher selten anzutreffen. Dies liegt nicht zuletzt daran, dass es ein entsprechendes Gesetz hierzu nicht gibt.

Die Beschreibung einer gesamtheitlichen IT-Dokumentation ist ein wesentliches Ziel dieses Buches.

2.2 Struktur der IT-Dokumentation

Die Struktur einer ganzheitlichen Dokumentation für den IT-Bereich muss sich an dessen Hauptaufgaben und deren Prozessen orientieren. Grundsätzlich lassen die sich die IT-Aufgaben in zwei Hauptbereiche unterteilen:

- IT-Betrieb
- Änderungen des IT-Betriebs

Der *IT-Betrieb* lässt sich unterteilen in den Regelbetrieb, das Supportmanagement, das klassischerweise die Supportaufgaben umfasst, sowie das Notfallmanagement, das bei einer schwerwiegenden Störung des Betriebs zum Einsatz kommt und die Wiederherstellung des Betriebs zur Aufgabe hat.

Der Bereich *Änderung* umfasst die Konzeption, die Entwicklung und die Einführung neuer oder geänderter IT-Systeme und -Verfahren. Für die IT spielt dieser Bereich eine wesentliche Rolle, denn nur wenige Branchen sind wohl derartig häufig Änderungen und Anpassungen unterworfen, wie die IT. Dabei können die Auslöser von Änderungen sehr unterschiedlicher Natur sein:

- Gesetzliche Anforderungen
- Organisatorische Anforderungen (beispielsweise organisatorische Umstrukturierungen)
- Technische Anforderungen
- Anforderungen, die sich aus Optimierungsprozessen ergeben

beispiel

Insbesondere aus den Ergebnissen von Optimierungsprozessen ergeben sich häufig Notwendigkeiten zur Veränderung des IT-Betriebs. So ist es beispielsweise möglich, dass Prozesse der proaktiven Kapazitätsüberwachung zeigen, dass es notwendig ist, die Festplattenspeicher eines Servers zu erweitern, womit eine Anpassung des IT-Betriebs ausgelöst wird.

Änderungen im Rahmen von Projekten

Änderungsaufgaben können sowohl innerhalb des IT-Regelbetriebs erfolgen, aber auch im Rahmen von Projekten. Insbesondere größere Veränderungen, die zusätzliche Ressourcen erfordern, werden meist als Projekt durchgeführt. Betrachtet man dazu noch einmal das Beispiel der notwendigen Erweiterung des Festplattenspeichers eines Servers, so gehört diese Erweiterung zu den Aufgaben des Regelbetriebs und erfordert wohl kaum die Durchführung eines Projekts. Ergibt der Optimierungsprozess jedoch, dass es erforderlich ist, ein komplettes SAN-System einzuführen, so ist die Durchführung eines Projekts durchaus gerechtfertigt.

Eine detailliere Betrachtung des Zusammenspiels zwischen IT-Betrieb und Projekten finden Sie aus Sicht des Betriebs in Abschnitt 4.3.1.3 und aus Sicht der Projektdokumentation in Abschnitt 6.3.6.

Wie sich die IT-Dokumentation in der Unternehmensstruktur abbildet, zeigt Abbildung 2.1.

Eine gesamtheitliche Dokumentation für die IT (im Folgenden als *IT-Dokumentation* bezeichnet) muss alle genannten Aufgabenbereiche abdecken. Im nächsten Schritt gilt es, auf der Basis der beschriebenen Aufgaben eine Struktur für eine IT-Dokumentation herauszuarbeiten.

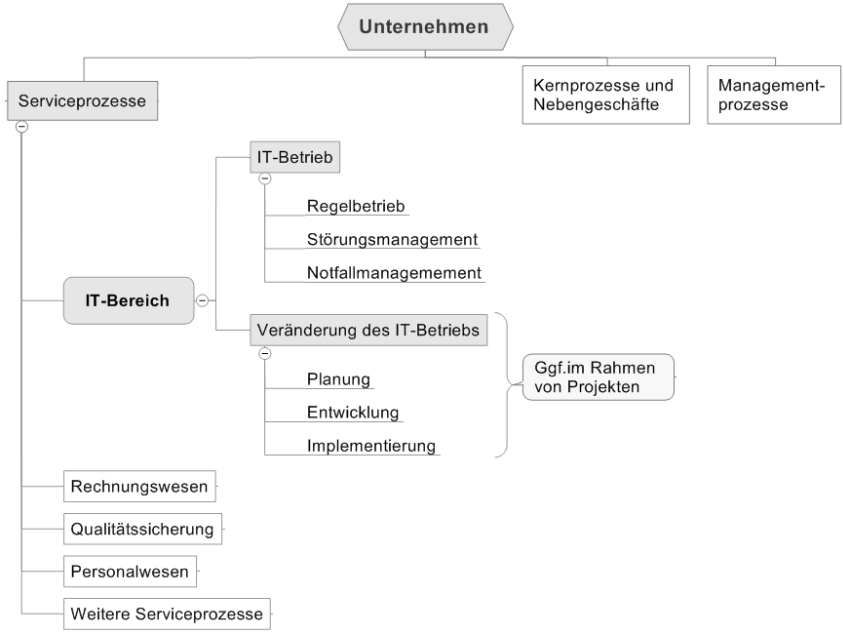


Abbildung 2.1: IT-Dokumentation in der Unternehmenstruktur

2.2.1 Handbuch für den IT-Betrieb

Zur Umsetzung der Dokumentationsanforderungen ist für den IT-Betrieb ein *Betriebshandbuch* zu erstellen und regelmäßig zu pflegen. Dieses dient in erster Linie der Sicherstellung eines reibungslosen Betriebs der IT-Systeme und der Betriebsabläufe.

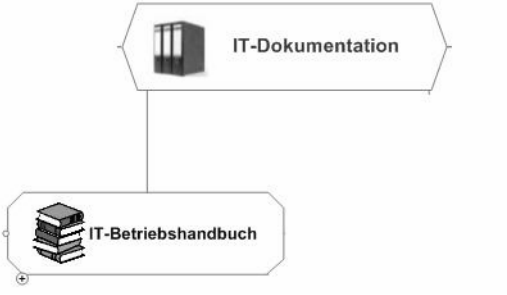


Abbildung 2.2: Ein IT-Betriebshandbuch ist die wichtigste Komponente der IT-Dokumentation.

Welchen Inhalt und Umfang muss ein Betriebshandbuch haben?

Definition Betriebs-handbuch

Wohl viele, die in der Situation sind, ein Betriebshandbuch erstellen zu müssen, werden zunächst bei *www.wikipedia.de* nachschlagen. Im ersten Teil der Erklärung heißt es hier:

> *„In einem Betriebshandbuch sind alle direkten und vorbeugenden Maßnahmen beschrieben, die für den Betrieb einer Anlage notwendig sind. Nicht nur das "Was" und "Wie", also die eigentliche Bedienung, sondern insbesondere auch "Wer" (die Person mit der entsprechenden Kompetenz) und das "Wann" beziehungsweise das "Wie oft" für wichtige und vorgeschriebene Wartungsmaßnahmen sind im Betriebshandbuch festgelegt. In einem Kapitel sind die Sicherheitshinweise zusammengefasst. Ein Kapitel beschreibt meistens auch Maßnahmen oder Schritte, die im Falle einer Störung des Anlagenbetriebes zu ergreifen sind".*

Demzufolge muss ein Betriebshandbuch alle mit dem IT-Betrieb verbundenen Aufgaben „Wer" und „Was" einschließlich der erforderlichen Kontroll- und Wartungsarbeiten beschreiben. Auch sind alle Tätigkeiten im Zusammenhang mit dem Störungsmanagement zu beschreiben. Es genügt aber nicht, nur die jeweiligen Aufgaben zu beschrieben. Zusätzlich ist jeweils zu benennen, wer eine Aufgabe zu erledigen hat („Wer" und „Wann").

Ausgliederung des Notfallhandbuches

Nicht Gegenstand des Betriebshandbuches ist bei dieser Definition das *Notfallmanagement*. Dieser Auffassung schließen sich die Autoren des vorliegenden Buches an.

Das Management eines Notfalls als schwerwiegende Störung des Betriebs unterliegt zwingend anderen Abläufen – mit vom Betrieb abweichenden Regelungen. Zudem enthalten Dokumentationen für den Notfall häufig Inhalte, die höheren Geheimhaltunganforderungen unterliegen als Dokumente für den Regelbetrieb. So ist beispielsweise ein Dokument zur Wiederherstellung von Exchange nach einem Angriff als sicherheitskritisches Dokument zu behandeln, da dessen Inhalte einem potenziellen Angreifer wichtige Informationen liefern könnten.

Aus diesem Grund ist das Notfallhandbuch als eigenständiges Handbuch im Rahmen der IT-Dokumentation zu führen.

2.2.1.1 Prozessorientierter versus systemorientierter Aufbau

Wie sehen bisher die meisten Betriebshandbücher aus?

Im besten Fall gibt es für jedes System ein Betriebshandbuch, das die in der zitierten Definition genannten Punkte enthält. Dass bedeutet: Das Betriebshandbuch enthält eine Beschreibung der bestehenden Systemeinrichtung, der möglicherweise die Installations- und Konfigurationsanleitung vorausgeht. Anschließend folgt in der Regel eine Beschreibung der administrativen Aufgaben, bevor möglicherweise noch Backup- und Überwachungstätigkeiten erläutert werden.

beispiel

Die folgende Auflistung zeigt die Hauptpunkte der Gliederung eines systemorientierten Betriebshandbuches am Beispiel von DHCP, wie es heute klassischerweise zu finden ist:

BETRIEBSHANDBUCH DHCP

ÄNDERUNGSHISTORIE

ERGÄNZENDE DOKUMENTATION/MITGELTENDE UNTERLAGEN

1 EINFÜHRUNG

2 INSTALLATION UND KONFIGURATION

- Begriffsdefinitionen
- Konfiguration des Clusters
- Namenskonventionen für den Cluster

3 SYSTEMBESCHREIBUNG

- Konfiguration des DHCP-Servers
- Konfiguration der DHCP-Clients

4 VERWALTUNG IM BETRIEB

- Verantwortlichkeiten
- DHCP-Server Administration
- Monitoring

5 DHCP BACKUP / RECOVERY

- Automatische Sicherung
- Regelmäßige geplante Sicherung

6 VERZEICHNISSE

- Tabellenverzeichnis
- Abbildungsverzeichnis

ANHANG

- Liste der DHCP-Bereiche
- DHCP-Konfigurationslisten

Abbildung 2.3: Gliederung eines systemorientierten Betriebshandbuches

Wie ist ein solches Betriebshandbuch zu bewerten?

Ein Betriebshandbuch, das ein System in seiner Gesamtheit beschreibt, bietet sicherlich den Vorteil, dass man sich ohne langes Suchen einen guten Überblick über das ganze System, in diesem Fall über die DHCP-Server, verschaffen kann. Doch ist dies eine Anforderung, die nur sehr selten besteht.

Problembereiche des klassischen Betriebshandbuches

Vielmehr werden in der Regel von unterschiedlichen Mitarbeitern für ihre individuellen Aufgaben unterschiedliche Informationen aus diesem Betriebshandbuch benötigt. Daher ist ein solches Betriebshandbuch häufig wenig praxistauglich.

Welche Schwächen das gezeigte Beispiel-Betriebshandbuch hat, zeigt die folgende Auflistung:

- *Beschreibung der Installation und Konfiguration*: Im gezeigten Beispiel wird DHCP zur Gewährleistung von Ausfallsicherheit im Cluster betrieben. Das Betriebshandbuch enthält demzufolge eine kurze Beschreibung der Systemkonfiguration des Clusters und eine Anleitung wie die DHCP-Clusterressource einzurichten ist. Abgesehen davon, dass die Systembeschreibung des Clusters an dieser Stelle redundant zum Cluster-Betriebshandbuch und damit problematisch ist, wird eine erneute vollständige Installation der DHCP-Clusterressource wohl nur bei gravierenden Änderungen oder in einem Notfall erforderlich sein. Im ersten Fall aber wird ohnehin eine neue Anleitung für die Umsetzung der Änderungen benötigt, und für den zweiten Fall gibt es hoffentlich ein Notfallhandbuch, das die Wiederherstellung des Clusters einschließlich der Wiederherstellung aller Clusterressourcen (also auch der DHCP-Ressourcen) enthält.
- *Systembeschreibung DHCP-Server*: Eine Systembeschreibung, die eine Übersicht über die Konfiguration von DHCP bietet, ist sicherlich erforderlich und richtig. Hierzu gehört eine Aufstellung der eingerichteten Bereiche, der vergebenen Reservierungen und der Aussschlussbereiche genauso wie eine Auflistung der konfigurierten Optionen (Serveroptionen, Lease-Dauer, Klasseneinstellungen u. Ä.). Allerdings handelt es sich hierbei um Informationen, die häufigen Änderungen unterliegen, was für ein abgenommenes Betriebshandbuch problematisch ist. Aus diesem Grund wurden im Beispiel die Listen mit den DHCP-Bereichen in den Anhang aufgenommen und vereinbart, dass bei Änderungen im Anhang keine erneute Abnahme erforderlich ist. Dies ist zwar eine mögliche, aber keine besonders elegante Lösung. Außerdem handelt es sich hierbei um Informationen, die bei einem Einsatz entsprechender Tools automatisiert erfasst werden können. In diesem Fall würde eine Pflege dieser Informationen im Betriebshandbuch keinen Sinn machen.
- *Systembeschreibung der DHCP-Clients:* Das Beispiel-Betriebhandbuch enthält weiter eine Beschreibung bzw. Anleitung, wie DHCP-Clients hinsichtlich der Einstellungen für das Automatic Private IP Adressing (APIPA) und Benutzerklassen zu konfigurieren sind. Hierbei handelt es sich um Informationen, die aus Sicht des DHCP-Administrators natürlich in das DHCP-Betriebshandbuch gehören, die aber in erster Linie für diejenigen interessant sind, die Clientrechner installieren.

- *Verwaltung im Betrieb:* Dieser Teil beschreibt zum Teil in Schritt-für-Schritt-Anleitungen alle Aufgaben, die im Rahmen der DHCP-Verwaltung anfallen. Hierzu zählen das Einrichten neuer bzw. das Löschen bestehender Bereiche, das Ändern der DHCP-Optionen, das Einrichten zusätzlicher Benutzerklassen, das Ändern der Ausschlussbereiche, das Einrichten und Löschen von Reservierungen sowie das Überwachen der DHCP-Bereiche. Die Beschreibung der benannten Tätigkeiten ist sicherlich richtig und wichtig. Hier aber wird der systemorientierte Ansatz besonders deutlich, denn eine solche Beschreibung geht vom System und nicht von den Arbeitsabläufen im Unternehmen aus. So ist beispielsweise das Eintragen von Reservierungen erforderlich, wenn neue Server installiert werden. Demzufolge wäre eine solche Beschreibung in der Installationsanleitung für Server wesentlich sinnvoller aufgehoben.

Häufig wenig praxistauglich

Wie die wenigen Beispiele zeigen, ist ein solches Betriebshandbuch für den täglichen Einsatz im Betrieb nur wenig geeignet, da es sich nicht an den Arbeitsabläufen orientiert und für den einzelnen Mitarbeiter und seine Aufgaben zuviel Ballast enthält. So interessiert beispielsweise denjenigen Mitarbeiter, der für die Wartung des DHCP-Servers zuständig ist, die Clientkonfiguration überhaupt nicht.

Vor allem aber wegen der mangelnden Praxistauglichkeit verstauben so viele mit viel Aufwand erstellte Betriebshandbücher unbenutzt in den Aktenschränken. Und werden sie dann irgendwann einmal benötigt, sind sie häufig völlig veraltet.

2.2.1.2 Inhalt eines prozessorientierten Betriebshandbuches

Unabhängig davon, ob die Unternehmensorganisation bereits prozessorientiert ausgeprägt ist oder nicht, werden viele Betriebshandbücher nach dem zuvor beschriebenen Schema erstellt.

Nur langsam findet die Umorientierung hin zur Prozessausrichtung auch in der IT-Dokumentation statt. Bei einem an den Arbeitsabläufen ausgerichteten Betriebshandbuch werden die Funktionen nicht einzeln für sich betrachtet. Vielmehr stehen die Zusammenhänge im Vordergrund. Dies bietet den Vorteil, dass Lücken und Ineffizienzen an den Schnittstellen der einzelnen Funktionen früher erkannt und behoben werden können. Der prozessorientierte Ansatz bei der IT-Dokumentation ergibt sich auch daraus, dass nahezu alle Qualitätsaudits und Zertifizierungen die Prozessbewertung in den Vordergrund stellen. Auch Modelle, wie beispielsweise ITIL, folgen diesem Ansatz.

hinweis

Das vorliegende Buch möchte hierfür einen Ansatz liefern und stellt in der Folge Struktur und Inhalt eines an den Prozessen ausgerichteten Betriebshandbuches vor.

In einem an den Prozessen ausgerichteten Betriebshandbuch spielen natürlich die Prozessbeschreibungen die Hauptrolle.

Wichtiger Bestandteil: Systemakten

Zusätzlich zu den Prozessdokumenten muss es aber auch bei einer prozessorientierten Ausrichtung eine Dokumentation der eingesetzten Hard- und Softwaresysteme (Betriebssysteme, Datenbanksysteme, Clusterinfrastruktur usw.) geben. Es ist jedoch nicht sinnvoll, diese Dokumentation in die Prozessbeschreibungen aufzunehmen, da vielfach ein System an mehreren Prozessen beteiligt ist. Das würde zur Unübersichtlichkeit und zu Redundanzen führen. Daher ist es sinnvoll, die eingesetzten Systeme in *Systemakten* zu dokumentieren und auf diese in den Prozessbeschreibungen zu verweisen. Hierzu zählen beispielsweise auch Netzwerkpläne, Beschaltungspläne sowie die Dokumentation der Netzwerkhardware.

Aus den genannten Anforderungen können die folgenden beiden Teilbereiche eines Betriebshandbuches abgeleitet werden:

- Beschreibung der Systeme und der Infrastruktur
- Prozessbeschreibungen für alle relevanten Aufgaben des IT-Betriebs

Die nachstehende Grafik zeigt die oberste Ebene eines prozessorientierten Betriebshandbuches. Eine detaillierte Beschreibung der Struktur und des Inhalts dieses Betriebshandbuches finden Sie in Kapitel 4, „Dokumentation des IT-Betriebs".

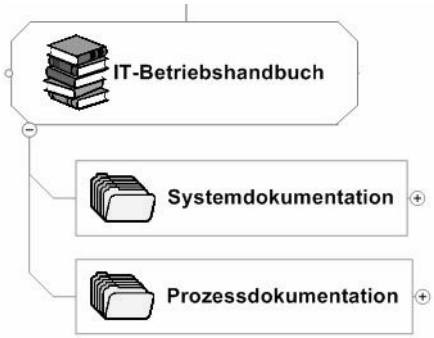


Abbildung 2.4: Die Grundstruktur des IT-Betriebshandbuches

achtung

Auch wenn der Begriff Betriebshandbuch den Eindruck vermittelt, es würde sich hierbei um ein einziges Handbuch oder sogar eine einzige Datei handeln, ist es in der Praxis, zumindest für größere Systemumgebungen, natürlich nicht sinnvoll, so zu verfahren. Vielmehr sollten sowohl das Betriebshandbuch als auch das Notfallhandbuch modular im Sinne einer Loseblattsammlung aufgebaut sein, die jederzeit ergänzt und aktualisiert werden kann.

Falls erforderlich, kann die im vorliegenden Buch vorgestellte Strukturierung aber durchaus auch auf ein einziges Dokument bezogen werden, dass in entsprechende Kapitel unterteilt ist.

Beispiel DHCP-Betriebshandbuch

Betrachten wir noch einmal das im Beispiel dargestellte DHCP-Betriebshandbuch, so ergibt sich mit dem neuen Ansatz eine klare Trennung zwischen den administrativen Aufgaben und der Systembeschreibung. Hierbei umfasst die Systemakte für den Cluster dessen gesamte Konfiguration, also auch die Einrichtung der DHCP-Clusterressource. Die Konfiguration des DHCP-Servers ist sinnvollerweise in einer separaten Systemakte zu beschreiben, die bei Systemänderungen zeitnah angepasst werden kann.

Die administrativen Tätigkeiten können verschiedenen Prozessbereichen zugeordnet werden. Hierbei handelt es sich um Prozesse zur *Verwaltung der Serversysteme*, aber auch um Prozesse zur *Desktopverwaltung*, zu denen beispielsweise das Beschaffen, Bereitstellen, Austauschen und Entsorgen von Arbeitsplatzrechnern zählen. Weitere Tätigkeiten könnten den Prozessbereichen *Datensicherung und Wiederherstellung* sowie *Systemüberwachung* zugeordnet werden.

Problem Installationsanleitung

Ein Abgrenzungsproblem ergibt sich häufig bei der Fragestellung, wie mit Installationsanleitungen umzugehen ist. Handelt es sich beispielsweise um die Beschreibung der Installation und Konfiguration von Arbeitsplatzrechnern, die im Rahmen des IT-Betriebs regelmäßig bereitzustellen sind, ist die Frage einfach zu beantworten. Diese Installationsanleitungen sind den Prozessen zuzuordnen, da sie Arbeitsanweisungen für regelmäßig durchzuführende Prozesse des IT-Betriebs darstellen.

Schwieriger ist hingegen beispielsweise die Einordnung der Installationsanleitung für die Clusterumgebung, die, nachdem sie erstmalig eingerichtet wurde, nicht noch einmal installiert und konfiguriert werden muss. Da aber in einem Notfall eine Neueinrichtung erforderlich werden kann, muss zumindest von Seiten der Notfalldokumentation ein Zugriff auf die Installationsanleitung möglich sein. Sie sollte deshalb sinnvollerweise den Wiederherstellungsprozessen im Notfallhandbuch beigefügt werden.

2.2.2 Notfallhandbuch

Wie in Kapitel 1, „Anforderungen an die IT-Dokumentation“, dargestellt wurde, gehört das Notfallhandbuch zu denjenigen Dokumenten, zu dessen Erstellung und Pflege die meisten Unternehmen bereits aufgrund gesetzlicher Vorgaben verpflichtet sind. Ein Notfallhandbuch sollte aber nicht nur als lästige Pflicht angesehen werden. Vielmehr kann von ihm im Notfall das Überleben des ganzen Unternehmens abhängen. In der Praxis basieren die eigentlichen Katastrophen vielfach auf Fehlentscheidungen in vermeintlich beherrschbaren Situationen. Das nachstehende Beispiel soll dies verdeutlichen:

> *Durch einen Wasserschaden wird ein Server eines Unternehmens außerhalb der Geschäftszeit vollständig zerstört. Der zuständige Administrator ist nicht erreichbar, eine Dokumentation nicht vorhanden oder zumindest nicht auffindbar. In der Hektik des Geschehens macht der herbeigeeilte IT-Leiter einen fatalen Fehler. Er übersieht, dass die Daten auf dem gespiegel-*

ten System noch bis zum Abschluss des Tages aktuell vorhanden gewesen waren. Er geht aber davon aus, dass die Daten auf beiden Systemen beschädigt sind, und veranlasst, dass die Datensicherung des Vortages vom Band zurückgespielt wird. Damit ist die gesamte Tagesproduktion zerstört.

In diesem Szenario basiert der Datenverlust nicht auf technischen Fehlern oder einem vernachlässigten Backup, sondern auf organisatorischen Unzulänglichkeiten und Fehlentscheidungen. Es zeigt damit einen typischen Mangel vieler Unternehmen: Zwar wurden ausreichende technische Vorkehrungen für einen Notfall getroffen, diese aber sind nur sehr unzureichend dokumentiert oder nicht aktuell. Außerdem fehlen häufig Regelungen, wer in einem derartigen Fall befugt ist, entsprechende Maßnahmen zu veranlassen bzw. durchzuführen. Häufig verlaufen zwar kleinere Störfälle „gerade noch einmal" glimpflich, weil man Glück im Unglück hat und die richtige Person zur richtigen Zeit am richtigen Ort ist. Die Gefahr einer Katastrophe ist in einem solchen Fall allerdings jederzeit vorhanden. Insbesondere dann, wenn sich mehrere Fehler in ihrer Wirkung addieren.

Aufgabe des Notfallhandbuches

An dieser Stelle setzt das Notfallhandbuch an. Hier sind alle Maßnahmen, die nach Eintritt eines Notfall auslösenden Ereignisses zu ergreifen sind, und alle dazu erforderlichen Informationen zu dokumentieren. Im Vordergrund stehen demzufolge die Notfallprozesse.

Da sich diese Prozesse von den Abläufen des IT-Regelbetriebs unterscheiden, sind sie von diesem getrennt zu behandeln. Damit bildet das Notfallhandbuch den zweiten wichtigen Baustein der IT-Dokumentation.

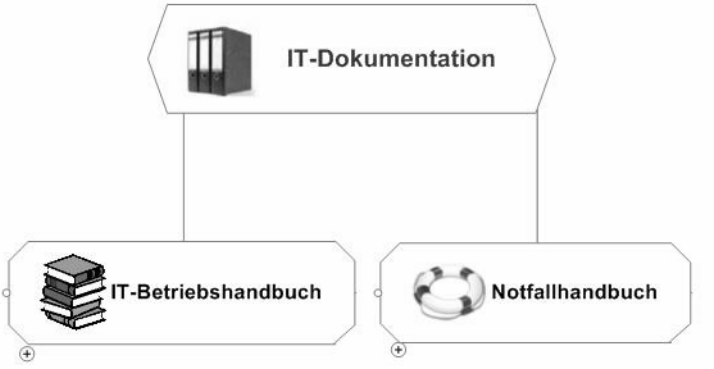


Abbildung 2.5: Das Notfallhandbuch ist nicht Bestandteil des Betriebshandbuches.

hinweis

Was alles zu einer Notfalldokumentation dazugehört, und worauf bei der Erstellung eines Notfallhandbuches zu achten ist, können Sie in Kapitel 5, „Dokumentation für den Notfall", nachlesen.

2.2.3 Projektdokumentation

Zusätzlich zum IT-Betriebshandbuch und zum Notfallhandbuch muss die IT-Betriebsdokumentation die Projektdokumentation als weiteren Teil beinhalten.

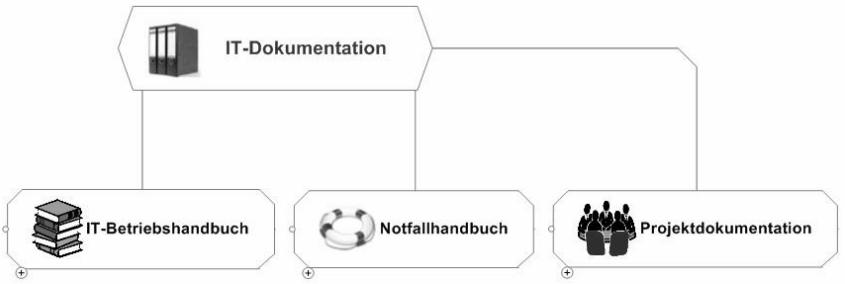


Abbildung 2.6: Die Projektdokumentation ist der dritte Hauptteil der IT-Dokumentation.

Bevor der Inhalt der Projektdokumentation betrachtet wird, soll zunächst die Frage beantwortet werden, was ein Projekt charakterisiert.

Projektdefinition gemäß DIN 69901

Einen guten Ansatz zur Projektdefinition liefert die DIN 69901. Diese regelt Begriffe im Projektmanagement. Gemäß DIN 69901, Ausgabe 8/87 gilt ein Projekt als ein Vorhaben, das im Wesentlichen gekennzeichnet wird durch [PJMGR]

- *„die Einmaligkeit der Bedingungen in ihrer Gesamtheit,*
- *Zielvorgaben,*
- *zeitliche, finanzielle, personelle oder andere Begrenzungen,*
- *Abgrenzungen gegenüber anderen Vorhaben und*
- *eine projektspezifische Organisation.“*

Die *Deutsche Gesellschaft für Projektmanagement e. V.* (*GPM*) [GPM]erweitert diese Definition um den Aspekt der Arbeitsteilung und definiert Projekte als arbeitsteilige Prozesse.

Bei IT-Projekten handelt es sich demzufolge um zielgerichtete sowie zeitlich, personell und sachlich abgegrenzte IT-Vorhaben. Sie beinhalten die Konzeption, die Entwicklung, die Einführung bzw. wesentliche Änderungen von IT-Systemen und IT-Verfahren. Damit dienen IT-Projekte der Erweiterung und dem Umbau des IT-Betriebs.

Normenfamilie Projektwirtschaft DIN 69900 bis DIN 69906

Die DIN 69901 „Projektmanagement, Begriffe“ wurde im August 1987 verabschiedet. Sie stellt die wesentlichen Grundbegriffe des Projektmanagements zusammen und ist entstanden aus den Arbeiten an der DIN 69900 „Netzplantechnik“, die in den ersten Versionen diese Begriffe mit enthielt. Ergänzend zur DIN 69901 definieren auch die DIN 69902, 69903, 69904 und 69905 weitere Projektmanagement-Begriffe.

Derzeit werden die deutschen Normen DIN 69900 bis 69905 für Projektmanagement überarbeitet und liegen seit Oktober 2007 in einer vorläufigen Version vor.

- DIN 69900: Teil 1 und 2 Netzplantechnik Begriffe/Darstellungstechnik – 08/1987
- DIN 69901: Projektmanagement, Begriffe – 08/1987
- DIN 69902: Einsatzmittel, Begriffe – 08/1987
- DIN 69903: Kosten und Leistung – 08/1987
- DIN 69904: Projektmanagementsysteme, Elemente und Strukturen – 11/2000
- DIN 69905: Projektabwicklung, Begriffe Ergänzung der DIN 69901 – 05/1997
- DIN 69906: Logistik, Grundbegriffe – 12/1990

Was unterscheidet ein Projekt vom Betrieb?

Die Abgrenzung eines Projekts zum Betrieb ergibt sich aus der funktionalen und organisatorischen Unterschiedlichkeit. So gibt es häufig eine eigene Projektorganisation, die von der Betriebsorganisation abweicht. Gerade bei extern vergebenen Projekten ist zudem noch eine wichtige zivilrechtliche Abgrenzung wichtig. Erst nach der Implementierung und der Abnahme der Prozesse bzw. Systeme geht die Verantwortung auf das auftraggebende Unternehmen über.

Eine wesentliche Grundlage für den Projekterfolg sowie die anschließende Wartung und Pflege der Systeme bzw. IT-Prozesse ist die Qualität der erstellten Unterlagen. Qualitativ hochwertige Projektarbeit ist nur möglich, wenn durch die Dokumente die Projektschritte und Projektergebnisse nachvollziehbar sind.

2.2.3.1 Inhalte der Projektdokumentation

Die *Projektdokumentation* ist gemäß DIN 69901 eine

> *„Zusammenstellung ausgewählter, wesentlicher Daten über Konfiguration, Organisation, Mitteleinsatz, Lösungswege, Ablauf und erreichte Ziele des Projektes" [PJMGR].*

Abgrenzung wichtiger Begriffe

Von der Projektdokumentation abzugrenzen ist gemäß der DIN das Projektmanagement-Handbuch und das Projekthandbuch sowie der Projektplan.

- *Projektmanagement-Handbuch*: Das Projektmanagement-Handbuch (PM-Handbuch) ist eine „*Zusammenstellung von Regelungen, die innerhalb einer Organisation generell für die Planung und Durchführung von Projekten gelten*" [PJMGR].
- *Projekthandbuch*: Das Projekthandbuch ist die „*Zusammenstellung von Informationen und Regelungen, die für die Planung und Durchführung eines bestimmten Projekts gelten sollen*". Im Gegensatz zu einem Projektmanagement-Handbuch enthält das Projekthandbuch also die speziell für das betrachtete Projekt geltenden Vereinbarungen und ergänzt gegebenenfalls das Projektmanagement-Handbuch. In ihm finden sich zentral alle wichtigen Informationen zum Projekt. Typische Dokumente im Projekthandbuch sind der Projektauftrag, Zielvereinbarungen sowie Risikopläne [PJMGR].
- *Projektplan*: Der Projektplan bezeichnet gemäß DIN 69905 die Menge aller Pläne eines Projekts, einschließlich des Projektstrukturplans und aller Terminpläne [PROMAGZIN].

Zusätzlich oder auch alternativ zum unternehmensweiten Projektmanagement-Handbuch gibt es vielfach abteilungs- oder fachbereichsspezifische Projektmanagement-Handbücher. Diese enthalten Regelungen und Vorgaben, die für alle Projekte des jeweiligen Bereichs gelten. So könnte beispielsweise in einem großen Unternehmen die IT-Abteilung in Ergänzung zum unternehmensweiten Projektmanagement-Handbuch ein gesondertes IT-Projektmanagement-Handbuch verwalten, dessen Vorgaben für alle IT-Projekte gelten.

Wie diese kleine Zusammenstellung zeigt, gibt es viele, aber nicht klar abgegrenzte Richtlinien für die Verwendung der Begriffe. Es empfiehlt sich daher dringend, für die eigene IT-Dokumentation zu regeln, wie die Begriffe im Unternehmen zu verwenden sind.

Babylonisches Begriffs-Wirrwarr

Während die Definition der vorstehenden Begriffe an dieser Stelle noch klar zu sein scheint, kann man sehr leicht mit einer näheren Betrachtung für völlige Verwirrung sorgen. Denn in Wahrheit herrscht eine wahrhaft babylonische Begriffsvielfalt:

In der Literatur wird zunehmend der Begriff *Projektakte* als Sammelbegriff für alle Dokumente eines Projekts verwendet. Viele, die diesen Begriff verwenden, meinen damit den Begriff der *Projektdokumentation* (manchmal als PDO abgekürzt) zu ersetzen bzw. verwenden beide Begriffe synonym.

Im Gegenteil aber hat die *Projektakte* nichts mit der *Projektdokumentation* zu tun, denn Letztere bezeichnet gemäß DIN 69901 eine Auswahl der wichtigen Projektdokumente mit dem Ziel, eine schnelle Erfassbarkeit von Projektablauf und Ergebnissen zu ermöglichen. Aus diesem Grund wird die Projektdokumentation gelegentlich auch als *Projektabschlussbericht* bezeichnet, was deren Intention viel besser beschreibt.

Von der Projektdokumentation abzugrenzen sind daher auch das *Projekthandbuch* und das *Projektmanagement-Handbuch*. Selbstverständlich aber können Teile des Projekthandbuches (nicht aber des Projektmanagement-Handbuches) Bestandteil der Projektdokumentation sein. Und werden Projektakten verwendet, ersetzen diese auch das Projekthandbuch, da dessen Inhalte Bestandteile der entsprechenden Projektakte sind.

Im Übrigen definiert die DIN 6789 Dokumentationssystematik, Aufbau Technischer Erzeugnis-Dokumentationen (09/1990) „eine *Dokumentation* als eine für einen bestimmten Zweck vollständige Zusammenstellung von Dokumenten …“ – Alles klar?

Verwendung der Begriffe im Buch

Für das vorliegende Buch gilt Folgendes:

- In Anlehnung an die DIN 6789 und damit abweichend von der DIN 69901 wird der Begriff *Projektdokumentation* als übergeordnete Bezeichnung für alle Dokumente verwendet, die Bestandteil der IT-Dokumentation sind und im Rahmen von Projekten erstellt wurden oder für IT-Projekte gelten. Die Projektdokumentation umfasst die Zusammenstellung und Archivierung aller Unterlagen, die es ermöglicht, sich jederzeit umfassend über alle Projekte zu informieren. Sie steht auf einer Ebene mit dem Betriebshandbuch, das die entsprechende Aufgabe für den IT-Betrieb übernimmt.

- Die Projektdokumentation besteht wiederum aus den *Projekttakten*. Projektakten bezeichnen die Zusammenstellung aller auf ein Projekt bezogenen Dokumente. Hierbei kann es sich sowohl um Dokumente des Projektmanagements als auch um Ergebnisdokumente handeln. Für jedes Projekt ist innerhalb der Projektdokumentation eine Projektakte zu führen. Der Begriff der Projektakte wurde gewählt, da er nach Ansicht der Autoren griffiger ist und weniger Verwechslungsgefahr mit dem Projektmanagement-Handbuch bietet als der Begriff Projekthandbuch.

Die nachstehende Grafik zeigt die obersten Ebenen der Projektdokumentation. Eine detaillierte Beschreibung von Struktur und Inhalt der Projektdokumentation finden Sie in Kapitel 6, „Dokumentation von IT-Projekten".

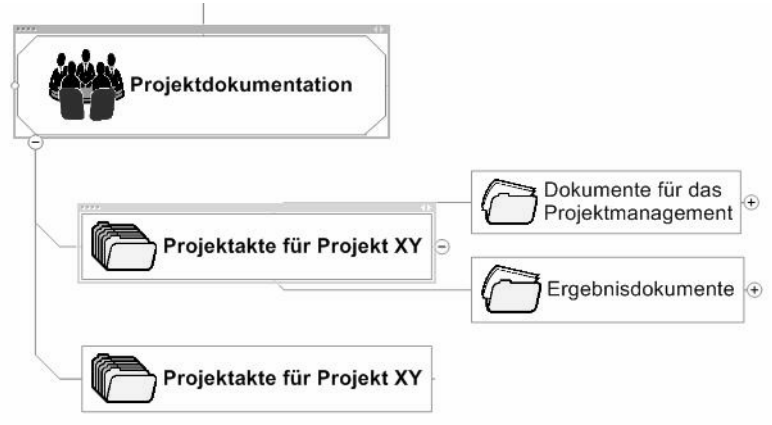


Abbildung 2.7: Gliederungsstruktur der Projektdokumentation

2.2.3.2 Systemeinführungen ohne Projekt

Wie bereits ausgeführt, erfolgen nicht alle Systemeinführungen in Form eines Projekts. Die mit dem Änderungsprozess verbundenen Aufgaben zur Planung, Entwicklung und Implementierung können sowohl innerhalb des Regelbetriebs als auch in einem Projekt erfolgen.

Soll beispielsweise eine neue Faxsoftware eingerichtet werden, so ist es durchaus möglich, dass der für das Messaging-System zuständige Administrator diese Aufgabe vollständig eigenständig durchführt. Die Einrichtung eines Projekts mit einer entsprechenden Projektorganisation wäre in diesem Fall wohl deutlich überzogen.

Einordnung in die Dokumentation

Die Implementierung neuer Systeme und Prozesse sowohl im Projekt als auch innerhalb des IT-Betriebs muss ihren Niederschlag in der IT-Dokumentation finden. Damit stellt sich die Frage, wo derartige Änderungsprozesse, die nicht im Rahmen eines Projekts erfolgen, zu betrachten sind.

Um Abgrenzungsproblemen zu begegnen, ist die folgende Aufteilung von Dokumenten für Planungs- und Entwicklungs- bzw. Implementierungsaufgaben zu empfehlen:

- Erfolgt die Entwicklung und Implementierung eines neuen Systems in Form eines Projekts, so sind alle damit verbundenen Dokumente der *Projektdokumentation* zuzuordnen.
- Erfolgt die Entwicklung und Implementierung eines neuen Systems als Sonderaufgabe im laufenden Betrieb, ist die Dokumentation dem *Betriebshandbuch* zuzuordnen.

2.3 Fazit

Aus den Ausführungen der vorstehenden Kapitel lassen sich drei wesentliche Dokumentationsbereiche ableiten:

- Betriebshandbuch für den IT-Regelbetrieb
- Notfallhandbuch
- Projektdokumentation

Zusätzlich erforderlich: Rahmendokumente

Zusätzlich werden noch *Rahmendokumente* benötigt, die zum einen allgemeine Vorgaben und Normierungen regeln und zum anderen die aufbauorganisatorischen Zuordnungen sowie die Funktionszuordnungen festlegen. Die Rahmendokumente stellen somit die Klammer für die den drei anderen Bereichen zugeordneten Dokumente dar.

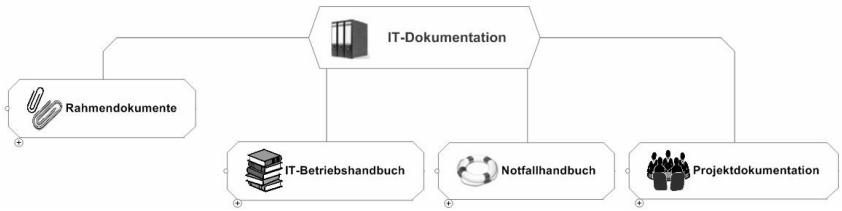


Abbildung 2.8: Die Struktur der im Buch vorgestellten IT-Dokumentation

Die in der vorstehenden Abbildung gezeigte Struktur bildet die Basis für das vorliegende Buch. In den folgenden Kapiteln werden diese vier Bereiche ausführlich vorgestellt. Die Beschreibung beinhaltet sowohl Hinweise und Vorschläge zu deren Strukturierung als auch Erläuterungen zu Strukturierung und Erstellung der jeweiligen Einzeldokumente.

cd-rom

Auf der beigefügten CD-ROM befindet sich eine mit MindManager erstellte Datei, die die vorgestellte Gliederung der IT-Dokumentation grafisch darstellt und eine Betrachtung der im Folgenden vorgestellten Einzelbereiche in einer Zusammenschau ermöglicht. Mit dem ebenfalls beigefügten MindManager Viewer kann diese Datei angesehen werden. Außerdem ist es möglich, Zweige zu öffnen, zu schließen und in sie hineinzuzoomen.

3 Rahmendokumente

Vielfach werden Dokumente ausschließlich vor dem Hintergrund einer technischen Lösung für eine bestehende Anforderung erstellt. Dabei wird häufig vergessen, dass die wenigsten Lösungen für sich stehen, sondern in einem Systemverbund funktionieren müssen. Aus diesem Grund werden zusätzlich *Rahmendokumente* benötigt, die die organisatorischen und betrieblichen Belange regeln und eine funktionierende Gesamtkonzeption sicherstellen. Ein typisches Beispiel hierfür ist das IT-Sicherheitskonzept. Seine Hauptaufgabe ist es, den Schutzbedarf der IT-Anwendungen und IT-Systeme für alle Bereiche festzustellen und dafür angemessene Sicherheitsmaßnahmen vorzusehen.

Das folgende Kapitel stellt die wichtigsten der für die IT-Dokumentation relevanten Rahmendokumente vor und zeigt, wie sich diese Dokumente gegen die übrigen im vorliegenden Buch beschriebenen Dokumente abgrenzen.

3.1 Rahmendokumente bilden die Klammer

Bevor die Rahmendokumente im Einzelnen vorgestellt werden, gilt es zunächst zu klären, was überhaupt ein Rahmendokument ist.

3.1.1 Einordnung der Rahmendokumente

Wie bereits ausgeführt, besteht die IT-Dokumentation aus drei wesentlichen Dokumentationsbereichen:

- Betriebshandbuch
- Notfallhandbuch
- Projektdokumentation

Bei den Dokumenten, die diesen drei Bereichen zugeordnet sind, handelt es sich um tätigkeitsbezogene Dokumente.

Klammer für alle anderen Dokumente

Im Gegensatz dazu handelt es sich bei den Rahmendokumenten, wie beispielsweise dem IT-Konzept oder einer IT-Namenskonvention um Regelwerke. Diese regeln übergreifend zum einen die allgemeinen Vorgaben und Normierungen und legen zum anderen Zuordnungen (beispielsweise Zuordnungen von Mitarbeitern zu Rollen) fest. Damit stellen die Rahmendokumente eine Klammer für die anderen Dokumente einer Dokumentation dar.

Die Aufgaben der einzelnen Rahmendokumente können dabei sehr unterschiedlich sein. Während einige überwiegend strategischen Charakter haben, wie beispielsweise das IT-Konzept, haben andere Dokumente direkten Einfluss auf den operativen Betrieb. Zu Letzteren zählen beispielsweise das Berechtigungskonzept und die Betriebsmatrix.

Welche Dokumente als Rahmendokumente der IT-Dokumentation zuzuordnen sind, hängt vom Unternehmen und dessen Dokumentenverwaltung ab und muss im Einzelfall betrachtet werden.

Unternehmensweit gültige Dokumente

So ist es möglich, dass bereits Dokumente für das Unternehmen existieren, die auch für die IT-Organisationseinheiten Gültigkeit haben. Ein typisches Beispiel stellt das Projektmanagement-Handbuch dar. Insbesondere große Unternehmen verfügen häufig über ein solches Dokument, das die Verfahren festlegt, nach denen Projekte im Unternehmen durchzuführen sind. Möglich ist aber auch, dass das unternehmensweite Projektmanagement-Handbuch lediglich allgemeine Vorgaben macht (beispielsweise die Projektorganisation vorgibt), für IT-Projekte aber zusätzlich ein gesondertes IT-Projektmanagement-Handbuch existiert. In Letzterem kann beispielsweise festgelegt werden, dass IT-Projekte grundsätzlich nach dem PRINCE2-Projektmodell durchzuführen sind.

Ein weiteres Bespiel eines unternehmensweiten Dokuments ist das Risikohandbuch für das Unternehmen. Im Rahmen des gesetzlich verankerten Risikomanagements pflegen viele Unternehmen ein unternehmensweites Risikohandbuch. Dieses muss unternehmensgefährdende Risiken enthalten. Da aber für den Bereich der IT nicht nur unternehmensgefährdende, sondern auch servicegefährdende Risiken betrachtet werden müssen, kann es sinnvoll sein, ein gesondertes IT-Risikohandbuch zu führen. Dieses stellt somit eine Detaillierung des unternehmensweiten Risikohandbuches dar.

3.1.2 Begriffschaos nicht nur bei den Rahmendokumenten

Was ist ein Konzept?

Besonders beliebt ist für Dokumente, die dem Bereich der Rahmendokumente zuzuordnen sind, der Begriff *Konzept* (Berechtigungskonzept, Sicherheitskonzept, Administrationskonzept, Rollenkonzept, IT-Konzept). Dabei können die meisten dieser Dokumente kaum der später im Buch noch zu erörternden Kategorie „Konzepte" zugeordnet werden.

Dass beispielsweise ein IT-Berechtigungskonzept mit verbindlichen Regelungen zu Zugriffsberechtigungen nichts mit einem Konzept gemein hat, wird deutlich, wenn man sich die Definition von Konzept betrachtet. Gemäß dem Duden ist ein Konzept ein erster Entwurf bzw. die erste Fassung einer Rede oder eines Schriftstücks. Wikipedia erweitert diese Definition um die Begriffe *Plan* und *Programm für ein Vorhaben*. Konzepte haben also grundsätzlich planerischen und strategischen Charakter.

Verschärft wird die Situation noch dadurch, dass es keine verbindliche Definition oder Richtlinien für die Verwendung von Dokumentbezeichnungen gibt. Sucht man im Internet nach dem Begriff *IT-Konzept* findet man mehrere Tausend Einträge. Und fast genauso unterschiedlich ist das, was inhaltlich in einem IT-Konzept dargestellt wird. Während die einen unter einem IT-Konzept ein strategisches Papier der Unternehmensleitung verstehen, verwenden andere den Begriff IT-Konzept als Synonym für das Betriebshandbuch.

Eigene Standards festlegen

Die vorstehenden Beispiele verdeutlichen, dass man von einer Normung von Dokumentbezeichnungen gerade im Bereich der IT weit entfernt ist. Es ist daher dringend zu empfehlen, beim Aufbau der eigenen IT-Dokumentation die Verwendung der Dokumentbezeichnungen für das eigene Unternehmen zu definieren und diese deutlich von einander abzugrenzen. Weiter muss die verbindliche Verwendung der Begriffe kommuniziert und sichergestellt werden, dass jeder, der Dokumente erstellt, die Bezeichnungen wie definiert verwendet.

Das folgende Kapitel möchte für eine derartige Standardisierung einige Anhaltspunkte liefern. Es stellt die wichtigsten Rahmendokumente exemplarisch vor und zeigt, wie sich diese Dokumente gegen die übrigen im vorliegenden Buch beschriebenen Dokumentationen abgrenzen.

hinweis

Für die Verwendung von Dokumentbezeichnungen im Buch gilt Folgendes:

Dokumente werden mit den dafür üblicherweise verwendeten Begriffen bezeichnet. Werden für Dokumente in der Literatur üblicherweise auch andere Namen verwendet, so werden diese (soweit bekannt) zusätzliche angegeben. Beispielsweise wird der Begriff IT-Rahmenkonzept manchmal anstelle von IT-Konzept verwendet.

Diese Vorgehensweise gilt auch für Dokumente mit dem Begriff „Konzept" im Namen wie beispielsweise Sicherheitskonzept und Berechtigungskonzept, auch wenn sie definitionsgemäß keine Konzepte sind.

3.2 Die Rahmendokumente im Überblick

In diesem Kapitel werden einige wichtige Rahmendokumente der IT-Dokumentation im Überblick vorgestellt. Dabei steht nicht eine detaillierte Anleitung zu deren Erstellung im Vordergrund, sondern vielmehr eine Beschreibung der Aufgaben des jeweiligen Rahmendokuments. Dies hat mehrere Gründe: Zum einen könnte allein beispielsweise die Betrachtung des zu den Rahmendokumenten zählenden IT-Risikohandbuches und der dahinterstehenden Prozesse das Kapitel füllen. Dies würde den Rahmen des Buches schnell sprengen. Zum anderen gibt es aufgrund der Wichtigkeit dieser Dokumente zu den meisten der Rahmendokumente eine umfangreiche Literatur.

Die nachstehende Grafik zeigt die wichtigsten Rahmendokumente der IT-Dokumentation. Welche Dokumente im Einzelfall zu erstellen sind, und ob darüber hinaus noch Dokumente benötigt werden, hängt vom Unternehmen und dessen Aufgaben ab und muss im Einzelfall entschieden werden.

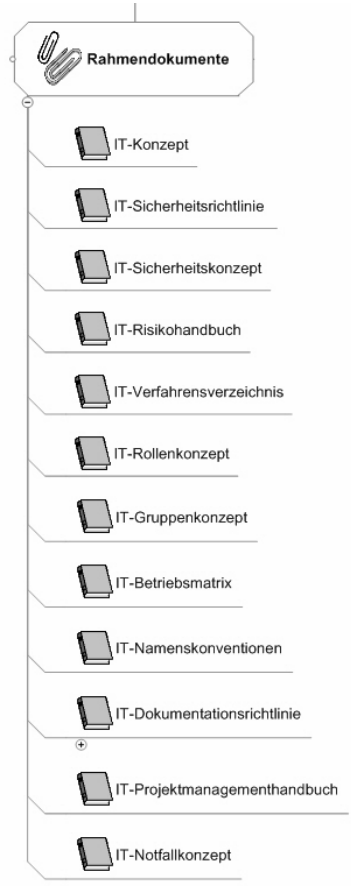


Abbildung 3.1: Wichtige Rahmendokumente der IT-Dokumentation

3.2.1 IT-Konzept

» Für *IT-Konzept* häufig synonym verwendete Begriffe: IT-Betriebskonzept, IT-Rahmenkonzept, Betriebskonzept. Auch das „Betriebshandbuch" wird manchmal als IT-Konzept bezeichnet. «

Das IT-Konzept ist ein strategisches Dokument, das der grundsätzlichen Einordnung der IT in das Unternehmen dient und die übergeordnete strategische Ausrichtung des Unternehmens im Hinblick auf die IT festlegt. So wird typischerweise im IT-Konzept festgelegt, ob die IT zentral oder dezentral strukturiert ist und mit welcher Ausprägung.

Es sollte auch für die IT beschreiben, mit welcher Technik und welchen Verfahren das Unternehmen welche Zwecke verfolgt. Damit soll es einen Orientierungsrahmen für die weitere Entwicklung und geplante Maßnahmen aufzeigen.

Was im IT-Konzept letztendlich geregelt wird, liegt allein in der Verantwortung des Unternehmens. So kann ein IT-Konzept durchaus auch Festlegungen (Methoden und Verfahren) zur Einordnung von IT-Projekten beinhalten. Wichtig ist aber, dass es keine Details beschreibt, sondern nur grundsätzliche Regelungen festschreibt, ohne diese zu spezifizieren.

3.2.2 IT-Sicherheitsrichtlinie

» Für *IT-Sicherheitsrichtlinie* synonym verwendete Begriffe: Sicherheits-Policy, Security Policy, Sicherheitsleitlinie «

Die IT-Sicherheitsrichtlinie schreibt die zentralen Richtlinien für die IT-Sicherheit in einem Unternehmen fest. Sie definiert die Sicherheitsziele und die Grundsätze für den Umgang mit Informationen sowie die Verantwortungsbereiche für die IT-Sicherheit. Vor allem für große Unternehmen ist der Einsatz einer Sicherheitsrichtlinie wichtig, um übergreifende IT-Sicherheitsregeln unternehmensweit durchzusetzen. So kann beispielsweise in der Sicherheitsrichtlinie festgelegt werden, dass unternehmensweit ausschließlich vom Unternehmen bereitgestellte Rechnersysteme und Speichersysteme eingesetzt werden dürfen und technisch sicherzustellen ist, dass keine Fremdrechner Zugang zum lokalen Netzwerk erhalten.

Kleinere Unternehmen können zwar gegebenenfalls auf eine IT-Sicherheitsrichtlinie verzichten, sollten aber in jedem Fall ein IT-Sicherheitskonzept erstellen, das dann zusätzlich die übergeordneten Richtlinien beinhalten kann.

Inhalt der IT-Sicherheitsrichtlinie

Gemäß den Empfehlungen des BSI (hier wird sie als IT-Sicherheitsleitlinie bezeichnet) sollte die IT-Sicherheitsrichtlinie Aussagen zu den nachfolgenden Punkten enthalten:

- Bedeutung der IT-Sicherheit für die Geschäftsprozesse
- Ziele und Strategien des Unternehmens in Bezug auf die IT-Sicherheit

- Organisationsstruktur für die Umsetzung der IT-Sicherheitsrichtlinie und Benennung der Verantwortlichen (zum Beispiel die Ernennung eines IT-Sicherheitsbeauftragten)
- Maßnahmen zur regelmäßigen Überprüfung der Einhaltung der Sicherheitsstandards

Entsprechend dem IT-Konzept beschreibt die IT-Sicherheitsrichtlinie keine Details, sondern macht grundsätzliche Vorgaben, ohne diese zu spezifizieren. Sie sollte kurz und prägnant sein. Sie wird in der Regel sehr selten geändert.

3.2.3 IT-Sicherheitskonzept

» Für *IT-Sicherheitskonzept* synonym verwendete Begriffe: Sicherheitskonzept, Sicherheitshandbuch. «

Das IT-Sicherheitskonzept regelt die Struktur und die konkrete Umsetzung der IT-Sicherheit. Fälschlicherweise wird das IT-Sicherheitskonzept manchmal auch als IT-Sicherheitsrichtlinie bezeichnet, obwohl es sich klar von dieser abgrenzen lässt. Während die Richtlinie Schutzziele und allgemeine Sicherheitsmaßnahmen im Sinne offizieller Vorgaben des Unternehmens vorgibt, beschreibt das IT-Sicherheitskonzept detaillierte Sicherheitsmaßnahmen und Handlungsanweisungen zum Umgang mit IT-Sicherheit. Eine durchaus sinnvolle Alternative ist hingegen die Verwendung des Begriffs IT-Sicherheitshandbuch.

Zu kaum einem anderen sicherheitsrelevanten Dokument findet man so viele Informationen und Beispiele, wie zum IT-Sicherheitskonzept. Dies liegt vor allem an seiner Bedeutung. Das IT-Sicherheitskonzept ist für ein Unternehmen erforderlich, damit konkrete Sicherheitsmaßnahmen geplant, umgesetzt und später aktualisiert werden können. Es ist „das" zentrale Dokument im IT-Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete Maßnahme muss sich letztlich darauf zurückführen lassen.

Wichtiger Baustein im IT-Grundschutz

Zum anderen ist das IT-Sicherheitskonzept ein zentraler Bestandteil im IT-Grundschutz gemäß BSI (siehe hierzu Abschnitt 1.2.3) und dort ausführlich beschrieben. Gemäß IT-Grundschutzhandbuch werden im IT-Sicherheitskonzept die Risiken für die Geschäftsprozesse, IT-Anwendungen und IT-Systeme bewertet. Ebenso wird konzipiert, welche Sicherheitsmaßnahmen einen angemessenen Schutz bieten.

3.2.3.1 Inhalt des IT-Sicherheitskonzepts

Die Basis für jede Risikobewertung ist die genaue Kenntnis der zu schützenden Systeme, Anwendungen und IT-Prozesse. Aufbauend auf einer Dokumentation aller Systeme sollte das IT-Sicherheitskonzept eine Auflistung der vorhandenen Schwachstellen, der möglichen Bedrohungen und der bereits umgesetzten Maßnahmen liefern. Das BSI empfiehlt, die genannten Punkte für sämtliche IT-Systeme und Prozesse zu beschreiben und die Maßnahmen umzusetzen. Zusätzlich wird für Komponenten mit hohem oder sehr hohem Schutzbedarf empfohlen, eine weitergehende Sicherheitsanalyse durchzuführen.

IT-Grundschutz nach BSI

Mit der Version 2005 hat das BSI das ehemalige „IT-Grundschutzhandbuch" zugunsten einer Zweiteilung aufgegeben. In der Neufassung gibt es zum einen ein Handbuch mit den Standards 100-1 bis 100-3 (der Standard 100-4 liegt derzeit als Entwurf vor), das die grundsätzlichen Anforderungen und Vorgehensweisen nach IT-Grundschutz sowie zur Risikoanalyse beschreibt. Zum anderen wurden aus den Bausteinen und Maßnahmen die IT-Grundschutz-Kataloge in Form einer Loseblattsammlung erstellt. Standards und Kataloge bilden dabei eine inhaltliche Einheit, wobei die Standards die Klammer um die Grundschutz-Kataloge bilden.

Systemdokumentation als Basis

Die Erfassung aller vorhandenen IT-Systeme ist demzufolge eine Grundvoraussetzung für die Erstellung eines wirksamen IT-Sicherheitskonzepts. Es ist jedoch nicht sinnvoll, diese in das Sicherheitskonzept aufzunehmen. Wird der im vorliegenden Buch entwickelte Ansatz einer Systemdokumentation als Bestandteil des Betriebshandbuches umgesetzt, stellt dies gleichzeitig die Basis für die Risikoanalyse und aller anderen Grundschutzmaßnahmen dar. Eine ausführliche Beschreibung der Systemdokumentation finden Sie in Abschnitt 4.2.

Der Weg zum IT-Sicherheitskonzept

Für die Erstellung eines IT-Sicherheitskonzepts bietet sich nachfolgende Vorgehensweise an, die gleichzeitig eine sinnvolle Strukturierung des IT-Sicherheitskonzepts darstellt. Diese folgt weitgehend den Vorgaben des BSI-Standards. Bei dieser Vorgehensweise wird vorausgesetzt, dass eine Systemdokumentation und eine Dokumentation der IT-Prozesse vorliegen:

1. *Schutzbedarfsfeststellung*: Die Schutzbedarfsfeststellung umfasst drei Schritte. Im Vordergrund steht dabei die Fragestellung, wie groß der maximale Schaden ist, wenn die Verfügbarkeit, die Integrität oder die Vertraulichkeit der zu untersuchenden IT-Systeme und Informationen beeinträchtigt werden:
   - Analyse, welche Gefährdungen bzw. Risiken für das Unternehmen bei unzureichender IT-Sicherheit bestehen
   - Identifizierung möglicher Schäden durch einen Verlust an Vertraulichkeit, Integrität oder Verfügbarkeit
   - Analyse und Bewertung der potenziellen Auswirkungen auf die Geschäftstätigkeit oder die Aufgabenerfüllung durch IT-Sicherheitsvorfälle und andere IT-Sicherheitsrisiken

2. *Bewertung der erfassten IT-Systeme und IT-Prozesse*: Im nächsten Schritt werden die Systeme bewertet und kategorisiert. Dazu werden die in der Schutzbedarfsfeststellung identifizierten Risiken auf die erfassten IT-Systeme angewendet und für die darauf verarbeiteten Informationen die Maximalschäden bestimmt. Dies schließt die Identifikation und Beurteilung sicherheitsrelevanter Informationen, Geschäftsprozesse und organisatorischer Abläufe ein. Ziel ist, Systeme und Prozesse mit gängigen Risiken von denen mit hohen oder sehr hohen Risiken zu unterscheiden.

3. *Sicherheits-Ist-Analyse/Risikoanalyse*: Im nächsten Schritt sind die vorhandenen Sicherheitsmaßnahmen zu erfassen und mögliche Defizite aufzuzeigen (Soll-Ist-Vergleich). Auch hierbei ist eine Unterteilung sinnvoll. Diese kann wie folgt aussehen:

   - Vorhandene Sicherheitsmaßnahmen und Risiken übergeordneter Komponenten mit hohem Schutzbedarf (Organisation, Personal, Notfallvorsorge, Datensicherung, Datenschutz)
   - Vorhandene Sicherheitsmaßnahmen und Risiken von Infrastruktur-Komponenten (Gebäude, Verkabelung, Büroräume, Serverräume/Rechenzentrum, Datenträgerarchiv, Räume für die technische Infrastruktur) sowie der betrachteten IT-Systeme
   - Vorhandene Sicherheitsmaßnahmen und Risiken für die betrachteten IT-Prozesse

4. *Festlegung der IT-Grundschutzmaßnahmen:* Für alle untersuchten IT-Systeme und Prozesse mit gängigen Risiko werden pauschal Maßnahmenempfehlungen festgelegt.

5. *Zusätzliche Maßnahmen für Systeme mit höheren Risiko:* Für alle Systeme und Prozesse, die der Gruppe mit höherem Risiko zuzuordnen sind, sollte zusätzlich eine detaillierte Sicherheitsanalyse durchgeführt werden. Diese muss sowohl Schwachstellenanalyse als auch eine individuelle Risikoanalyse gemäß dem IT-Sicherheitskonzept des BSI umfassen.

Risikoanalyse als Basis für Grundschutzmaßnahmen

Die Risikoanalyse liefert für ausgewählte IT-Systeme und IT-Prozesse auf der Basis der Ergebnisse von Bedrohungs- und Schwachstellenanalysen die Wahrscheinlichkeit für das Eintreffen eines gefährdenden Ereignisses und den damit verbundenen potenziellen Schaden.

Der *BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz* beschreibt ausführlich Methoden zur Durchführung zusätzlicher IT-Risikoanalysen (siehe hierzu Abschnitt 1.2.3).

Maßnahmenbereiche

Im Rahmen der Maßnahmenempfehlungen müssen eine Reihe von konkreten Festlegungen getroffen werden. Zu den typischen Maßnahmenbereichen gehören unter anderem die folgenden:

- Passwortrichtlinien (Komplexität, Länge, Historie, Gültigkeitsdauer u. Ä.)
- Sicherheitsrichtlinien für alle Rechnersysteme, die zur Sicherheitsklasse mit normalem Risiko gehören (physische Sicherheit, BIOS-Absicherung, lokale Sicherheitsrichtlinien, Zugriffsschutz für Systemordner u. Ä.)
- Regelungen für den Umgang mit E-Mail (Verschlüsselung, private E-Mail-nutzung, Funktionspostfächer usw.)
- Regelungen zur Internetnutzung (Möglichkeiten zum Herunterladen von Software, Freischaltung von Freemailern usw.)
- Zugriffsschutz für mobile Geräte
- Regelungen für den Umgang mit USB-Schnittstellen (blockiert, kontrollierte Freigabe) und mit Wechseldatenträgern
- Richtlinien für die WLAN-Nutzung
- Umgang mit anderen drahtlosen Schnittstellen [BSI]

hinweis

Ein Sicherheitskonzept enthält in der Regel vertraulich zu behandelnde Informationen, die nicht beliebig weitergegeben werden dürfen. Hierzu können zum Beispiel Informationen über noch nicht beseitigte Schwachstellen zählen. Es sollte deshalb bereits bei der Erstellung darauf geachtet werden, dass es möglich ist, für die unterschiedlichen Zielgruppen die für sie relevanten Teile ausgliedern zu können. Eine entsprechende Gliederung des IT-Sicherheitskonzepts kann dies unterstützen.

Weitere Informationen zum hier vorgestellten IT-Grundschutz sind in der zahlreichen Literatur zum IT-Sicherheitskonzept zu finden. Eine der wichtigsten Informationsquellen stellt hier sicherlich das BSI dar. Hervorzuheben ist der *BSI-Standard 100-1 – Managementsysteme für Informationssicherheit (ISMS)* sowie Kapitel 4 des *BSI-Standards 100-2 - IT-Grundschutz-Vorgehensweise*. Diese beiden Schriften liefern eine detaillierte Anleitung zur Erstellung einer IT-Sicherheitskonzeption gemäß IT-Grundschutz.

hinweis

Mit dem Tool IT-Grundschutz (GSTOOL) stellt das BSI außerdem eine Software bereit, die den Anwender bei der Erstellung, Verwaltung und Fortbeschreibung von IT-Sicherheitskonzepten entsprechend dem IT-Grundschutz nach den BSI-Standards 100-1 bis 100-3 unterstützt.

Nähere Informationen zu Systemanforderungen, Bezugsmöglichkeiten und Preisen für die aktuelle Version von GSTOOL finden Sie im Steckbrief in Anhang D.1.

Eine gute Informationssammlung mit einer Musterdokumentation für ein IT-Sicherheitskonzept findet sich weiterhin im Infoportal des Landesdatenbeauftragten für Datenschutz und Informationsfreiheit Saarland [LFDI].

3.2.3.2 Zusammenspiel mit dem Notfallhandbuch

Aufgabe des IT-Sicherheitskonzepts ist es auch zu regeln, wie mit vertraulichen Daten wie Administrator-Passwörtern oder Lizenzschlüsseln umgegangen werden soll. Derartige Regelungen, die auch für den Notfall relevant sind, sollten herausgehoben betrachtet werden.

Ohne Passwörter geht im Notfall gar nichts

Eigentlich hört es sich trivial an, trotzdem muss es erwähnt werden: Bei einem Notfall müssen alle erforderlichen Informationen verfügbar sein. Hierzu zählen insbesondere auch Lizenzschlüssel und Administrator-Passwörter. So ist beispielsweise für die Autorisierung eines DHCP-Servers in Active Directory die Berechtigung eines Organisations-Administrators erforderlich. Ist dieser „wichtige Mensch" bei einem Notfall nicht erreichbar und das Kennwort nicht verfügbar, stellt dies ein ernsthaftes Problem dar. Gleiches gilt, wenn beispielsweise ein externer Mitarbeiter im Notfall die Active Directory-Datenbank zurücksichern soll, aber nicht autorisiert ist.

Da derartige Informationen nicht ausschließlich im Notfall verfügbar sein müssen, da sie gegebenenfalls auch bei normalen Änderungsprozessen benötigt werden, ist es nicht sinnvoll, die damit verbundenen Regelungen ausschließlich im Notfallhandbuch zu definieren. Besser ist es diese Informationen im IT-Sicherheitskonzept zu pflegen und in das Notfallhandbuch als Verweis bzw. in Kopie aufzunehmen.

3.2.4 IT-Risikohandbuch

» Für *IT-Risikohandbuch* synonym verwendete Begriffe: Risikohandbuch, Risikoplan «

Ein unternehmensweites Risikohandbuch bildet die Grundlage eines unternehmensweiten Risikomanagements. Es stellt organisatorische Maßnahmen und Regelungen dar, die zur Risikoerkennung, -quantifizierung, -kommunikation, -steuerung und Risikokontrolle zu beachten sind. Zusätzlich liefert dieses Handbuch die Basis für die Prüfung des Risikomanagements, die sowohl extern durch den Abschlussprüfer als auch intern durch die interne Revision oder den Aufsichtsrat vorgenommen werden kann.

Nicht nur das 1998 verabschiedete *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)* (siehe Abschnitt 1.1.2.1) fordert, bestehende Risiken aufzuzeigen und der Unternehmensleitung sowie den Anteilseignern oder Investoren transparent zu machen. Während früher aber vor allem Finanzrisiken betrachtet wurden, treten heute zunehmend auch die operativen Risiken in den Vordergrund, wie sie sich beispielsweise aus dem IT-Betrieb ergeben. Zumindest in großen Unternehmen wird deshalb zunehmend vom IT-Bereich ein eigenes IT-Risikohandbuch verlangt.

Schwierige Abgrenzung zum IT-Sicherheitskonzept

Aus der historischen Entwicklung heraus ergibt sich aber ein Problem mit der Abgrenzung zum IT-Sicherheitshandbuch. Weil nämlich Riskohandbücher in der Vergangenheit die Risiken, die sich aus dem IT-Betrieb ergaben, nicht berücksichtigten, hat das BSI die Riskoanalyse als Ergänzung des IT-Grundschutz-Sicherheitskonzepts in seine Bausteine aufgenommen. Gemäß der obigen Beschreibung fordert aber auch das IT-Risikohandbuch entsprechende Risikoanalysen und Maßnahmenkataloge.

Wie bereits mehrfach betont, bleibt an dieser Stelle nur eine klare Definition und Abgrenzung der jeweils im Unternehmen benötigten Dokumente. So kann beispielsweise das IT-Risikohandbuch als strategisches Dokument definiert werden, das auf einem abstrakten Level das Risikomanagement regelt, während das IT-Sicherheitskonzept einen konkreten Maßnahmenkatalog auf der Grundlage einer Risikoanalyse liefert, die gemäß BSI-Standard erstellt wurde. Alternativ kann auch das IT-Risikohandbuch einen Risikoplan mit allen ermittelten Risiken enthalten, während das IT-Sicherheitskonzept systematische Gegenmaßnahmen beschreibt.

Regelmäßige Überprüfung

Da die Gewährleistung der IT-Sicherheit ein kontinuierlicher Prozess ist, genügt es nicht, das IT-Risikohandbuch einmal zu erstellen und dann alle Sicherheitsmaßnahmen umzusetzen. Vielmehr muss das Risikomanagement auf neue technische Entwicklungen reagieren und das Risikohandbuch ständig überprüfen und aktualisieren.

Business Impact-Analyse ist Basis für Risikohandbuch

Mit der zunehmenden Ausrichtung der Unternehmen an Prozessen gewinnt auch die *Business Impact-Analyse (BIA)* zunehmend an Bedeutung. Auch das Risikohandbuch sollte auf einer BIA aufbauen. Was aber verbirgt sich hinter einer die „Auswirkungsanalyse", d. h. einer BIA. Business Impact-Analyse ist eine Methode des *Business Continuity Managements (BCM)* und dient der Identifizierung und Erfassung von Prozessen innerhalb eines Unternehmens. Ziel ist es, wechselseitige Abhängigkeiten zwischen den Prozessen und/oder den Unternehmensbereichen aufzuzeigen und die Auswirkungen bei Ausfall von Prozessen bzw. die benötigten Wiederanlaufzeiten zu ermitteln.

Zusammen mit der Risikoanalyse bildet die BIA die Grundlage für eine Sicherheits- und Notfallstrategie und die Basis für das Notfallkonzept bzw. das Notfallhandbuch. Einige weitere Erläuterungen zur Business Impact-Analyse finden Sie in Abschnitt 5.1.3.1.

Da es sich bei der Business Impact-Analyse um eine Unternehmensaufgabe handelt und alle Geschäftsprozesse eines Unternehmens in die Analyse einbezogen werden sollten, sind die dabei entstehenden Dokumente nicht der IT-Dokumentation zuzuordnen.

3.2.5 IT-Notfallkonzept

» Für *Notfallkonzept* synonym verwendete Begriffe:
Notfallhandbuch «

In den vorstehenden Abschnitten wurde mehrfach auf das Notfallkonzept verwiesen. Hierbei handelt es sich um ein Dokument, dass die *Notfallvorsorge* im Blickpunkt hat. Damit grenzt es sich vom Notfallhandbuch ab, dessen Aufgabenschwerpunkt die Notfallbewältigung ist.

Als übergeordnetes Regelwerk sollte es den Rahmendokumenten zugeordnet werden. Es beschreibt die Strategien und Vorgaben für alle Aktivitäten der Notfallbewältigung. Alle Maßnahmen und Tätigkeiten, die hingegen zur eigentlichen Bewältigung eines Notfalls beitragen, sind im Notfallhandbuch zu beschreiben.

Inhalt des Notfallkonzepts

Was genau im Notfallkonzept geregelt wird, obliegt dem Unternehmen und ist von diesem festzulegen. Möglicherweise gibt es ein unternehmensweites Notfallkonzept, das lediglich durch ein separates IT-Notfallkonzept ergänzt werden muss.

Eine nähere Betrachtung des Notfallkonzepts erfolgt in Kapitel 5, „Dokumentation für den Notfall".

3.2.6 IT-Verfahrensverzeichnis

Das Bundesdatenschutzgesetz (BDSG) definiert verbindlich für alle Unternehmen, die der gesetzlichen Meldepflicht unterliegen, klare Anforderungen bezüglich der Einhaltung des Datenschutzes und der Datensicherheit. Zur Einhaltung eines gesetzeskonformen Datenschutzmanagements ist unter anderem die Pflege eines sogenannten *Verfahrensverzeichnisses* durch den Datenschutzbeauftragen des Unternehmens für alle Unternehmen vorgeschrieben,

Das Verfahrensverzeichnis muss alle automatisierten Verfahren einer Organisation auflisten, mit denen im Rahmen eines automatisierten Verfahrens ermittelte personenbezogene Daten gespeichert werden.

Definition Verfahren

Der Begriff *Verfahren* wird vorrangig im datenschutzrechtlichen Zusammenhang verwendet und bezeichnet hier Vorgänge, in denen personenbezogene Daten verarbeitet oder genutzt werden. Ein typisches Verfahren ist eine automatisierte Zeiterfassung. Die für ein Verfahren verantwortliche Stelle muss im Verfahrensverzeichnis Angaben zu sämtlichen von ihr betriebenen automatisierten Verfahren machen, mit denen sie personenbezogene Daten verarbeitet.

Entsprechend der Zielsetzung des Verfahrensverzeichnisses konzentriert sich sein Inhalt auf die Offenlegung der für die Verarbeitung personenbezogener Daten verantwortlichen Stellen und Personen, auf die Zweckbestimmung der Verarbeitung sowie auf die betroffenen Personengruppen. Außerdem müssen Regelfristen für die Datenlöschung definiert werden. Konkret schreibt das BDSG vor, dass der für den Datenschutz Zuständige in geeigneter Weise gemäß § 4e Abs. 1 die folgenden Angaben für alle Betroffenen verfügbar zu machen hat.

„Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind folgende Angaben zu machen:

1. *Name oder Firma der verantwortlichen Stelle,*
2. *Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,*
3. *Anschrift der verantwortlichen Stelle,*
4. *Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,*
5. *eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,*
6. *Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,*
7. *Regelfristen für die Löschung der Daten,*
8. *eine geplante Datenübermittlung in Drittstaaten,*
9. *eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.“*

tipp

Es gibt im Internet eine ganze Reihe von Musterdokumentationen, die bei der Erstellung der Dokumente für das Verfahrensverzeichnis hilfreich sein können. Hervorzuheben ist die Publikation *Verfahrensverzeichnis und Verarbeitungsübersicht nach BDSG – Ein Praxisleitfaden,* die vom *Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM)* bereitgestellt wird. Das Dokument liefert neben einer umfassenden Übersicht, einem Beispiel eines Verfahrensverzeichnisses und diversen Formularen auch Beispiele für Programme zur Erstellung des Verfahrensverzeichnisses [BITKOM].

3.2.7 IT-Rollenkonzept

» Für *Rollenkonzept* synonym verwendete Begriffe: Rollenmodell, Berechtigungskonzept «

Was ist eine Rolle?

Für das Funktionieren der IT-Prozesse ist das IT-Rollenkonzept von besonderer Bedeutung. Während es früher üblich war, Rechte und Pflichten einzelnen Mitarbeitern zuzuweisen, werden beim prozessorientierten Ansatz *Rollen* verwendet. Eine Rolle kann dabei als die Beschreibung einer Menge von Aufgaben, Verantwortlichkeiten und Berechtigungen definiert werden, die von einem aber auch von mehreren Mitarbeitern wahrgenommen werden können.

Ein *Beispiel* ist die Rolle „Support-Mitarbeiter“: Ein Mitarbeiter, der diese Rolle innehat, soll bestimmte Aufgaben erfüllen und benötigt bestimmte Rechte und Befugnisse, um seine Aufgaben erfüllen zu können. So ist der Inhaber dieser Rolle beispielsweise befugt, Störungen anzunehmen und Störungsmeldungen im Ticket-System einzutragen. In der Beschreibung der Rolle muss also genau festgelegt sein, was ein Support-Mitarbeiter überhaupt ist, welche Tätigkeiten er auszuführen hat, welche Befugnisse er hat und welche fachlichen und persönlichen Fähigkeiten für die Ausübung der Rolle erforderlich sind. In der Prozessbeschreibung für die Annahme und Abwicklung von Störungen wiederum steht als Bearbeiter nicht der Mitarbeiter XY, sondern die Rolle „Support-Mitarbeiter“. Dies gewährleistet die Unabhängigkeit von organisatorischen und projektspezifischen Rahmenbedingungen.

Aufgabe des Rollenkonzepts

Das Rollenkonzept definiert und beschreibt alle im Bereich der IT eingesetzten Rollen. Mit Hilfe dieser Rollenbeschreibungen können in der Betriebsmatrix die Mitarbeiter bzw. die Organisationseinheiten den Rollen zugeordnet werden. Wechselt beispielsweise ein Mitarbeiter des Backup-Teams in eine andere Abteilung, wird ihm lediglich die Rolle „Backup-Operator“ entzogen. Entsprechend seiner neuen Rolle in der neuen Abteilung können dem Mitarbeiter anhand des Rollenkonzepts alle erforderlichen Kompetenzen und Berechtigungen zugewiesen werden, ohne dass eine Änderung der Prozessdokumentation erforderlich ist. Lediglich die IT-Betriebsmatrix muss angepasst werden. Erläuterungen zur Erstellung einer IT-Betriebsmatrix finden Sie im nachfolgenden Abschnitt.

Die Zielgruppe für das Rollenkonzept sind die Organisationsverantwortlichen sowie die für das Personalmanagement verantwortlichen Mitarbeiter. Zwar müssen jedem Mitarbeiter die ihm übertragenen Verantwortlichkeiten und die ihn betreffenden Regelungen bekannt sein, doch ist dies eine Aufgabe der Prozessbeschreibungen und nicht des Rollenkonzepts. Entsprechend der Zielgruppe sind die Rollen abstrakt zu beschreiben.

hinweis

Ein Beispiel für eine Rollenbeschreibung finden Sie in Abschnitt 8.1.

Vorgaben bei ITIL

Für die Standardprozesse, wie beispielsweise die Support-Prozesse, lohnt ein Blick auf das Rollenmodell von ITIL, da für diese Prozesse bereits zahlreiche Dokumentationen vorliegen, von denen vielfach zumindest Teile in die eigene Dokumentation übernommen werden können. Die in ITIL beschriebenen Prozesse definieren jeweils einen Prozesseigner, der die Zielvorgaben und die Kontrolle des Prozesses verantwortet, einen Prozess-Manager, der für die Umsetzung des Prozesses verantwortlich ist, und einen oder mehrere Servicetechniker für die operative Umsetzung des Prozesses.

3.2.8 IT-Betriebsmatrix

» Für *Betriebsmatrix* synonym verwendete Begriffe:
Betriebsorganigramm. «

Wie im vorstehenden Kapitel beschrieben, werden beim prozessorientierten Ansatz Rollen definiert, denen Aufgaben und Verantwortlichkeiten zugewiesen werden.

Darüber hinaus muss es ein Dokument geben, in dem die Zuordnung von Organisationseinheiten und Personen zu den Rollen erfolgt, also ein Dokument, in dem konkret steht, welcher Rolle der Mitarbeiter XY zugeordnet ist. Dies ist die Aufgabe der sogenannten *Betriebsmatrix*. Diese definiert die organisatorische Platzierung der Aufgaben und Rollen. Dabei kann eine Person mehrere Rollen besetzen; ebenso kann aber auch eine Rolle von mehreren Personen eingenommen werden.

Vorteile einer Betriebsmatrix

Eine Betriebsmatrix ermöglicht demzufolge eine eindeutige Zuordnung von Personen und Rollen und hilft dabei, Doppelbesetzungen, unklare Zuständigkeiten und Überschneidungen zu verhindern. Zeigt sich beispielsweise bei der Erstellung, dass ein Mitarbeiter Rollenträger für sehr viele Rollen ist, sollte überprüft werden, ob nicht einzelne Rollen auf andere Mitarbeiter übertragen werden können. Zwar ist es durchaus üblich, dass ein Mitarbeiter mehrere Rollen ausübt, doch wenn dieser Rolleninhaber dreier Rollen ist, die eigentlich jeweils 100 Prozent seiner Arbeitszeit beanspruchen, so stimmt etwas nicht. Möglicherweise wird dabei aber auch deutlich, dass wichtige Rollen überhaupt nicht eindeutig zugeordnet sind und im operativen Betrieb „irgendwie von irgendjemanden" erledigt werden.

Die Betriebsmatrix kann entweder zentral für das gesamte Unternehmen gepflegt werden oder auch gesondert von jeder Organisationseinheit. In den meisten Unternehmen gibt es zwar Dokumente, aus denen hervorgeht, welcher Mitarbeiter welche Position einnimmt. Eine rollenbasierte Betriebsmatrix ist aber noch eher selten zu finden. Fehlt also eine solche Betriebsmatrix, ist die Aufnahme der Matrix für den IT-Betrieb in die IT-Dokumentation zu empfehlen.

hinweis

Das Beispiel in Abschnitt 8.2 zeigt an einem Auszug, wie eine solche Betriebsmatrix für den IT-Betrieb aussehen kann.

3.2.9 IT-Gruppenkonzept

» Für *Gruppenkonzept* synonym verwendete Begriffe:
Berechtigungskonzept, Administrationskonzept. «

Wie in den vorstehenden Kapiteln ausgeführt wurde, werden alle für die Prozesse erforderlichen Rollen im Rollenkonzept definiert. Hierbei handelt es sich um eine rein organisatorische Zuordnung, in der keine systemtechnischen Zuordnungen festgelegt werden. Zusätzlich gibt es mit der Betriebsmatrix ein Dokument, in dem die Zuordnung von Organisationseinheiten und Personen zu den Rollen erfolgt.

Zuordnung einer Rolle zu einer Systemgruppe

Damit ist aber noch nicht festgelegt, wie Rollen systemtechnisch umzusetzen sind. Hierfür wird ein weiteres Dokument benötigt, das im vorliegenden Buch als IT-Gruppenkonzept bezeichnet wird. Dieses bildet im Hinblick auf die Benutzerverwaltung eine Schnittstelle zwischen der Prozessdokumentation und der Systemdokumentation, indem es alle systemtechnischen Gruppen aufführt, erläutert und eine Zuordnung zu den Rollen festschreibt.

Beispielsweise kann im Gruppenkonzept eine Active Directory-Sicherheitsgruppe „Helpdesk“ zu finden sein. Für diese Gruppe werden hier die systemseitigen Rechte definiert (beispielsweise Zugriffsberechtigungen für das Ticket-System). Weiter wird definiert, dass jeder Mitarbeiter, der die Rolle Support-Mitarbeiter inne hat, der Gruppe Active Directory-Gruppe „Helpdesk“ hinzuzufügen ist.

hinweis

Nicht in jedem Fall ist die Erstellung eines eigenständigen IT-Gruppenkonzepts erforderlich. Während in großen Unternehmen, die erfahrungsgemäß große Anzahl an Gruppen ein eigenständiges Dokument rechtfertigt, ist es unter Umständen auch möglich, die Zuordnung von Rollen zu Gruppen in einer Tabelle dem Rollenkonzept hinzuzufügen.

3.2.10 IT-Namenskonventionen

Auf den ersten Blick mögen Namenskonventionen zweitrangig erscheinen, jedoch sind sie in größeren Unternehmen unverzichtbar. Beispielsweise ist ein im Vorfeld sorgfältig geplantes, einheitliches Schema der Namenskonventionen für alle Objekte der Active-Directory-Gesamtstruktur insbesondere in großen Unternehmen unerlässlich, um Wildwuchs zu vermeiden. Wichtig ist, dass alle mit der Vergabe von Namen betrauten Mitarbeiter von den Regelungen – dies gilt vor allem auch für externe Berater – Kenntnis haben und sie auch anwenden.

Namenskonvention für eine Active Directory-Umgebung

Die nachstehende Aufstellung zeigt die wichtigsten Systeme und Komponenten, für die typischerweise in einer Active Directory-Umgebung die Verwendung von Namen standardisiert werden sollte. Die Auflistung erhebt keinen Anspruch auf Vollständigkeit und muss im Einzelfall angepasst werden.

- Server (ausgenommen Cluster-Systeme)
- Cluster-Systeme (virtuelle Server und Clusterknoten)
- Linux-/UNIX-Server
- Clients
- Domänen (ROOT-Domäne und Sub-Domänen)
- Standorte im Active Directory (Standorte, Standort-Links und Standorteigenschaften)
- Organisationseinheiten (OUs)

- Gruppenrichtlinien (GPOs)
- Gruppen
- Benutzer (Anmeldename, angezeigter Name, E-Mail-Adresse, Beschreibung)
- Administrative Benutzer (Anmeldename, angezeigter Name, E-Mail-Adresse, Beschreibung)
- Funktionsbenutzer, z. B. Hotline-Benutzer (Anmeldename, angezeigter Name, E-Mail Adresse, Beschreibung)
- Dienstkonten
- Dateinamen, Verzeichnisnamen, Freigabebezeichnungen, persönliche Ordner, servergespeicherte Benutzerprofile
- Drucker (Druckername, Druckerstandort)
- Messaging-Dienst Exchange (Exchange Server-Name, Routing Group, Connectoren, öffentliche Ordner, Verteilerlisten, persönliche Postfächer, Postfach-Alias, Funktions-Postfächer)

Sind für die Produktionsumgebung und die Testumgebung unterschiedliche Namensrichtlinien erforderlich, sollte dies entsprechend berücksichtigt werden.

Daneben gebt es für den IT-Betrieb aber noch weitere Komponenten, für die eine Standardisierung von Namen sinnvoll ist. Hierzu zählen beispielsweise Konventionen zur Benennung von Prozessen und Unterprozessen sowie Regelungen zur Benennung von Rollen (beispielsweise ob englische oder deutsche Bezeichnung).

Konventionen auch für Dokumente

Und schließlich sollten auch für Dokumente verbindliche Namensregeln (sowohl Dokumententitel als auch Dateinamen) festgelegt werden. Im Rahmen der IT-Dokumentation nehmen Namenskonventionen einen hohen Stellenwert ein, da sie Auswirkungen auf alle anderen Dokumente haben.

3.2.11 IT-Projektmanagement-Handbuch

Das IT-Projektmanagement-Handbuch (PM-Handbuch) regelt die verbindlichen Sollvorgaben, die für alle IT-Einzelprojekte gelten. Aufgrund des übergeordneten Charakters wird es den Rahmendokumenten zugeordnet. Da eine inhaltliche Betrachtung des IT-Projektmanagement-Handbuches jedoch besser in Kapitel 6, „Dokumentation von IT-Projekten", passt, sei an dieser Stelle lediglich auf das genannte Kapitel verwiesen.

3.2.12 IT-Dokumentationsrichtlinie

Mit wachsender Unternehmensgröße wird die Erstellung und Durchsetzung einer Dokumentationsrichtlinie zunehmend wichtiger. Diese wird sinnvollerweise übergeordnet auf Unternehmensebene definiert. Wo eine solche übergeordnete Richtlinie fehlt, sollte sie zumindest für die Ebene der IT-Dokumentation entwickelt werden.

Die Aufgabe einer Dokumentationsrichtlinie ist es, verbindliche Regelungen für den formalen Aufbau einzelner Dokumente festzulegen sowie verbindliche Dokumentationsprozesse zu definieren. Zum Inhalt einer solchen Richtlinie sollten die folgenden Punkte zählen:

- Richtlinien und Klassifizierungen, die für alle Dokumente gelten (Namenskonventionen, Bearbeitungsstatus, Nummerierungssystem u. Ä.)
- Formaler Aufbau der Einzeldokumente
- Dokumentationsprozesse (Freigabeprozesse, Beauftragungsprozesse, Review-Verfahren usw.)
- Regelungen zur Speicherung der Dokumente im Dateisystem bzw. im Dokumentenmanagement-System

Eine ausführliche Beschreibung der möglichen Inhalte einer Dokumentationsrichtlinie unter Berücksichtigung der genannten vier Punkte erfolgt in Abschnitt 7.1.

3.2.13 Rahmendokumente und ihre Abhängigkeiten

Die einzelnen Rahmendokumente können, wie bereits dargestellt wurde, nicht isoliert betrachtet werden, sondern stehen miteinander in Beziehung. Einen Ausschnitt aus diesen Beziehungen zeigt die nachstehende Grafik.

Ein weiteres Bespiel (Abhängigkeiten der Sicherheitsdokumente) finden Sie in Abschnitt.5.1.3.2.

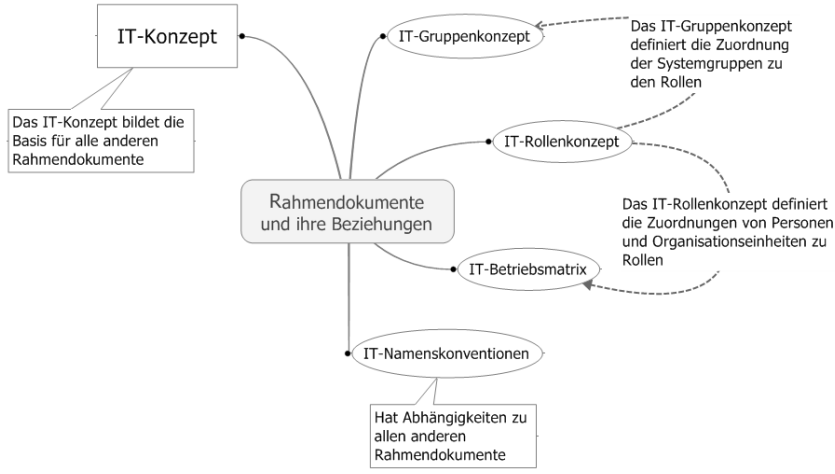


Abbildung 3.2: Rahmendokumente der IT-Dokumentation und ihre Abhängigkeiten: ein Ausschnitt

3.3 Fazit

Wie in diesem Kapitel gezeigt wurde, gibt es eine Reihe von Dokumenten, die übergeordneten Charakter haben und einen Rahmen für die Dokumente der drei Bereiche der IT-Dokumentation darstellen. Sie werden daher im vorliegenden Buch als Rahmendokumente bezeichnet.

Alle vorgestellten Dokumente können sowohl auf der Ebene der IT-Dokumentation als auch auf Unternehmensebene verwaltet werden. So ist es beispielsweise möglich und auch üblich, ein unternehmensweites Risikohandbuch zu führen und die IT-Service gefährdenden Risiken in einem gesonderten IT-Risikohandbuch im Rahmen der IT-Dokumentation zu pflegen.

Welche IT-Rahmendokumente also im individuellen Fall zu erstellen sind, hängt weitgehend davon ab, ob und mit welcher Ausprägung unternehmensweit gültige Dokumente existieren. Im Idealfall gibt es übergeordnete Unternehmensdokumente, die auf einem hohen Abstraktionsniveau allgemeingültige Richtlinien enthalten. Diese werden durch detaillierte Vorgaben in den entsprechenden Dokumenten der Organisationseinheiten ergänzt.

4 Dokumentation des IT-Betriebs

Das folgende Kapitel stellt die für den IT-Betrieb erforderliche Dokumentation vor. Es handelt sich hierbei also um den Teil der IT-Dokumentation, der im allgemeinen Sprachgebrauch als *Betriebshandbuch* bezeichnet wird.

Entsprechend dem prozessorientierten Ansatz in diesem Buch stehen hierbei die Prozesse des IT-Betriebs im Vordergrund. Nach einer Einführung in die *Prozessdokumentation* zeigen exemplarische Beispiele, wie sich Prozesse anforderungsgerecht sowie auch praxistauglich beschreiben lassen.

Die Basis aller Prozesse bildet die Dokumentation der eingesetzten Hard- und Softwaresysteme (Betriebssysteme, Datenbanksysteme, Clusterinfrastruktur usw.). Wie eine solche *Systemdokumentation* sinnvoll aufgebaut und gepflegt werden kann, ist ein weiterer Schwerpunkt dieses Kapitels.

4.1 Aufbau eines prozessorientierten Betriebshandbuches

Die Notwendigkeit einer prozessorientierten Ausrichtung der IT-Dokumentation wurde bereits an verschiedenen Stellen angesprochen. Dieser Notwendigkeit folgt konsequenterweise auch der Aufbau des IT-Betriebshandbuches.

Systemdokumentation ist die Basis

Die Kenntnis und Beschreibung aller vorhandenen IT-Systeme ist die Basis für die Prozesse. So ist beispielsweise die sinnvolle Einbindung eines neuen DNS-Servers kaum möglich, ohne die genaue Kenntnis der vorhandenen DNS-Struktur.

Die Einrichtung und Pflege einer Systemdokumentation als Bestandteil des Betriebshandbuches ist daher zwingend erforderlich. Die Systemdokumentation muss die Dokumentation der eingesetzten Hardware (Server- und Clientsysteme) und der Basissoftware (Betriebssysteme, Datenbanksysteme, Datensicherungssysteme usw.) genauso beinhalten wie Dokumentationen zum Verzeichnisdienst, zu Server- und Netzwerkdiensten, zu eingesetzten Anwendungen sowie Beschreibungen der Netzwerkhardware, Netzwerkpläne und anderer Komponenten wie beispielsweise (gerne vergessen) der TK-Anlage. Es ist jedoch nicht sinnvoll, diese Dokumentationen in die Prozessbeschreibungen aufzunehmen, da vielfach ein System an mehreren Prozessen beteiligt ist. Das würde zur Unübersichtlichkeit und zu Redundanzen in der Dokumentation führen.

Zudem wird die Systemdokumentation auch von anderen Seiten benötigt. So bildet sie nicht nur für die Risikoanalyse die Basis, sondern ebenfalls für das Notfallhandbuch.

Prozessorientierung anstelle systemorientierter Ausrichtung

Den zweiten Kernbereich eines prozessorientierten Betriebshandbuches bilden folglich die Prozessbeschreibungen. Daraus ergibt sich ein Aufbau des Betriebshandbuches, der kaum noch etwas mit dem traditionellen Aufbau von Betriebshandbüchern gemein hat. Diese enthalten klassischerweise (ebenfalls) einen Teil, in dem das System einschließlich seiner Konfiguration beschrieben wird, und zusätzlich Kapitel mit Beschreibungen und Anleitungen zur Administration, Wartung und Installation des Systems. Zumeist finden sich in Betriebshandbüchern auch Anleitungen zum Umgang mit Problemen oder sogar mit Notfällen.

Der prozessorientierte Ansatz betrachtet die Systeme nicht einzeln für sich, sondern stellt die Zusammenhänge in den Vordergrund. Der Vorteil der Prozessorientierung besteht darin, dass Lücken und Ineffizienzen an den Schnittstellen der einzelnen Funktionen früher erkannt und behoben werden können. Auch wenn bereits die Merkmale der Prozessorientierung herausgearbeitet wurden, soll dies hier noch einmal an einem Beispiel verdeutlicht werden:

beispiel

Der Betrieb von Active Directory dient vorrangig dazu, den Mitarbeitern schnellen und jederzeit verfügbaren Zugriff auf benötigte Ressourcen zu ermöglichen. Folglich stellen die Prozesse zum Einrichten, Umziehen oder Löschen von Benutzern einige der zentralen Aufgaben dar. Sie umfassen jedoch weit mehr als das alleinige Einrichten und Verwalten von Benutzerkonten im Active Directory. So muss bei der Einrichtung eines neuen Benutzers zusätzlich in Exchange ein Postfach eingerichtet und der Clientarbeitsplatz bereitgestellt werden. Darüber hinaus sind gegebenenfalls zusätzliche Berechtigungen in Anwendungen wie beispielsweise SAP einzurichten. Alle diese Aufgaben können in einer Prozessbeschreibung in der richtigen Abfolge, möglicherweise in detaillierten Teilprozessen, dargestellt werden.

Selbstverständlich benötigen aber auch hier die Ausführenden dieser Prozesse Anleitungen mit detaillierten Beschreibungen. Diese werden aber gezielt dem jeweiligen (Teil-)Prozess zugeordnet und nicht in einem „großen" Administrationshandbuch „versteckt". Dabei kann einer Prozessbeschreibung zur Einrich-

tung eines neuen Benutzers durchaus auch eine Schritt-für-Schritt-Anleitung beigefügt werden, die in einem automatisierten Workflow sogar „auf Knopfdruck" verfügbar ist.

Im klassischen, nicht prozessorientierten Betriebshandbuch würde der Prozess des Einrichten eines Benutzers im Active Directory-Betriebshandbuch lediglich als einzelne administrative Aufgabe im Rahmen der Active Directory-Verwaltung betrachtet werden. Dabei aber steht Active Directory und nicht die Benutzerverwaltung im Vordergrund. Daraus folgt auch, dass zum Einrichten eines Benutzers Informationen aus weiteren Dokumenten (für Exchange, zur Clientverwaltung und gegebenenfalls verschiedene Anwendungen) herangezogen werden müssten.

Systemverwaltungsprozesse zusätzlich erforderlich

Auch wenn bei einer prozessorientierten Betrachtung die Systeme nicht mehr im Vordergrund stehen, müssen sie selbstverständlich dennoch verwaltet und gewartet werden. Hierfür werden wiederum Prozesse (beispielsweise Prozesse, die die regelmäßige Überwachung sicherstellen oder Prozesse für das Patch-Management) definiert und dokumentiert.

Aus den genannten Überlegungen ergibt sich für das Betriebshandbuch die folgende Unterteilung:

- Beschreibung der Systeme und der Infrastruktur in Systemakten
- Prozessbeschreibungen für alle relevanten Aufgaben des IT-Betriebs, einschließlich Arbeitsanweisungen, Formulare und Checklisten. Zu den an dieser Stelle betrachteten Prozessen gehören sowohl Prozesse für den Regelbetrieb als auch Support-Prozesse und Regelungen für Änderungsabläufe.

Betriebshandbuch als Loseblattsammlung

Grundsätzlich ist zu beachten, dass es sich, auch wenn der Name dies suggeriert, bei einem derartigen Betriebshandbuch nicht um ein einziges Handbuch oder sogar um eine einzige Datei handelt. Vielmehr sollte das Betriebshandbuch modular im Sinne einer Loseblattsammlung aufgebaut sein, die jederzeit ergänzbar und aktualisierbar ist. Außerdem lässt sich auf diese Weise den durchführenden Stellen jeweils der für sie relevante Teil der Betriebsdokumentation zur Verfügung stellen. Trotzdem ist es selbstverständlich auch möglich, das Betriebshandbuch als ein (einziges) Handbuch zu behandeln und die hier vorgestellte Strukturierung als Kapitelunterteilung zu verstehen und verwenden.

cd-rom

Die folgenden Kapitel stellen die beiden Bereiche *Systemdokumentation* und *Prozessdokumentation* im Einzelnen vor. Auf der beigefügten CD-ROM finden Sie eine mit MindManager erstellte Datei, die die vorgestellte Gliederung der IT-Dokumentation grafisch darstellt und eine Betrachtung der im Folgenden vorgestellten Einzelbereiche in einer Zusammenschau ermöglicht. Mit dem ebenfalls beigefügten MindManager Viewer kann diese Datei angesehen werden. Außerdem ist es möglich, Zweige zu öffnen, zu schließen und in sie hineinzuzoomen.

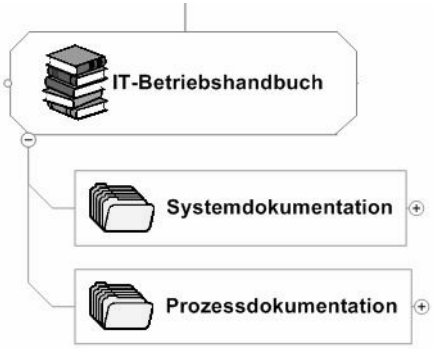


Abbildung 4.1: Die Hauptteile des Betriebshandbuches: Systemdokumentation und Prozessdokumentation

4.2 IT-Systemdokumentation

Systemakten als Basis der Systemdokumentation

Eine sinnvolle Gliederung der Systemdokumentation ist mit der Verwendung sogenannter *Systemakten* möglich. Diese beinhalten alle relevanten Informationen für ein System, das heißt, sie werden gesondert für jedes System angelegt und gepflegt. Als System werden hier beispielsweise sowohl einzelne Server (*Hardware-Systemakten*) als auch das Standard-Softwarepaket für die Clientrechner oder der Verzeichnisdienst Active Directory (*Software-Systemakten*) betrachtet.

Die Systemakte beispielsweise für einen Server sollte mindestens den Aufstellungsort und Unterlagen zur Hard- und Softwareausstattung, Garantieleistungen, Wartungsverträge, Lizenzen und Ähnliches enthalten. Darüber hinaus sind Angaben zu Änderungen an der Hard- und Softwarekonfiguration, zu durchgeführten Reparaturarbeiten und zu aufgetretenen Problemen sinnvoll. Auch wer für den Server verantwortlich ist, stellt neben den Regelungen zur Datensicherung (Umfang, Verfahren, Rhythmus usw.) eine wichtige Information dar.

Eine solche Systemdokumentation erfüllt mehrere Zwecke. Zum einen dienen die Systemakten der Unterstützung der Prozesse. Gut dokumentierte IT-Systeme erleichtern Administrationsarbeiten, die Planung und Neuinstallation von Software oder auch das Beseitigen aufgetretener Fehler. Liefert beispielsweise ein Monitoring-Prozess Hinweise darauf, dass die Speicherkapazitäten für eine Datenbankanwendung nicht mehr ausreichen, kann die Systemakte des betroffenen Systems alle Informationen für die notwendige Hardwareweiterung liefern. Selbstverständlich müssen die Systemakten auch im Notfall zur Verfügung stehen.

Wichtig für den Bestandnachweis

Zum anderen dient eine Systemdokumentation dem Bestandsnachweis. Werden alle Systeme erfasst, kann aus der Systemdokumentation das Inventarverzeichnis generiert werden. Das Inventarverzeichnis dokumentiert beispielsweise, welche IT-Geräte eingesetzt werden, in welchen Räumlichkeiten sie stehen und welche Programme auf ihnen installiert sind.

Dies ist manuell natürlich nur bis zu einer gewissen Netzwerkgröße möglich. Sinnvoll ist der Einsatz einer Datenbankanwendung zur Verwaltung der Systemkomponenten. Diese ermöglicht dann unterschiedliche Sichten auf die Daten. Aber auch für kleine Unternehmen ist der Einsatz einer Software bei der Erstellung der Systemdokumentation durchaus sinnvoll (siehe Abschnitt 4.3.4).

hinweis

Die nachstehend vorgestellte Strukturierung von Systemakten orientiert sich wesentlich am IT-Grundschutzmodell des BSI. Dieses bietet den Vorteil, dass die dokumentierten Systeme vielfach direkt den IT-Grundschutzbausteinen zugeordnet werden können. Die Bausteine der IT-Grundschutzkataloge enthalten jeweils eine Kurzbeschreibung für die betrachteten Komponenten, Vorgehensweisen sowie einen Überblick über die Gefährdungslage und die Maßnahmenempfehlungen des BSI.

4.2.1 Strukturierung der Systemakten

Die Schwierigkeit bei der Erstellung der Dokumentation für den IT-Betrieb besteht in der Gratwanderung, möglichst alle Systeme und Prozesse zu dokumentieren und sinnvoll einzuordnen, und andererseits die Dokumentation in nicht zu viele Ebenen aufzuteilen, da ansonsten die Übersichtlichkeit, die eigentlich erreicht werden soll, verloren geht.

Für die Systemdokumentation hat sich eine Unterteilung der Systemakten in die nachstehend gezeigten vier Gruppen als sinnvoll erwiesen:

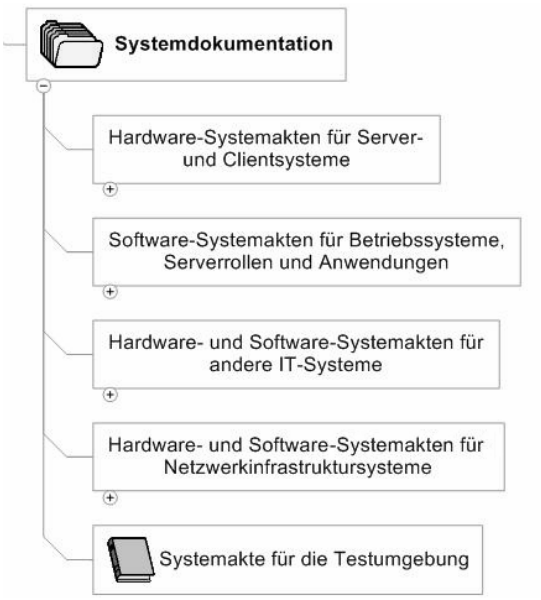


Abbildung 4.2: Systemakten können in vier Gruppen unterteilt werden.

Systemakte Testumgebung

Gerne vergessen wird die Dokumentation der Testumgebung. Für diese sollte eine gesonderte Systemakte geführt werden. Abhängig von der Größe der Testumgebung, kann auch eine weitere Unterteilung in Systemakten für die Hardware- und die Softwarekomponenten sinnvoll sein.

Welche Systemakten den einzelnen Gruppen zuzuordnen sind, zeigen die folgenden Auflistungen. Diese nennen jeweils die wichtigsten zu dokumentierenden Systeme. Ob weitere zu dokumentieren sind, ist von der Systemumgebung des Unternehmens abhängig.

4.2.1.1 Systemakten für Server- und Clientsysteme

In diese Gruppe können die Systemakten für die Server und für die Clientrechner eingeordnet werden. Sinnvollerweise ist für jeden Server eine gesonderte Systemakte anzulegen. Dabei spielt es keine Rolle, ob es sich um einen Windows-, UNIX- oder Netware-Server handelt.

Rechner möglichst gruppieren

Für die Clientrechner ist es in den meisten Umgebungen kaum sinnvoll, für jeden einzelnen Rechner eine Systemakte zu führen. In vielen Unternehmen werden Standard-Clientsysteme verwendet. In diesem Fall genügt es, eine Systemakte für den oder die Standard-Clientsysteme zu führen, was die Dokumentation deutlich vereinfacht. Andernfalls sollte versucht werden, die Clientrechner zu Gruppen zusammenzufassen und diese in einer einzigen Systemakte zu dokumentieren.

In sehr großen Unternehmen mit mehreren hundert Servern werden häufig auch die Server zu Standard-Serverklassen zusammengefasst. In diesem Fall können natürlich auch die Systemakten für Server zu Klassen zusammengefasst werden. Allerdings ist in diesem Fall darauf zu achten, dass die Verlaufsdokumentation und die Dokumentation der Zuständigkeiten für die einzelnen Server sichergestellt ist. Da dies in derartigen Umgebungen aber ohnehin nur datenbankgestützt möglich ist, stellt dies meist kein Problem dar.

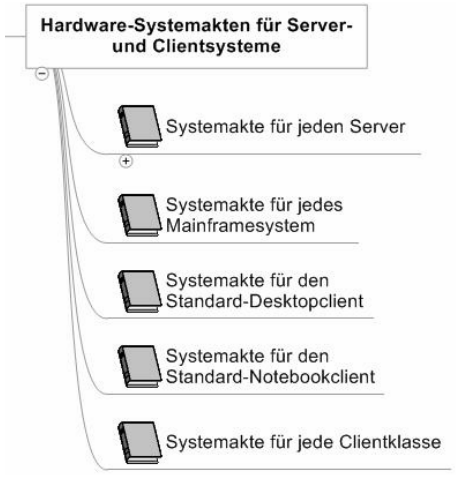


Abbildung 4.3: Erforderliche Systemakten der Gruppe „Server- und Clientsysteme“

4.2.1.2 Systemakten für Betriebssysteme, Serverrollen und Anwendungen

Während die erste Gruppe die Hardware-Systemakten für die Rechner beinhaltet, gehören in die zweite Gruppen alle Systemakten, die Betriebssysteme, Serverrollen oder Anwendungen beschreiben, also die Softwareseite der Server- und Client-Rechner zum Gegenstand haben. Hierzu zählen neben den Betriebssystemen auch Serverrollen und Serverdienste, wie beispielsweise die Zertifikatdienste oder DNS und DHCP. Dieser Gruppe zuzurechnen sind damit auch der Verzeichnisdienst Active Directory und Exchange.

Weiter gehören in diese Gruppe alle IT-Anwendungen, die im Unternehmen genutzt werden (beispielsweise SAP, andere ERP-Systeme sowie Individualsoftware). Sinnvoll kann für diesen Bereich eine Unterteilung in clientbasierte und serverbasierte Dienste und Anwendungen sein.

Bei Bedarf zu ergänzen

Die nachstehenden Auflistungen gelten vorrangig für Windows- bzw. Active Directory-Umgebungen. Sie sind bei einem Einsatz anderer Systeme dementsprechend anzupassen. Auch erheben die Listen keinen Anspruch auf Vollständigkeit und müssen gegebenenfalls bei einem Einsatz weiterer Dienste und Anwendungen ergänzt werden.

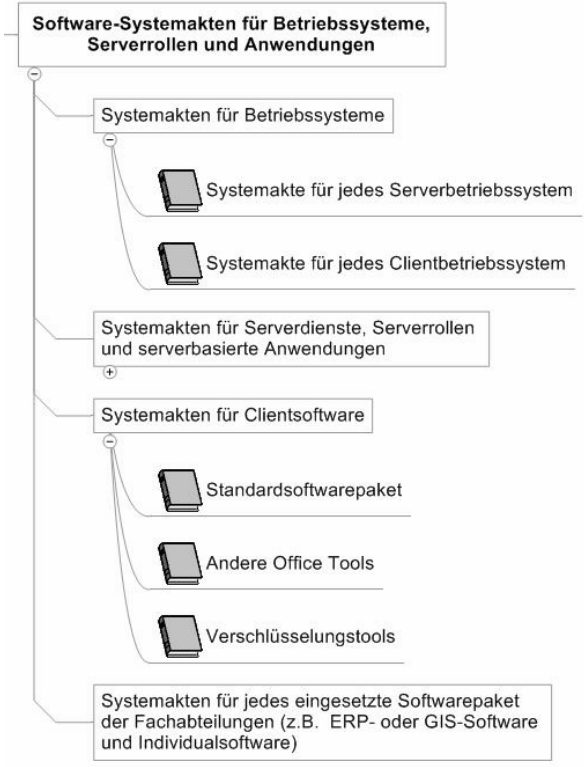


Abbildung 4.4: Erforderliche Systemakten der Gruppe „Betriebssysteme, Serverrollen und Anwendungen"

Aus Gründen der Übersichtlichkeit zeigt die folgende Abbildung gesondert den Bereich der Systemakten für Serverrollen, Serverdienste und serverbasierte Anwendungen.

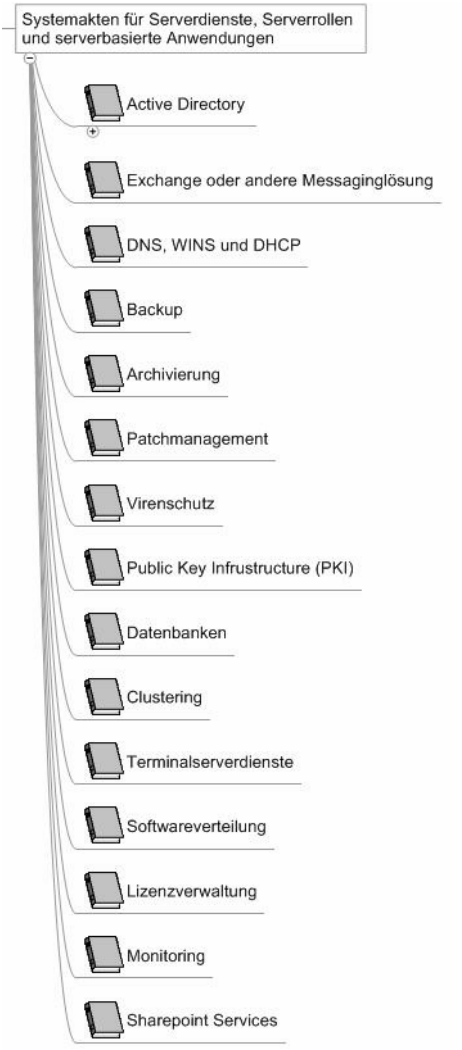


Abbildung 4.5: Systemakten für Serverdienste, Serverrollen und serverbasierte Anwendungen

4.2.1.3 Systemakten für andere IT-Systeme

Neben den Server- und Clientsystemen gibt es eine Reihe weiterer Hardwarekomponenten wie beispielsweise Drucker, die dokumentiert werden sollten. Abhängig von der Systemumgebung sind darüber hinaus gegebenenfalls weitere Geräteklassen zu dokumentieren.

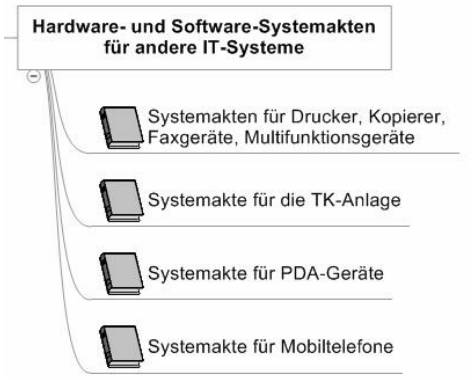


Abbildung 4.6: Erforderliche Systemakten der Gruppe „Andere IT-Systeme"

4.2.1.4 Systemakten für Netzwerkinfrastruktursysteme

Die Gruppe der Netzwerkinfrastruktursysteme betrachtet alle Systeme, die der Vernetzung und der Kommunikation der Einzelkomponenten untereinander dienen. Dies beinhaltet sowohl Netzkomponenten, wie Switches, Router und Gateways, als auch beispielsweise Verteilerschränke und Patchfelder. Zum Inhalt dieser Systemakten gehören zwingend auch Pläne, wie beispielsweise ein Netzwerkplan, der die Vernetzung der IT-Geräte untereinander grafisch darstellt.

Daneben können dieser Gruppe, in Anlehnung an BSI, alle Netzwerktechnologien, wie zum Beispiel WLAN und VPN für die entsprechende Softwareware-Systemakten zu pflegen sind, zugeordnet werden.

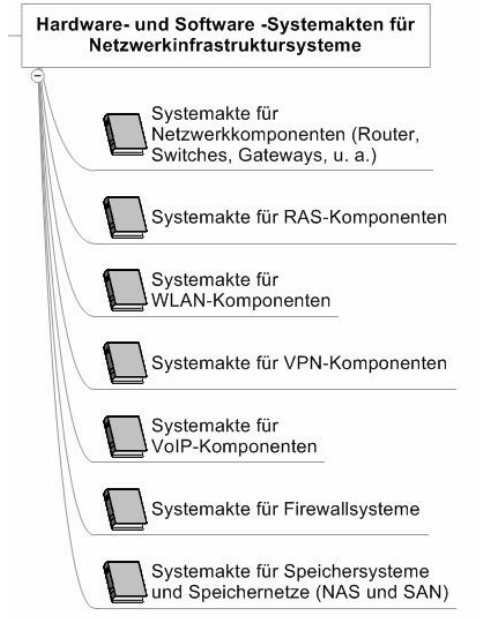


Abbildung 4.7: Erforderliche Systemakten der Gruppe „Netzwerkinfrastrukturssysteme"

4.2.1.5 Weitere zu dokumentierende Systeme

Neben den Systemen, die sich einer der vorstehend genannten Gruppe zuordnen lassen, gibt es eine Reihe weiterer Komponenten, die für den IT-Betrieb von Bedeutung und grundsätzlich zu dokumentieren sind. Hierzu zählen alle baulich-physischen Komponenten: Gebäude, Serverräume, Klimaanlagen usw. Diese Komponenten werden heute unter dem Begriff *Facility*, was in Deutsch etwa *Anlage* bedeutet, zusammengefasst. Zum Facility zählen technische Anlagen und Einrichtungen, Geräte, Gebäude aber auch Infrastruktur, Arbeitsmittel und Energie.

Verantwortung für die Dokumentation klären

Die Dokumentation der Facility-Komponenten obliegt in der Regel jedoch nicht den IT-Organisationseinheiten, sondern ist dem Gebäudemanagement (bzw. dem Facility-Management) zugeordnet. Empfehlenswert ist jedoch, sich von Seiten der IT zu versichern, dass derartige Systeme dokumentiert sind und die Dokumentation auch gepflegt wird. Ein lesender Zugriff auf diese Dokumentation sollte im Bedarfsfall möglich sein. Im IT-Betriebshandbuch ist dann lediglich festzuhalten, dass diese Systeme existieren. Es reicht aus, auf die Dokumentation zu verweisen. Fehlen derartige Dokumente, ist es von Seiten des IT-Betriebs wichtig, diese einzufordern. Möglicherweise ist es auch sinnvoll, die Facility-Komponenten direkt in die IT-Betriebsdokumentation mit aufzunehmen.

Die folgende Liste enthält (ohne Anspruch auf Vollständigkeit) Systeme, deren Dokumentation unter Umständen nicht im Verantwortungsbereich der IT liegt, von dieser jedoch benötigt wird:

Facility-komponenten

- Gebäude
- Rechenzentrum
- Serverräume
- Technikräume
- Schutzschränke
- Besprechung-, Veranstaltungs- und Schulungsräume
- Verkabelung
- Klimaanlagen
- Löschsysteme
- Stromversorgung
- USV-Geräte
- Physische Zugangssysteme

hinweis

Die Dokumentation der vorstehend genannten Systeme ist insbesondere auch für Notfälle wichtig. So ist es zum Beispiel bei einem Ausfall der Stromversorgung oder der Klimaanlage entscheidend, umgehend die richtigen Ansprechpartner zu kontaktieren.

4.2.2 Inhalt der Systemakten

Nachdem festgestellt wurde, für welche Systeme sinnvollerweise Systemakten zu pflegen sind, gilt es im nächsten Schritt darzustellen, welchen Inhalt die Systemakten haben sollten. In der Praxis werden allerdings die Systemakten nicht nur inhaltlich, sondern auch in ihrer Struktur sehr unterschiedlich sein. Schließlich hängt der Inhalt vom zu dokumentierenden System ab. Eine Hardware-Systemakte für einen Domänen-Controller oder ein Cluster-System wird zwangsläufig anders aussehen als eine Software-Systemakte für die Standard-Arbeitsplatzrechner oder die Infrastrukturdienste WINS und DNS. Der nachfolgend genannte inhaltliche Gliederungsvorschlag kann daher nur eine Leitlinie darstellen:

Gliederung einer Systemakte

- Systembeschreibung
  (Aufgabe und Schnittstellen)
- Informationen zum System
  (Hardware, Betriebssystem, Systembeschreibung)
- Konfigurationseinstellungen
  (insbesondere Abweichungen von den Standardeinstellungen)
- Berechtigungen und Berechtigungsmatrix
- Datensicherung
- Informationen zum Hersteller-Support und zu Wartungsverträgen
- Laufende Systemdokumentation
  (Übersicht über durchgeführte Änderungen, z. B. Rollenänderungen, Patches, Installation zusätzlicher Dienste)
- Protokolle und Monitoring-Auswertungen
- Erfasste Stör- und Notfälle
- Pflege und Verwaltung der Systemakte

Systemakten dienen grundsätzlich der Beschreibung des Aufbaus des zu beschreibenden Systems sowie der Konfigurationsbeschreibung. Demzufolge gehören in eine Systemakte auch alle Konzepte (sofern diese nicht Bestandteil der Projektdokumentation sind), Beschreibungen, Verträge und ähnliche Dokumente, die sich speziell auf das System beziehen und nicht durch Rahmendokumente abgedeckt werden.

Dokumentation erforderlicher Berechtigungen

Weiter sind die notwendigen Berechtigungen, die für den Betrieb des Systems erforderlich sind, zu dokumentieren. So sollten beispielsweise die Berechtigungen der Domänen-Admins an einem Datenbankserver in der Systemakte des Datenbankservers dokumentiert werden. Ziel ist, feststellen zu können, in welcher Gruppe ein Mitarbeiter Mitglied sein muss, damit er beispielsweise den Datenbankserver verwalten kann. Bei den Gruppen kann es sich sowohl um Active Directory-Sicherheitsgruppen als auch um systemspezifische Gruppen handeln.

Nicht gemeint sind damit die grundsätzlichen Befugnisse und notwendigen Kompetenzen der Rolle des Datenbankadministrators, die im Rollenkonzept (siehe Abschnitt 3.2.7) festgelegt werden. Während nämlich die Rollen die organisatorische Zuordnung darstellen, müssen in den Systemakten die systemtechnischen Berechtigungen festgelegt werden.

Berechtigungsmatrix

Eine gute Möglichkeit zur Dokumentation derartiger Berechtigungen bietet eine Berechtigungsmatrix. In dieser kann tabellarisch eine Zuordnung von Aktivitäten und Aufgaben bzw. von Berechtigungen zu Gruppen erfolgen. Ein Beispiel für eine solche Berechtigungsmatrix finden Sie in Abschnitt 8.3. Diese zeigt beispielhaft einige administrative Tätigkeiten aus dem Bereich der DHCP-Server-Verwaltung auf und definiert, welche Gruppe zur Durchführung der jeweiligen Tätigkeit berechtigt ist. In Einzelfällen kann es sinnvoll sein, für ein einzelnes Systemobjekt die Berechtigungen zu spezifizieren. Ein weiteres Beispiel für eine differenziertere Berechtigungsmatrix ist im selben Kapitel zu finden.

4.2.2.1 Pflege der Verlaufsdokumentation

Neben der Zustandsbeschreibung nimmt die laufende Dokumentation einen hohen Stellenwert beim Führen der Systemakte ein. So gehören regelmäßige Protokolle über Systempflegearbeiten genauso in die Systemakte wie durchgeführte Konfigurationsänderungen oder Änderungen in der Verantwortlichkeit. Alle Änderungen, die an dem betreffenden System vorgenommen werden, sind unverzüglich schriftlich in der Systemakte festzuhalten. Wichtig ist auch die Dokumentation möglicher Störungen des betreffenden Systems, allein aus Gründen der Nachvollziehbarkeit. Durch deren Erfassung (zum Beispiel durch Hardware-Probleme) wird es später außerdem möglich, eventuelle zukünftige Störungen und Probleme mit dem System sowie Trends zu erkennen.

Sinnvoll ist in diesem Zusammenhang die Pflege einer *Berechtigungshistorie*. Beispielsweise sollten in der Systemakte für ein Datenbanksystem mit einer eigenen Benutzerverwaltung Änderungen an den systemspezifischen Gruppen dokumentiert werden. Dies kann insbesondere in größeren Umgebungen kaum manuell erfolgen, sondern beispielsweise durch die Sicherung entsprechender Protokolldateien. Aufgabe einer Berechtigungshistorie ist es dabei, beispielsweise gegenüber der internen Revision die Frage beantworten zu können, wer zu einem bestimmten Zeitpunkt administrative Rechte auf einem System hatte.

Dokumentation des Lifecycle

Systemakten begleiten also das System während seiner gesamten Einsatzdauer, das heißt, sie dokumentieren den gesamten Lifecycle eines Systems. Alle Änderungen sollten so viel wie möglich automatisiert dokumentiert werden, damit es nicht dem Administrator überlassen bleibt, ob er dokumentiert oder nicht. Um sicherzustellen, dass die Systemakten regelmäßig gepflegt werden, sollte dies in den entsprechenden Prozessen verankert werden. Außerdem sollte für jede Systemakte ein dafür Verantwortlicher benannt und namentlich in der Systemakte genannt werden. In der Regel wird dies der Systemverantwortliche sein.

Wichtig sind derartige Informationen auch für den Notfall. Denn im Falle einer Notfallwiederherstellung stellt die jeweilige Systemakte die für den Wiederaufbau des Systems notwendigen Informationen bereit. Daher ist die Aktualität der Akte eine zwingende Forderung. Wurde also beispielsweise der Verantwortliche gewechselt, sollte dies unbedingt in der Systemakte vermerkt werden.

4.2.2.2 Wichtige Abgrenzungen

In der Praxis nicht immer einfach voneinander abzugrenzen, sind die Inhalte der Hardware-Systemakten für die Server- und die Clientrechner von den Software-Systemakten für die Serverdienste und die Anwendungen. Warum erfolgt dann überhaupt diese Unterscheidung?

Betrachtet man einen einzelnen Server, der dediziert für die Bereitstellung einer Anwendung (z. B. als Faxserver) eingesetzt wird, ist eine Trennung zwischen Serverhardware und Betriebssystem sowie den installierten Anwendungen nicht zwingend erforderlich. In diesem Fall könnte die Beschreibung aller Komponenten auch problemlos in einer Systemakte erfolgen.

Beispiel Exchange

Anders verhält es sich mit Anwendungen, die auf unterschiedlichen Rechnern gehostet werden können, wie dies typischerweise bei Exchange der Fall ist. Hier nehmen in der Regel verschiedene Server die unterschiedlichen Exchange-Serverrollen wahr wie

- Backend-Server zur Verwaltung der Datenbanken,
- Server zur Verwaltung der öffentlichen Ordner und
- Frontend-Server, die beispielsweise OWA-Zugriff für die Anwender zur Verfügung stellen.

Um eine hohe Ausfallsicherheit zu erzielen, werden die Exchange-Backup-Server meist in einem Cluster eingesetzt und sind in die SAN-Infrastruktur (SAN = Storage Area Network) eingebunden. Nicht zu vergessen sind die Administrationskonsolen zur Verwaltung von Exchange, die auch auf Arbeitsplatzrechnern installiert werden können.

Das kleine Beispiel zeigt, dass es in modernen Systemumgebungen nur noch selten eine Eins-zu-Eins-Zuordnung zwischen Servern und Anwendungen gibt. Auch der Active Directory-Verzeichnisdienst selbst liefert hierfür ein gutes Beispiel.

Empfohlene Vorgehensweise

Aus diesem Grund ist eine gesonderte Betrachtung des Servers und der Infrastrukturdienste bzw. der Serverdienste und -anwendungen in getrennten Systemakten erforderlich. Eine sinnvolle Vorgehensweise könnte hier folgendermaßen aussehen:

Die Hardware-Systemakten für die Server enthalten alle serverspezifischen Hardwareinformationen und benennen die Verantwortlichkeiten. Das installierte Betriebssystem, installierte Anwendungen und die Rolle, die der Server in Active Directory innehat, werden hier lediglich benannt. Die Konfiguration der installierten Softwarekomponenten ist jedoch nicht Gegenstand dieser Systemakte. Diese ist der Systemakte für die betreffende Anwendung zu entnehmen.

Beispielsweise ist in der Hardware-Systemakte für den Server zu vermerken, dass es sich um einen Frontend-Server für Exchange handelt und auf die entsprechende Systemakte für Exchange zu verweisen, die wiederum alle relevanten Informationen zur Exchange-Konfiguration enthält.

Keine Anleitungen zu Installation oder Administration

Weiter ist eine klare Trennung zwischen den Systemakten und den Anleitungen zur Installation oder Administration der installierten Komponenten oder für deren Wiederherstellung bei einem Datenverlust sinnvoll. Hierbei handelt es sich um Implementierungs- und Administrationsprozesse, die im Rahmen der jeweiligen Prozessdokumentation zu beschreiben sind. Die Systemdokumentation sollte ausschließlich Bestandsdaten und keine Prozessbeschreibungen beinhalten.

Eine solche Unterscheidung ist vor allem auch in Umgebungen sinnvoll, in denen die Installation mittels Softwareverteilungsverfahren automatisiert erfolgt. Für die Installation eines Standard-Clients wird es in diesen Fällen ein entsprechendes Installationspaket geben. Dieses Installationspaket einschließlich der Konfiguration muss in einer eigenen Systemakte beschrieben sein. Eine Installationsanleitung ist in diesem Fall ohnehin nicht erforderlich.

Die nachstehend gezeigte Gliederung zeigt exemplarisch den möglichen inhaltlichen Aufbau einer Hardware-Systemakte für Server:

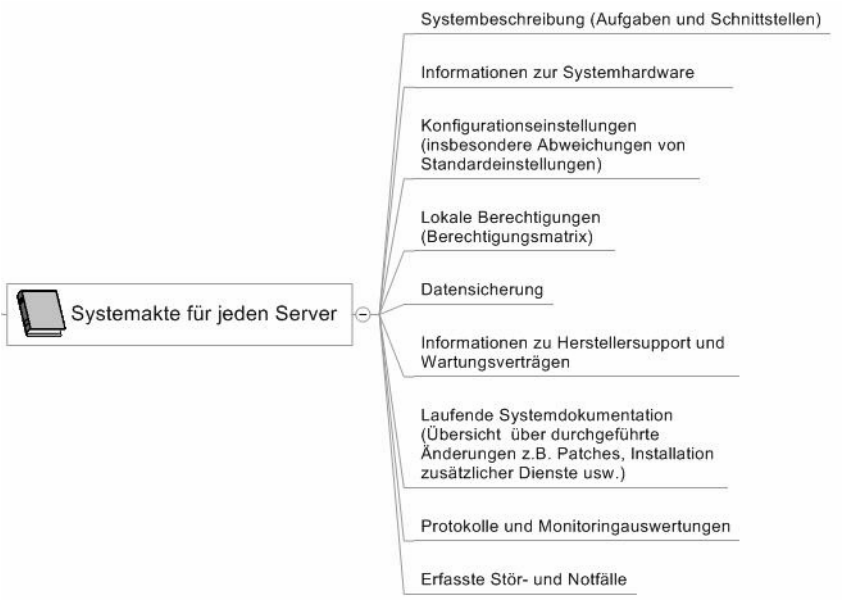


Abbildung 4.8: Exemplarische Gliederung einer Hardware-Systemakte für Server

hinweis

Betrachtet wird an dieser Stelle ausschließlich der inhaltliche (Haupt-)Teil der Systemakten. Informationen zum formalen Aufbau von Dokumenten finden Sie in Abschnitt 7.1.2.

Eine Software-Systemakte für Active Directory könnte hingegen folgendermaßen aufgebaut sein:

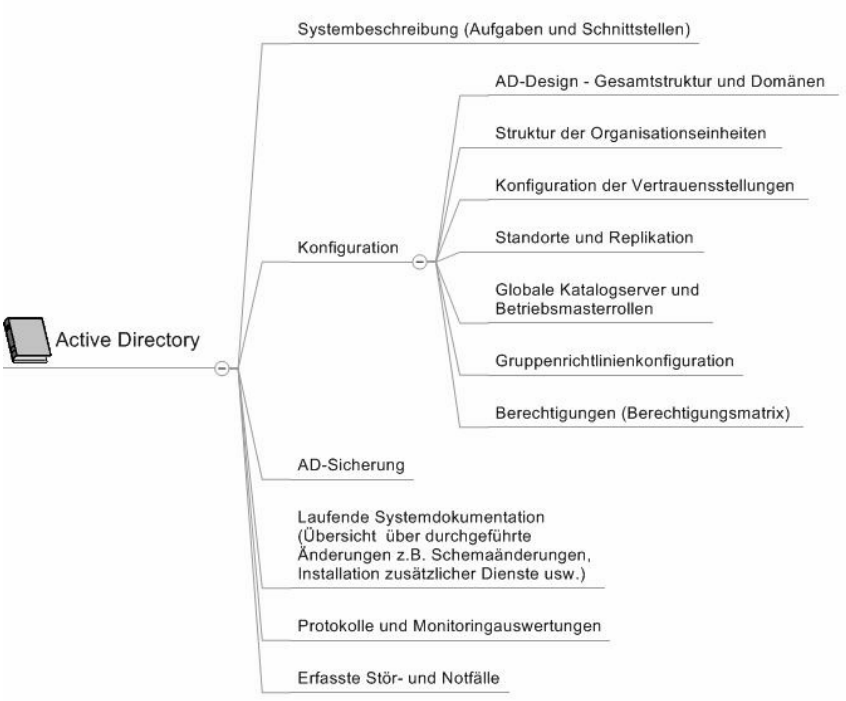


Abbildung 4.9: Exemplarische Gliederung einer Software-Systemakte am Beispiel Active Directory

cd-rom

Eine Musterdokumentation für eine Hardware-Systemakte, die auch als Vorlage für die eigene Dokumentation verwendet werden kann, finden Sie sowohl in Abschnitt 8.4 als auch auf der beigefügten CD-ROM. Die Muster-Systemakte wurde mit dem Tool DocuSnap erstellt, das im anschließenden Kapitel vorgestellt wird.

4.2.2.3 Zusammenspiel zwischen Bestandsdatenbank und Dokumentation

Wie bereits beschrieben, ist die manuelle Pflege der Systemdokumentation ab einer bestimmten Netzwerkgröße nicht mehr nur aufwendig, sondern schlicht nicht mehr handhabbar. Zur Lösung dieses Problems stehen eine ganze Reihe von Inventarisierungstools für jede Netzwerkgröße und für jedes Budget zur Verfügung, mit denen sich zumindest die Hardware-Systemakten automatisiert erstellen lassen.

Alle Lösungen verfügen über Funktionen, mit denen regelmäßig die Rechner eines Netzwerks gescannt und ausgewertet werden können. Erfasst wird hierbei unter anderem, auf welchem Betriebssystem die Rechner laufen, welche Hard- und Software vorhanden ist, und wie die Registry-Werte aussehen. Daneben erkennen die meisten Programme Netzwerkgeräte wie etwa Switches oder Router. Und auch sicherheitsrelevante Informationen wie beispielsweise Gruppen und Gruppenmitgliedschaften, Freigaben und deren Berechtigungen sowie Einstellungen der Sicherheitsrichtlinien liefern die meisten dieser Tools. Ein Beispiel für eine derartige Inventarisierungssoftware und ihre Dokumentationsmöglichkeiten können Sie dem Abschnitt 4.2.3 entnehmen.

ITIL und CMDB sind untrennbar

Ein Begriff, der im Zusammenhang mit Inventarisierung immer wieder auftaucht, lautet: *CMDB – Configuration Management Data Base*. Datenbanken, die lange Zeit unter dem Titel „zentrales IT-Repository" oder „Inventardatenbank" geführt wurden, werden durch die Verbreitung des ITIL-Standards heute als CMDB bezeichnet.

Allerdings gehen die Auffassungen, was eine CMDB ist und was sie enthalten sollte, weit auseinander. Gemäß ITIL handelt es sich bei der CMDB um eine Datenbank, über die Konfigurationsinformationen zu Personen, Hardware, Software, Verfahren, Verträgen und Ähnliches, sogenannte *Configuration Items (CIs)*, sowie ihre Beziehungen zueinander und Historie abgerufen werden können. ITIL sieht die grundsätzliche Aufgabe einer CMDB darin, alle Service-Prozesse zu unterstützen. Am engsten ist sie jedoch mit den Prozessen des Change Managements und des Konfigurationsmanagements verbunden, in deren Kontext sie in der Regel auch bereitgestellt wird.

Welche Konfigurationsinformationen eine CMDB enthalten kann oder sollte, ist jedoch nicht geregelt. Möglich ist unter anderem die Verwaltung der folgenden Configuration Items:

- Stammdaten der Mitarbeiter (Person, Ort, Abteilung)
- Kunden, Lieferanten (Kostenstelle, Kontaktdaten)
- IT-Systeme (PC, Server, Drucker, Netzwerkkomponenten usw.)
- Konfigurationsinformationen (IP- und MAC-Adressen, Hostnamen, Netzwerkmasken/-ranges, VLAN, WLAN usw.)
- Facility-Komponenten (Technikräume, Klimaanlagen, Löschsysteme, Verkablungen usw.)
- Leistungskomonenten (Kosten, Budget, Kontierung, AfA-Verrechung usw.)
- Lizenzen
- Berechtigungen
- Verträge (Vertragspartner, Laufzeiten, Konditionen, Service Level Agreements usw.)

Beziehungen zwischen CIs sind darstellbar

Diese „bunte“ Liste, die keineswegs vollständig ist, zeigt, dass eine CMDB weit über eine reine Inventardatenbank zur Systemverwaltung hinausgehen kann. In der Praxis bezieht eine CMDB ihre Daten aus einer ganzen Reihe von Anwendungen und Systemen, die ohnehin zur Unterstützung der operativen Prozesse eingesetzt werden – wie beispielsweise Software-Verteilungstools. Entscheidend ist hierbei aber, dass in einer CMDB die verschiedenen Konfigurationsdaten in Beziehung zueinander gesetzt werden. Damit kann eine CMDB zielgruppengenaue Informationen liefern. Beispielsweise alle Daten, die der Service Desk-Mitarbeiter bei der Erfassung und Lösung einer Störungsanfrage benötigt, oder alle Wartungsverträge für ausgewählte Server.

IT-unterstützte CMDB

Dabei ist die Integrität der Daten in der CMDB unabdingbar. Die Möglichkeiten einer CMDB sind nur dann nutzbar, wenn die Informationen widerspruchsfrei, vollständig und aktuell sind. Diese Anforderungen sind selbstverständlich nicht ohne entsprechende Softwareunterstützung möglich – auch wenn ITIL lediglich den Inhalt der CMDB beschreibt, und nicht, wie diese Informationen zu erfassen, pflegen und zu verwalten sind.

Entsprechend der zunehmenden Forderung nach einer umfassenden, aber einfach zu pflegenden und in der Detailtiefe anpassbaren Dokumentation für den IT-Betrieb stehen heute zahlreiche Programme zum Aufbau und zur Pflege einer CMDB zur Verfügung. Dabei reicht das Angebot von kostenlosen Tools (beispielsweise *i-doit* [IDOIT] und *rimacon* [RIMACON]) bis hin zu komplexen Lösungen, die auch die Verwaltung von Prozessen und Workflows unterstützen.

Da zum Thema CDMB und entsprechender Tools sowohl im Internet als auch in zahlreichen Büchern alle erforderlichen Informationen zu finden sind, soll an dieser Stelle das Thema nicht näher betrachtet werden. Selbstverständlich ist aber die Frage, ob eine CMDB vorhanden oder deren Einführung im Unternehmen geplant ist, für den Aufbau der IT-Dokumentation von entscheidender Bedeutung und dementsprechend zu berücksichtigen.

4.2.3 Toolunterstützte Inventarisierung am Beispiel von DocuSnap

Wie bereits in den vorstehenden Ausführungen betont wurde, ist die Pflege der Systemdokumentation ohne Einsatz entsprechender Programme kaum zu leisten und darüber hinaus sehr fehleranfällig. Glücklicherweise bietet der Markt eine ganze Reihe entsprechender Lösungen an. Es würde aber den Rahmen dieses Buches sprengen, eine Bewertung und Abgrenzung verschiedener Inventarisierungstools anzubieten, zumal ein solcher Vergleich wohl nur für kurze Zeit einen Anspruch auf Aktualität hätte.

4.2.3.1 Einsatzmöglichkeiten und Arbeitsweise von DocuSnap

Um trotzdem die Möglichkeiten aufzuzeigen, die eine automatisierte Inventarisierung im Rahmen der IT-Dokumentation bieten kann, haben sich die Autoren dieses Buches entschieden, exemplarisch eine Inventarisierungsanwendung vorzustellen.

Die Wahl ist dabei auf das Programm *DocuSnap* des Herstellers *itelio GmbH* gefallen. DocuSnap ist vorrangig eine Software zur Inventarisierung, die die Erfassung von Windows- und Linux-Systemen und die Dokumentation von Active Directory, DHCP-und DNS-Servern, Exchange 2003-Umgebungen, SNMP-fähigen Geräten und Ähnlichem ermöglicht. Dies schließt auch eine Analyse der effektiven Freigabe- und der NTFS-Rechte und sowie eine Lizenzverwaltung mit ein.

Schwerpunkt Dokumentation

Als Analyse- und Dokumentationstool legt DocuSnap – und das ist für die Auswahl entscheidend gewesen – den Schwerpunkt auf die Dokumentation. Im Gegensatz zu den meisten Inventarisierungstools, die ausschließlich die Erstellung programminterner Berichte ermöglichen, unterstützt DocuSnap unter anderem die Ausgabe der Informationen mit Microsoft Word, Microsoft Excel und Crystal Reports sowie die Generierung von Übersichtsplänen für Netzwerksegmente inklusive aller Systeme, der logischen Active Directory-Struktur und der Active Directory-Standorte in Microsoft Visio. Zusätzlich können alle Ergebnisse als vollständig verlinktes HTML-Dokument bereitgestellt und damit sehr gut in die IT-Dokumentation eingebunden werden.

Wichtig ist hierbei, dass DocuSnap agentenfrei arbeitet. Das heißt, es muss keinerlei Software auf den auszulesenden Systemen installiert werden, und diese müssen sich nicht am DocuSnap-Rechner anmelden. Auch erfolgen durch DocuSnap, mit Ausnahme der Eintragungen in die Inventarisierungsdatenbank, ausschließlich lesende und niemals schreibende Zugriffe auf die gescannten Systeme.

Darüber hinaus ist DocuSnap beliebig skalierbar, da die Daten sowohl in einer Access- als auch in einer SQL-Datenbank abgespeichert werden können. Aufgrund einer Preisstaffelung und des damit relativ niedrigen Einstiegspreises ist DocuSnap auch für den Einsatz in kleineren Netzwerkumgebungen interessant. Dabei wird DocuSnap als Basispaket erworben. Diesem können zu einem beliebigen Zeitpunkt nachträglich die folgenden Module hinzugefügt werden: Exchange Server, SQL Server, DHCP-Server, DNS-Server, Linux-Systeme, Lizenzverwaltung und Rechteanalyse.

hinweis

Nähere Informationen zu Systemanforderungen, Bezugsmöglichkeiten und Preisen der aktuellen Version können Sie dem Steckbrief zu DocuSnap in Anhang D.3 entnehmen.

4.2.3.2 Dateninventarisierung

Nach der Installation von DocuSnap, dem Einspielen der Lizenzdatei und der Anlage eines neuen Firmenobjekts kann die erste Datenerfassung erfolgen. Die zu erfassenden Windows-Clients können Mitglied in Active Directory, einer NT-Domäne oder einer Arbeitsgruppe sein. Sind in einer Firma mehrere Verzeichnisbäume oder Arbeitsgruppen vorhanden, müssen diese getrennt eingelesen werden. Hierbei müssen jedes Mal entsprechende Anmeldedaten für den RPC-Zugriff angegeben werden, welche das Programm sofort verifiziert.

Offline-Datenerfassung

Für Rechner, die überwiegend vom Netz getrennt betrieben werden, ermöglicht DocuSnap das Skript-gesteuerte Erfassen der Daten. Die erzeugte XML-Datei lässt sich dann importieren. Auch in Netzwerken, die durch Firewalls segmentiert sind, bietet sich diese Methode zur Offline-Erfassung an, um nicht den kritischen Port 135 sowie ICMP öffnen zu müssen.

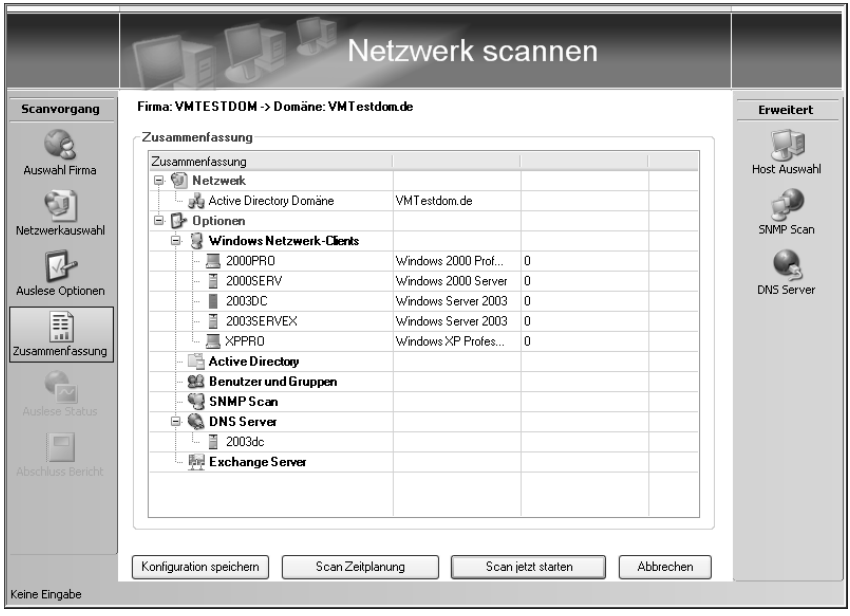


Abbildung 4.10: Durchführung eines Scans zur Dateninventarisierung

Die Ergebnisse der System- und Netzwerkerfassung zeigt DocuSnap im eigenen Datenexplorer an. Hier können zahlreiche Informationen zu den untersuchten Systemen und auch einige standardmäßig erzeugte Berichte ausgewertet werden.

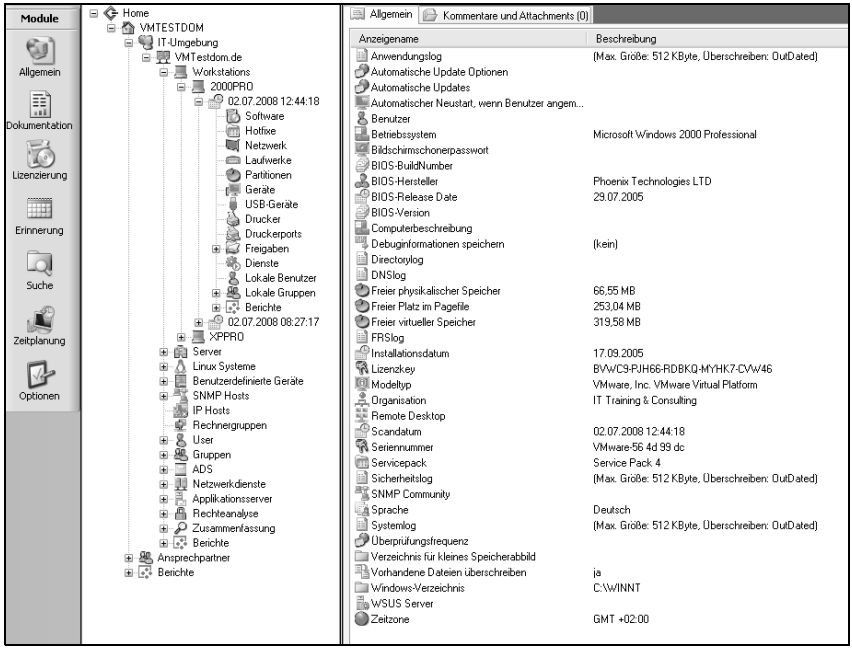


Abbildung 4.11: Analyse der gesammelten Systeminformationen im DocuSnap-Datenexplorer

Dokumentation mit DocuSnap erzeugen

Die Stärke von DocuSnap aus Sicht des Buches liegt aber in den vielfältigen Exportmöglichkeiten für die Dokumentation. Direkt im Anschluss an die Inventarisierung oder auch zu jedem späteren Zeitpunkt kann eine umfassende Dokumentation erzeugt werden. Möglich sind die Erstellung von Netzwerkplänen (optional mit Netzwerksegmenten und einer Gruppierung der Workstations) sowie die Ausgabe von Übersichten über Computer, Software, Betriebssystem, Benutzer und Gruppen. Zudem können Datenblätter für die Server, Workstations, SNMP-Geräte und die Verteilung der FSMO-Rollen erzeugt und Active Directory-Übersichten erstellt werden. Sofern das entsprechende Modul erworben wurde, können auch DHCP-, DNS-, Exchange Server- und SQL Server-Pläne erstellt werden. Alle Dokumente speichert DocuSnap in einem wählbaren Speicherpfad ab.

Im Hinblick auf die im Rahmen der IT-Dokumentation zu pflegenden Hardware-Systemakten verdienen die von DocuSnap generierten Datenblätter besondere Beachtung. DocuSnap erstellt für jeden gescannten Rechner ein mehrseitiges Dokument im Word- und im HTML-Format mit allen relevanten Systeminformationen, sodass damit eine automatische Erstellung der Hardware-Systemakten möglich wird.

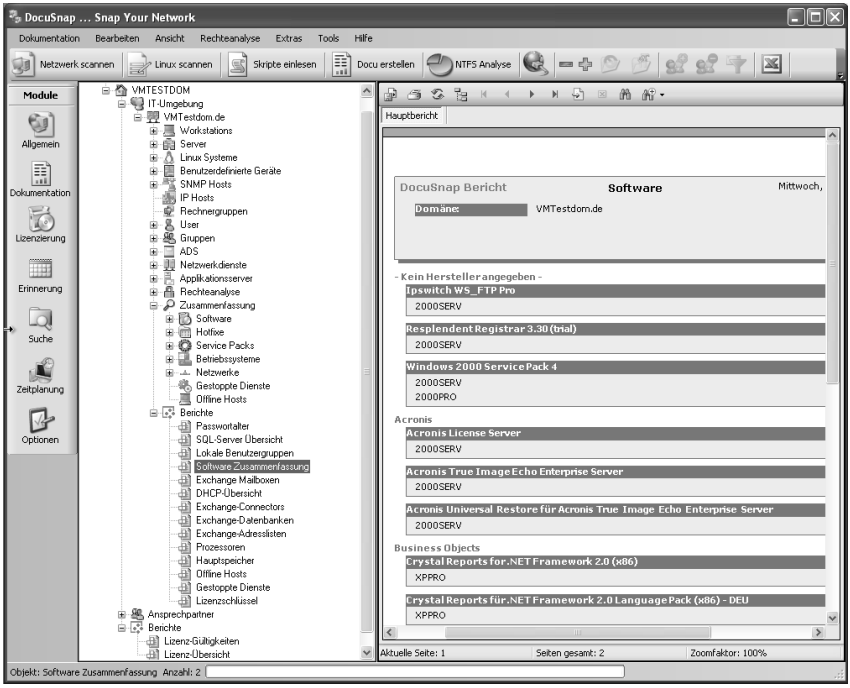


Abbildung 4.12: DocuSnap kann eine umfassende Dokumentation erstellen.

Serverdatenblatt			
Stand:	02.07.2008	Objektname:	2000SERV.VMTestdom.de
Version:	1.0	Autor:	
Firma:	VMTESTDOM		
Dateiname:	db-2000serv.htm		

Datenblatt: Server

Servername	**2000SERV**
IP-Adresse	Ethernetadapter der AMD-PCNET-Familie DHCP: deaktiviert IP: 10.50.10.51 Subnetz: 255.0.0.0 Gateway: DNS-Server: 10.50.10.50, Prim. WINS: 127.0.0.0 Sek. WINS: 127.0.0.0 MAC-Adresse: 00-0C-29-E0-42-F1
Standort	
Installationszeitpunkt	11.07.2004
Ansprechpartner beim Kunden, Telefonnr.	
Hersteller	VMware, Inc. VMware Virtual Platform

Abbildung 4.13: Ausschnitt aus einem mit DocuSnap erzeugten Server-Datenblatt

cd-rom

In Abschnitt 8.4 und auf der beigefügten CD-ROM finden Sie das komplette Server-Datenblatt. Die automatisch generierten Informationen dienen gleichzeitig als Anhaltspunkt für den erforderlichen Inhalt einer Hardware-Systemakte.

Wie bereits ausgeführt, genügt es nicht, einmalig den Zustand eines Systems zu erfassen. Vielmehr muss nicht nur die Dokumentation laufend gepflegt und aktualisiert werden, sondern es ist darüber hinaus erforderlich, den jeweils aktuellen Zustand mit einem älteren Zustand abgleichen zu können, was bei manueller Pflege einen hohen Aufwand bedeutet.

Automatische Versionshistorie

DocuSnap bietet mit den beiden Funktionen *Scanhistorie* und *Versionsvergleich* auch hierbei Unterstützung, da jeder Scan für jedes System unter dem entsprechenden Datum und der Uhrzeit gespeichert wird. Standardmäßig archiviert DocuSnap die letzten fünf Scanergebnisse; dieser Wert lässt sich allerdings ändern.

Ergänzende Informationen

Aber nicht alle Informationen können automatisiert dokumentiert werden. Wie in früheren Abschnitten ausgeführt wurde, ist beispielsweise die Erfassung möglicher Störungen (zum Beispiel Hardware-Probleme) des betreffenden Systems wichtig. Derartige Informationen erleichtern eine spätere Nachvollziehbarkeit und bieten Hinweise im Hinblick auf mögliche, zukünftige Störungen und Probleme mit dem System. Auch Informationen zum Hersteller-Support und Wartungsverträge müssen nach wie vor manuell erfasst werden.

Diese Anforderungen unterstützt DocuSnap mit der Möglichkeit, Kommentare und Datei-Anhänge (Attachments) anzufügen, sodass eine vollständige Systemdokumentation in DocuSnap möglich ist. Die Kommentare wiederum können (frei definierbaren) Klassen zugeordnet und mit Hilfe benutzerdefinierter Crystal Reports dokumentiert werden. Alternativ können die Systemakten als normale Office-Dokumente erstellt werden, die wiederum Verlinkungen auf die automatisiert erstellten Datenblätter enthalten. Im Einzelfall muss das gewünschte Ausgabeformat unter Berücksichtigung der verfügbaren Ausgabeschnittstellen (HTML-Dokumentation, SharePoint Server usw.) gewählt werden.

Dokumentation in HTML

Hervorzuheben ist die Möglichkeit, die komplette Dokumentation als verlinkte HTML-Dokumentation bereitzustellen. Damit ist es beispielsweise möglich, Mitarbeitern Zugriff auf die Systemdokumentation zu geben, ohne dass diese DocuSnap installiert haben müssen.

cd-rom

Ein Beispiel für eine mit DocuSnap erstellte und in HTML konvertierte Dokumentation befindet sich auf der CD-ROM. Für eine vollständige Anzeige der Beispiele wird wegen der integrierten ActiveX-Komponenten der Internet Explorer benötigt. Die Anzeige mit anderen Browsern ist nur eingeschränkt möglich.

4.2.3.3 Rechteanalyse und Lizenzverwaltung

Die Funktionen der beiden optionalen Module *Rechteanalyse* und *Lizenzverwaltung* können ebenfalls für die Systemdokumentation interessant sein.

Rechteanalyse

Die NTFS-Rechteanalyse ist sinnvollerweise aus dem normalen Inventarisierungslauf ausgeklammert. Denn je nach Plattenkapazität und Dateninhalt kann diese recht lange dauern. Sie muss daher nach der Auswahl der zu überprüfenden Systeme separat gestartet werden. Bei der Ermittlung der effektiven Zugriffsberechtigungen werden eventuell geerbte Rechte mit einbezogen..Mit Hilfe graphischer Übersichten und diverser Filtermöglichkeiten kann DocuSnap einen guten Überblick über die Berechtigungssituation – auch für Linux-Systeme – liefern.

Lizenzverwaltung

Eine interessante Funktion verbirgt sich hinter der Lizenzverwaltung. Diese liefert nach einer entsprechenden Erfassung der erforderlichen Daten zu den im Unternehmen eingesetzten Anwendungen Übersichten über Unter- und Überlizenzierungen oder ablaufende Gültigkeiten. Außerdem können Soll-Ist-Abgleiche der installierten Software erstellt und dokumentiert werden. Damit unterstützt DocuSnap auch die Prozesse zur Softwareverwaltung bzw. zur Softwareverteilung.

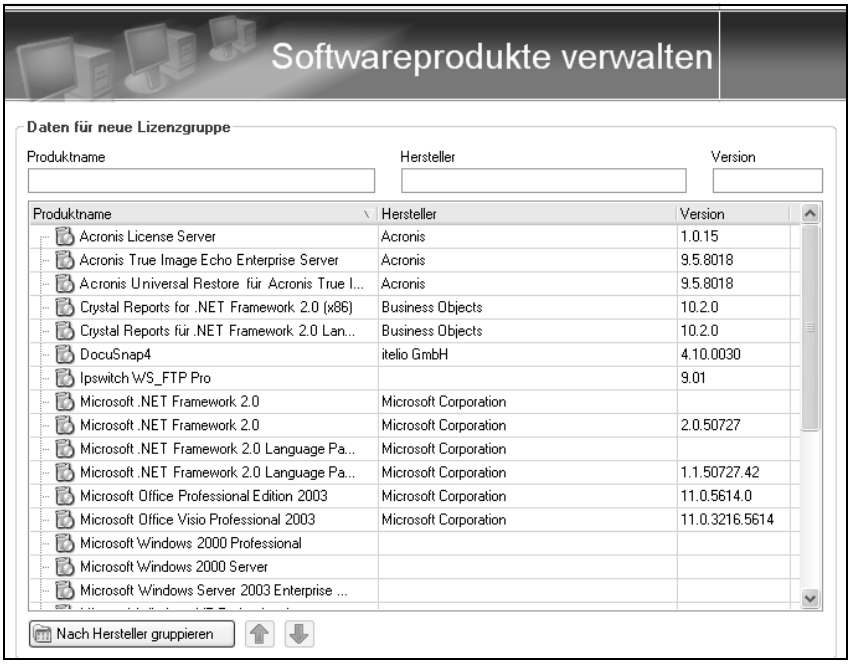


Abbildung 4.14: Ausschnitt aus der Ergebnisanzeige der Softwarelizenzverwaltung

4.2.3.4 Facility-Dokumentation mit FaciPlan

In Abschnitt 4.2.1.5 wurde ausgeführt, dass es aus dem Facility-Bereich eine Reihe von Systemen gibt, deren Inventarisierung und Dokumentation für den IT-Betrieb wichtig ist. Hierzu zählen zum Beispiel Klimaanlagen, Löschsysteme oder Serverräume.

Die Verwaltung der Facility-Komponenten im Rahmen des Facility- oder Gebäudemanagements ist – zumindest in größeren Unternehmen – ohne Softwareunterstützung kaum zu bewältigen. Anwendungen, die dies unterstützen, werden der Gruppe *Computer Aided Facility Management (CAFM)* zugerechnet. Hierbei handelt es in der Regel um Datenbankanwendungen, die eine Facility-Inventarisierung unterstützen.

Nun liegt die Dokumentation der Facility-Komponenten sicherlich nicht im Fokus des vorliegenden Buches. Doch da das im vorstehenden Kapitel vorgestellte Programm DocuSnap eine Schnittstelle zu einer solchen CAFM-Anwendung bietet, ist ein kurzer Blick „über den Tellerrand" sicherlich sinnvoll.

Visio Add-on

Es handelt sich hierbei um das Programm *FaciPlan* der Firma FaciWare GmbH. FaciPlan ermöglicht eine datenbankunterstützte Inventarisierung von Gebäuden und Infrastrukturanlagen. Hierbei steht jedoch nicht die Datenbankverwaltung im Vordergrund, sondern die Erweiterung für Microsoft Visio. Dieses Add-on erweitert die Grafikfähigkeiten von Vision um Funktionen zur Darstellung von Gebäuden und stellt eine grafische Plattform für das Inventarisierungsmanagement bereit. Damit ist FaciPlan in erster Linie ein Werkzeug zur Visualisierung, das Flächen- und Sachdaten miteinander verknüpft.

Die folgende Abbildung zeigt die Arbeitsoberfläche von FaciPlan, also die Visio-Oberfläche mit den Erweiterungen von FaciPlan, zu denen eine ganze Reihe zusätzlicher Shapes, Symbolleisten und entsprechend konfigurierte Vorlagen zählen.

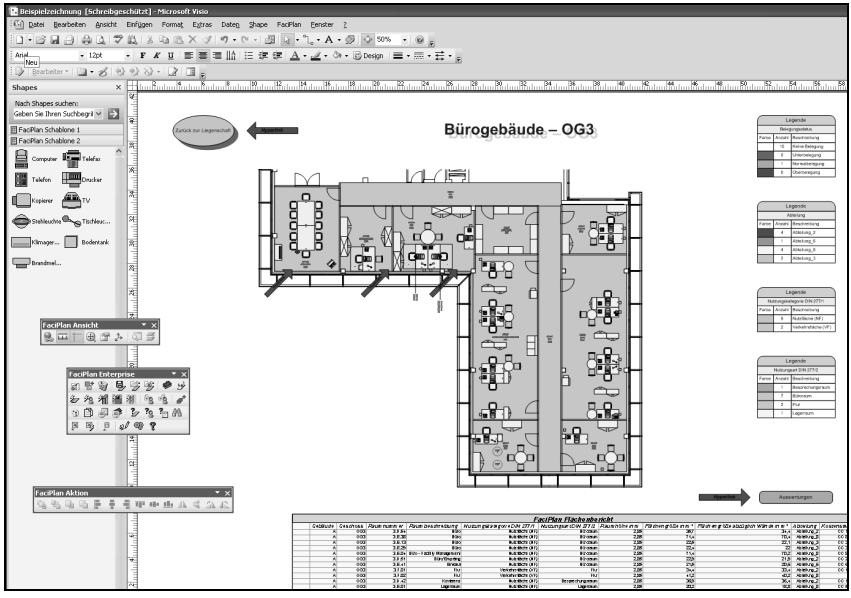


Abbildung 4.15: FaciPlan bindet sich als Add-on in Visio ein.

Schnittstelle zu DocuSnap

Im Hintergrund arbeitet FaciPlan mit einer Access- (oder wahlweise SQL-Datenbank). Zu dieser bietet DocuSnap eine Schnittstelle, mit deren Hilfe es möglich ist, die in DocuSnap automatisiert erfassten Systeme (Rechner, Drucker, Netzwerkgeräte usw.) an FaciPlan zu übergeben, dort mit zusätzlichen Informationen zu verknüpfen und diese wiederum in Form von Gebäude- und Raumplänen zu visualisieren. Die grafischen Ergebnisse und die Auswertungen von FaciPlan können damit eine nützliche Ergänzung der IT-Dokumentation darstellen.

hinweis

Nähere Informationen zu Systemanforderungen, Bezugsmöglichkeiten und Preisen der aktuellen Version entnehmen Sie bitte dem Steckbrief zu FaciPlan in Anhang D.4.

4.3 IT-Prozessdokumentation

Zur Organisation des IT-Betriebs rückt die Prozessorientierung aus mehreren Gründen zunehmend mehr in den Vordergrund. Die IT-Organisationen müssen ein immer breiteres Aufgabenspektrum abdecken – bei gleichzeitig steigender Anforderung an deren Verfügbarkeit. Als Reaktion darauf werden Organisationsmodelle wie ITIL, aber auch Sicherheitsstandards wie der BSI-Grundschutz immer stärker prozessorientiert ausgerichtet. In dieselbe Richtung gehen gesetzliche Normen und Zertifizierungsnormen. Nicht zuletzt erfordert der zunehmende Rationalisierungsdruck eine fortwährende Optimierung der IT-Organisation.

Damit aber rückt auch die Qualität der IT-gestützten Prozesse stärker in den Vordergrund. Ein wesentliches Qualitätsmerkmal und Erfordernis ist dabei die Prozessdokumentation. Das nachstehende Kapitel erläutert, was beim strukturellen Aufbau der Prozessdokumentation zu beachten ist, und liefert anhand exemplarischer Beispiele Anleitungen zur Dokumentation von Prozessen.

4.3.1 Struktur der IT-Prozessdokumentation

Der Nachweis eines wirksamen Qualitätsmanagementsystems ist eine Anforderung, der sich heute jedes Unternehmen stellen muss. Damit die Regelungen für das Qualitätsmanagement nachvollziehbar sind, müssen sie dokumentiert werden. Dabei reicht es aber nicht aus, dass allein der Vorgesetzte diese Regelungen kennt. Und für eine Zertifizierung als Nachweis der Qualitätsorientierung ist eine Qualitätsmanagement-Dokumentation einschließlich einer Prozessdokumentation zwingend vorgeschrieben.

Darüber hinaus ist sie aber auch für das Unternehmen nützlich, damit alle Mitarbeiter auf derselben Grundlage arbeiten und definierte Standards auch umgesetzt werden. Aus juristischer Sicht ist sie sogar dringend angeraten. Im Falle eines schweren Fehlverhaltens eines Mitarbeiters geht der zuständige Geschäfts-/Betriebsleiter das Risiko des Organisationsverschuldens ein und damit die Gefahr, persönlich haftbar gemacht zu werden, sofern es entsprechende Arbeitsanwei-

sungen nicht gegeben hat oder diese dem beschuldigten Mitarbeiter nicht bekannt waren.

Welche Dokumente sollte eine Dokumentation zum Nachweis der Erreichung von Qualitätsstandards beinhalten? Die Norm ISO 9001:2000 (siehe Abschnitt 1.2.2.1) fordert eine Dokumentation, die folgende Teile beinhaltet:

- **Qualitätsmanagement-Handbuch:** Das Qualitätsmanagement-Handbuch (QM-Handbuch) beschreibt verbindlich, wie im Unternehmen Zuständigkeiten, Tätigkeiten, Abläufe, Dokumentation und Verbesserungen als Mittel der Qualitätsmanagement-Planung gehandhabt werden. Inhalt und Aufbau, für das QM-Handbuch sind dabei detailliert in der Norm festgelegt. Aufgrund der wachsenden Bedeutung des Qualitätsmanagements für Unternehmen sind Informationen und Musterdokumentationen zum Thema „Qualitätsmanagement-Handbuch" sowohl in zahlreichen Fachbüchern als auch im Internet zu finden. An dieser Stelle wird daher auf eine detaillierte Betrachtung des QM-Handbuches verzichtet. Weitere Informationen sind unter den beiden nachstehenden Links zu finden [EN ISO1] und [EN ISO2].
- **Dokumentierte Verfahren:** Die Prüfung der Prozessbeschreibungen ist bei einem Audit wesentlicher Bestandteil. Sie dient als Basis für die Beurteilung von Prozessen und somit für die Zertifizierung. Aus der Beurteilung muss hervorgehen, ob die Prozesse geeignet sind, die gesetzten Ziele zu erreichen. ISO 9001:2000 fordert von dem zu zertifizierenden Unternehmen ausdrücklich, dass es „dokumentierte Verfahren" für die folgenden sechs Tätigkeiten haben muss:
  - Lenkung von Dokumenten
  - Lenkung von Aufzeichnungen
  - Internes Audit
  - Lenkung fehlerhafter Produkte
  - Korrekturmaßnahmen
  - Vorbeugungsmaßnahmen
- **Arbeitshilfen:** Zusätzlich zur Dokumentation der Prozesse werden Dokumente benötigt, die die Durchführung und Lenkung der Prozesse unterstützen. Hierbei kann es sich um Arbeitsflussdiagramme, Arbeitsanweisungen in Form von Schritt-für-Schritt-Anleitungen, Formulare, Checklisten und Ähnliches handeln.

Der tatsächliche Aufbau der IT-Prozessdokumentation eines Unternehmens muss sich also zum einen an den Vorgaben des Unternehmens für die Prozessdokumentation und zum anderen an dem Modell und den Methoden ausrichten, nach denen der IT-Betrieb organisiert ist (zum Beispiel ITIL oder MOF). In der Folge ergeben sich daraus unterschiedliche Prozessdokumentationen.

Um im vorliegenden Buch unabhängig von einzelnen Modellen den möglichen Aufbau einer IT-Prozessdokumentation zeigen zu können, wird als Grundlage der Qualitätskreis nach Deming verwendet, der die Basis aller wichtigen Qualitätsansätze und Prozessmodelle darstellt. Diese Vorgehensweise ermöglicht die Darstellung einer allgemeingültigen Struktur ohne die Einschränkung auf ein Modell.

hinweis

Im Zusammenhang mit der Dokumentation von Prozessen stößt man in der Literatur immer wieder auf folgende Begriffe: *Prozessdokumentation, Prozessbeschreibung* und *Verfahrensanweisung* (bzw. *Verfahrensbeschreibung*). Allerdings werden diese sehr uneinheitlich verwendet.

Im vorliegenden Buch wird der Begriff *Prozessbeschreibung* immer dann verwendet, wenn es sich um die Dokumentation des *einzelnen* Prozesses handelt. Die Prozessbeschreibung kann in einem einzigen Dokument zusammengefasst sein, aber auch aus mehreren Einzeldokumenten bestehen.

Die *Prozessdokumentation* hingegen umfasst als Gesamtdokument alle Einzel-Prozessbeschreibungen.

Prozessbeschreibungen und *Verfahrensanweisungen* hingegen beschreiben im Grunde das Gleiche. Was unter der früheren ISO 9001:1994 als Verfahrensanweisung bezeichnet wurde, wird in der aktuellen Norm ISO 9001:2001 als Prozessbeschreibung geführt. Die Prozessbeschreibung kann als visuelle Verfahrensbeschreibung und damit als eine Weiterentwicklung der früher überwiegend textlich gestalteten Verfahrensanweisung betrachtet werden. Allerdings gibt es durchaus einige Unterschiede. Im Gegensatz zur Verfahrensanweisung muss es für einen Prozess immer einen Prozessverantwortlichen geben. Zudem sollten Prozesse immer Kennzahlen enthalten, die eine Überprüfung der Zielereichung des Prozesses ermöglichen.

4.3.1.1 Das PDCA-Modell

Deming-Kreis ist die Basis vieler Standards

Der *Deming-Kreis* (auch als *PDCA-Modell* bezeichnet) beschreibt einen iterativen vierphasigen Prozess. *PDCA* steht hierbei für *Plan-Do-Check-Act*, was im deutschen als „Planen-Ausführen-Überprüfen-Agieren" übersetzt wird.

Der Qualitätskreis wird verwendet, um daraus Darstellungsmodelle für Arbeitsprozesse und den von der ISO-Norm geforderten *kontinuierlichen Verbesserungsprozess (KVP)* abzuleiten. KVP ist die Grundlage aller Qualitätsmanagement-Systeme. Damit wird im Unternehmen eine stetige Verbesserung der Prozesse und Abläufe verfolgt mit dem Ziel, die Effizienz, Kunden- und Mitarbeiterzufriedenheit des Unternehmens zu verbessern. Und auch der ISO-Standard 27001 sowie der BSI-Standard 100-1 basieren auf dem PDCA-Modell.

Und betrachtet man das ITIL-V3-Service-Lebenszyklus-Modell oder das MOF-Prozessmodell von Microsoft [MOF], so ist unschwer zu erkennen, dass auch diesen Modellen der Deming-Kreis zugrunde liegt.

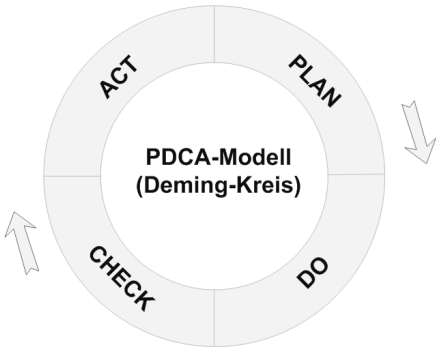


Abbildung 4.16: Qualitätskreis nach Deming (PDCA-Modell)

4.3.1.2 Aufbau der IT-Prozessdokumentation

Übertragung des PDCA-Modells auf den IT-Betrieb

Die in diesem Kapitel vorgestellte Struktur für die IT-Dokumentation soll einen Gliederungsansatz liefern, der sich möglichst direkt auf die eigene Prozessorganisation übertragen lässt. Das Vierphasen-Modell auf der Basis des PDCA-Modells bietet diese Grundvoraussetzung.

In Bezug auf die Aktivitäten von IT-Organisationseinheiten lassen sich die vier Phasen des Deming-Kreis wie folgt übertragen:

- *Plan*: Prozesse, die der Planung und Änderung des IT-Betriebs dienen
- *Do*: Prozesse des IT-Regelbetriebs
- *Check*: Prozesse, die der Prüfung und Bewertung des IT-Betriebs dienen (Supportmanagement)
- *Act*: Prozesse, die der Anpassung des IT-Betriebs im Sinne einer Optimierung dienen

Demzufolge kann die Prozessdokumentation für den IT-Betrieb, wie nachstehend gezeigt, unterteilt werden:

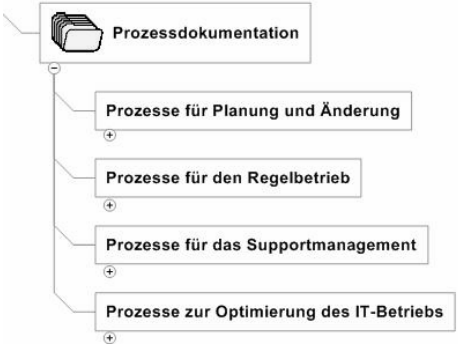


Abbildung 4.17: Struktur der Prozessdokumentation auf oberster Ebene

Prozesse für Planung und Änderung Die Prozesse in diesem Bereich dienen einer geplanten, kontrollierten und standardisierten Einführung neuer Technologien, Systeme, Anwendungen, Hardware und Prozesse in den IT-Betrieb. Den Schwerpunkt bilden die Prozesse des Änderungsmanagements (meist bekannt unter engl. Begriff *Change Management*, der bei ITIL Verwendung findet). Während der Änderungsphase wird eine Änderung geplant und getestet, und erst nach einer Prüfung und der anschließenden Freigabe wird die Änderung in der Produktionsumgebung und damit im IT-Betrieb bereitgestellt.

Die folgenden Prozesse können diesem Bereich zugeordnet werden:

- *Analyse und Beurteilung von Änderungen:* Ein Hauptziel des Änderungsmanagements besteht in einer schnellen Einführung von Änderungen in der IT-Umgebung bei nur minimaler Dienstunterbrechung. Wichtig ist daher die Identifizierung und Beurteilung der Auswirkungen von Änderungen. Die Analyseprozesse dienen daher vor allem auch der Informationsbeschaffung.
- *Autorisierung von Änderungen:* Diese Prozesse umfassen die Freigabe neuer Software, Hardware sowie Prozessfreigaben für die Produktionsumgebung und gegebenenfalls auch für die Integrationstestumgebung. Die Freigabeverwaltung schließt alle technischen und organisatorischen Aspekte einer Freigabe ein.
- *Änderungssteuerung- und Umsetzung:* Die Änderungssteuerung muss außerdem sicherstellen, dass die Auswirkungen von Änderungen allen Beteiligten bekannt sind und die Bereitstellungsverfahren getestet wurden. Außerdem muss sichergestellt werden, dass Rollback- und Notfallpläne erstellt wurden. Weiter umfasst dieser Bereich die Prozesse zur Bereitstellung der Änderungen in der Produktionsumgebung sowie Prozesse zur Prüfung und Bewertung der Ergebnisse.
- *Konfigurationsmanagement:* Auch die Prozesse des Konfigurationsmanagements können diesem Bereich zugeordnet werden. Das Konfigurationsmanagement umfasst vor allem das Einrichten und Durchführen einer Versions- und Releaseverwaltung. Im Rahmen der Versionsverwaltung werden alle relevanten Dokumente und Programmbestandteile mit ihrem jeweiligen Änderungsstand archiviert und dokumentiert. Im Gegensatz dazu stellt die Releaseverwaltung sicher, dass die einzelnen Releases (Auslieferungsstände) der Anwendungen dokumentiert und verwaltet werden.

Bildet die Schnittstelle zu den Projekten

Gleichzeitig bilden die Prozesse dieses Bereichs eine Schnittstelle zu den Projekten. Abhängig vom Umfang werden Änderungen entweder im Rahmen von Projekten oder auch direkt im IT-Betrieb durchgeführt. So ist für die Änderung der Einstellungen einer Gruppenrichtlinie sicherlich kein eigenes Projekt erforderlich – gleichwohl handelt es sich um eine Änderung, die die Änderungsprozesse durchlaufen muss. Die Änderung einer Exchange-Umgebung von der Version 2003 auf die Version 2007 wird im Normalfall aber im Rahmen eines Projektes erfolgen. (Nähere Erläuterungen zu diesem Punkt finden Sie in nachfolgenden Kapitel.)

Prozesse für den IT-Regelbetrieb Dieser Bereich bildet einen wesentlichen Schwerpunkt der IT-Dokumentation. Hier sind alle Prozesse des operativen Regelbetriebs einzuordnen: Unter anderem alle Prozesse der Systemverwaltung und Systemüberwachung, der Benutzerverwaltung und der Sicherheitsverwaltung.

Typische Prozesse dieses Bereichs sind:

- *Verwaltung der Serversysteme:* Hierzu zählen alle Prozesse des täglichen Betriebs für die betreuten Serversysteme. Diese umfassen den Betrieb, die Wartung, den Support, die Systemprogrammierung und das Schnittstellenmanagement.
- *Verzeichnisdienst- und Anwendungsverwaltung:* Umfasst die Verwaltung und Wartung des Verzeichnisdienstes sowie der serverbasierten Anwendungen.
- *Benutzerverwaltung:* Prozesse der Benutzerverwaltung umfassen das Einrichten neuer Benutzer, das Löschen vorhandener Benutzer, das Umziehen von Benutzern sowie das Einrichten von Zugriffsberechtigungen.
- *Desktopverwaltung:* Hierzu zählen Beschaffung, Bereitstellung, Austausch und Entsorgung von Arbeitsplatzrechnern, Druckern und anderer IT-Komponenten, mit denen Benutzer auf die IT-Dienste zugreifen.
- *Netzwerkmanagement:* Prozesse des Netzwerkmanagements umfassen die Beschaffung, Bereitstellung und Wartung von Netzwerkkomponenten.
- *Datensicherung und Wiederherstellung:* In diesen Bereich fallen alle Prozesse zur Durchführung von Datensicherungen sowie die Prozesse zur Daten- und Systemwiederherstellung.
- *Überwachung der Systeme und der IT-Services:* Die Systemüberwachung umfasst die kontinuierliche Durchführung von Standardanalysen und regelmäßigen Tests einschließlich der Auswertung sowie die Erstellung von Berichten.
- *Sicherheitsmanagement:* Das Sicherheitsmanagement ist für die Umsetzung von Sicherheitsanforderungen und deren Überwachung sowie für Ausbildungsmaßnahmen verantwortlich.
- *Softwareverwaltung:* Die Softwareverwaltung umfasst die Prozesse zur Beschaffung und Bereitstellung von Software, zur Paketierung von Software sowie zur Lizenzverwaltung.
- *Speichermanagement:* Zu den Prozessen des Speichermanagements gehören die Beschaffung, die Bereitstellung sowie die Wartung von Speicherkomponenten (NAS, SAN, Archivierung)

Prozesse für das Supportmanagement Insbesondere eine Unterteilung der Prozessdokumentation in Prozesse für den Regelbetrieb und in Support-Prozesse ist sinnvoll, da diese häufig unterschiedlichen Zuständigkeiten und Regelungen unterliegen. So ist es beispielsweise nicht unüblich, zumindest Teile des Supportmanagements, wie beispielsweise den Helpdesk oder den System-Support in gesonderte Organisationseinheiten oder gänzlich extern zu vergeben.

Die folgenden Prozesse können dem Supportmanagement zugeordnet werden:

- *Erkennen und Beheben von Vorfällen (Störungen):* Die Verwaltung von Störungen umfasst die Behandlung von Fehlern oder Unterbrechungen der Produktionssysteme. Ebenso gehören Eskalationsprozesse in diesen Bereich.
- *Beheben von Problemen:* Aufgabe der Problemverwaltung ist die Untersuchung, Diagnose, Auflösung und Behebung von Problemen.
- *Servicemanagement:* Aufgaben des Servicemanagements sind die Annahme und Umsetzung von Serviceanfragen von Benutzern.

Supportprozesse gemäß ITIL

Die drei genannten Prozesse des Supportmanagements entsprechen denen des *Incident Managements* und des *Problem Managements* von ITIL. Während jedoch ITIL V2 die Abwicklung von Serviceaufträgen (Service Requests) als Vorfall (Incident) behandelt, und damit keine gesonderte Betrachtung von Serviceanfragen und Störungsanfragen ermöglicht, wird mit ITIL V3 mit dem Prozess *Request Fulfilment* eine Unterscheidung möglich. Diese Unterscheidung ist wichtig, da die Aktivitäten bei Serviceabrufen, im Gegensatz zu Störungsprozessen, vollständig bekannt sind.

Prozesse für die Optimierung des Betriebs In diesem Bereich sind alle Prozesse einzuordnen, die der Optimierung des IT-Betriebs dienen. Diese Prozesse haben daher eher strategischen als operativen Charakter.

Typische Prozesse dieses Bereichs sind:

- Prozesse zur Überwachung der Leistung der IT-Abteilung sowie deren periodische Überprüfung auf die Einhaltung der SLAs
- Prozesse zur Optimierung der Leistung oder Kapazität, Erhöhung der Verfügbarkeit oder Verringerung der Kosten bei der Bereitstellung von IT-Diensten
- Prozesse der proaktiven Kapazitätsverwaltung und Sicherstellung ausreichender Kapazitäten
- Prozesse des proaktiven Verfügbarkeitsmanagements zur Sicherstellung der dauerhaften Verfügbarkeit von IT-Services

4.3.1.3 Zusammenspiel zwischen Änderungen in Betrieb und in Projekten

Aus Sicht der IT-Dokumentation verdienen die Prozesse des Änderungsmanagements besondere Beachtung, da Änderungen immer die Notwendigkeit der Dokumentation einschließen. Außerdem stellt das Änderungsmanagement die wesentliche Schnittstelle zwischen dem IT-Betrieb und den IT-Projekten dar. In der Projektliteratur werden das Änderungsmanagement und das Veränderungsmanagement voneinander abgegrenzt (s. Kasten). Auf das Erfordernis, die jeweili-

gen Anpassungen zu dokumentieren, hat diese Abgrenzung keinen Einfluss. Daher wird in dem vorliegenden Buch für beide Fälle von Änderungen bzw. Änderungsmanagement gesprochen.

Änderungsmanagement, Veränderungsmanagement und Change Management

Das *Änderungsmanagement* ist verantwortlich für die Steuerung und Überwachung von Änderungen. Ziel ist, dass Änderungen an Systemen oder Prozessen kontrolliert und dokumentiert erfolgen. Im Rahmen des Änderungsmanagements werden Änderungen identifiziert, beschrieben, klassifiziert, bewertet, genehmigt, durchgeführt und verifiziert.

Abzugrenzen davon ist das *Veränderungsmanagement*, das sich auf betriebliche Veränderungsprozesse im Unternehmen bzw. auf Veränderungen im Projektumfeld bezieht.

Zu beachten ist, dass der englische Begriff *Change Management* sehr häufig für beides verwendet wird, was zu Missverständnissen führen kann. Besser ist es daher den Begriff *Change Management* nur für das Veränderungsmanagement und den Begriff *Change Control* für das Änderungsmanagement zu verwenden, der auch der offizielle Terminus nach dem Project Management Body of Knowledge (PMBOK) ist [PMBOK].

Die folgende Grafik soll die Funktion des Änderungsmanagements als Schnittstelle zwischen Projekt und Betrieb verdeutlichen:

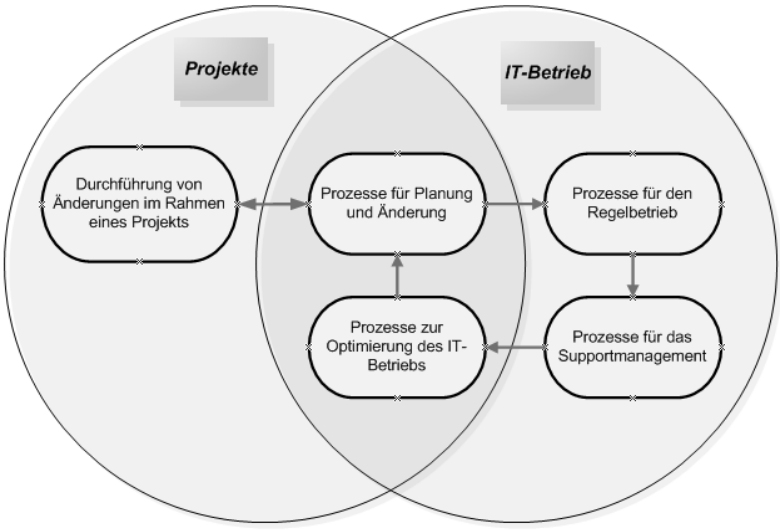


Abbildung 4.18: Das Änderungsmanagement bildet die Schnittstelle zwischen Betrieb und Projekt.

Auslöser von Änderungen

Dabei können Änderungen sehr unterschiedliche Auslöser haben:

- Gesetzliche Anforderungen
- Organisatorische Anforderungen (beispielsweise organisatorische Umstrukturierungen)
- Technische Anforderungen
- Anforderungen, die sich aus Optimierungsprozessen ergeben

Optimierungsprozesse beispielsweise können die Notwendigkeit zur Änderungen von Hardware, Software oder eines Verfahren zum Ergebnis haben. Dabei kann es sich um kleine Anpassungen handeln, aber auch um umfangreiche Änderungen.

Aufgaben des Änderungsmanagements

Das Änderungsmanagement umfasst alle Aufgaben, die einer geplanten, kontrollierten und standardisierten Einführung neuer oder geänderter IT-Systeme und IT-Verfahren dienen. Es definiert die Verantwortlichkeiten und plant die auszuführenden Arbeiten. Der Umfang der Änderungssteuerung ist dabei abhängig von der Komplexität und den erwarteten Auswirkungen einer Änderung und demzufolge sehr unterschiedlich. Er kann von einer automatischen Genehmigung kleinerer Änderungen bis hin zu vollständigen Überprüfungen auf Projektebene reichen.

Klassifizierung von Änderungen erforderlich

Eine entscheidende Frage, die es bei jeder Änderungsanforderung zu beantworten gilt, ist die, ob eine Änderung im Regelbetrieb erfolgen kann, oder ob die Einrichtung eines Projekts erforderlich ist. Nicht nur zur Beantwortung dieser Frage ist die Klassifizierung von Änderungen erforderlich.

Eine allgemeinverbindliche Klassifizierung hat sich bisher nicht herausgebildet. Das mag damit zusammenhängen, dass die Abgrenzung je nach betrieblichen Ressourcen und Anforderungen individuell für jedes Unternehmen getroffen werden muss. Insofern stellt die folgende Klassifizierung ein Angebot dar, dass auf die eigenen Bedürfnisse anzupassen ist.

- *Kleine Änderungen:* Kleine Änderungen wirken sich nicht erheblich auf die IT-Umgebung aus, haben nur geringe Risiken und erfordern keine oder nur geringe zusätzliche personelle oder finanzielle Ressourcen. Ein typisches Beispiel einer Änderung dieser Klasse ist die Anpassung einiger Einstellungen in einer Gruppenrichtlinie. Eine derartige Änderung hat nur geringe Auswirkungen auf andere Systeme, diese aber müssen im Rahmen eines Änderungsprozesses identifiziert und dokumentiert werden. Änderungen dieser Klasse erfolgen im Regelbetrieb und können von einem Fachverantwortlichen oder dem für die Änderungen zuständigen Koordinator freigegeben werden.

- *Erhebliche Änderungen:* Ein Beispiel für eine erhebliche Änderung ist das Bereitstellen eines neuen Release-Standes (z. B. eines Service Packs). Diese Änderungen müssen den Änderungsprozess komplett durchlaufen und in einer Änderungskonferenz (dem *Change Advisory Board*, *CAB*, gemäß ITTL) genehmigt werden. Wichtig ist bei derartigen Änderungen, dass die Bereitstellungsverfahren getestet und Rollback-Pläne erstellt werden. Derartige Änderungen erfolgen – trotz des teilweise erheblichen Aufwandes – in aller Regel im Rahmen des Regelbetriebs.
- *Große Änderungen:* Derartige Änderungen haben mitunter grundlegende Auswirkungen auf das System und werden meist in Form von Projekten durchgeführt. Ein Beispiel für eine derartige Änderung ist die Aktualisierung von Exchange Server 5.5 auf Exchange Server 2003. Große Änderungen erfordern das Planen, Erstellen und Implementieren erheblicher Ressourcen und müssen in der Änderungskonferenz genehmigt werden. Hier ist zu entscheiden, ob für die Änderung die Initiierung eines Projekts erforderlich ist.
- *Standardänderungen:* Standardänderungen haben den Änderungsprozess bereits durchlaufen, werden regelmäßig durchgeführt, sind gut bekannt und werden in der Betriebsdokumentation beschrieben. Der Austausch einer Festplatte im SAN-System oder die Vergabe von erweiterten Zugriffsberechtigungen sind typische Standardänderungen, die keinerlei weitere Eingriffe durch das Änderungsmanagement erfordern. Sinnvollerweise werden derartige Prozesse nach einem einmaligen Freigabeverfahren in einen entsprechenden Katalog aufgenommen. Eine erneute Betrachtung durch das Änderungsmanagement ist nur dann erforderlich, wenn Änderungen an einem als Standardänderung katalogisierten Prozess erforderlich sind.

hinweis

Vor allem aufgrund der Wichtigkeit, die es bei ITIL einnimmt, gehören das Change Management und dessen Prozesse zu den am besten dokumentierten. Die vorstehenden Ausführungen dienen lediglich dem Verständnis der grundlegenden Abläufe des Change Managements, ohne dieses vollständig zu beschreiben, was auch durch eine bewusst abweichende Begriffswahl verdeutlicht werden soll. Ausführliche Erläuterungen zum Change Management sind in der zahlreich vorhandenen Literatur zu ITIL zu finden.

In Bezug auf die Dokumentation von Änderungen ergeben sich nahezu die gleichen Anforderungen – unabhängig davon, ob eine Änderung im Betrieb oder im Projekt erfolgt.

Erforderliche Dokumente

Eine Änderung muss initiiert werden. Hierfür ist ein Antrag erforderlich. Ein wichtiges Dokument in diesem Prozess ist daher die *Änderungsanforderung*. In der Praxis wird diese auch als *Change Request (CR)* oder *Request For Change (RFC)* bezeichnet.

Während des Änderungsprozesses müssen die geplanten Änderungen getestet werden, was die entsprechenden Testdokumente erforderlich macht. Erst nach einer Prüfung und der anschließenden Freigabe wird die Änderung in der Produktionsumgebung und damit im IT-Betrieb bereitgestellt. Hierfür werden wiederum Abnahmedokumente benötigt. Zudem ist eine Anpassung der vorhandenen Betriebsdokumente erforderlich.

Um doppelte Ausführungen zu vermeiden, wird an dieser Stelle auf eine Vorstellung dieser Dokumente verzichtet. Stattdessen werden die für das Änderungsmanagement relevanten Dokumente im Rahmen der Beschreibung der Projektdokumentation in Abschnitt 6.3 betrachtet.

4.3.2 Anforderungen an die Prozessdokumentation

Die Prozessdokumentation für den IT-Betrieb ist einer der wichtigsten Teile der IT-Dokumentation und steht bei der Betrachtung eines prozessorientierten Qualitätsmanagements im Fokus. Die Ausrichtung an die Anforderungen des Qualitätsmanagements ist daher wichtig.

4.3.2.1 Formale Anforderungen

Betrachtet man die formalen Anforderungen der ISO-Normen, so sind diese sehr überschaubar. Da es keine konkreten Vorgaben gibt, können die Dokumente in jeder Form und Art und mit jedem beliebigen Medium erstellt werden. Alle für die Zertifizierung benötigten Dokumente müssen aber auch in Papierform vorliegen. Wichtig ist, dass alle Mitarbeiter Kenntnis von den Prozessen haben können. Dazu müssen ihnen die Dokumente entweder in Papierform vorliegen oder beispielsweise im Intranet einsehbar sein.

Prozess zur Lenkung von Dokumenten

Es muss darüber hinaus einen unternehmensweiten Prozess zur Lenkung von Dokumenten, Daten und Aufzeichnungen geben. Dieser Prozess sollte die folgenden Aspekte regeln:

- Wie erfolgt die Erstellung, Änderung und Freigabe von Dokumenten und wer ist für die Freigabe verantwortlich?
- Wie werden Dokumente im Unternehmen bereitgestellt?
- Wo sind Dokumente, Daten und Aufzeichnungen aufzubewahren und wie lange?

tipp

Unabhängig von den Anforderungen des Qualitätsmanagements, das lediglich eine Bereitstellung der QM-Dokumente in Papierform fordert, sollten auch alle Notfall-Dokumente, ebenfalls in ausgedruckter Form zur Verfügung stehen. Zudem müssen die Systemakten für die wichtigsten Systeme (Domänen-Controller, Active Directory, Datenbankserver usw.) als Ausdruck vorliegen. Ist im Notfall kein Zugriff auf die gespeicherten Dokumente möglich, hilft auch eine vorbildlich gepflegte Prozessdokumentation nicht weiter.

4.3.2.2 Inhaltliche Anforderungen

Prozessbeschreibungen müssen so aufgebaut sein, dass sie alle wesentlichen Aspekte des Prozesses darstellen und eine Bewertung ermöglichen.

Bewertungskriterien für Prozesse

Bei einem Audit werden für die Bewertung der zu prüfenden Prozesse die nachstehenden Kriterien zugrunde gelegt. Hier wird insbesondere darauf geachtet, dass die Prozesse eindeutig, lückenlos und konsistent beschrieben sind. Die Prozessdokumentation sollte deshalb die folgenden Kriterien darstellen.

- *Prozessziele:* Die Prozesse wurden auf der Grundlage von Zielsetzungen entwickelt und umgesetzt. Die Prozessbeschreibung der Einzelprozesse muss demzufolge das Prozessziel und die daraus abzuleitenden Zielsetzungen messbar beschreiben.
- *Orientierung an Unternehmenszielen:* Die Zielsetzungen der einzelnen Prozesse stehen in Einklang mit den Unternehmenszielen und sind an diesen ausgerichtet.
- *Prozesswirksamkeit:* Die Wirksamkeit der Prozesse ist langfristig sichergestellt. Dazu wird die Qualität der Prozesse regelmäßig anhand von Kennzahlen überprüft und gegebenenfalls angepasst. Die Dokumentation der Prozesse wird gepflegt und ist mit den realisierten Prozessen konsistent, das heißt, die Prozesse werden tatsächlich in der dokumentierten Form angewendet.
- *Prozessverantwortlichkeiten:* Den Prozessen und jedem Prozessschritt sind eindeutige Verantwortlichkeiten zugeordnet.
- *Qualitätssicherung:* Die Prozesse beinhalten Prozessschritte, die die Qualität der erreichten (Zwischen-)Ergebnisse sicher stellen und die Ergebnisse dokumentieren..
- *Risiken:* Die Risiken und Gefahren, die mit einem Prozess verbunden sind, sind analysiert und beschrieben.

hinweis

IT-Prozessdokumentation zunehmend im Focus des QM-Managements

Auch wenn die vorstehende Betrachtung der QM-Dokumentation für das Gesamtunternehmen gilt und das Augenmerk auf den Kernprozessen liegt, gelten die genannten Anforderungen in gleicher Weise auch für die Prozessdokumentation des IT-Betriebs. Mit der wachsenden Bedeutung der IT-Prozesse rücken auch die Prozesse des IT-Betriebs zunehmend in den Focus des Qualitätsmanagements.

Anforderungen der Anwender

Die Schwierigkeit bei der Erstellung der Prozessdokumentation besteht in der Gratwanderung, alles Wichtige zu beschreiben und trotzdem die einzelne Prozessbeschreibung nicht zu detailliert zu gestalten. Soll diese nicht nur als Nachweis gegenüber der Unternehmensleitung und gegebenenfalls einem Prüfer dienen, sondern auch ein Arbeitsmittel für die Mitarbeiter darstellen, sind

detaillierte Beschreibungen der Arbeitsabläufe sowie Checklisten und Formulare als Anlage zu den Prozessbeschreibungen unverzichtbar. Es gilt also, alle Prozesse so detailliert wie nötig darzustellen. Wichtig ist, dass sich die Mitarbeitenden in den Prozessen wieder finden. Nur dann kann die Dokumentation als verbindliche Sollvorgabe für die vorhandenen Mitarbeiter und deren Vertretung sowie für die Einarbeitung neuer Mitarbeiter Verwendung finden.

Neben den zuvor beschriebenen Anforderungen, die Prüfer an die Prozessdokumentation stellen, muss diese daher auch die Anforderungen erfüllen, die die Anwender an sie stellen. Im Idealfall sind Prozessbeschreibungen so aufgebaut, dass sich einerseits die Unternehmensleitung einen schnellen Überblick verschaffen kann, und andererseits der Anwender in der Lage ist, die ihm zugeordneten Aktivitäten in der festgelegten Art und Weise zu erledigen.

hinweis

In Abschnitt 8.5 finden Sie eine musterhafte Prozessbeschreibung. Anhand eines ausgewählten Prozesses werden der Aufbau und mögliche Inhalte einer Prozessbeschreibung über alle Detaillierungsstufen hinweg dargestellt. Dies schließt auch Arbeitshilfen wie Checklisten und Formulare ein.

4.3.3 Inhalte einer Prozessbeschreibung

Dokumentationen zum Thema Prozessbeschreibungen und Prozessdesign füllen ganze Bücherregale. Ist es da noch notwendig, das Thema in diesem Buch zu behandeln?

Im Gegensatz zu vielen Abhandlungen zum Thema Prozessdokumentation, steht hier nicht das „Wie ", sondern das „Was zu Dokumentieren ist" im Vordergrund. Es geht also nicht darum, mit welchen Methoden Prozesse zu beschreiben sind (auch wenn dies in einer kurzen Einführung behandelt wird), sondern darum, die Prozessdokumentation und die einzelnen Prozessbeschreibungen so zu gestalten und zu strukturieren, dass sie die revisionsüblichen Anforderungen an Vollständigkeit und Nachvollziehbarkeit erfüllen.

Checklisten und Formulare dienen dem Nachweis

Gemäß den Ausführungen des vorstehenden Kapitels sollten Prozessbeschreibungen detaillierte Regelungen für die (wichtigsten) Arbeitsprozesse beinhalten. Die zusätzlich erforderlichen Arbeitsanweisungen beinhalten Vorgaben für die Tätigkeitsausführung und werden in der Praxis von Checklisten, Formularen und Mustern zur Unterstützung der täglichen Arbeit begleitet sein. Checklisten und Formulare können während der Prozessausführung ausgefüllt und abgezeichnet werden und dienen als wichtige Ergebnisdokumentation der Arbeit.

Wie aber sollte eine Prozessbeschreibung aufgebaut sein?

Empfehlenswert ist der nachstehend beschriebene Aufbau. Dabei wird jede Prozessbeschreibung als eine Akte behandelt, die alle zum beschriebenen Prozess erforderlichen Dokumente enthält. Diese können natürlich auch in gesonderten Dateien gespeichert werden. Ebenso ist es möglich, die Gesamtheit aller Pro-

zessbeschreibungen entweder zu einem einzigen Dokument zusammen zufassen oder als gesonderte Dokumente zu behandeln. Welche Vorgehensweise die richtige Wahl ist, hängt vor allem von der Art der Bereitstellung ab (Dokumentenmanagement-System, Tooleinsatz zur automatisierten Abwicklung von Arbeitsabläufen).

Gliederung einer Prozessbeschreibung

Wichtig ist jedoch, dass die wesentlichen Teile der Prozessbeschreibungen immer gleich aufgebaut sind. Die Übersicht wird dadurch verbessert. Die nachstehende Abbildung zeigt eine mögliche Strukturierung für Prozessbeschreibungen.

Abbildung 4.19: Mögliche Gliederung einer Prozessbeschreibung

Im Folgenden werden die genannten Komponenten der Prozessbeschreibung vorgestellt.

4.3.3.1 Prozesssteckbrief

Der Prozesssteckbrief soll einen schnellen Überblick über alle wichtigen Prozessmerkmale liefern. Hierzu sollte er folgende Informationen beinhalten:

- *Prozessname:* Jeder Prozess erhält einen Namen, der möglichst eindeutig und prägnant das Ziel des Prozesses erkennen lässt. Möglich ist beispielsweise festzulegen, dass der Prozessname immer aus einem Substantiv und einem Verb bestehen muss (zum Beispiel „Benutzerkonto einrichten").
- *Prozessnummer.* Jeder Prozess benötigt eine eindeutige Nummer. Diese ermöglicht es beispielsweise, in unterschiedlichen Dokumenten auf den Prozess zu verweisen. Pflegt das Unternehmen eine unternehmensweit durchgängige Prozessnummerierung (entweder in tabellarischer Form oder in

einer Prozesslandkarte), so ist diese natürlich zu berücksichtigen. In diesem Fall enthält jeder IT-Prozess eine entsprechende übergeordnete Nummer vorangestellt, die die Einordnung in den Unternehmens-Prozesskontext ermöglicht. Alternativ ist eine gesonderte Nummerierung der IT-Prozesse möglich. Ein Beispiel für einen Prozesssteckbrief finden Sie in Abschnitt 8.5.1. Im gleichen Kapitel befindet sich auch ein Vorschlag für eine unternehmensweite Nummerierung von Prozessen.

Prozesslandkarte

In einer Prozesslandkarte, auch als *Prozessarchitekturmodell* bezeichnet, werden alle wesentlichen Prozesse eines Unternehmens und wie diese logisch zusammenhängen, dargestellt. Eine Prozesslandkarte beschreibt demnach die Struktur der Unternehmensprozesse und das Zusammenwirken der einzelnen Teilprozesse. Was für die Darstellung der Organisationsstruktur eines Unternehmens das Organigramm ist, das ist für die Ablauforganisation die Prozesslandkarte. Die Prozesslandkarte dient als grafische Darstellung der Prozesse. Ihre Publikation soll auch dazu beitragen, dass die Mitarbeiter und Führungskräfte die Einordnung „ihres" Prozesses in das Gesamtgefüge erkennen und so die Bedeutung ihrer Leistung beurteilen können.

Neben den Kernprozessen sollte die Prozesslandkarte alle Prozesse berücksichtigen, die einen wesendlichen Teil der Geschäftstätigkeit ausmachen. Sie enthält aber weder Informationen zu den Prozessen selbst, noch Input-Output-Informationen noch Informationen bezüglich der Prozessschrittabfolge. Diese sollten zusätzlich in einer entsprechenden tabellarischen Form dargestellt werden.

In der Praxis ist allerdings die Pflege und Nutzung von Prozesslandkarten bisher kaum üblich.

- *Beschreibung:* Die Beschreibung soll in aller Kürze die Aufgabe und das Ergebnis des Prozesses beschreiben.
- *Prozessziel:* Jeder Prozess muss zwingend ein definiertes Ziel haben. Dieses muss überprüfbar und eindeutig sein. Das Ziel muss außerdem durch den Prozess erreichbar sein. Ein Prozess darf also keine Parameter oder Ereignisse definieren, die nicht der Kontrolle des Prozesses unterliegen.
- *Prozessverantwortlicher:* Für jeden Prozess muss es einen Verantwortlichen geben. Dieser ist als Rolle und ggf. mit der Funktion in der Aufbauorganisation zu benennen.
- *Prozessteam:* Für alle Prozessschritte muss die Rolle benannt werden, die die jeweilige Aktivität zu erledigen hat. Dies kann in der grafischen Darstellung des Prozesses erfolgen oder in der detaillierten Beschreibung des Prozesses. Im Projektsteckbrief dagegen genügt es, die beteiligten Rollen aufzuführen.

- *Prozessauslösendes Ereignis:* Es muss eindeutig beschrieben sein, durch welches Ereignis der Prozess ausgelöst wird. So löst beispielsweise der Eingang einer E-Mail beim Service Desk einen Störungsprozess aus.
- *Prozessinput (Daten/Dokumente):* Es sollten die Input-Komponenten benannt werden, die den Prozess auslösen. Hierbei kann es sich sowohl um Dokumente handeln wie beispielsweise ein Formular oder auch um Daten, die das Ergebnis eines anderen Prozesses sind.
- *Prozessoutput (Daten/Dokumente):* Im Prozesssteckbrief sollten die wichtigsten Prozessergebnisse, z. B. eine ausgefüllte Checkliste, genannt werden. Dies gilt insbesondere für Dokumente oder Daten, die einen Input für einen Folgeprozess darstellen.
- *Schnittstellen zu anderen Prozessen:* Hat ein Prozess Schnittstellen zu anderen Prozessen – und es wird kaum Prozesse geben, bei denen dies nicht der Fall ist –, sind diese im Projektsteckbrief zu benennen.
- *Risiken und Gefahren:* Unter dem Punkt „Risiken und Gefahren" sind Einflüsse zu benennen, die den Prozessverlauf behindern können.
- *Prozesskennzahlen/Messgrößen:* Ein Prozess kann nur dann im Sinne des Qualitätsmanagements optimiert werden, wenn sein Ergebnis messbar ist. Zu jeder Zielformulierung gehören daher sinnvolle und messbare Kriterien, mit denen der Erfüllungsgrad des Ziels ermittelt werden kann.
- *Prozess freigeben am und Freigegeben durch:* Prozesse müssen, wiederum im Rahmen eines entsprechenden Prozesses, geprüft und freigegeben werden. Im Prozesssteckbrief sollte auch vermerkt werden, wann und durch wen der Prozess vor der Inbetriebnahme freigegeben wurde.
- *Prozessbewertung (Verantwortlicher und Termin):* Prozesse sollten turnusmäßig darauf hin überprüft werden, ob sie noch effizient sind und ob das gewünschte Ziel mit dem minimal erforderlichen Aufwand erzielt wird. Es ist sinnvoll, im Prozesssteckbrief einzutragen, wann die nächste Überprüfung erfolgen soll und durch wen.
- *Arbeitshilfen:* Sind dem Prozess andere Dokumente, wie beispielsweise Formulare oder Checklisten zugeordnet, sollten diese im Prozesssteckbrief aufgeführt werden.

Typische Rollen qualitätsüberwachter Prozesse

Wie beschrieben, sind im Projektsteckbrief der Prozessverantwortliche und alle beteiligten Rollen zu benennen. ITIL definiert für die beschriebenen Prozesse jeweils einen *Prozesseigner* (engl. *Process owner*), der die Zielvorgaben und die Kontrolle des Prozesses verantwortet und für das Erreichen seiner Leistungsziele verantwortlich ist. Zusätzlich gibt es für jeden Prozess einen oder mehrere Rollen, die für die operative Umsetzung des Prozesses verantwortlich sind (*Prozessnutzer*).

Überträgt man diesen Ansatz auf die Aufgaben im Bereich der Dokumentation von Prozessen, können hierfür folgende Rollen mit den benannten Zuständigkeiten definiert werden:

Rolle	Zuständigkeiten
Prozesseigner (Verantwortlicher des Prozesses)	• Gesamtverantwortung für den Prozess • Klärung der Schnittstellen zu anderen Prozessen • Bewertung und Freigabe des Prozesses • Bewertung der Prozessrisiken und der Maßnahmen zur Risikoreduzierung • Turnusmäßige Überprüfung des Prozesses hinsichtlich Zielerreichung und Effizienz anhand der Prozesskennzahlen und gegebenenfalls Anpassung des Prozesses • Erstellung und Pflege der Prozessdokumente • Turnusmäßige Überprüfung der Prozessdokumente • Bereitstellung der Prozessdokumente (z. B. im Intranet) • Mithilfe bei der Schulung im Umgang mit den Dokumenten • Überprüfung und Abnahme von prozessergänzenden Dokumenten (Arbeitsanweisungen, Formulare, Checklisten usw.)
Prozessnutzer (Prozessausführende)	• Erstellung der prozessergänzenden Dokumente • Ausführung der im Prozess definierten Aktivitäten • Einhaltung der Vorgaben • Einreichung von Optimierungsvorschlägen zum Prozess • Melden von Problemen, die im Rahmen der Prozessausführung auftreten

Tabelle 4.1: Rollen und Zuständigkeiten für den Bereich Prozessdokumentation

hinweis

In der Literatur wird manchmal noch der *Prozess-Manager* als Rolle benannt. Es ist durchaus möglich, zusätzlich eine derartige Rolle zu verwenden. Dieser würde vom Prozesseigner eingesetzt und könnte im oben genannten Fall beispielsweise alle Aufgaben zur Pflege der Prozessdokumentation übernehmen. In der Praxis ist die Unterscheidung zwischen Prozesseigner und Prozess-Manager häufig schwierig, sodass diese beiden Rollen auch zusammengefasst werden können. Dies gilt insbesondere für Unternehmen, in denen aus personaltechnischen Gegebenheiten beide Rollen ohnehin von einem Mitarbeiter wahrgenommen werden.

4.3.3.2 Beschreibung der Haupt- und Unterprozesse

Prozesse können auf unterschiedliche Weise dokumentiert werden. Dies kann im einfachsten Fall sogar Fließtext oder eine Tabelle sein. In der Praxis werden Prozesse meist grafisch in Form eines Ablaufdiagramms dargestellt, das den Prozess veranschaulicht, und von einer textlichen Beschreibung begleitet wird. Dabei ist die grafische Darstellung der Prozesse als Ergänzung der Prozessbeschreibung zu betrachten. Sie kann in der Regel eine detaillierte Beschreibung der Abläufe nicht ersetzen.

Da es keine standardisierte Notation für die Prozessmodellierung gibt, obliegt es dem Unternehmen, die Modellierungstechnik und die Darstellungsform auszuwählen. Bevor also mit der Dokumentation von Prozessen begonnen werden kann, müssen das Prozessmodell und die Modellierungswerkzeuge ausgewählt und im Unternehmen eingeführt sein. Zur Auswahl stehen dafür eine Reihe von Techniken vom einfachen Flussdiagrammen bis zu standardisierten Modellierungsmodellen, wie beispielsweise: *Business Process Modeling Notation (BPMN), Unified Modeling Language (UML)* und *Ereignisgesteuerte Prozessketten (EPKs).*

hinweis

Fast erwartungsgemäß findet man auch im Bereich der Prozessmodellierung viele unterschiedliche Begriffe, die auch noch mit gänzlich unterschiedlicher Bedeutung verwendet werden. Ein typisches Beispiel hierfür ist der Begriff *Workflow*, der in mannigfaltiger Weise benutzt wird. Im vorliegenden Buch werden die folgenden Begriffe wie folgt verwendet:

- *Prozess:* Ein Prozess ist eine Kette aufeinander aufbauender Aktivitäten und dient der Herstellung eines Produktes oder einer Dienstleistung. Ein Prozess hat einen definierten Anfang, einen beschriebenen Ablauf und ein definiertes Ende. Die einzelnen Aktivitäten stehen in Abhängigkeit zueinander.
- *Arbeitsablauf:* Ein Arbeitsablauf ist ein zusammenhängend ablaufender Teil eines Prozesses, bei dem die operative Sicht im Vordergrund steht. Arbeitsabläufe stellen demnach operative Detailansichten eines Prozesses dar. Sie können, müssen jedoch nicht IT-unterstützt durchgeführt werden.
- *Aktivität:* Eine Aktivität bildet die kleinste Einheit in einem Arbeitsablauf.

Auf eine Verwendung des Begriffs *Workflow* wird an dieser Stelle verzichtet, da dieser Begriff mit so unterschiedlichen Bedeutungen besetzt ist, dass dies zu Verwirrungen führen würde. Ein Beispiel soll dies verdeutlichen: Obwohl Workflow die wörtliche Übersetzung von Arbeitsablauf ist, werden Workflows vielfach mit Prozessen gleichgesetzt, die sich allein dadurch unterscheiden, dass sie IT-gestützt und automatisiert ablaufen. Aber auch die Darstellung von Arbeitsabläufen in Flussdiagrammen wird im allgemeinen Sprachgebrauch vielfach als Workflow bezeichnet.

Prozessdarstellungsarten

Nachdem mit den vorstehenden Ausführungen geklärt wurde, was zu dokumentieren ist, geht es darum zu klären, wie Prozesse und Arbeitsabläufe dokumentiert werden können. Zu den am weitesten verbreiteten Darstellungsformen gehören EPKs und Darstellungen als Flussdiagramme.

Ereignisgesteuerte Prozessketten (EPK) *Ereignisgesteuerte Prozesskette (EPK)* ist ein Modell zur Darstellung von Prozessen und ein wesentliches Element des ARIS-Konzepts der Firma IDS Scheer. Das Modell wurde 1992 von einer Arbeitsgruppe an der Universität des Saarlandes zusammen mit der SAP AG zur Dokumentation von Geschäftsprozessen entwickelt. ARIS (Architektur integrierter Informationssysteme) und die Ereignisgesteuerten Prozessketten haben sich mittlerweile zu einem Quasi-Standard für die Geschäftsprozessmodellierung insbesondere bei SAP-gestützen Unternehmensprozessen entwickelt.

Alternierende Kette aus Funktionen und Ereignissen

EPKs stellen einen Prozess als eine Kette von Aktivitäten (im EPK-Modell als *Funktionen* bezeichnet) dar, die wiederum durch *Ereignisse* verknüpft sind. Eine Funktion hat als Eingang definierte Ereignisse, die eingetreten sein müssen, bevor die Funktion ausgeführt werden kann (Startereignisse). Eine Funktion, die ausgeführt wird, erzeugt wiederum ein oder mehrere Ereignisse. Jede Funktion kann zusätzlich mit einem Informationsobjekt verbunden werden. Diese dienen dazu, das Einspielen oder Speichern von Informationen darzustellen.

Durch eine zusätzliche Verknüpfung von Ereignissen durch logische Konnektoren können parallele Abläufe oder alternative Abläufe dargestellt werden:

- AND – „und"-Verknüpfung: Die Aussage ist wahr, wenn beide Aussagen gleichzeitig wahr sind.
- OR – „und/oder"-Verknüpfung: Die Aussage ist wahr, wenn mindestens eine Aussage gleichzeitig wahr ist.
- XOR – „entweder-oder"-Verknüpfung: Die Aussage ist wahr, wenn genau eine der beiden Aussagen wahr ist.

Eine Ereignisgesteuerte Prozesskette besteht demzufolge aus drei möglichen Knotentypen:

- *Funktion:* Funktionen bilden die Grundbausteine des Diagramms. Jede Funktion entspricht einer ausgeführten Aktivität.
- *Ereignis:* Ereignisse können vor und/oder nach der Ausführung einer Funktion auftreten und sind durch Ereignisse verbunden.
- *Konnektor:* Konnektoren verknüpfen Funktionen und Ereignisse. Es gibt drei Typen: UND, ODER sowie das ausschließende ODER (XOR).

Zusätzlich zu den genannten Grundelementen können EPKs um zusätzliche Elemente erweitert werden. Beim Verwenden dieser Elemente spricht man von *erweiterten EPKs (eEPK)*. So können beispielsweise die mit der Ausführung von Funktionen betrauten Organisationseinheiten sowie ein- und ausgehende Datenobjekte dargestellt werden. Somit ermöglichen erweiterte EPKs eine Prozessverfolgung über mehrere Organisationseinheiten hinweg.

EPK-Beispiel

Die folgende Abbildung zeigt einen exemplarischen Ausschnitt aus einem in EPK-Notation verfassten Prozess.

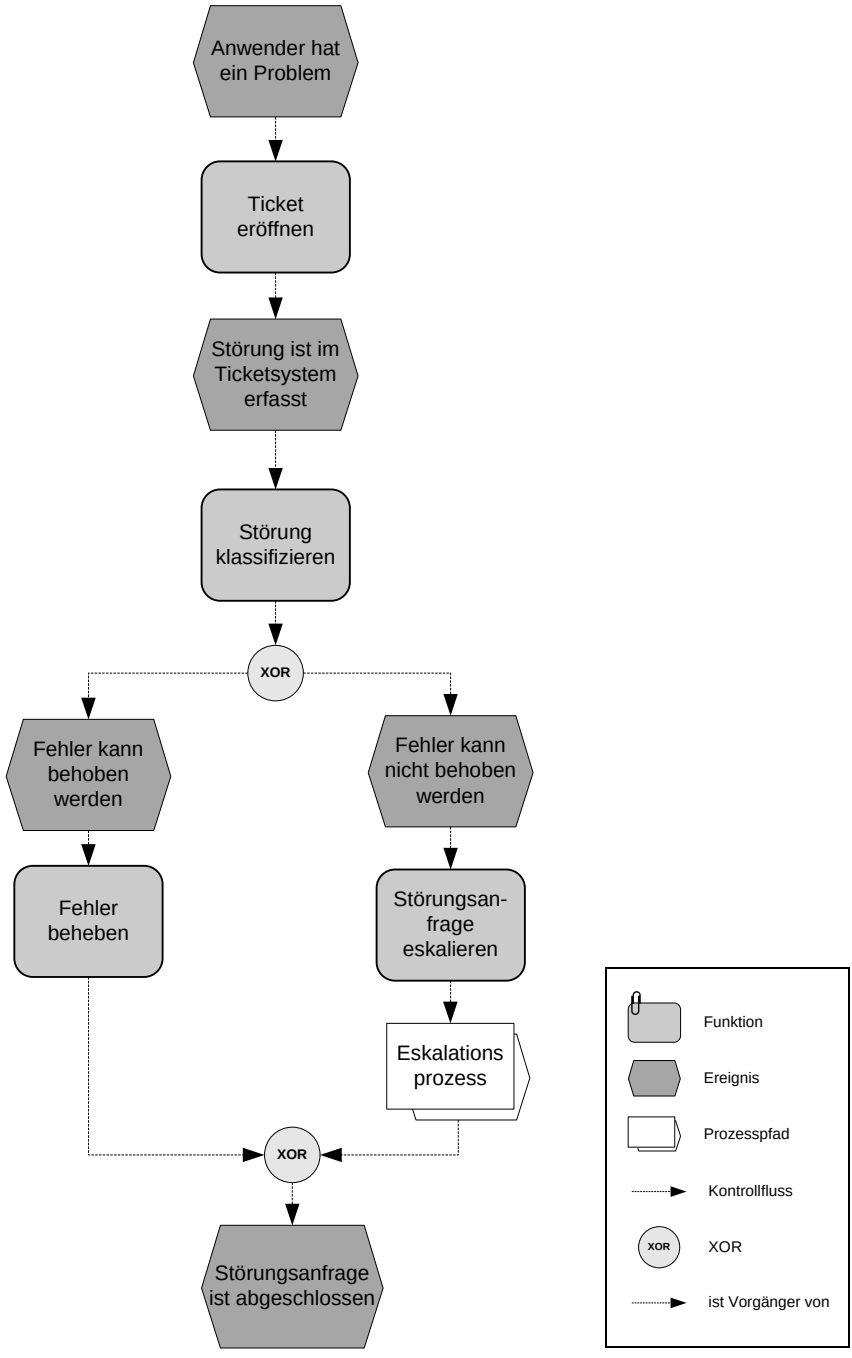


Abbildung 4.20: Beispielprozess in EPK-Notation

EPKs sind gut geeignet für die Darstellung von Prozessen, können jedoch sehr lang werden, da für alle Funktionen dargestellt werden muss, durch welche Ereignisse sie initiiert werden. Die formale Form der EPKs bedingt auch, dass Verzweigungen und Schleifen schwer darstellbar sind, sodass sie für die Darstellung von Arbeitsabläufen nicht gut geeignet sind.

Für Darstellung von Arbeitsabläufen nicht geeignet

Flussdiagramme Flussdiagramme sind eine einfache und häufig eingesetzte Darstellungsform, um Prozesse und Arbeitsabläufe zu dokumentieren. Im Gegensatz zu EPKs unterliegen Flussdiagramme keinen Standardisierungsregeln. Zwar definiert die DIN 66001 von 1966 bzw. die ISO-Norm 5807 einen Satz von Symbolen (engl. Shapes) für Datenfluss- und Programmablaufpläne, und dieser hat sich ebenfalls weitgehend als Symbolsatz zur Darstellung von Prozessen und Aktivitäten durchgesetzt, verbindliche Regelungen für deren Verwendung, wie dies bei EPKs der Fall ist, gibt es aber nicht.

Weit verbreitet ist die Verwendung von *Funktionsbändern* in Flussdiagrammen (auch als Swimlanes – Schwimmbahnen bezeichnet) Mit Hilfe von Funktionsbändern kann die Beziehung zwischen einer Aktivität und den für diese Aktivität verantwortlichen Bearbeiter bzw. der Organisationseinheit dargestellt werden. Hierzu werden die Aktivitäten in den Bändern platziert, die den für diese Schritte verantwortlichen Funktionseinheiten entsprechen. Grundsätzlich können Funktionsbänder auch bei der Modellierung mit EPKs eingesetzt werden. Sie finden dort aber seltener Anwendung.

Funktionsbänder zur Darstellung der Verantwortlichkeiten

Die Abbildung 4.21 zeigt exemplarisch ein Flussdiagramm mit Funktionsbändern.

RACI-Diagramme Eine spezielle Form der Flussdiagrammdarstellung ergibt sich aus der Kombination von Flussdiagrammen und RACI- bzw. RASCI-Modellen. RACI ist eine Technik zur Analyse und Darstellung von Verantwortlichkeiten, deren Name sich aus den Anfangsbuchstaben der englischen Begriffe *Responsible*, *Accountable*, *Supportive*, *Consulted* und *Informed* ableitet.

Hinter den Begriffen verbergen sich die folgenden Bedeutungen:

RACI beschreibt die Verantwortlichkeiten

- *Responsible (R):* Verantwortlich, das heißt, der Rolleninhaber ist für die Durchführung verantwortlich. Dies wird auch als sachliche Verantwortung bezeichnet.
- *Accountable (A):* Rechenschaftspflichtig, das heißt, der Rolleninhaber muss „genehmigen und abzeichnen" und ist im rechtlichen oder kaufmännischen Sinne verantwortlich. Dies wird auch als Verantwortung aus Kostenstellensicht bezeichnet.
- *Supportive (S):* Unterstützend. Der Rolleninhaber hat eine unterstützende Funktion und kann Sachmittel zur Verfügung stellen.
- *Consulted (C):* Beratend. Der Rolleninhaber hat eine beratende Funktion. Dies wird auch als Verantwortung aus fachlicher Sicht bezeichnet.
- *Informed (I):* Informiert. Der Rolleinhaber erhält Informationen über den Verlauf bzw. das Ergebnis der Tätigkeit oder besitzt die Berechtigung, Auskunft zu erhalten.

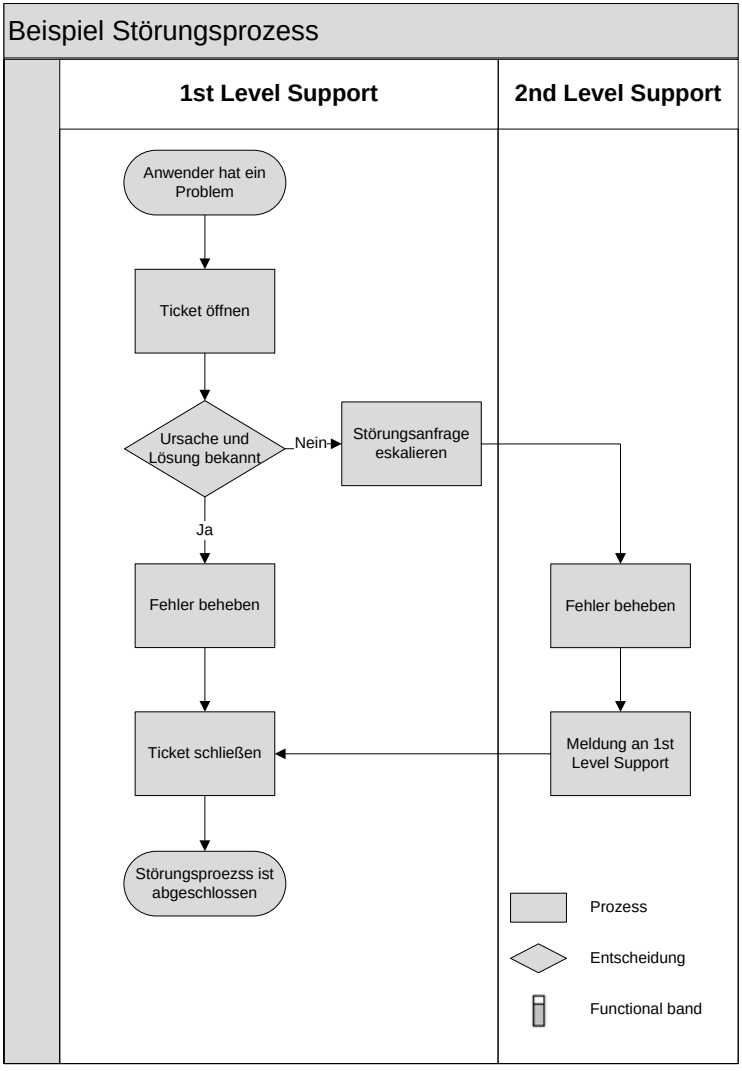


Abbildung 4.21: Beispielprozess in Flussdiagramm-Notation

RACI-Diagramme dienen dazu zu beschreiben, welche Rolle für welche Aktivitäten verantwortlich ist und welche Rollen zu beteiligen sind. Für jeden Prozessschritt wird bei dieser Darstellung zusätzlich angegeben, welche Rolle verantwortlich ist, wer Richtlinienkompetenz besitzt und genehmigt, wer den Prozess beratend unterstützt und welche Rolle informiert wird. Im Vordergrund steht hierbei die Beschreibung der Verantwortlichkeiten und Zuständigkeiten.

Da bei dieser speziellen Form eines Flussdiagramms nicht der Prozessablauf, sondern die Darstellung der Verantwortlichkeiten im Vordergrund steht, ist der verfügbare Platz für das eigentliche Flussdiagramm zwangsläufig beschränkt. Insofern eignen sich RACI-Diagramme weniger für eine detaillierte Darstellung

komplexer Arbeitsflüsse, als vielmehr zur übersichtlichen Dokumentation von Prozessen und den damit zugeordneten Verantwortlichkeiten. Im Rahmen der Dokumentation zur Erlangung einer ISO-Zertifizierung stellen sie allerdings eine häufig verwendete Darstellungsform dar.

Die nachstehende Abbildung zeigt exemplarisch ein an die RACI-Notation angelehntes Flussdiagramm. Das Diagramm wurde mit dem Prozessmodellierungstool SemTalk erstellt (siehe hierzu Abschnitt 4.3.4). Die Notation bei SemTalk betrachtet – abweichend von RACI – nur die Verantwortungen *Responsible*, *Supportive* und *Informed.*

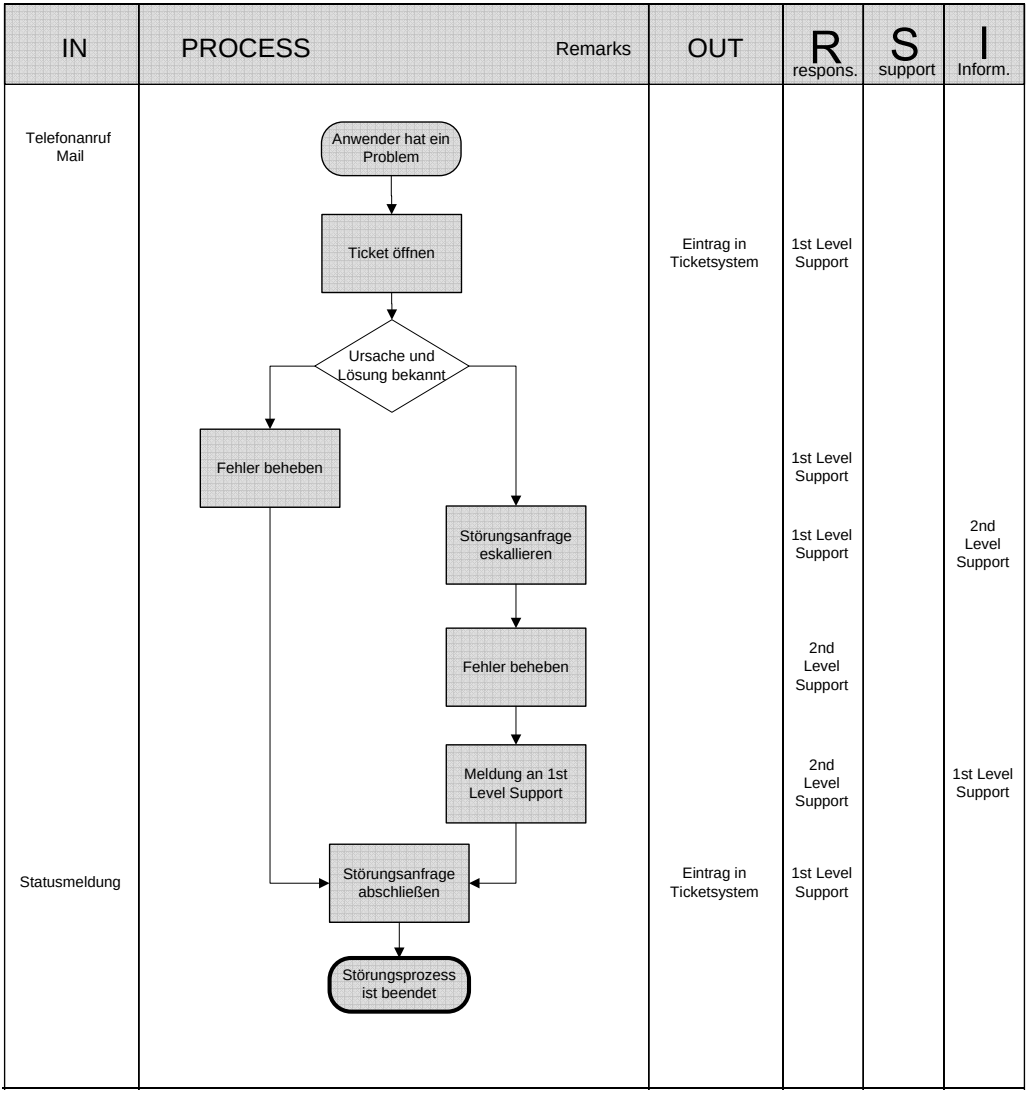


Abbildung 4.22: Beispielprozess in RSI-Notation

Kommunikationsstrukturanalyse (KSA) Die KSA-Methode ist in den späten 80er-Jahren an der Technischen Universität Berlin unter dem Namen *Kommunikationsstrukturanalyse (KSA)* entwickelt worden. KSA-Modelle zählen zur Gruppe der Informationsmodelle und dienen der hierarchischen Strukturierung der zu bearbeitenden Aufgaben und Informationen. Der Fokus von KSA-Modellen liegt also auf der Beschreibung, Analyse und Optimierung von Informationsflüssen. Betrachtet wird dabei der Austausch von Informationen und Informationsträgern zwischen den Prozessschritten und ihren Bearbeitern. Die Vorgehensweise dabei ist Top-Down. Ein Prozess im KSA-Modell ist eine Abfolge von Aktivitäten (Aufgaben) mit definierten Schnittstellen wie Eingängen und Ausgängen. Zwischen diesen Prozesselementen gibt es Informationsflüsse (z. B.: „schickt Info"), bei denen angegeben werden kann, welche Informationen zwischen zwei Aktivitäten sowie den Prozessschnittstellen fließen. Weitere Prozesselemente sind Sachmittel und Speicher, die mit den Aktivitäten verbunden werden können. Alle Prozesselemente können wahlweise auch in Funktionsbändern angeordnet und so einem Bearbeiter zugeordnet werden.

Workflow-Management Coalition (WfMC)

KSA-Modelle werden bevorzugt im Qualitätsmanagement eingesetzt. Außerdem entsprechen sie den Standards der *Workflow Management Coalition (WfMC)*. Diese Organisation wurde 1993 gegründet und stellt einen Verbund von mehreren hundert Herstellern, Nutzern, Beratern und Wissenschaftlern im Bereich des Workflow-Managements dar. Hauptziel der WfMC ist die Etablierung eines Workflow-Referenzmodells. Dieses spezifiziert die Struktur für Workflow-Management-Systeme sowie dessen Charakteristika, Funktionen und Schnittstellen.

Die Abbildung 4.23 zeigt exemplarisch einen Prozess in KSA-Notation.

Empfehlungen für die Prozessdokumentation Vor der Wahl eines Prozessmodells für die Dokumentation von Prozessen ist es wichtig zu klären, welchen Einsatzzweck die Dokumentation hat und in welchem Kontext sie benötigt wird. Steht bei der Dokumentation der Prozesse die ISO-Zertifizierung im Vordergrund, ist ein anderer Abstraktionsgrad erforderlich, als wenn die Prozessdokumentation in erster Linie die Mitarbeiter bei der Erledigung ihrer Aufgaben unterstützten soll. Und werden Prozessdokumentationen als Grundlage für die Implementierung automatisierter Abläufe benötigt, sind wiederum andere Anforderungen zu berücksichtigen, da in diesem Fall die Frage der Standardisierung im Vordergrund stehen muss.

Von der Zielsetzung der Prozessdokumentation hängt nicht nur die Auswahl der Methode, sondern auch deren Inhalt und Detaillierungsgrad ab. Die Festlegung der Notation ist in der Praxis außerdem häufig mit der Einführung eines Tools zur Prozessmodellierung verknüpft. An dieser Stelle sollen daher nur einige grundsätzliche Hinweise gegeben werden:

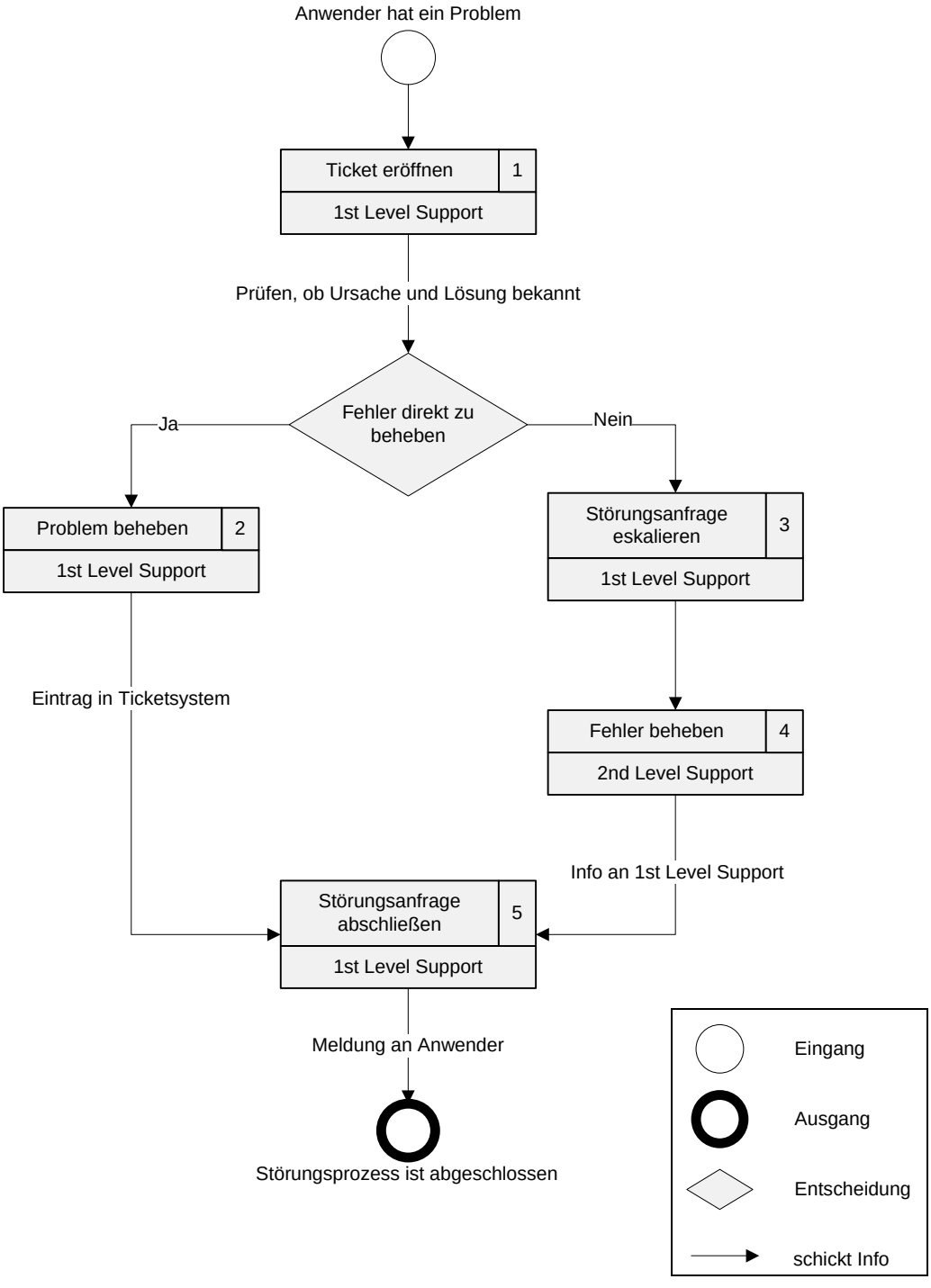


Abbildung 4.23: Beispielprozess in KSA-Notation

Wahl der Prozessnotation

EPKs bieten als quasi-standardisiertes Modellierungsmodell den Vorteil, dass Konventionen für die Prozessmodellierung im Unternehmen einfacher durchgesetzt werden können und diese allgemeingültig sind. Außerdem können erstellte Prozesse bei einer späteren Einführung eines Prozessmodellierungstools übernommen werden. Allerdings bedingt die Struktur der EPKs, dass sich komplexe Prozesse oder Arbeitsabläufe nur schwer darstellen lassen. Zum einen werden EPKs in diesen Fällen sehr lang, da für alle Funktionen dargestellt werden muss, durch welche Ereignisse sie initiiert werden, und zum anderen sind Verzweigungen und Schleifen nur schwer darstellbar.

Flussdiagramme sind im Gegensatz zu EPKs gut zur Darstellung komplexer Prozessabläufe geeignet. Die Prozessmodellierung mit Flussdiagrammen wird, weil sie weniger starren Regeln unterliegt, häufig als einfacher empfunden. Diese Darstellungsart ist somit zur Modellierung operativer Arbeitsabläufe meist besser geeignet als EPKs. Aus den beschriebenen Vor- und Nachteile beider Notationen lässt sich fast zwangsläufig ableiten, dass eine Kombination ein sinnvoller Weg sein kann. Während EPKs oder eEPKs zur Modellierung der Prozesse auf einer abstrakten Ebene eingesetzt werden, erfolgt die Darstellung der operativen Arbeitsabläufe in Form von Flussdiagrammen.

Zur Darstellung von Prozessen im Rahmen des Qualitätsmanagements kann auch die Verwendung der KSA- oder RACI-Notation sinnvoll sein. Zur Modellierung der operativen Arbeitsabläufe ist allerdings auch hier die Verwendung von Flussdiagrammen zu empfehlen.

Darstellungskonventionen

Unabhängig vom verwendeten Modellierungsmodell ist es sinnvoll verbindliche Richtlinien für die grafische Darstellung von Prozessen festzulegen und dabei die folgenden Aspekte zu regeln:

- Verwendung der grafischen Symbole (insbesondere bei Verwendung von Flussdiagrammen und eEPKs)
- Darstellung des Bearbeiters im Diagramm mittels Symbol oder durch Verwendung von Funktionsbändern
- Gliederungsfunktion. Hier gilt es festzulegen, ob nur Aktivitäten zu nummerieren sind oder beispielsweise auch Dokumente, Datenspeicher, Entscheidungen und Unterprozesse.

Die Bedeutung der Symbole muss in jedem Dokument in einer Legende dargestellt werden. Dies ist wichtig, um sicherzustellen, dass der Ersteller des Prozesses und der Anwender das Gleiche sehen, also das gleiche Verständnis über die verwendeten Symbole haben.

Detaillierungsgrad

Ein wichtiger und schwieriger Punkt ist der anzuwendende Detaillierungsgrad. Bei der Modellierung der Abläufe stellt sich meist die Frage, wie genau diese modelliert werden sollen. Einerseits möchte man eine möglichst genaue Modellierung um Mehrdeutigkeiten auszuschließen, andererseits möchte man die Modelle klein halten, um Übersichtlichkeit zu gewährleisten. An dieser Stelle kann nur auf die Ausgangsfrage verwiesen werden: Was ist der Einsatzzweck und wer ist die Zielgruppe? Der Detaillierungsgrad muss an dieser Frage ausgerichtet werden.

Hilfreich ist hierbei eine mehrstufige Vorgehensweise, d.h. eine Unterteilung in Haupt- und Unterprozesse und eine Verfeinerung einzelner Aufgaben in gesonderten Arbeitsabläufen. Eine Verfeinerung der Prozesse auf mehreren Ebenen ermöglicht es, alle Modelle einer Ebene möglichst gleich granular darzustellen und trotzdem einzelne Prozesse stärker zu verfeinern.

4.3.3.3 Arbeitshilfen

Arbeitshilfen sind alle Formen von Anleitungen und Beschreibungen, welche die in den Arbeitsabläufen benannten Tätigkeiten detaillieren. Hierbei kann es sich unter anderem um Folgendes handeln

- Arbeitsanweisungen (vielfach synonym als Arbeitsanleitungen bezeichnet)
- Checklisten
- Mustervorlagen
- Formulare
- Fragenkataloge

Inhalt der Arbeitshilfen Nimmt man beispielsweise den Arbeitsablauf „Einrichtung eines Clientarbeitsplatzes", so wäre es sinnvoll, dem Ausführenden der damit verbundenen Tätigkeiten eine Arbeitsanweisung zur Verfügung zu stellen, in der alle Arbeitsschritte (Aufstellen und Anschließen der Hardware, Installieren, Aufgaben nach der ersten Anmeldung) beschrieben sind. Zusätzlich benötigt der Mitarbeiter gegebenenfalls ein ausgefülltes Formular, in dem er alle Informationen findet, die für die individuelle Einrichtung des Rechners benötigt werden (Standort, Rechnername, zu verwendende Bodentankdose usw.). Hilfreich wäre außerdem eine Checkliste, in der er alle erledigten Arbeiten abhaken kann. Diese kann gleichzeitig als Arbeitsnachweis dienen und einem Verantwortlichen zur Unterschrift vorgelegt werden.

Beispiel „Einrichtung Clientarbeitsplatz"

Ein besonderes Augenmerk sollte auf die Arbeitsanweisungen gelegt werden. Hierbei handelt es sich typischerweise um Schritt-für-Schritt-Anleitungen. Einen Eindruck einer solchen Anleitung kann die nachstehende Abbildung vermitteln, die einen Ausschnitt aus einer Anleitung zur Benutzung von Scannern der Bibliothek der TU Chemnitz zeigt.

Besonders wichtig: Arbeitsanweisungen

Arbeitsanweisungen müssen als solche aus sich heraus, ohne Rückgriff auf Informationsquellen außerhalb der Prozessbeschreibung verständlich sein. Die einzelnen Schritte wiederum müssen die auszuführende Tätigkeit, die betroffenen Objekte sowie die jeweiligen Randbedingungen (z. B. Ortsangaben) enthalten.

Methode zur Entwicklung von Arbeitshilfen Die Bedeutung, aber auch der zeitliche Aufwand für die Erstellung geeigneter Arbeitshilfen darf nicht unterschätzt werden. Die wichtigste Frage, die es immer zu beantworten gilt, lautet daher: „Wie detailliert müssen die Arbeitshilfen sein?". Diese Fragestellung betrifft vor allem Arbeitsanweisungen.

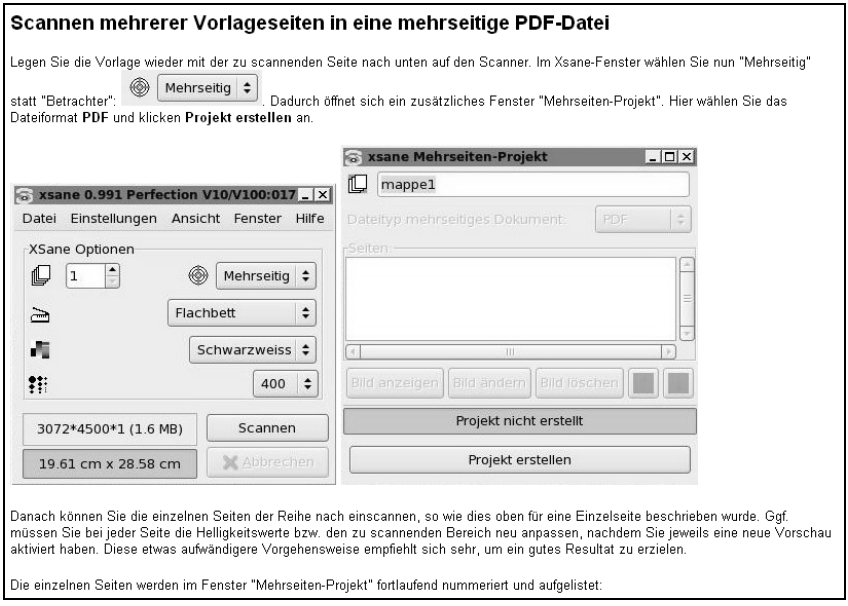


Abbildung 4.24: Beispiel einer detaillierten Arbeitsanweisung (Quelle: www.bibliothek.tu-chemnitz.de/service/arbeitsanleitungen)

Frage der Detaillierung

Grundsätzlich sollten Art und Umfang der Beschreibungen die Qualifikation und Kenntnisse der Ausführenden berücksichtigen. Erfordert beispielsweise eine Aufgabe die Ausführung durch eine Rolle mit einer Qualifikation als Microsoft Certified Engineer (MCSE), ist es wohl nicht erforderlich, eine Schritt-für-Schritt-Anleitung für das Einrichten eines Benutzerkontos in Active Directory beizufügen. Sehr wohl wird aber ein Formular benötigt, das alle Objektinformationen für den neu einzurichtenden Benutzer enthält. Auf der anderen Seite kann es erforderlich sein, die Einrichtung eines Clientarbeitsplatzes im Rahmen einer Migration sehr detailliert zu beschreiben, da für diese Aufgabe externe Mitarbeiter hinzugezogen werden, die ihre Tätigkeiten ausschließlich und streng nach den Vorgaben ausführen sollen.

hinweis

Hinter einer Arbeitsanweisung kann sich durchaus ein komplettes Installationshandbuch verbergen. Wer in diesem Buch bislang also die Behandlung von Installationshandbüchern oder Benutzerhandbüchern vermisst hat, findet diese hier wieder. Beim funktionalen Ansatz werden bekanntermaßen für jedes System ein allgemeines Benutzerhandbuch und ein Installationshandbuch erstellt und in den entsprechenden Ordnern für Installations- und Benutzerhandbücher abgelegt. Im Gegensatz dazu werden bei einer prozessorientierten IT-Dokumentation alle Beschreibungen, die typischerweise in den genannten Handbüchern zu finden sind, den damit verbundenen Prozesstätigkeiten zugeordnet.

Tipps zur Erstellung von Arbeitshilfen

Bei der Entwicklung von Arbeitshilfen ist es sinnvoll, in mehreren Schritten vorzugehen:

- Im ersten Schritt geht es darum, die Tätigkeiten genau zu definieren, sie gegenüber anderen Aufgaben abzugrenzen und ihre Ziele zu definieren.
- Im zweiten Schritt werden die zur Erfüllung der Tätigkeit notwendigen Arbeitsschritte beschrieben. Wichtig ist bei diesem Schritt die Einbeziehung aller mit der Aufgabe betrauten Mitarbeiter, denn diese kennen ihre Arbeitsabläufe in der Regel am besten. Das Einbeziehen der Mitarbeiter kann durch eine Befragung erfolgen. Dabei gilt es zu klären, welche Verfahrensschritte wann erfolgen, welche Informationsquellen zur Verfügung stehen, und wer formell beteiligt und wer informell einbezogen werden muss. Dabei ist es nicht unüblich, die Mitarbeiter mit der Erstellung der von ihnen später zu verwendenden Arbeitshilfen zu betrauen.
- Im dritten Arbeitsschritt sollte sich eine Testphase anschließen. Dabei werden im Produktiveinsatz die Arbeitshilfen von den Mitarbeitern getestet und bewertet. Die Erprobungsphase sollte zeitlich beschränkt, und die Rückmeldungen sollten systematisch ausgewertet werden. Die daraus resultierenden Anweisungen können dann in die Arbeitshilfen eingearbeitet und diese endgültig freigegeben werden.

hinweis

Um einen Endruck von den bisherigen theoretischen Ausführungen zur Prozessbeschreibung zu vermitteln, wird in Abschnitt 8.5 eine Beispiel-Prozessbeschreibung über alle Ebenen vorgestellt. Dies schließt einige Beispiele für Arbeitshilfen ein.

Gewählt wurde der Prozess „Umzug eines IT-Mitarbeiters“, bei dem ein bislang in einer dezentralen Außenstelle eingesetzter IT-Mitarbeiter in die Zentrale des für das Unternehmen zuständigen IT-Betriebs wechselt.

4.3.4 Toolunterstützte Prozessmodellierung am Beispiel von SemTalk

Grundsätzlich lassen sich zwei Gruppen von Modellierungstools unterscheiden:

Zwei Gruppen von Modellierungstools

- *Grafikorientierte Modellierungstools:* Das bekannteste und am häufigsten eingesetzte grafikorientierte Modellierungswerkzeug ist Microsoft Visio. Ein derartiges Programm stellt das Zeichnen von Diagrammen in den Mittelpunkt. Zur Erstellung von Prozessdiagrammen bieten sie in der Regel Vorlagen und stellen verschiedene Symbole zur Modellierung bereit. Alle gezeichneten Symbole werden ausschließlich als Grafikelement behandelt, nicht als Objekt. Daher können keine speziell auf das Prozessmanagement ausgelegten Funktionen bereitgestellt werden. Damit verbunden ist zwangsläufig, dass es keine Unterstützung oder Vorgaben hinsichtlich der Notation gibt.

- *Objektorientierte Modellierungstools:* Programme dieser Gruppe sind speziell auf die Modellierung von Prozessen ausgerichtet. Sie unterstützen die Modellierung, sodass diese zwingend einer definierten Notation folgt. Dadurch ist sichergestellt, dass alle Prozesse einheitlich beschrieben sind. Die Prozesse werden objektorientiert und nicht als Grafik gespeichert, was beispielsweise durchgängige Änderungen und das Erfassen der Abläufe in der dahinterliegenden Datenbank ermöglicht. Auch kann damit ein Prozess von verschiedenen Anwendern mit unterschiedlichen Rollen bearbeitet werden. Zu den bekanntesten Vertretern dieser Gruppe zählt das ARIS-Toolset.

Viele Unternehmen, die mit der Modellierung ihrer Prozesse beginnen, setzen zunächst Microsoft Visio als verfügbares Office-Tool ein. Dies ist gut möglich, da Visio sowohl für die EPK-Notation als auch für die Modellierung von Flussdiagrammen eine Reihe von Vorlagen mit den erforderlichen Symbolen bereitstellt. Doch mit der steigenden Anzahl an Prozessen werden auch die Nachteile der „Visio-Methode" deutlich:

Nachteile der „Visio-Methode"

- Die Durchsetzung von Standards (Darstellungssystematik, Namenskonventionen) für die Prozessdiagramme ist kaum möglich, sobald Prozesse von mehreren Mitarbeitern modelliert werden. Dies gilt insbesondere für die Darstellung von Flussdiagrammen.
- Nachträgliche Änderungen an den Prozessdiagrammen erfordern einen hohen manuellen Aufwand.
- Eine verteilte Modellierung durch unterschiedliche Rolleninhaber ist kaum darstellbar. Wenn diese stattfindet, werden häufig nur Teilprozesse modelliert und dokumentiert, da kein übergeordnetes Modell existiert, das das Abbilden der gesamten Prozesskette sicherstellt.
- Die Veröffentlichung der Prozesse und deren Aktualisierung wird nicht unterstützt, sodass viele Prozessdokumentationen zu „Schrankware" werden.
- Weiter fehlen Schnittstellen zu Programmen wie SAP und Biztalk, Simulationsmöglichkeiten und Möglichkeiten, um die Prozesse auszuwerten.

Die genannten Probleme sind typisch für grafikorientierte Modellierungswerkzeuge. Aufgrund der benannten Einschränkungen dieser Tools stellt sich daher die Frage nach den Alternativen. Grundsätzlich ist die Dokumentation von Prozessen ohne speziell dafür ausgelegte Programme kaum durchführbar.

Es gibt eine ganze Reihe von speziellen Programmen, die als Vertreter der zweiten Gruppe, die Erfassung, Dokumentation und die Optimierung von Prozessen unterstützen. Allerdings sind diese Anwendungen häufig sehr komplex und vom Anwender nur nach einer intensiven Einarbeitung nutzbar. Außerdem sind diese Tools nicht ohne Anpassungen einsetzbar; der Konfigurationsaufwand ist vielfach hoch.

Tool muss zum Unternehmen passen

Bei der Wahl der „richtigen" Prozessdokumentationslösung besteht die Schwierigkeit deshalb darin, zwischen Programmen wie Visio und Modellierungswerkzeugen wie ARIS, das für das eigene Unternehmen passende Programm zu finden. Diese Aufgabe muss unternehmensspezifisch entschieden werden und erfordert sorgfältige Analysen. Das vorliegende Buch kann daher keine allgemeingültige Bewertung verschiedener Anwendungen liefern.

Um aber auch für den Bereich der Prozessdokumentation zumindest ein Angebot im Bereich der Modellierungstools machen zu können, haben sich die Autoren das Programm *SemTalk* der Firma *Semtation* näher angesehen. Auch alle im Buch dargestellten Beispielprozesse wurden mit diesem Programm erstellt.

4.3.4.1 SemTalk im Überblick

Bei SemTalk handelt es sich um ein Programm zur Modellierung von Geschäftsprozessen, das zwar auf Microsoft Visio aufsetzt, die graphischen Möglichkeiten von Visio aber durch eine integrierte XML-Datenbank ergänzt und damit die typischen Schwächen grafikbasierter Werkzeuge adressiert.

Visiobasiert und trotzdem objektorientiert

Da SemTalk auf Microsoft Visio basiert, ist es im Prinzip genauso zu verwenden. Die Anwender finden eine vertraute Umgebung wieder, die sie mit wenig Schulungsaufwand nutzen können. Trotzdem arbeitet SemTalk objektorientiert und kann daher Funktionen anbieten, die die Erstellung von Prozessen deutlich vereinfachen, eine Standardisierung im Unternehmen ermöglichen und verschiedene Dokumentationsmöglichkeiten unterstützen. So wird beispielsweise die Konsistenz der Prozessmodelle bereits während ihrer Erstellung sichergestellt, und bei der Detaillierung von Arbeitsabläufen werden die erforderlichen internen Ein- und Ausgänge automatisch erstellt und verlinkt. Da außerdem alle Objekte miteinander verknüpft sind, sind diverse Auswertungen und Simulationen über alle Prozessebenen hinweg möglich.

SemTalk erweitert Visio also nicht primär durch neue Symbole (engl. Shapes), sondern es hilft, Ordnung in die bestehenden Symbole zu bringen, indem nicht mehr jedes Symbol auf jedem Zeichenblatt verwendet und mit jedem anderen Symbol verbunden werden kann. Auch der manuelle Pflegeaufwand bei Änderungen ist aufgrund der Objektorientierung stark reduziert. Wird beispielsweise ein Objekt umbenannt, wird es auf allen Zeichenblättern aktualisiert.

Einsatz ohne Anpassungsaufwand möglich

Besonders hilfreich aber ist, dass die Konzeption von SemTalk einen sofortigen Einsatz ohne Anpassungsaufwand mit nur wenig Einarbeitungsaufwand ermöglicht, der in SemTalk vorhandene Funktionsumfang aber schrittweise erweitert werden kann. So können im ersten Schritt die Modellierer von der Konsistenzerhaltung profitieren, ohne ihre bisherige Arbeitsweise wesentlich umstellen zu müssen. SemTalk-Dokumente sind Visio-Dokumente ergänzt mit zusätzlichen Steuerdateien.

Später können dann Referenzmodelle entwickelt werden, die von dem Modellierer in anderen Modellen durch Import und gegebenenfalls Replikation genutzt werden können. Falls gewünscht, kann die verteilte Modellierung mit SemTalk bis hin zu unternehmensweiten Metamodellen ausgebaut werden.

hinweis

Nähere Informationen zu Systemanforderungen, Bezugsmöglichkeiten und Preisen der aktuellen Version können Sie dem Steckbrief zu SemTalk in Anhang D.3 entnehmen.

4.3.4.2 Arbeitsweise und wichtige Funktionen

SemTalk unterstützt verschiedene Methoden zur Prozessmodellierung wie BPMN, EPK, KSA und Flowcharts. Nach der Installation und dem ersten Start ist daher zunächst die gewünschte Modellierungsmethode auszuwählen:

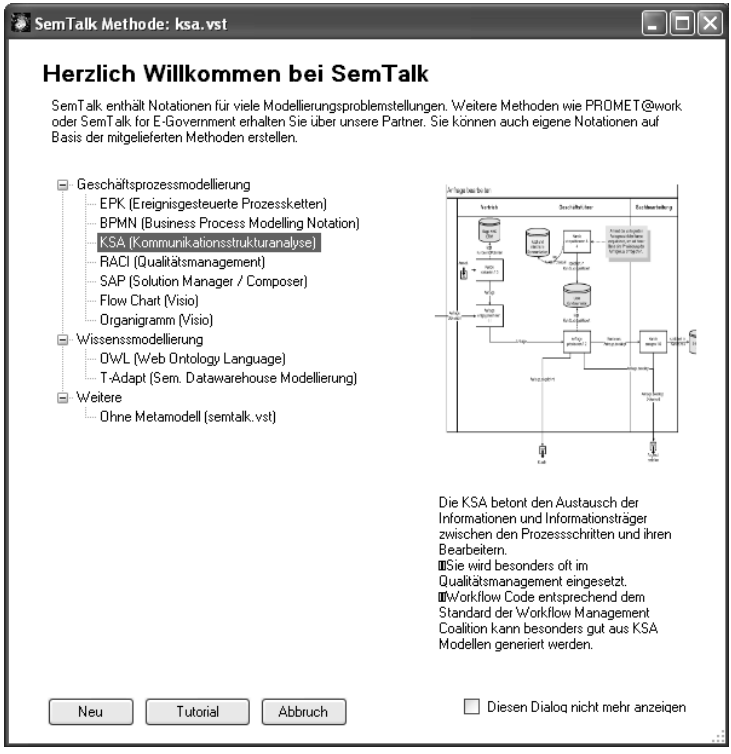


Abbildung 4.25: SemTalk- Willkommensdialogbox zur Auswahl der Modellierungsnotation

Die Modellierungsumgebung besteht aus dem *SemTalk Explorer* auf der linken Seite und aus der aus Visio bekannten Zeichenblatt-Oberfläche mit den zugehörigen vordefinierten Symbolen in den Objektvorlagen (Schablonen) auf der rechten Seite. Der SemTalk Explorer zeigt in einer Baumstruktur alle modellrelevanten Diagramme, Objekte und Relationen an und kann bei Bedarf über das Icon in der Symbolleiste oder über das Menü EXTRAS und die Option EXPLORER eingeblendet werden. Standardmäßig wird ein leeres Diagramm geöffnet, in dem sofort modelliert werden kann.

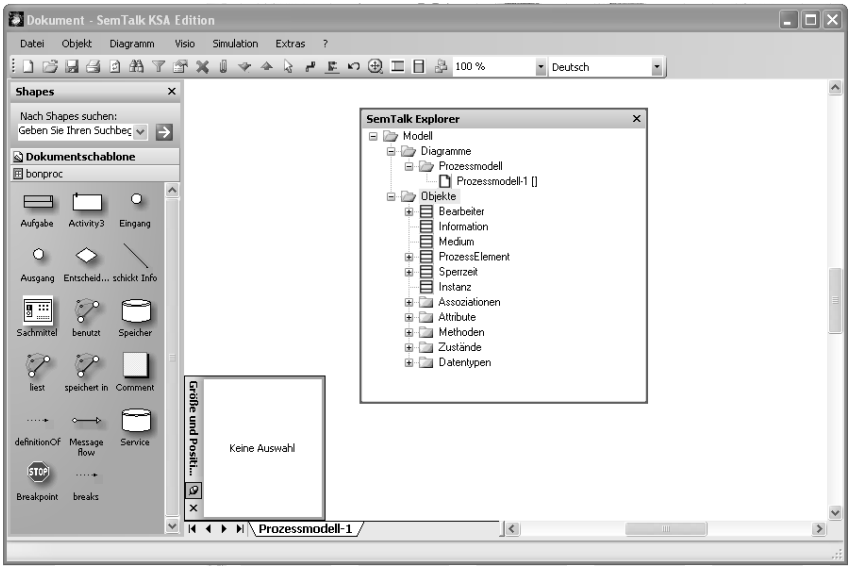


Abbildung 4.26: Die Arbeitsoberfläche von SemTalk

Auf der beigefügten CD-ROM befindet sich eine mit SemTalk erstellte Prozessbeschreibung für einen Beispielprozess im HTML-Format. Zur Erstellung dieser Dokumentation wurden zwei Funktionen von SemTalk angewendet, die überaus nützlich sind und daher hier kurz vorgestellt werden sollen.

Verfeinern von Objekten

Mit dem Befehl VERFEINERN im Kontextmenü ist es möglich, Hauptprozesse zu erstellen und einzelne Prozessschritte in einem Unterprozess detaillierter zu erläutern. Die Verfeinerung ist standardmäßig immer ein Diagramm vom selben Diagrammtyp. Es ist aber auch möglich, zwei Modelle mit unterschiedlicher Notation zu verlinken. Mit der Funktion der EXTERNEN VERFEINERUNG werden Prozesse aus verschiedenen SemTalk-Dateien verbunden.

Zwischen den so verlinkten Objekten ist eine Art Hyperlink-Navigation möglich. Verfeinerte Objekte erkennt man am unterstrichenen Namen im Diagramm. Außerdem ist das Ergebnis einer Verfeinerung auch im Diagramm-Explorer ersichtlich.

Berichte und Dokumentation

Aus Sicht dieses Buches sind natürlich die Möglichkeiten der Dokumentation zu betrachten. SemTalk bietet eine Reihe von Exportmöglichkeiten:

- *Microsoft PowerPoint:* Generierung einer Folienpräsentation aus den ausgewählten Diagrammen.
- *Microsoft Word:* Generierung eines Dokuments mit auswählbaren Prozessdiagrammen und Tabellen. Die tabellarischen Erläuterungen werden aus den Informationen generiert, die als Informationen den einzelnen Prozessschritten hinzugefügt wurden.

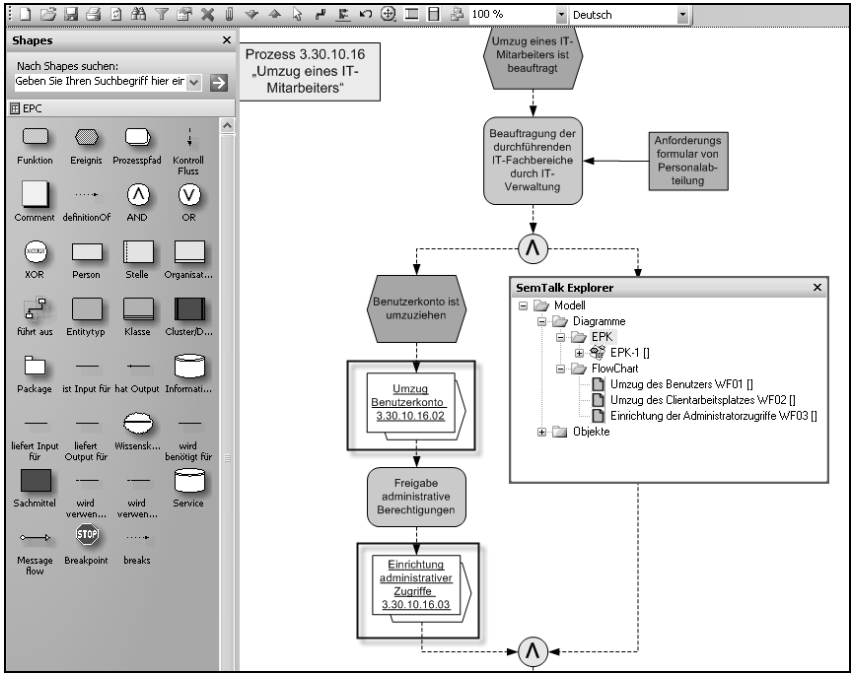


Abbildung 4.27: Unterprozesse können durch Verfeinern mit dem Hauptprozess verlinkt werden.

- *Microsoft Excel:* Exportmöglichkeiten von SemTalk nach Excel und umgekehrt.
- *Microsoft Project:* Schnittstelle für den Export von Modellen aus KSA, EPK und verwandten Notationen.
- *Microsoft Infopath:* Export von SemTalk-Objekten als Infopath-Objekte

Darüber hinaus ist die Erstellung einer Dokumentation im HTML-Format möglich. Sofern Diagramme durch Verfeinerungen verknüpft wurden, kann in der HTML-Ansicht bequem zwischen diesen navigiert werden. Die generierte HTML-Seite enthält auf der linken Seite einen Modellexplorer ähnlich dem SemTalk-Explorer und entsprechende Fenster für Zusatzinformationen und Funktionen. Auf der rechten Seite ist jeweils das aktuelle Diagramm als Bild (im JPEG-Format) zu sehen. Durch das Markieren eines Objekts werden im linken Eigenschaftsfenster seine Eigenschaften und Attribute angezeigt.

cd-rom

Die nachstehende Grafik zeigt einen Ausschnitt aus der Prozessbeschreibung eines Beispielprozesses im HTML-Format, die sich auf der beigefügten CD-ROM befindet. Für eine vollständige Anzeige der Beispiele wird wegen der integrierten ActiveX-Komponenten der Internet Explorer benötigt. Die Anzeige mit anderen Browsern ist nur eingeschränkt möglich.

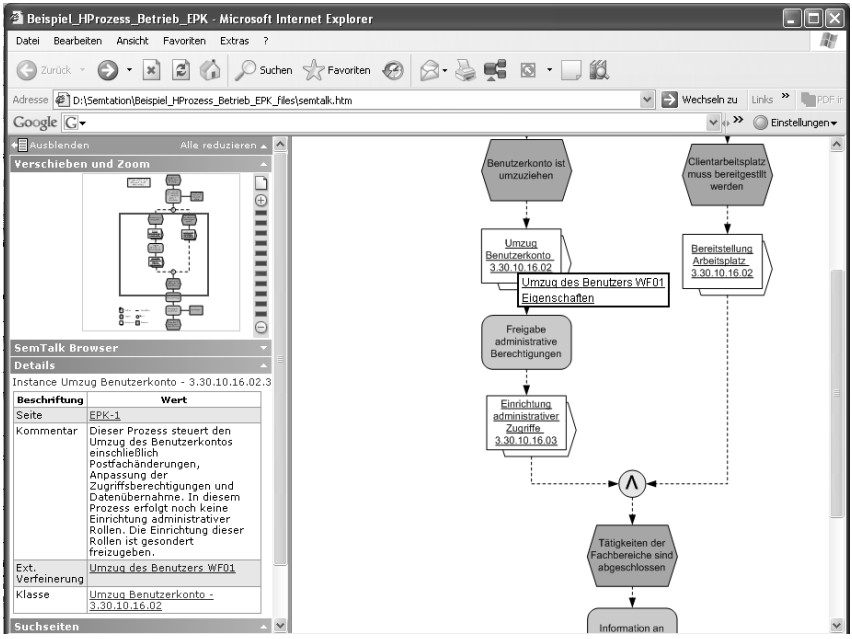


Abbildung 4.28: Abbildung 4.28:Die von SemTalk generierte HTML-Dokumentation erlaubt eine einfache Navigation durch Zoomen und Verlinkungen.

hinweis

Auf der Website der Firma Semtation [SEM] findet sich eine Reihe von Dokumentationen zu den Funktionen von SemTalk und zu den Nutzungsmöglichkeiten der verschiedenen Prozessmodelle. Dort können Informationen zu den weiteren Möglichkeiten von SemTalk bezogen werden.

4.4 Fazit

Nicht selten ist die erste Reaktion bei einem Blick auf die dargestellten Anforderungen und den Umfang der IT-Betriebsdokumentation ein zweifelnder Blick verbunden mit der Frage: Wer soll eigentlich all diese Dokumente erstellen und pflegen?

Dabei werden allerdings zwei Aspekte übersehen: Zum einen stellt die hier dargestellte Betriebsdokumentation sozusagen ein Komplettangebot dar, das in diesem Umfang wohl nur in sehr großen IT-Umgebungen umzusetzen ist. Viele Unternehmen werden einige der aufgeführten Dokumente gar nicht oder zumindest nicht so detailliert benötigen. Wird beispielsweise keine SAN-Infrastruktur oder kein Print-Cluster eingesetzt, können die entsprechenden Dokumente beruhigt von der Liste gestrichen werden.

Zum anderen steigt mit zunehmender Größe des IT-Betriebs zwangsläufig auch der Grad für den Einsatz von Automatisierungslösungen. Damit wird die Dokumentation zwar zunehmend komplexer, der Aufwand aber steigt durch entsprechende Toolunterstützung wahrscheinlich nicht in gleichem Maße an.

Unabhängig von der Größe des IT-Betriebs aber sollte das Ziel eine prozessorientierte IT-Dokumentation sein, die wiederum in einen Bereich *Systemdokumentation* und einen Bereich *Prozessdokumentation* unterteilt ist. Die Gründe für eine Prozessorientierung wurden ausführlich dargelegt. Und auch die Schwächen der klassischen, an den Systemen ausgerichteten Betriebsdokumentation wurden erörtert.

Auch wenn dieser Ansatz ggf. Umstellungen in der Herangehensweise erfordert und u. U. auf Akzeptanzprobleme stößt, lohnt es sich ihn zu verfolgen. Der beschriebene Ansatz ermöglicht den Aufbau einer IT-Betriebsdokumentation, die auch zukünftigen Anforderungen gewachsen ist.

5 Dokumentation für den Notfall

Die Vorhaltung eines funktionierenden Notfallmanagements ist im Falle eines Falles die notwendige Voraussetzung für das Überleben eines Unternehmens. Und die Pflege einer IT-Notfalldokumentation dient der Einhaltung der unternehmensbezogenen gesetzlichen Anforderungen.

Aber das Erstellen und die Pflege einer IT-Notfalldokumentation sollte nicht nur als lästige Pflicht betrachtet werden. Tritt ein Notfall ein, ist die Aufregung meist groß; und die Gefahr, die Situation durch fehlerhaftes Verhalten zu verschlimmern, darf nicht unterschätzt werden. Um in einer Notfallsituation handlungsfähig zu bleiben, muss jeder wissen, was zu tun ist. Das bedeutet: Es müssen entsprechende Notfallpläne vorhanden sein und diese müssen an den aktuellen Prozessen ausgerichtet sein. Angesichts der heutigen Komplexität der IT-Infrastruktur genügt es nicht, aus irgendeinem Tresor ein verstaubtes Word-Dokument hervorzuholen, auf dem „Notfallhandbuch" steht und das vor drei Jahren zuletzt aktualisiert wurde. Dass Revisoren und Wirtschaftsprüfer bei einer Prüfung mittlerweile auf ein Notfallkonzept, Notfallpläne und Notfalltestdokumente bestehen, hat daher auch ganz praktische Gründe.

5.1 IT-Notfallmanagement im Überblick

» Notfallmanagement wird auch als *Business Continuity Management* (*BCM*) oder *Betriebliches Kontinuitätsmanagement* bezeichnet. «

Mit der ständig größer werdenden Abhängigkeit der Geschäftsprozesse von der IT-Unterstützung wachsen auch die Anforderungen an einen wirksamen Schutz und damit die Bedeutung eines proaktiven Notfallmanagements. Dessen vorrangige Aufgabe ist es, Prozesse zu implementieren, um auf Schadensereignisse angemessen zu reagieren und nach einem Notfall die Geschäftstätigkeiten so schnell wie möglich wieder aufnehmen zu können. Im Vordergrund steht hierbei die Absicherung der wirtschaftlichen Existenz eines Unternehmens.

Die Aufgaben des Notfallmanagements können grundsätzlich in zwei Bereiche unterteilt werden:

- Notfallvorsorge
- Notfallbewältigung

Es ist daher sinnvoll, auch die Notfalldokumentation entsprechend zu gliedern und in das *Notfallkonzept* und das *Notfallhandbuch* zu unterteilen. Während alle für die Notfallvorsorge benötigten Dokumente dem Notfallkonzept zugeordnet werden können, umfasst das Notfallhandbuch (manchmal auch als *Krisenmanagement-Handbuch* oder *Kontinuitätspläne* bezeichnet) die Gesamtheit aller für die Notfallbewältigung benötigten Dokumente, was die Notfallpläne mit Beschreibungen aller erforderlichen Maßnahmen und Aktionen nach dem Eintritt eines Notfalles und die Testdokumente beinhaltet. Das Notfallhandbuch wird ausführlich im anschließenden Abschnitt 5.2 vorgestellt.

hinweis

In der Literatur wird, wie sollte es auch anders sein, eine saubere Trennung zwischen *Notfallhandbuch* und *Notfallkonzept*, nicht immer eingehalten. Da wird munter von einem Notfallkonzept gesprochen, obwohl das Notfallhandbuch gemeint ist und umgekehrt. Hier bleibt nichts anderes übrig, als aus dem jeweiligen Kontext zu schließen, wovon die Rede ist.

Im vorliegenden Buch werden die Begriffe in der zuvor genannten Definition verwendet:

Notfallvorsorge = Notfallkonzept;
Notfallbewältigung = Notfallhandbuch.

5.1.1 Definition eines Notfalls

Bevor mit der Erstellung des ersten Notfallplanes begonnen werden kann, muss die Frage beantwortet werden, was überhaupt ein Notfall ist. Denn nicht jede Unterbrechung von Prozessen ist auch gleich ein Notfall. Zu den Aufgaben des Notfallmanagements gehört daher die Festlegung, wann ein Notfall vorliegt.

Störungen gehören zum IT-Regelbetrieb. Hierzu zählen vergessene Benutzerkennwörter genauso wie beispielsweise Fehler bei der Active Directory-Replikation. Dies als Notfall zu bezeichnen, wäre wohl übertrieben.

Wann wird aus der Störung ein Notfall?

Gemäß BSI- Standard 100-4 ist eine *Störung*

> *„eine Situation, in der bestimmte Bereiche, Prozesse oder Ressourcen einer Behörde oder eines Unternehmens nicht wie vorgesehen funktionieren, so dass hierdurch Schäden entstehen, die aber als gering eingestuft werden, beispielsweise da sie im Verhältnis zum Gesamtjahresergebnis eines Unternehmens zu vernachlässigen sind oder die Aufgabenerfüllung nur unwesentlich beeinträchtigen. Störungen werden durch die im allgemeinen Tagesgeschäft integrierte Störungsbehebung beseitigt."*

Von einer Störung grenzt BSI einen *Notfall* folgendermaßen ab:

> *„Ein Notfall ist eine Situation, in der wesentliche Bereiche, Prozesse oder Ressourcen einer Behörde oder eines Unternehmens nicht wie vorgesehen funktionieren und bei denen innerhalb der geforderten Zeit deren Verfügbarkeit nicht wieder hergestellt werden kann. Es entstehen hohe bis sehr hohe Schäden, die sich signifikant und in nicht akzeptablen Rahmen auf das Gesamtjahresergebnis eines Unternehmens oder die Aufgabenerfüllung einer Behörde auswirken. Notfälle sind nicht mehr im allgemeinen Tagesgeschäft abzuwickeln, sondern erfordern eine gesonderte Notfallbewältigungsorganisation" [BSI-1004].*

Vor allem zwei Punkte weisen demnach einen Notfall aus: Eine erhebliche Schadenshöhe mit Auswirkungen auf das Gesamtunternehmen und das Erfordernis einer gesonderten Organisation zur Bewältigung des Notfalls.

Notfall kontra Krise und Katastrophe

BSI geht im Standard 100-4 an dieser Stelle noch einen Schritt weiter, indem hier zusätzlich zwischen Notfall, Krise und Katastrophe unterschieden wird. Demnach handelt es sich bei einer *Krise* um eine Eskalationsstufe des Notfalls, bei der die Existenz des Unternehmens und/oder das Leben und die Gesundheit von Personen gefährdet sind. Im Gegensatz zur *Katastrophe* kann die Krise aber, zumindest größtenteils, innerhalb der Institution selber behoben werden, während sich eine Katastrophe als zeitlich und örtlich nicht begrenztes Ereignis darstellt, dessen Behebung nicht im Einflussbereich des Unternehmens liegt.

hinweis

Inwiefern eine so detaillierte Unterscheidung sinnvoll bzw. notwendig ist, kann nur unternehmensspezifisch entschieden werden. Hinsichtlicht formaltechnischer Anforderungen an die Dokumentation ist sie von untergeordneter Bedeutung.

Ein Notfall im IT-Bereich tritt im Verständnis dieses Buches immer dann ein, wenn innerhalb einer fest definierten Zeit eine Wiederherstellung der Verfügbarkeit eines unternehmenskritischen Dienstes nicht gegeben ist und daraus ein das Unternehmen bedrohender Schaden droht oder eintritt.

5.1.2 Vorgaben für das Notfallmanagement

Kein Bereich der IT und damit der IT-Dokumentation ist durch Standards und dazugehörende Literatur so gut abgedeckt wie das Notfallmanagement, wozu vor allem auch das BSI beiträgt. Dies kann natürlich eine große Hilfe darstellen. Es ist daher sinnvoll, die Ausprägungen und die Anforderungen einiger Standards zu kennen.

5.1.2.1 Notfallmanagement gemäß BSI

Möchte man das Thema Notfallmanagement und Notfallhandbuch im eigenen Unternehmen angehen, führt sicherlich kein Weg an den Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) vorbei.

BSI-Standard 100-4 Notfallmanagement

Wie bereits in Abschnitt 1.2.3 ausgeführt wurde, legt das BSI mit dem noch nicht offiziell vorliegendem Standard 100-4 ein wichtiges Regelwerk für den Aufbau und die Dokumentation eines Notfallmanagements vor. Hier wird ein systematischer Weg aufgezeigt, um bei Notfällen der verschiedensten Art adäquat und effizient reagieren und die wichtigen Geschäftsprozesse schnell wieder aufnehmen zu können. Im Vordergrund steht hierbei die Vermeidung von Notfällen und die Minimierung von Schäden in einem Notfall.

Das ehemalige IT-Grundschutzhandbuch gibt es in der bisherigen Form nicht mehr.

Der Begriff „IT-Grundschutz" wurde vorrangig vom BSI geprägt und bezeichnet hier die Standardsicherheitsmaßnahmen für typische IT-Systeme. Hierfür bietet das BSI eine Sammlung von „Kochrezepten" für definierte Schutzniveaus an. Als Bestätigung für das erfolgreiche Umsetzen des Grundschutzes wird vom BSI ein Grundschutz-Zertifikat vergeben.

Noch immer verankert mit dem Begriff *Grundschutz* ist das *IT-Grundschutzhandbuch* des BSI. Dieses aber heißt seit der Version 2005 *IT-Grundschutz-Kataloge* und ist in verschiedenen Bereiche umstrukturiert worden. Im Vordergrund stand hierbei die Hinwendung zu einem prozessorientierten Ansatz – weg von der zuvor angewandten funktionsorientierten Betrachtung. Dies beinhaltet auch, dass die Beschreibungen der Grundschutz-Vorgehensweisen und die IT-Grundschutz-Kataloge getrennt wurden. Die IT-Grundschutz-Kataloge beinhalten nun die Baustein-, Maßnahmen- und Gefährdungskataloge, wohingegen Vorgehensweisen nach IT-Grundschutz, Ausführungen zum IT-Sicherheitsmanagement und zur Risikoanalyse bei den *BSI-Standards* zu finden sind.

Außerdem wurden zahlreiche einzelne Gefährdungen und Maßnahmen an neue technische Entwicklungen, neue Bedrohungsszenarien und neue Entwicklungen in der IT-Sicherheit angepasst. Außerdem wird das ganzheitliche Risikomanagement stärker als bisher in den Fokus gestellt [BSI].

Erforderliche Dokumente

Und auch wenn der BSI-Standard 100-4 noch keine offizielle Gültigkeit hat, bietet er bereits wichtige Anhaltspunkte. In der Entwurfsfassung wird die Notwendigkeit zur Erstellung eines Notfallhandbuches festgelegt. In diesem Zusammenhang werden unter anderem folgende Dokumente gefordert:

- Leitlinie zum Notfallmanagement
- Bericht der Business Impact-Analyse
- Bericht der Risikoanalyse
- Notfallvorsorgekonzept
- Notfallhandbuch inkl. Geschäftsfortführungsplänen
- Melde- und Eskalationswege
- Übungskonzept, Übungspläne und Übungsanlagen

Business Impact Analyse

Mit dem Standard 100-4 führt BSI die sogenannte *Business Impact-Analyse (BIA)* ein. Eine Business Impact-Analyse beinhaltet die Sammlung und Identifizierung von Prozessen und Funktionen innerhalb eines Unternehmens, um die den Prozessen zugrundeliegenden Ressourcen zu erfassen und wechselseitige Abhängigkeiten zwischen den Prozessen aufzuzeigen. Damit können die Auswirkungen bei Ausfällen von Prozessen und die benötigten Wiederanlaufzeiten aufgedeckt werden.

Welche Rolle der Business Impact-Analyse bei der Notfallvorsorge spielt, wird nachstehend noch ausgeführt.

5.1.2.2 Notfallmanagement gemäß ITIL

Wichtige Hinweise zum Notfallmanagement liefert auch ITIL. Bei ITIL handelt es sich um eine Verfahrensbibliothek, die Methoden für die Planung und Steuerung von IT-Services beschreibt (siehe hierzu auch Abschnitt 1.3.1).

Notfallmanagement = Continuity Management

Das Notfallmanagement ist bei ITIL durch das *IT Service Continuity Management (ITSCM)* beschrieben. Zielsetzung von ITSCM ist es, dass in einer Notfallsituation der Betrieb, also die Leistungserbringung, aufrechterhalten bleibt oder entsprechend wiederhergestellt wird. Hierzu müssen Risikoanalysen und für die zu definierenden Notfallsituationen spezifische Notfallpläne erstellt werden.

Gemäß ITIL muss für jedes neue IT-Verfahren bereits im Vorfeld festgelegt werden, welche Eskalationsvorgänge in Störfällen einzuleiten sind. Geregelte Prozesse müssen hierbei sicherstellen, dass alle Maßnahmen ermittelt und dokumentiert werden und auch von jedem nachgelesen werden können. Auch die Service- und Reaktionszeiten, innerhalb derer eine Störung bearbeitet werden muss, sind wesentliche Bestandteile eines solchen Dokuments.

hinweis

Eine gute Einführung in das Thema ITIL und Informationssicherheit einschließlich einer Gegenüberstellung von ITL und IT-Grundschutz stellt das BSI mit seiner Veröffentlichung „ITIL und Informationssicherheit – Möglichkeiten und Chancen des Zusammenwirkens von IT-Sicherheit und IT-Servicemanagement unter dem folgenden Link zur Verfügung: [BSI-ITIL]

Allerdings handelt es sich um ein Dokument aus dem Jahre 2005, sodass die neueren *Standards* nicht berücksichtsichtig sind.

5.1.2.3 Notfallmanagement gemäß ISO 20000

Die ISO 20000 ist eine speziell auf das IT-Servicemanagement ausgerichtete Norm und wurde im Jahr 2005 veröffentlicht (nähere Erläuterungen zu den ISO-Normen finden Sie in Abschnitt 1.2.2).

Im Gegensatz zu ITIL zertifizierbar

Im Gegensatz zu ITIL aber, das keinen Standard darstellt, sind die Prozesse des IT-Servicemanagements nach ISO 20000 international anerkannt zertifizierbar. Die Anforderungen an die IT-Notfallvorsorge beschreibt dort der Abschnitt 6.3, „Service Continuity and Availability Management".

Hinsichtlich des Notfallmanagements müssen gemäß BSI für eine Zertifizierung nach ISO 20000 die folgenden acht Punkte dokumentiert werden:

- Business plan requirements
- Annual reviews
- Re-testing plans
- Impact of changes
- Unplanned non-availability
- Availability of resources
- Business needs
- Recording tests

Auch wenn die verschiedenen Standards unterschiedliche Ausprägungen haben, lassen sich doch aus allen gemeinsame Anforderungen an die zu erstellenden Dokumente ableiten. Diese sind Gegenstand der nachfolgenden Kapitel.

5.1.3 Dokumente für die Notfallvorsorge

Alle für die Notfallvorsorge benötigten Dokumente können dem Notfallkonzept zugeordnet werden. Da das Notfallkonzept als Richtliniendokument übergeordneten Charakter hat, empfiehlt es sich, dieses bei den Rahmendokumenten einzugliedern.

Aufgaben der Notfallvorsorge

Die Inhalte des Notfallkonzepts sind durch die Aufgaben der Notfallvorsorge vorgegeben, zu denen im Wesentlichen die folgenden gehören:

- Festlegung von Regeln, wann ein Notfall vorliegt
- Identifizierung der kritischen IT-Prozesse (Business Impact-Analyse)
- Analyse der möglichen Ausfallfolgen für die Prozesse (Risikoanalyse)
- Festlegung der maximalen Ausfalldauer, nach der der Betrieb nach einem Ausfall wieder gewährleistet sein muss

Wie diese Aufstellung bereits zeigt, kann die Notfallvorsorge nicht als ein unabhängige Aufgabe betrachtet werden, sondern ist eher als ein Teil des Risikomanagements und des Sicherheitsmanagements zu behandeln. Aufbauend auf den im Rahmen der Risikoanalyse erarbeiteten Risikobewertungen und den Verfügbarkeitsanforderungen ist das Ergebnis der Notfallvorsorge schließlich als ein Teil der Risikosteuerungsmaßnahmen zu sehen.

Analysen bilden die Basis

Die Business Impact-Analyse und die Risikoanalyse bilden daher eine wesentliche Basis des Notfallmanagements. Auf diesen beiden Analysen aufbauend kann im Notfallkonzept festgelegt werden, was ein Notfall ist und wie mit den identifizierten Risiken umgegangen werden soll.

5.1.3.1 Business Impact-Analyse und Risikoanalyse

Um Notfällen wirksam begegnen zu können ist es zunächst wichtig, mögliche Abhängigkeiten und Bedrohungen zu identifizieren und zu bewerten. So macht es beispielsweise keinen Sinn, für einen Webshop den Ausfall des Faxservers als Notfall zu deklarieren, sofern keine unternehmenskritischen Prozesse davon abhängen. Der Ausfall der unternehmenseigenen Webservers ist hier aber durchaus als unternehmenskritisch einzustufen.

Business Impact-Analyse

Die Prozesse eines Unternehmens sind logisch miteinander verknüpft. Dies gilt insbesondere für die IT-Prozesse, denn kaum ein Geschäftsbereich kommt heute ohne IT-Unterstützung aus. Genau diese – oft unterschätzten – Abhängigkeiten können in einer Business Impact-Analyse (BIA) erfasst und dargestellt werden. Dies wiederum ermöglicht es, die kritischen Systeme zu identifizieren und zu priorisieren sowie Auswirkungen bei Ausfällen von Prozessen und die benötigten Wiederanlaufzeiten zu beschreiben. Hierzu umfasst die Business Impact-Analyse im Wesentlichen die folgenden Arbeitschritte.:

- Ermittlung und Auflistung aller relevanten Geschäftsprozesse
- Identifizierung kritischer Prozesse
- Ermittlung von kritischen Ausfallzeiten und realisierbaren Wiederanlaufzeiten bzw. Wiederbeschaffungszeiten
- Ermittlung von Verfügbarkeitsanforderungen für die eingesetzten Komponenten
- Entwicklung von Ausfallszenarien
- Dokumentation der Ergebnisse als Grundlage für die Ausarbeitung der Notfallpläne

Auf Unternehmensebene durchzuführen

Wie die Auflistung der Aufgaben zeigt, müssen in eine BIA alle Geschäftsprozesse eines Unternehmens einbezogen werden. Das heißt, es handelt sich hierbei um eine Aufgabe auf Unternehmensebene, weshalb die dabei entstehenden Dokumente auch nicht der IT-Dokumentation zuzuordnen sind. Da aber die Ergebnisse der Analyse die Grundlage der im Notfallhandbuch aufzunehmenden Prozesse bilden, ist es sinnvoll, die Ergebnisdokumente in das Notfallkonzept in Kopie einzufügen. Dies entspricht auch den Anforderungen des BSI, wonach die Berichte der Business Impact-Analyse und der Risikoanalyse Bestandteil des Notfallhandbuches sein sollten.

Nachdem mit Hilfe einer Business Impact-Analyse alle kritischen Prozesse ermittelt wurden, kann für diese eine Risikoanalyse durchgeführt werden. Die Risikoanalyse im Kontext des Notfallmanagements dient dazu, die Gefährdungen zu identifizieren und darauf ausgerichtete Notfallpläne zu entwickeln.

Risikoanalyse in jedem Fall erforderlich

Wie bereits bei den Erläuterungen zu den Rahmendokumenten ausgeführt wurde, wird eine Risikoanalyse ohnehin im Kontext der Erstellung und Pflege eines Risikohandbuches bzw. des IT-Sicherheitskonzepts benötigt. Schließlich fordert nicht nur das *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)*, bestehende Risiken aufzuzeigen. Während früher das Risikohandbuch vornehmlich aus kaufmännischer Sicht für die Kernprozesse erstellt wurde, wird deshalb heute, zumindest in großen Unternehmen, von der IT ein eigenes Risikohandbuch verlangt. Und wo dieses fehlt, sollte eine Riskoanalyse im IT-Sicherheitskonzept verankert sein.

5.1.3.2 IT-Notfallkonzept

In den vorstehenden Abschnitten wurde mehrfach auf das Notfallkonzept verwiesen. Als übergeordnetes Regelwerk beschreibt dieses Strategien und Vorgaben für alle Aktivitäten der Notfallvorsorge. Alle Maßnahmen und Tätigkeiten, hingegen die zur eigentlichen Bewältigung eines Notfalls beitragen, sind im Notfallhandbuch zu beschreiben.

Inhalt des Notfallkonzepts

Im Notfallkonzept sollten unter anderem die folgenden Punkte behandelt werden:

- Definitionen und Abgrenzung von Notfällen
- Geltungsbereich für das Notfallmanagement
- Verantwortlichkeiten für die Notfallvorsorge und die Notfallbewältigung
- Notfallorganisation
- Zugrunde liegende Vorgehensmodelle für die Notfallvorsorge und die Notfallbewältigung
- Regeln für den kontinuierlichen Verbesserungsprozess des Notfallmanagements

Was genau im Notfallkonzept geregelt wird, obliegt natürlich dem Unternehmen und ist von diesem festzulegen.

Rolle des Notfallbeauftragten

Das BSI ordnet der Rolle des *Notfallbeauftragten* alle Aktivitäten zur Steuerung der Notfallvorsorge zu. Demzufolge ist dieser für die Erstellung, Umsetzung und Pflege des Notfallmanagement-Prozesses sowie der zugehörigen Dokumente und Regelungen verantwortlich. In seiner Verantwortung liegen auch die Änderungen jeglicher Notfalldokumentationen wie beispielsweise der Notfall- oder Wiederherstellungspläne.

In jedem Fall ist es erforderlich, die notwendigen Rollen sowohl für die Notfallvorsorge als auch für die Notfallbewältigung zu definieren. Die Dokumentation der Rollen kann ebenfalls im Notfallkonzept erfolgen. Wird im Unternehmen aber ein Rollenkonzept gepflegt, sollten dort auch die Rollen des Notfallmanagements definiert werden (eine Beschreibung dieses Rahmendokuments finden Sie in Abschnitt 3.2.7).

hinweis

In der Literatur wird manchmal zwischen *Notfallkonzept* und *Notfallvorsorgekonzept* unterschieden. BSI beispielsweise definiert das Notfallvorsorgekonzept als eigenständigen Teil des Notfallkonzepts. Diese Unterscheidung ist zwar darstellbar, in der Praxis ist eine Abgrenzung aber häufig schwierig. Daher wird im vorliegenden Buch ausschließlich das Notfallkonzept als Planungsdokument des Notfallmanagements betrachtet.

Abschließend zeigt die nachstehende Grafik die am Notfallmanagement beteiligten Rahmendokumente und ihre Beziehungen.

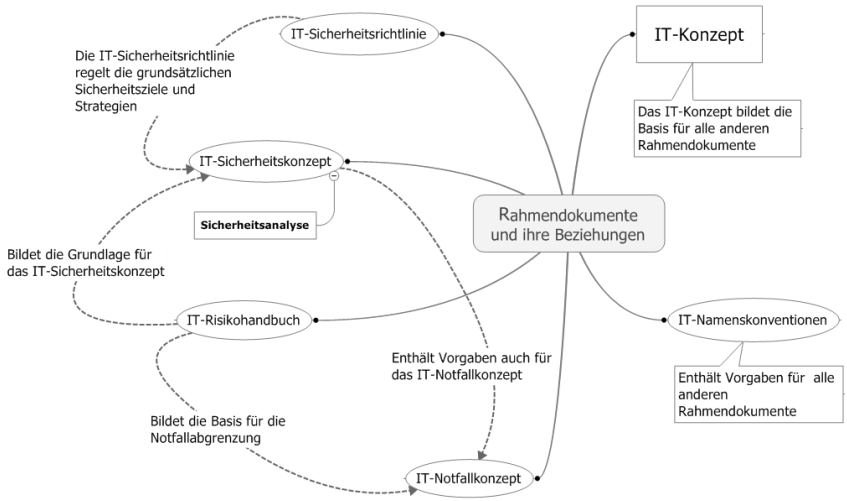


Abbildung 5.1: Sicherheitsrelevante Rahmendokumente und ihre Beziehungen

5.2 Aufbau des IT-Notfallhandbuches

Zu den in der Praxis wichtigsten Dokumenten gehört sicherlich das Notfallhandbuch.

Abhängig von der Art und der Branche eines Unternehmens genügt es aber nicht mehr, „Standard-Notfälle" wie Brand- oder Wasserschäden in einem klassischen Notfallhandbuch einfach nur zu beschreiben. So fordert der Gesetzgeber beispielsweise seit Januar 2007 für Finanzdienstleister mit den gültigen *Mindestanforderungen an das Risikomanagement (MaRisk, siehe Abschnitt 1.1.3.2)*, dass für alle kritischen Aktivitäten und Prozesse ein Notfallhandbuch vorliegen muss, das Geschäftsfortführungs- sowie Wiederanlaufpläne beinhaltet. Die *Geschäftsfortführungspläne* (engl. *Business Continuity Plan, BCP*) müssen gewährleisten, dass im Notfall zeitnah Ersatzlösungen zur Verfügung stehen und alle wichtigen Geschäftsprozesse nicht oder nur temporär unterbrochen werden. Außerdem müssen die Wiederanlaufpläne innerhalb eines angemessenen Zeitraums die Rückkehr zum Normalbetrieb ermöglichen. Die im Notfall zu verwendenden Kommunikationswege sind ebenfalls festzulegen.

Inhaltliche Strukturierung

Das Notfallhandbuch muss alle Informationen enthalten, um im Notfall die erforderlichen Maßnahmen zur Wiederaufnahme des unterbrochenen Betriebs durchführen zu können. Dazu muss es unter anderem die erforderlichen Systemdaten bereitstellen, Beschreibungen der im Notfall auszuführenden Prozesse enthalten, Melde- und Eskalationswege festlegen und Wiederanlaufpläne und Ausweichprozesse für den Notbetrieb beschreiben. Dabei muss es trotz der umfangreichen Anforderungen und der notwendigen Komplexität einfache und vollständige Handlungsanweisungen bieten. Der letzte Punkt ist deshalb besonders wichtig, damit in der Stresssituation eines Notfalls keine wichtigen Arbeitsschritte vergessen oder fehlinterpretiert werden.

Modularer Aufbau

Wie auch die beiden anderen Teile der IT-Dokumentation (IT-Betriebshandbuch und Projektdokumentation) sollte das Notfallhandbuch modular aufgebaut sein. Im Fall des Notfallhandbuches ist dies besonders wichtig, damit den verantwortlichen Mitarbeitern gezielt der für sie relevante Teil ausgehändigt werden kann.

Hinsichtlich der Gliederung gibt es keine Vorgaben. So kann die Struktur des Notfallhandbuches sowohl an den Phasen, also am zeitlichen Verlauf des Notfalls ausgerichtet werden als auch an den Notfallprozessen. Auch eine Gliederung, die sich an den Funktionen oder den Aufgaben orientiert, sowie eine Kombination der genannten Gliederungsansätze ist möglich. Letztendlich ist nur wichtig ist, dass das Notfallhandbuch alle notwendigen Informationen enthält und den Gegebenheiten und Anforderungen des Unternehmens entspricht.

Die nachstehend vorgestellte Gliederung zeigt ein Beispiel für eine überwiegende funktionsorientierte Gliederung:

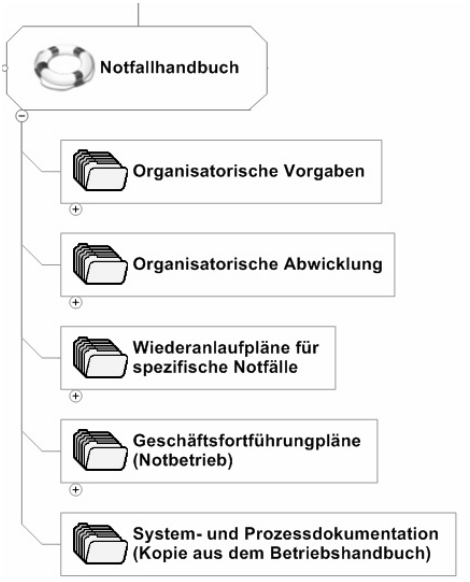


Abbildung 5.2: Mögliche Gliederung eines Notfallhandbuches (oberste Ebene)

Die genannten Bereiche werden im Folgenden näher vorgestellt.

cd-rom

Auf der beigefügten CD-ROM befindet sich eine mit MindManager erstellte Datei, die die im Folgenden vorgestellte Gliederung des Notfallhandbuches grafisch darstellt und eine Betrachtung der Einzelbereiche in einer Zusammenschau ermöglicht. Mit dem ebenfalls beigefügten MindManager Viewer kann diese Datei angesehen werden. Außerdem ist es möglich, Zweige zu öffnen, zu schließen und in sie hineinzuzoomen.

5.2.1 Organisatorische Vorgaben

Organisatorische Regelungen und Richtlinien sowie alle Kontaktdaten sollten in einem eigenen Bereich zusammengefasst werden. Dies umfasst mindestens die in der Abbildung 5.3 dargestellten Punkte

Wichtig ist die Nennung aller, die im Notfall Verantwortung übernehmen. Sofern ein IT-Rollenkonzept gepflegt wird und dieses auch die Notfall-Rollen beschreibt, können die betreffenden Rollen mit einem Verweis auf das Rollenkonzept aus diesem übernommen werden. Wichtig ist in diesem Fall, dass entsprechende Prozesse sicherstellen, dass Änderungen an Notfallrollen auch im Notfallkonzept berücksichtigt werden.

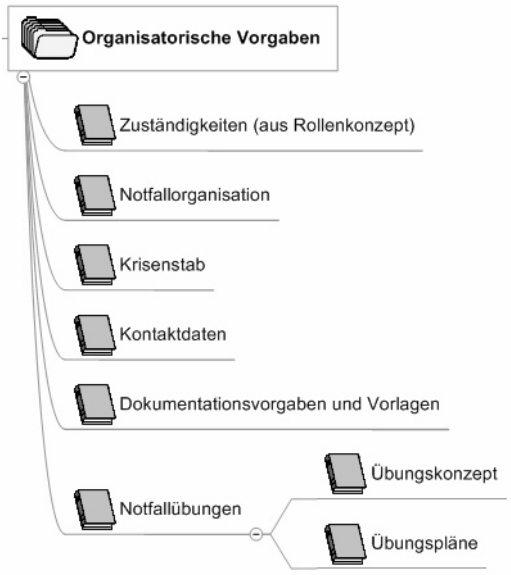


Abbildung 5.3: Der organisatorische Teil regelt vor allem Zuständigkeiten.

Wichtigstes Gremium: Krisenstab

Weiter sollte die Notfallorganisation beschrieben werden. Hier ist die Einrichtung eines *Krisenstabs* als zentrales Gremium der Notfallbewältigung erforderlich. Dieser Begriff wird allgemeingültig (und auch im Buch) unabhängig davon verwendet, ob es sich um einen Notfall, eine Krise oder sogar eine Katastrophe handelt. Abhängig von der Unternehmensgröße kann der Krisenstab durchaus aus nur wenigen Mitarbeitern bestehen. Wichtig ist, das im Notfall ein entscheidungsfähiges Gremium verfügbar ist und nicht der gerade anwesende Administrator allein der Verantwortung im Notfall ausgesetzt ist.

Der Krisenstab ist eine Gruppe von Personen, die ausschließlich im Notfall zusammenkommt und abteilungsübergreifend arbeitet. Zu den wichtigsten Aufgaben des Krisenstabs gehört die Koordination der Aktivitäten im Notfall, die Steuerung der Notfallprozesse und die Bereitstellung aller relevanter Informationen und Ressourcen zur Bewältigung des Notfalls. Der Krisenstab setzt sich in der Regel aus einem Leiter und einem Krisenstabsteam zusammen, das gegebenenfalls durch Fachberater unterstützt wird. Entscheidend ist, dass der Krisenstab im Notfall anderen Abteilungen gegenüber weisungsbefugt ist.

Bezüglich des Krisenstabs sollten im Notfallhandbuch alle wichtige Punkte geregelt werden. Dazu gehören unter anderem Festlegungen zu dessen Zusammensetzung und Einberufung genauso wie die Benennung der Räumlichkeiten und möglicher Catering-Versorgung (z.B. Pizza-Lieferservice). Auch die Regelungen zur Versorgung des Krisenstabs mit der erforderlichen Technik sollten selbstverständlich dokumentiert werden.

hinweis

Dass das Notfallhandbuch nicht allein im Firmennetzwerk gespeichert werden darf, ist nachvollziehbar und wird in den meisten Fällen auch beachtet. Viele Unternehmen speichern das Notefallhandbuch deshalb zusätzlich auf einem USB-Stick oder auf CD-ROM. Bei den organisatorischen Festlegungen für den Krisenstab sollte daher daran gedacht werden, dass diesem in jedem Fall ein Rechner (Notebook) zur Verfügung stehen muss, auf dem mit dem Notfallhandbuch gearbeitet werden kann. Zusätzlich sollte das Notfallhandbuch auch in gedruckter Form vorliegen.

Besonders wichtig: Kontaktdaten

Neben organisatorischen Regelungen enthält dieser Teil auch alle wichtigen Kontaktdaten. Hierzu zählen die Adresslisten und Telefonnummern (dienstlich, privat und mobil) der zu informierenden Mitarbeiter genauso wie beispielsweise die Notrufnummern für Feuerwehr, Notarzt, Wasser- und Stromversorger und Telekommunikationsanbieter, Netzwerkanbieter und Vertragsfirmen.

Weiter sollten hier die für den Notfallbetrieb geltenden Dokumentationsregelungen beschrieben und gegebenenfalls Vorlagen zur Verfügung gestellt werden.

Dokumentation während des Notfalls

Verständlicherweise gehört die Dokumentation nicht zu den ersten Dingen, woran in der Hektik eines Notfalls gedacht wird. Dennoch ist eine gewissenhafte Dokumentation sowohl der getroffenen Entscheidungen als auch der durchgeführten Maßnahmen während der Notfallbewältigung extrem wichtig.

Zum einen ist es für ein reibungsloses Ineinandergreifen der einzelnen Prozesse wichtig, jederzeit den aktuellen Status erfragen zu können. Zum anderen müssen gegebenenfalls Finanzierungs-, Versicherungs- und Rechtsangelegenheiten mit Hilfe der Aufzeichnungen durchgesetzt werden. Daher muss die Notfall-Dokumentation revisionssicher (siehe hierzu Abschnitt 7.1.1) und gegebenenfalls gerichtsverwertbar sein. Dies gilt insbesondere für alle Entscheidungen des Krisenstabs.

Um die Mitarbeiter hierbei zu unterstützen sollten Checklisten, Protokollvordrucke und Formulare bereitgestellt werden. Mit Hilfe dieser Vordrucke kann außerdem sichergestellt werden, dass alle erforderlichen Angaben dokumentiert werden. Nützlich sind auch kurze Anleitungen und Hinweise in den Vorlagen, worauf bei der Protokollierung zu achten ist.

Abschließend sei noch auf das Übungskonzept und die Übungspläne verwiesen, die ebenfalls hier eingeordnet werden können. Nähere Erläuterungen zum Übungskonzept und zum Durchführen von Übungen finden Sie an späterer Stelle.

5.2.2 Organisatorische Abwicklung

Im Teil der organisatorischen Abwicklung geht es um die Festlegung, Umsetzung und Kontrolle aller erforderlichen Maßnahmen. Damit werden in diesem Teil im Wesentlichen die Aufgaben des Krisenstabs beschrieben.

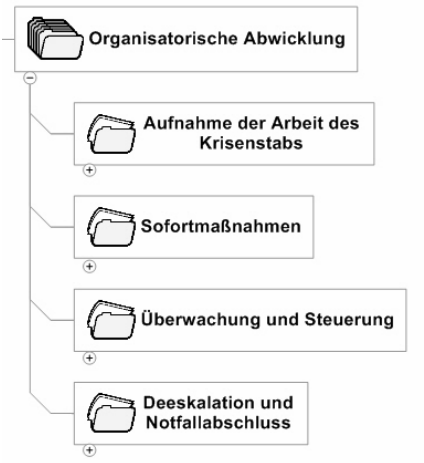


Abbildung 5.4: Phasenorientierte Gliederung der organisatorischen Maßnahmen

5.2.2.1 Aufnahme der Arbeit des Krisenstabs

In der ersten Phase gilt es, die Arbeit des Krisenstabs sicherzustellen und eine Bestandsaufnahme durchzuführen Die dafür erforderlichen Prozesse sind hier zu beschreiben, wobei vor allem das Vorgehen für eine erste Schadensaufnahme festzulegen ist. So ist es beispielsweise erforderlich zu regeln, woher und durch wen der Krisenstab im Notfall die erforderlichen Informationen und Unterlagen erhält, die er für die Beurteilung der Lage benötigt.

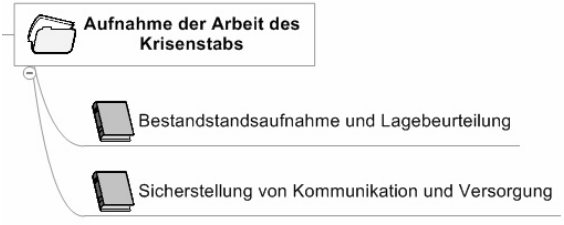


Abbildung 5.5: Im Vordergrund dieser Phase steht die Bestandaufnahme.

5.2.2.2 Sofortmaßnahmen

Alarmierungsplan

Die eigentliche Notfallbewältigung beginnt mit den Sofortmaßnahmen. Zu den ersten Maßnahmen gehört die Klassifizierung des Notfalls und die formale Feststellung eines Notfalls. Mit dieser Maßnahme wird der Regelbetrieb offiziell außer Kraft und stattdessen die entsprechenden Pläne in Kraft gesetzt.

Außerdem müssen die erforderlichen Mitglieder der Notfallorganisation alarmiert und gegebenenfalls die erforderlichen externen Stellen informiert werden. Hierfür wird ein Alarmierungs- und Eskalationsplan benötigt. Dieser muss festlegen, wer wen in welcher Reihenfolge über den Notfall zu informieren hat. Die dafür im Notfallhandbuch zu dokumentierenden Prozesse sollten beispielsweise auch festlegen, wie die Alarmierung außerhalb der normalen Arbeitszeit zu erfolgen hat. Wichtig ist anschließend die Festlegung des weiteren Vorgehens.

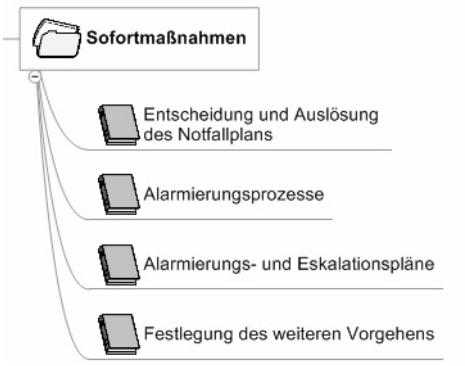


Abbildung 5.6: Die Sofortmaßnahmen entscheiden über das weitere Vorgehen.

Festlegung der weiteren Maßnahmen

Insbesondere die Festlegung der weiteren Maßnahmen ist in dieser Phase wichtig, So ist beispielsweise zu entscheiden ist, ob eine direkte Wiederherstellung des Regelbetriebs nach den Vorgaben eines Wiederanlaufplans möglich ist, oder ob die Einrichtung eines Notbetriebs unter Berücksichtigung des Geschäftsführungsplans erforderlich ist. Die hierfür erforderlichen Prozesse sind im Notfallhandbuch zu dokumentieren.

beispiel

Beispielsweise mussten wegen eines Ausfalls der Klimaanlage alle Server im Rechenzentrum heruntergefahren werden. Da die Klimaanlage kurzfristig instand gesetzt werden konnte, ist es möglich, den Regelbetrieb kurzfristig wieder anlaufen zu lassen. Hierbei ist entsprechend den Anleitungen und Prozessbeschreibungen des *Wiederanlaufplans* zu verfahren. Ist hingegen bei einem Brand das Rechenzentrum vollständig zerstört worden, ist eine kurzfristige Aufnahme des Regelbetriebs kaum möglich. In diesem Fall muss ein Notfallbetrieb eingerichtet und der entsprechende *Geschäftsfortführungsplan* in Kraft gesetzt werden. Dieser definiert, wie über einen vordefinierten ausgedehnten Zeitraum die Fortführung der kritischen Geschäftprozesse in einem Notbetrieb zu gewährleisten ist. Gleichzeitig wird ein Wiederanlaufplan benötigt. Dieser enthält Handlungsanweisungen, wie nach einem Brand der Regelbetrieb wieder einzurichten ist. Hierzu gehören beispielsweise auch Ersatzbeschaffungsmaßnahmen.

Während also die Wiederanlaufpläne die Wiederherstellung des Regelbetriebs zum Ziel haben, dienen die Geschäftsfortführungspläne der Bereitstellung einer dokumentierten Vorgehensweise und eines Prozesses, mit deren Hilfe ein Unternehmen die Geschäftsprozesse während des Notbetriebs und der Wiederanlaufzeit fortsetzen kann.

hinweis

In der Literatur wird häufig der Begriff *Notfallplan* verwendet, ohne diesen von *Geschäftsfortführungsplan* und *Wiederanlaufplan* abzugrenzen. Vielfach werden die Begriffe Notfallplan und Wiederanlaufplan synonym verwendet.

Im vorliegenden Buch werden die beiden Begriffe *Wiederanlaufplan* und *Geschäftsfortführungsplan* in der zuvor definierten Weise verwendet. In Abgrenzung dazu wird unter einem Notfallplan die Gesamtheit aller Notfalldokumente für ein Schadensereignis zusammengefasst. Dies schließt neben dem Geschäftsfortführungsplan und dem Wiederherstellungsplan auch beispielsweise die ereignisspezifischen Alarmierungspläne ein. Insofern handelt es sich bei einem Notfallplan nicht um ein eigenständiges Dokument, sondern um die Zusammenführung von Inhalten aus den genannten Dokumenten.

Der ebenfalls häufig zu findende Begriff *Wiederherstellungsplan* hingegen beschreibt die technische Seite der Wiederherstellung und enthält konkrete Arbeitsanweisungen zur Wiederherstellung eines Systems. Da dieser Begriff eine hohe Verwechslungsgefahr birgt, wird im vorliegenden Buch stattdessen der Begriff *Wiederherstellungsanleitung* verwendet.

5.2.2.3 Überwachung und Steuerung

Alle Aktivitäten während der Notfallbewältigung müssen überwacht werden. Wurde beispielsweise ein Geschäftsfortführungsplan in Kraft gesetzt, muss geprüft werden, ob die darin geforderten Maßnahmen auch erfolgreich durchgeführt wurden. Gegebenenfalls sind zusätzliche Maßnahmen durchzuführen.

Aus Gründen der Nachweisbarkeit sollte eine formale Abnahme der Wiederanlauf- und Geschäftsfortführungsmaßnahmen erfolgen. Die dafür notwendigen Prozesse sind ebenfalls in diesem Teil des Notfallhandbuches zu beschreiben.

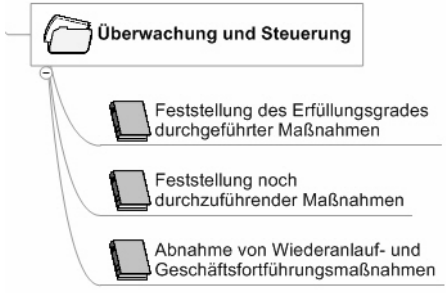


Abbildung 5.7: Alle Notfallmahnahmen müssen überwacht werden.

5.2.2.4 Deeskalation und Notfallabschluss

Nach der Behebung des Notfallereignisses sollte mittels eines geplanten Vorgehens der Normalbetrieb wiederhergestellt und der Notbetrieb beendet werden (Deeskalation), was in einem gesonderten Abschnitt im Notfallhandbuch zu dokumentieren ist. Hier muss beispielsweise definiert werden, wann dieser Zeitpunkt erreicht ist oder welche Bedingungen dazu erfüllt werden müssen.

Hinsichtlich der Rückführung in den Regelbetrieb werden an dieser Stelle ausschließlich die organisatorischen Prozesse zur Überführung des Notbetriebs in den Regelbetrieb betrachtet. Der operative Teil hingegen ist Gegenstand der Notfallpläne für die spezifischen Ereignisse.

Offizieller formaler Abschluss

Weiter sind in diesem Abschnitt alle Tätigkeiten und Prozesse zu beschreiben, die der Feststellung der erfolgreichen Rücküberführung in den Regeltrieb dienen. So muss beispielsweise genau festgelegt werden, wer nach einer erfolgreichen Abarbeitung des Rückführungsplans berechtigt ist, den Notfall offiziell zurückzunehmen und welche Abnahmedokumente erforderlich sind.

Als letzten Punkt sollte im Notfallhandbuch festgeschrieben werden, welche Tätigkeiten nach dem Abschluss erforderlich sind. Diese müssen sich sowohl auf die Ursachenklärung als auch auf die Notfallprozesse beziehen. So sollten beispielsweise die Notfallprozesse selbst hinsichtlich erkannter Schwachwachstellen analysiert werden. Die angewandten Verfahren und Pläne müssen anschließend überarbeitet und aktualisiert werden. Außerdem ist festzulegen, welche Abschlussberichte zu erstellen sind und welcher jeweiligen Vertraulichkeitsstufe diese unterliegen.

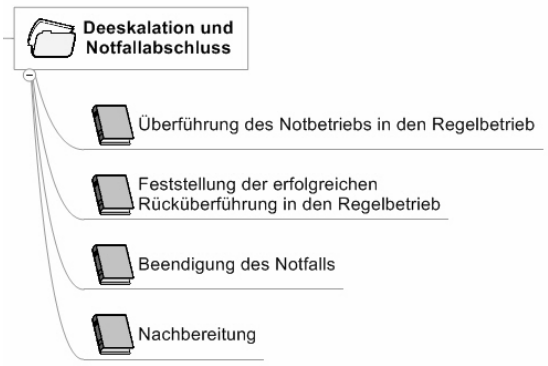


Abbildung 5.8: In dieser Phase wird der Regelbetrieb wiederhergestellt.

5.2.3 Wiederanlaufpläne für spezifische Notfälle

Wiederanlaufpläne müssen innerhalb eines angemessenen Zeitraums die Rückkehr zum Normalbetrieb ermöglichen. Dazu müssen sie Handlungsanweisungen für spezielle Ereignisse enthalten, die beschreiben, was in welcher Reihenfolge zu tun ist. Dazu zählen auch Wiederbeschaffungsmaßnahmen und Ausweichmöglichkeiten.

Im Wiederanlaufplan sollten deshalb sowohl die Wiederbeschaffungsmöglichkeiten einschließlich der Adressen und Ansprechpartner der bisherigen Lieferanten für Hardware und Zubehör als auch interne oder externe Ausweichmöglichkeiten benannt werden. Gibt es beispielsweise ein externes Rechenzentren, mit dem ein Servicevertrag abgeschlossen wurde, und kann auf einem dort vorgehaltenen System direkt mit dem Wiederanlauf begonnen werden, so ist dieses einschließlich der Ansprechpartner selbstverständlich zu beschreiben. Möglicherweise stehen aber auch intern bzw. in einer Niederlassung Ersatzgeräte einschließlich einer Remote-Verbindung bereit, sodass von dort aus die wichtigsten Dinge wieder anlaufen können.

Wiederherstellungsanleitung

Den Schwerpunkt des Wiederanlaufplans bildet die Beschreibung der Prozesse und Tätigkeiten zur eigentlichen Wiederherstellung der IT-Komponenten.

Die erforderlichen Schritte sind detailliert in einer Wiederherstellungsanleitung aufzuzeigen. Diese sollte alle Tätigkeiten vom Systemstart einer IT-Komponente bis hin zur Einbindung in das IT-System umfassen, wobei die genauen Inhalte vom wiederherzustellenden System abhängig sind. Grundsätzlich ist eine Beschreibung der folgenden Schritte sinnvoll:

- Aufbau, Installation und Konfiguration der erforderlichen Hardware-Komponenten
- Installation der Systemsoftware
- Installation der Einspielen der Anwendungssoftware
- Wiederherstellung der Daten einschließlich der Konfigurationsdateien aus der Datensicherung
- Wiederanlauf des Systems

Für ein Datenbanksystem sollte eine solche Anleitung beispielsweise zusätzlich eine Liste der erforderlichen Sicherungsdatenträger sowie Angaben zum Speicherplatzbedarf für die Datenbank und das Wiederherstellungsprotokoll beinhalten. Auch Hinweise zur Registrierung von Lizenzen können erforderlich sein.

Wiederanlaufreihenfolge

Zudem ist es erforderlich, eine Reihenfolge für den Wiederanlauf der Systeme und Anwendungen festzulegen. Es sollte im Wiederanlaufplan definiert werden, welche Maßnahmen die Wiederherstellung abschließen und welche Bedingungen erfüllt sein müssen, damit der Regelbetrieb als wieder aufgenommen gilt.

Wiederanlaufpläne für spezifische Notfälle

Im Notfallhandbuch ist es sinnvoll, alle Wiederanlaufpläne in einem gesonderten Kapitel zusammenzufassen. Die nachstehende Abbildung zeigt exemplarisch einem Auszug aus diesem Bereich des Notfallhandbuches.

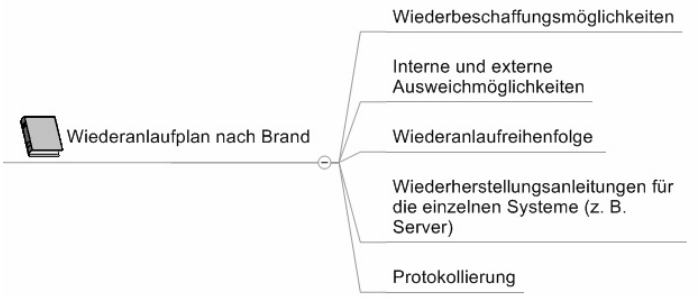


Abbildung 5.9: Beispiel-Gliederung eines Wiederanlaufplans

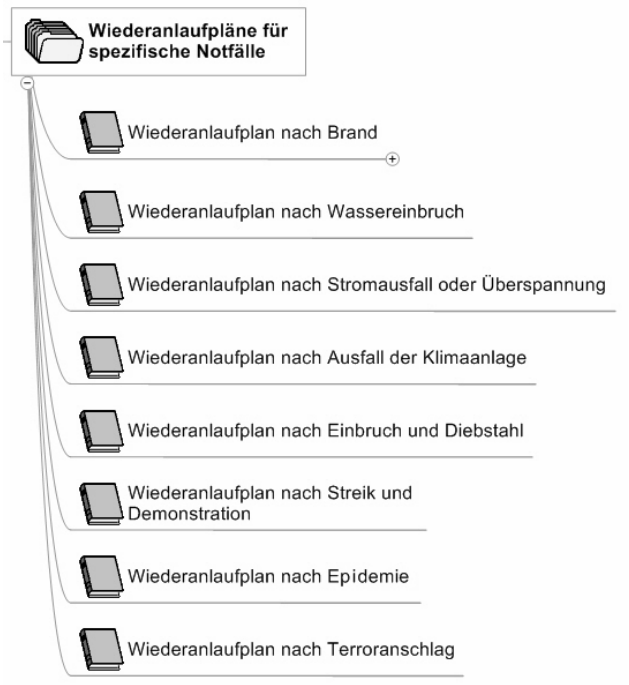


Abbildung 5.10: Liste möglicher Wiederanlaufpläne

tipp

Um die Anzahl der Wiederanlaufpläne (bzw. der Notfallpläne) überschaubar zu halten, sollten allgemeine Szenarien erarbeitet werden, die mehrere spezifische Schadensfälle zusammenfassen. So können beispielsweise bei einem schadensorientierten Ansatz alle Ereignisse, die zu Mitarbeiterausfällen führen (Streik, Demonstration, Epidemie) zu einem Szenario zusammengefasst werden. Ein weiteres Szenario könnte den Ausfall des Rechenzentrums zum Inhalt haben. Denn in der Praxis spielt es für die Notfallbewältigung letztendlich kaum eine Rolle, ob der Ausfall durch einen Wasserschaden oder durch Brand verursacht wurde.

5.2.4 Geschäftsfortführungspläne (Notbetrieb)

Der Hauptzweck der Geschäftsfortführungspläne besteht darin, dass wichtige Geschäftsprozesse selbst in kritischen Situationen und in Notfällen nicht oder nur temporär unterbrochen werden und die wirtschaftliche Existenz des Unternehmens trotz des Schadens gesichert bleibt. Hierzu müssen die Geschäftsfortführungspläne auch den Notbetrieb für die Zeit bis zum Wiederanlauf des Regelbetriebs sicherstellen. Die Erstellung der Geschäftfortführungspläne ist die Aufgabe des *Kontinuitätsmanagements* (engl. *Business Continuity Managements*.

Wie bei den Wiederanlaufplänen ist es zweckmäßig, ebenfalls alle Geschäftsfortführungspläne in einem gesonderten Bereich des Notfallhandbuches zusammenzufassen. Die nachstehende Abbildung zeigt exemplarisch einem Auszug aus diesem Bereich des Notfallhandbuches. In diesem Beispiel wurden die einzelnen Geschäftsfortführungspläne zu Szenarien zusammengefasst.

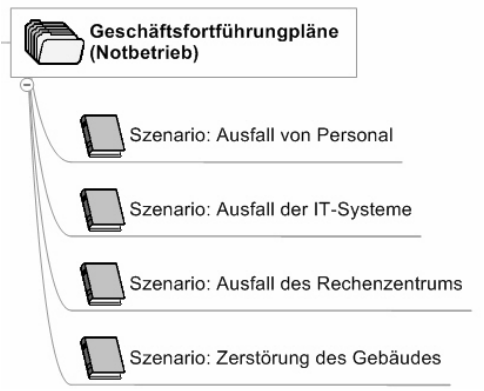


Abbildung 5.11: Geschäftsfortführungspläne für mögliche Notfallszenarien

5.2.5 Systemdokumentation

Wie zuvor beschrieben, sind die für den Wiederanlauf der einzelnen IT-Systeme erforderlichen Schritte detailliert im Notfall-Handbuch aufzuzeigen Um alle Schritte durchführen zu können, wird natürlich eine Beschreibung des wiederherzustellenden Systems benötigt, denn schließlich kann nur etwas wieder hergestellt werden, das auch bekannt ist. Daraus wird deutlich, dass eine aktuelle Systemdokumentation die Basis der Notfalldokumentation darstellt.

Systemdokumentation sollte vorhanden sein

Gemeinhin gilt die Zusammenstellung der Systeminformationen als der hinsichtlich der Erstellung aufwendigste Teil des Notfallhandbuches. Dem sollte eigentlich nicht so sein, denn eine aktuelle gepflegte Systemdokumentation wird bereits als Basis für die Prozesse des IT-Betriebs ohnehin benötigt. Sie sollte also vorhanden sein.

Zwar ist den Autoren des Buches durchaus bewusst, dass diese Forderung nicht immer gegeben ist. Fehlt jedoch eine Systemdokumentation, sollte die Erstellung des Notfallhandbuches als Anlass genommen werden, eine solche aufzubauen. Dies aber darf nicht aus Sicht der Notfalldokumentation erfolgen. Vielmehr muss die Systemdokumentation so eigenständig gehalten sein, dass sie sowohl für die Prozesse des IT-Betriebs als auch für die Notfalldokumentation alle wichtigen Daten bereitstellt. Detaillierte Erläuterungen zu Struktur und Aufbau einer solchen Systemdokumentation finden Sie in Abschnitt 4.2.

Da bei einem Notfall nicht davon ausgegangen werden kann, dass ein Zugriff auf die Systemdokumentation möglich ist, muss eine Kopie in das Notfallhandbuch eingefügt werden.

5.3 Organisation und Pflege des IT-Notfallhandbuches

Bei einem Notfall hängt die Handlungsfähigkeit vor allem von der Qualität, der Aktualität und der Verfügbarkeit der Notfalldokumentation ab. So nutzt auch das aktuellste Notfallhandbuch nichts, wenn es nicht verfügbar ist, oder niemand weiß, wie damit umzugehen ist. Welche Maßnahmen zur Erfüllung der genannten drei Forderungen sinnvoll sind, ist Gegenstand dieses letzten Abschnitts zum Thema Notfallhandbuch.

5.3.1 Sicherstellung der Qualität

Für die Qualität des Notfallhandbuches sind zwei Kriterien entscheidend. Zum einen ist bei der Erstellung des Handbuches und beim Design der Notfallprozesse eine entsprechende Qualitätssicherung erforderlich. Zum anderen müssen die Inhalte der Notfallpläne regelmäßig getestet und trainiert werden. In den meisten Unternehmen werden zwar Notfallhandbücher bzw. Notfallpläne erstellt, aber entweder gar nicht oder nur einmal getestet bzw. geübt. Viele dieser Pläne versagen dann beim ersten umfassenden Test oder schlimmstenfalls im konkreten Notfall.

Regelmäßige Tests und Übungen

Nur in einem Test kann zum Beispiel festgestellt werden, ob innerhalb der vereinbarten Zeit alle erforderlichen Verantwortlichen auch wirklich verfügbar sind und die Wiederherstellungsanleitungen auch tatsächlich funktionieren. Sinnvoll ist es deshalb, die Pläne in Übungen regelmäßig zu trainieren. Derartige Übungen haben gleich zwei Funktionen: Während der Übungen erlernen die Mitarbeiter die erforderlichen Notfalltätigkeiten und können so im Ernstfall besser reagieren. Dabei werden gleichzeitig die Maßnahmen auf ihre Funktionsfähigkeit hin geprüft. So kann bei einem solchen Test beispielsweise festgestellt werden, ob das Notstromaggregat funktioniert.

Übungskonzept erforderlich

Die Regelungen zur Durchführung derartiger Übungen sollten in einem Übungskonzept, das als Bestandteil des Notfallhandbuches verwaltet wird, festgeschrieben werden. Zusätzlich werden Übungspläne für die einzelnen Übungen benötigt. Das Übungskonzept regelt die grundsätzliche Organisation der Notfallübungen und gilt für alle Übungen. Hierfür sollte das Übungskonzept Aussagen zu den folgenden Punkten beinhalten:

- Verantwortlicher (für die Übungsorganisation und das Übungskonzept)
- Zeitpläne (Festlegung, in welchem Turnus und wann welche Übungen durchzuführen sind)
- Grundsätzliche Regeln für alle Notfallübungen

Übungspläne für die einzelnen Übungen

Zusätzlich werden für die einzelnen Notfallübungen Übungspläne benötigt, die unter anderem Folgendes regeln:

- Verantwortlicher für die Übung
- Erforderlicher Teilnehmerkreis (hierzu zählen auch gegebenenfalls Dienstleister und externe Berater)
- Hinweise und Anleitungen zum Ablauf der Übung. Für besonders komplexe Szenarien kann ein Übungsdrehbuch erstellt werden. In diesem sind der zeitliche Ablauf und die vordefinierten Ereignisse der Übung detailliert in ihrem zeitlichen Ablauf zu beschreiben.
- Kriterien für einen Abbruch der Übung. Ein Abbruch kann beispielsweise erforderlich sein, wenn die noch benötigte Zeitspanne oder die noch durchzuführenden Übungen den Produktivbetrieb beeinflussen würden oder die umgesetzten Maßnahmen nicht den erwarteten Erfolg bringen.
- Erforderliche Dokumentation

Alle Übungen müssen detailliert protokolliert und revisionssicher dokumentiert werden. Außerdem sollten sie sorgfältig ausgewertet werden. Häufig ergeben sich aus den Notfallübungen Änderungserfordernisse für die Notfallpläne. Diese Änderungen sollten zeitnah im Rahmen eines Änderungsprozesses eingearbeitet werden.

5.3.2 Sicherstellung der Aktualität und Verfügbarkeit

Nur ein aktuelles Notfallhandbuch, das allen Verantwortlichen in der aktuellen Fassung vorliegt, kann seinen Zweck erfüllen. In der Literatur liest man deshalb immer wieder, dass weniger die Erstellung als vielmehr die Pflege des Notfallhandbuches erheblichen Arbeitsaufwand verursacht.

5.3.2.1 Erforderliche Änderungen

Bei genauerer Betrachtung wird jedoch deutlich, dass diese pauschale Aussage so nicht haltbar ist. Hierzu sollen noch einmal die Hauptteile des Notfallhandbuches betrachtet werden:

- Formaler Teil mit den organisatorischen Regelungen
- Organisatorische Notfallprozesse
- Notfallpläne für einzelne Systeme oder Szenarien einschließlich Wiederanlaufpläne und Geschäftsfortführungspläne
- Systemdokumentation

Systemdokumentation ohnehin erforderlich

Der Kern der Aussage bezieht sich meist auf die Systemdokumentation. Diese muss in der Tat aktuell sein, damit die Systeme im Notfall wiederhergestellt werden können. Doch eine aktuelle Systemdokumentation wird ohnehin für den IT-Betrieb benötigt und muss im IT-Betrieb aktualisiert werden. Derartige Aktualisierungsprozesse können überhaupt nicht dem Notfallmanagement obliegen, da dieses nicht in die Änderungsprozesse des Betriebs eingebunden ist.

Betrachtet man weiterhin die Notfallprozesse und Notfallpläne hinsichtlich ihrer Aktualisierungshäufigkeit, so wird deutlich, dass diese nur selten Änderungen unterliegen. Die Notfallpläne und Notfallprozesse wurden getestet und geübt. Es gibt damit bei normalen Geschäftabläufen kaum Anlass, diese zu ändern. Eine Ausnahme stellen natürlich Änderungen an den Betriebsprozessen dar (was in der Regel aber ebenfalls nicht allzu häufig vorkommt). In der Mehrzahl der Fälle wird es daher lediglich erforderlich sein, neue Notfallpläne in das Notfallhandbuch aufzunehmen, wenn dem IT-Betrieb neue Systeme hinzugefügt werden.

Bleibt noch der formale Teil mit den organisatorischen Regelungen. Dieser muss in der Tat regelmäßig aktualisiert werden, da er unter anderem Kommunikationsdaten und Zuständigkeiten beschreibt, die sich natürlich ändern können. Aus diesem Grund ist es sinnvoll, diese Informationen an zentraler Stelle der Notfalldokumentation zusammenzufassen.

5.3.2.2 Einsatzmöglichkeiten von Tools zur Erstellung eines Notfallhandbuches

Wie die vorstehenden Betrachtungen gezeigt haben, unterliegt das Notfallhandbuch sehr viel seltener Änderungen und ist sehr viel statischer, als vielfach angenommen wird. Trotzdem ist eine Notfallplanung und Notfallbewältigung ohne den Einsatz von Tools nur schwer zu bewältigen.

Manuelle Pflege fehleranfällig

So ist allein das Auffinden und Zusammenstellen aller erforderlichen Dokumententeile aus der Systemdokumentation, der Prozessdokumentation und den Rahmendokumenten und die Zusammenführung in der Notfalldokumentation ohne Toolunterstützung nur schwer möglich und vor allem fehleranfällig. Und auch die Bereitstellung eines jeweils aktuellen Notfallhandbuches bedarf manuell einigen Aufwandes. In Bezug auf die Verteilung müssen Prozesse zur Änderungsbenachrichtigung definiert werden, die sicherstellen, dass alle Beteiligten über Änderungen möglichst zeitnah informiert werden. In großen Unternehmen kann dies einigen Aufwand bedeuten.

Der Einsatz eines Tools zur Notfallplanung und Notfallbewältigung ist daher sinnvoll – zumal neuere Tools eine Vielzahl an Funktionen bieten, die über die Erstellung klassischer Handbücher und Notfallpläne weit hinausgehen.

So bieten viele Tools die Möglichkeit, Daten zu Hardware und Software sowie Personenstammdaten aus vorhandenen Datenbanken automatisiert zu importieren. Diese Funktion ist wichtig, um doppelte Datenhaltung zu vermeiden, sofern bereits entsprechende Tools im Unternehmen im Einsatz sind. Und wo noch keine Tools für das Betriebs- oder das Dokumentenmanagement vorhanden sind, können viele der Tools einen wirklichen Mehrwert bieten, da sie nebenbei auch Funktionen für die Risiko- und Business Impact-Analyse oder DMS-Funktionen mitbringen.

Tool muss zum Unternehmen passen

Bei der Evaluierung einer Notfallplanlösung können daher eine Reihe von Kriterien gemäß nachstehender Liste herangezogen werden. Welche davon wichtig sind, muss unternehmensspezifisch entschieden werden.

- Schnittstellen (gegebenenfalls auch XML-Schnittstellen) für den Datenbankimport
- Importmöglichkeiten für externe Daten
- Anpassbare Benutzeroberfläche
- Unterstützung beim Aufbau der Notfallorganisationstruktur auf der Basis vorhandener Unternehmensdaten
- Möglichkeiten zur Verwaltung der kompletten IT-Dokumentation
- Automatische Benachrichtigung aller Beteiligten per Mail und SMS einschließlich der Alarmierung des Krisenstabs
- Multiuser- und Mandantenfähigkeit
- Ausgabe des Notfallhandbuches als Textdokument entweder online, auf Papier oder im HTML-Format
- Online-Unterstützung bei der Durchführung von Notfallübungen
- Dokumentation von Prozessen
- Unterstützung bei der Erstellung und Verwaltung von Notfallszenarien und Wiederanlaufplänen
- Online-Begleitung bei der Durchführung von Notfallplänen einschließlich automatischer Erstellung von Ablaufprotokollen
- Unterstützung des Redaktionsprozesses für Notfalldokumente (Versionierung, Benachrichtigung bei Änderungen usw.)
- Möglichkeit der Speicherung des Systems und der Daten auf mobilen Datenträgern
- Unterstützung von Risiko- und Business Impact-Analysen

- Dokumentenmanagementsystem-Funktionen
- Funktionsübergreifende Komponenten für das SLA- und Lizenzmanagement
- Bereitstellung einer integrierten CMDB
- Unterstützung bei Zertifizierungen nach BSI, ISO 9000 und ISO 20000
- Funktionen zur Erstellung eines Verfahrensverzeichnisses nach dem Bundesdatenschutzgesetz

hinweis

Die vorstehende Liste wurde zusammengestellt aus dem Funktionsangebot diverser Notfalltools ohne eine Wichtung der einzelnen Funktionen. Sie erhebt keinen Anspruch auf Vollständigkeit.

Allerdings haben Tools, die ein komplettes Business-Continuity-Management-Framework zur Verfügung stellen, durchaus ihren Preis, der häufig im fünfstelligen Bereich oder darüber liegt. Preiswerte Tools für ein paar hundert Euro bieten hingegen nur selten Funktionen, die über eine Systeminventarisierung plus Dokumentation hinausgehen.

Unter dem nachstehenden Link finden Sie eine Website mit einer Marküber-sicht zu aktuell verfügbaren Notfall- und BCM-Tools [BCMTOOL].

5.4 Fazit

Kein Unternehmen verzichtet auf einen angemessenen Versicherungsschutz. In Bezug auf ein Notfallhandbuch aber handeln immer noch viele nach dem Grundsatz: „Es wird schon nichts passieren."

Dies ist nicht nur sträflicher Leichtsinn, sondern widerspricht auch den Anforderungen, die sich aus Gesetzen wie KontrG und MaRisk ableiten – von den Anforderungen der BSI-Standards ganz abgesehen. Ein gut geplantes Notfallvorsorge- und Notfallbewältigungsmanagement zur Absicherung der Verfügbarkeit aller wichtigen Geschäftsprozesse ist ein absolutes Muss für jedes Unternehmen.

Kernstück einer solchen Dokumentation ist das Notfallhandbuch, das nicht nur alle wichtigen organisatorischen Notfallprozesse beschreibt, sondern auch Notfallpläne für die einzelnen Systeme bzw. für Notfallszenarien enthält. Sinnvollerweise sollte es neben Wiederanlaufplänen auch Geschäftsfortführungspläne beinhalten. Die Grundlage des Notfallhandbuches ist eine aktuelle System- und Prozessdokumentation.

Damit wird deutlich, dass das Notfallhandbuch sehr stark mit der IT-Dokumentation verzahnt sein muss und kein isoliertes Dokument darstellt. Die in den Notfallplänen und Notfallszenarien beschriebenen Abläufe müssen getestet und vor allem regelmäßig geübt werden. Nur wenn alle Verantwortlichen ihre Rolle genau kennen, können sie in der Hektik eines Notfalls richtig und besonnen handeln.

Die komplexen Anforderungen, die an ein Notfallhandbuch gestellt werden, rechtfertigen den Einsatz eines entsprechenden Notfalltools durchaus. Moderne Notfalltools unterstützen vor allem die Einbindung des Notfallmanagements in die Geschäftsprozesse und decken alle Bereiche eines modernen Notfallmanagements ab.

6 Dokumentation von IT-Projekten

Eigentlich gelten die für den IT-Betrieb definierten Regeln, Vorgehensweisen und Strukturen zur Erstellung und Verwaltung von Dokumenten in gleicher Weise auch für Projekte. Und doch ist bei Projekten vieles anders. Da sich Projekte gerade durch das Merkmal der Einmaligkeit vom IT-Regelbetrieb unterscheiden, steht hier nicht die Dokumentation wiederkehrender Prozesse und Tätigkeiten im Vordergrund.

Vielmehr geht es um die Dokumentation der Konzeptionierung und Realisierung von Lösungen für eine konkret gestellte Aufgabe. Konzepte gehören daher zu den wichtigsten Ergebnisdokumenten der Projektdokumentation. Die in den Konzepten beschriebenen Lösungen müssen realisiert, getestet, abgenommen und gegebenenfalls noch einmal geändert werden. Die dafür erforderlichen Dokumente gehören ebenfalls zu den Ergebnisdokumenten, die den Schwerpunkt dieses Kapitels bilden.

Daneben ist ein Projekt durch eine eigene Projektorganisation geprägt. Da sich Projekte per Definition durch eine Begrenzung an zeitlichen, personellen und finanziellen Ressourcen auszeichnen, muss mit diesen sorgsam umgegangen werden, was entsprechende Planungen erfordert. Diese Planungsdokumente gehören zu den Projektmanagement-Dokumenten. Ebenfalls in diesem Kapitel wird das Projektmanagement-Handbuch betrachtet, das den Rahmendokumenten zuzuordnen ist und für alle Einzelprojekte verbindliche Sollvorgaben enthält.

Die alleinige Betrachtung, was zu dokumentieren ist, genügt aber auch hier nicht. Denn Projekte stellen besondere Anforderungen an die Organisation der Dokumentenablage. Daher ist die Verwaltung der IT-Dokumentation ebenfalls Gegenstand dieses Kapitels.

6.1 Bestandteile der Projektdokumentation

Bei IT-Projekten handelt es sich um zielgerichtete, zeitlich, personell und sachlich abgegrenzte IT-Vorhaben, die der Konzeption, Entwicklung, Einführung bzw. Änderung von IT-Systemen und IT-Verfahren dienen. Nähere Erläuterungen, dazu was ein Projekt auszeichnet und welchen grundsätzlichen Inhalt eine Projektdokumentation haben sollte, finden Sie in Abschnitt 2.2.3.

In diesem Kapitel wird zunächst die mögliche Struktur einer Projektdokumentation näher beleuchtet. Diese ist auf der obersten Ebene sehr einfach gehalten, da es hier lediglich für jedes Projekt eine Projektakte gibt.

Abbildung 6.1: Oberste Ebene der Projektdokumentation

cd-rom

Auf der beigefügten CD-ROM finden Sie eine mit MindManager erstellte Datei, die die im Folgenden vorgestellte Gliederung der Projektdokumentation grafisch darstellt und eine Betrachtung der Einzelbereiche in einer Zusammenschau ermöglicht. Mit dem ebenfalls beigefügten MindManager Viewer kann diese Datei angesehen werden. Außerdem ist es möglich, Zweige zu öffnen, zu schließen und in sie hineinzuzoomen.

6.1.1 IT-Projektmanagement-Handbuch

Das IT-Projektmanagement-Handbuch (PM-Handbuch) regelt die verbindlichen Sollvorgaben, die für alle Einzelprojekte gelten. Bei der im Buch vorgestellten Struktur der IT-Dokumentation wird das Projektmanagement-Handbuch aufgrund des übergeordneten Charakters den Rahmendokumenten zugeordnet. Alternativ ist es aber durchaus möglich, es als Teil der Projektdokumentation zu behandeln.

Das PM-Handbuch ist nach DIN 69905 eine Zusammenstellung von Regeln und Vorgaben, die innerhalb eines Unternehmens für die Planung und die Durchführung von Projekten gelten. Insbesondere größere Unternehmen führen ein Projektmanagement-Handbuch meist auf Unternehmensebene. In diesem Fall enthält es Richtlinien, die für alle im Unternehmen durchzuführenden Projekte gelten. Damit ist es möglich, dass alle Projekte im Unternehmen nach einheitlichen Standards durchgeführt werden.

Spezifizierung im bereichsspezifischen PM-Handbuch

Es kann aber durchaus sinnvoll sein, zusätzlich ein IT-spezifisches Projektmanagement-Handbuch zu pflegen, das ergänzend zum übergeordneten PM-Handbuch die bereichsspezifischen Richtlinien für Projekte festlegt. So ist es beispielsweise möglich, im PM-Handbuch für das Unternehmen zwar den grundlegenden Aufbau der Projektorganisation verbindlich zu definieren, die Vorgehensmodelle aber im fachspezifischen IT-Projektmanagement-Handbuch zu regeln. Dieses könnte beispielsweise festlegen, dass alle IT-Projekt nach dem PRINCE2-Standard durchgeführt werden.

PRINCE2 (PRrojects IN Controlled Environments)

Dieser Projektstandard wurde von dem britischen *Office of Government Commerce (OGC)* entwickelt und ist eine Methode zur Organisation, zum Management und zur Steuerung von Projekten [PRINCE]. PRINCE2 enthält verschiedene in der Praxis bewährte Methoden und liefert standardisierte Projekte, die ein einheitliches Vorgehen, einheitliches Vokabular und einheitliche Dokumente haben.

Inhalte des PM-Handbuches

Fehlt ein unternehmensweites PM-Handbuch ist ohnehin die Erstellung eines IT-spezifischen Projektmanagement-Handbuches dringend anzuraten, zu dessen typischen Inhalten die folgenden Punkte zählen:

- Festlegungen, was ein Projekt ist und welche Rahmenbedingungen zur Durchführung eines Projekts führen
- Definition und Abgrenzungen der Projektarten (Entwicklungsprojekte, Organisationsprojekte, externe Projekte bei Kunden, Großprojekte usw.)
- Vorgehensmodelle für die verschiedenen Projektarten
- Grundlegender Aufbau der Projektorganisation
- Standardisierte Projektmanagement-Prozesse
- Methoden und Instrumente der Projektplanung und der Projektsteuerung
- Projektmanagement-Glossar mit der unternehmensspezifischen Terminologie

Darüber hinaus kann das IT-Projektmanagement-Handbuch Ergänzungen zu anderen unternehmensweit gültigen Dokumenten oder zu Rahmendokumenten der IT-Dokumentation beinhalten. Hierbei kann es sich beispielsweise um projektspezifische Namenskonventionen oder ergänzende Teile zur Dokumentationsrichtlinie handeln.

Ergänzungen zur Dokumentationsrichtlinie

Sinnvoll kann es beispielsweise sein, in der ergänzenden Dokumentationsrichtlinie eine Liste aufzunehmen, die wesentliche projektbezogene Dokumente auflistet und vorgibt, ob diese verpflichtend zu erstellen und in die Projektakte aufzunehmen sind. Zur Kennzeichnung der Dokumentationspflicht ist die folgende Unterscheidung empfehlenswert:

- *Obligatorisch*: Das Dokument ist vorgeschrieben.
- *Projektabhängig*: Das Dokument ist abhängig von der Projektkategorie oder beim Vorliegen der genannten Vorgaben verpflichtend zu erstellen. So kann beispielsweise ein Schulungskonzept verpflichtend vorgeschrieben sein, sofern sich aus dem Projekt die Notwendigkeit für Schulungen ergibt.
- *Optional:* Die Entscheidung, ob eine Dokumentation erforderlich ist, ist von den Projektverantwortlichen zu treffen.

Die nachstehende Tabelle zeigt einen Ausschnitt aus einer solchen Übersichtsliste:

Dokument	Beschreibung	Verbindlichkeit	Kategorie
Projektmanagement-Dokumente			
Projektsteckbrief	Er enthält alle wichtigen Daten und Rahmenbedingungen. Bei extern zu vergebenen Projekten kann er die Grundlage für den Projektauftrag bilden.	obligatorisch	Alle
Machbarkeitsstudie	Um Fehlinvestitionen zu verhindern, wird bei Zweifeln an der Erreichbarkeit des Projektziels eine Machbarkeitsstudie durchgeführt.	projektabhängig	Großprojekte und im Vorfeld von Forschungs- und Entwicklungsprojekten
Meilenstein-Plan	Im Meilenstein-Plan sind alle Meilensteine des Projekts zusammengefasst. Damit strukturiert er das Projekt durch das zeitliche Festlegen von Teilzielen.	obligatorisch	Alle

Dokument	Beschreibung	Verbindlichkeit	Kategorie
interne Veröffentlichungen	Broschüren, Flyer, Newsletter, Intranet-Veröffentlichungen usw. Bei vielen Projekten (insbesondere Großprojekten) ist das Akzeptanzmanagement ein wesentlicher Erfolgsfaktor.	projektabhängig	Großprojekte Soweit Informationen oder Unterlagen erarbeitet werden, sind diese der Projektdokumentation beizufügen.
Pressemitteilungen	Presse- und Öffentlichkeitsarbeit ist bei Großprojekten oftmals üblich.	optional	
Change Request Bericht	Änderungen (Change Requests), die sich im Hinblick auf den ursprünglichen Projektinhalt ergeben und wesentliche Auswirkungen haben, sind in einem Bericht zu dokumentieren.	obligatorisch	Alle
usw.	usw.	usw.	usw.
Ergebnisdokumente			
Konzepte	Konzepte beschreiben die technisch zu realisierende Lösung für eine bestimmte Aufgabe. Sie liefern damit für einen spezifischen Themenbereich eine Absichtserklärung über das, was gemacht werden soll und beschreiben den Weg zum Ziel.	obligatorisch	Die Art der erforderlichen Konzepte ist projekt- und prozessabhängig.
Schulungskonzept	Schulungen sollen die anwenderbezogene Nutzung im täglichen Betrieb sicherstellen. Das Schulungskonzept dient der Planung der Schulungen.	projektabhängig	Sofern Anwenderschulungen erforderlich sind, ist ein Schulungskonzept zu erstellen.
Testkonzept	Umfasst Testorganisation, Testpläne, Testabläufe, konkrete Testfallbeschreibungen, und Testtools.	obligatorisch	Alle
Übergabeprotokoll	Dokumentation des Überführungsprozesses (Verantwortliche und Beteiligte, Zeitpunkt, Ergebnisse, Mängel usw.)	obligatorisch	Alle
usw.	usw.	usw.	usw.

Tabelle 6.1: Auszug aus der Übersichtliste zur Dokumentationspflicht für Projekte

hinweis

Auch wenn die Vorgaben eines solchen Projektmanagement-Handbuches grundsätzlich für alle Projekte gelten, sollte die Umsetzbarkeit im Hinblick auf das spezielle Projekt überprüft und darauf abgestimmt werden. So kann beispielsweise bei einem sehr kleinen Projekt die Organisationsstruktur durchaus flacher sein, als gefordert. Auch hinsichtlich der zu erstellenden Dokumente ist eine Überprüfung sinnvoll. Schließlich ist es schwierig in einem übergreifenden Regelwerk alle Besonderheiten für alle Projekte abzudecken.

6.1.2 Projektakten

Die Projektdokumentation besteht aus den einzelnen Projektakten. Für jedes Projekt ist eine gesonderte Projektakte einzurichten und zu pflegen.

Innerhalb der Projektakten ist eine Unterscheidung in Dokumente für das Projektmanagement und in Ergebnisdokumente sinnvoll. Diese Unterscheidung ergibt sich bereits daraus, dass Dokumente für die Projektplanung und Projektsteuerung zumeist von der Projektleitung oder einem Project Management Office (PMO) erstellt und gepflegt werden, während die Ergebnisdokumente zumeist aus dem Projektteam heraus entstehen.

Die nachstehende Abbildung 6.2 zeigt eine mögliche Gliederung für eine Projektakte.

Anforderungen an Projektakten

Die Projektakten müssen so abgelegt werden, dass jeder Projektmitarbeiter jederzeit auf die für ihn relevanten Informationen Zugriff hat. Darüber hinaus sind an Projektakten die folgenden Anforderungen zu stellen:

- In der Projektakte darf sich nur die jeweils aktuell gültige Version eines Dokuments befinden.
- Die Dokumente müssen leicht auffindbar sein
- Die Projektschritte und -ergebnisse müssen anhand der Projektakte nachvollziehbar sein

hinweis

Die genannten Anforderungen sind wohl nur bei kleinen Projekten mit kleinen Projektteams ohne Unterstützung eines Dokumentenmanagement-Systems realisierbar. In Abschnitt 7.4.2 können Sie nachlesen, welchen Nutzen der Einsatz eines entsprechenden Systems bringt und worauf bei seiner Einführung zu achten ist.

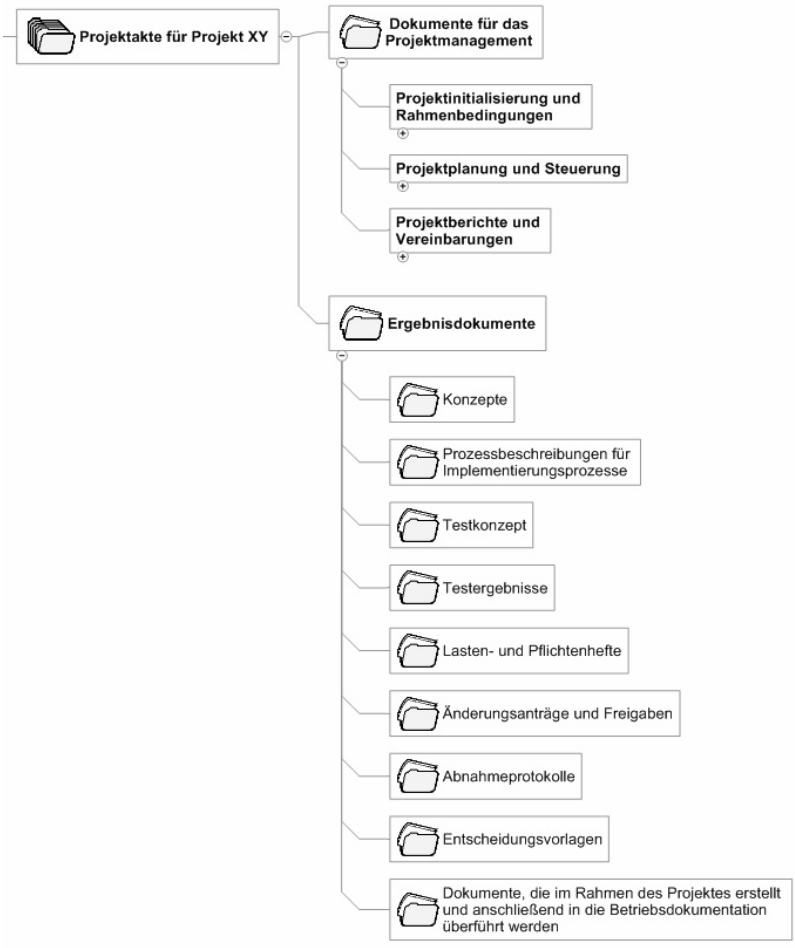


Abbildung 6.2: Mögliche Gliederung einer Projektakte

6.2 Projektakten entstehen im Projektverlauf

Die im Rahmen eines Projekts entstehenden Dokumente können verschiedenen Projektphasen zugeordnet werden.

6.2.1 Projektphasen

Projektphasen bilden die oberste Ebene der ablaufbezogenen Projektstruktur. Eine Projektphase ist ein zeitlicher Abschnitt im Projektverlauf, der sachlich von anderen Abschnitten getrennt ist und mit einem definierten Ergebnis endet. Die Unterteilung eines Projekts in Projektphasen erlaubt es, die anstehenden Aufgaben detailliert zu planen. Der Übergang von einer abgeschlossenen Phase zur nächsten ermöglicht außerdem einen Rückblick auf die bislang erreichten Ergebnisse und eine Kontrolle hinsichtlich der Projektziele. Allerdings folgen in

der Praxis Projektphasen nicht immer streng sequenziell aufeinander, sondern überlappen sich zeitlich.

Ein wesentlicher Nachweis der Ergebnisse der einzelnen Phasen sind die in der Phase erstellten Dokumente. Diese werden Bestandteil der Projektakte, die damit im Laufe des Projekts anwächst. Wird bereits zu Beginn die in Abbildung 6.2 gezeigte Gliederungsstruktur eingerichtet, erleichtert dies die Einordnung der Dokumente während des Projekts.

Verschiedene Phasengliederungen möglich

Die Phasengliederung ist abhängig von der Art des Projekts und vom verwendeten Vorgehensmodell. Bei den Projektarten wird üblicherweise zwischen Investitionsprojekten, Organisationsprojekten und Forschungs- und Entwicklungsprojekten unterschieden. Zusätzlich werden zunehmend IT-Projekte als eigene Projektart behandelt. So weisen zum Beispiel Investitionsprojekte, die dem Bau eines Rechenzentrums dienen, nachvollziehbarerweise andere Phasen auf als beispielsweise Software-Entwicklungsprojekte.

Vorgehensmodelle bieten den Rahmen, in dem ein Projekt geordnet ablaufen kann. Sie bestimmen die Methoden und Elemente des Projektmanagements und geben Prozesse und Phasen eines standardisierten Projektablauf vor. Aus diesem Grund bilden die zugrunde liegenden Vorgehensmodelle auch den zentralen Bestandteil des Projektmanagement-Handbuches. Bekannte Vorgehensmodelle sind das V-Modell, das Wasserfallmodell und CMMI. Daneben gibt es noch herstellerabhängige Vorgehensmodelle. Zu Letzteren zählt beispielsweise das *Microsoft Solutions Framework (MSF-Modell),* das speziell für die Einführung von Microsoft-Technologien entwickelt wurde. MSF hilft dabei, Lösungen auf Basis von Microsoft-Produkten zu entwickeln bzw. in den Betrieb zu überführen und stellt dafür eine Sammlung von Konzepten, Methoden und Best Practices zur Verfügung.

Um die folgenden Ausführungen modellunabhängig zu gestalten, werden die folgenden vier Phasen zugrunde gelegt, die so oder ähnlich in fast allen Modellen bzw. Projekten zu finden sind.

Abbildung 6.3: Mögliche Projektphasen

hinweis

Die Projektinitiierungs- und die Planungsphase werden in der Literatur häufig zusammenfassend als Startphase bezeichnet.

6.2.2 Die Dokumentation im Verlauf der Phasen

In den folgenden Kapiteln wird betrachtet, in welcher Phase typischerweise welche Dokumente zu erstellen sind.

6.2.2.1 Dokumente der Projektinitialisierungsphase

In dieser Phase werden die geschäftlichen Anforderungen für das Projekt definiert und dokumentiert. Aufgaben in dieser Phase sind vor allem:

- Informationssammlung
- Zieldefinition (Grobziele)
- Projektumfeldanalyse
- Machbarkeitsstudie
- Finanzplanung
- Risikoanalyse
- Festlegung der Projektorganisation und gegebenenfalls auch bereits der Projektmitarbeiter
- Pflichten- und Lastenheft für das Projekt

Das Ergebnis dieser Phase ist die Dokumentation aller Projektanforderungen und Zielsetzungen. Die wichtigsten Projektmanagement-Dokumente dieser Phase zeigt die nachstehende Abbildung:

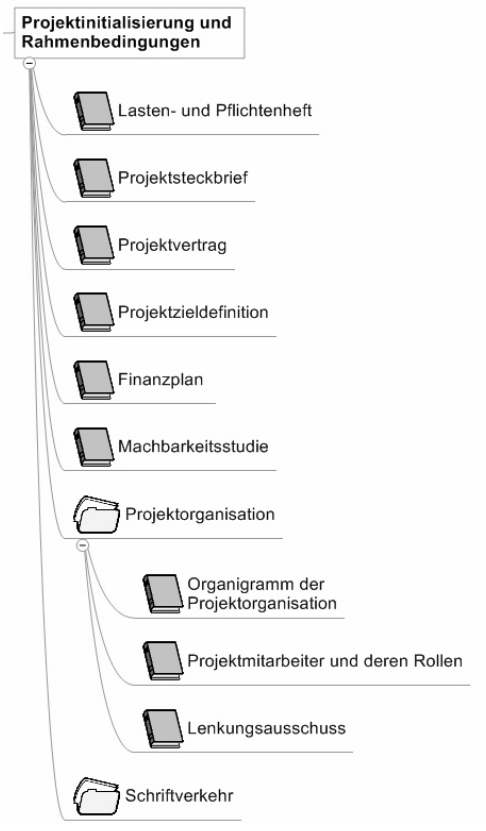


Abbildung 6.4: Gliederung der Projektmanagement-Dokumente der Projektinitialisierungsphase

6.2.2.2 Dokumente der Planungsphase

Auch diese Phase ist ausschließlich durch die Erstellung von Projektmanagement-Dokumenten geprägt. Sie schließt mit genehmigten Projektdokumenten ab. Basierend auf den geschäftlichen Anforderungen und den Ergebnissen der ersten Phase werden vor allem die erforderlichen Pläne (Meilenstein-Plan, Projektplan und andere) in dieser Phase erstellt.

Aufgaben in dieser Phase sind vor allem:

- Planung der Projektphasen
- Strukturierung des Projekts in Arbeitspakete
- Definition von Meilensteinen
- Zuweisung der Ressourcen zu Arbeitspaketen
- Terminplanung
- Kosten- und Budgetplanung
- Analyse und Bewertung von Risiken

Das Ergebnis dieser Phase sind freigegebene Projekt-Planungsdokumente, die es ermöglichen, mit der fachlichen Projektarbeit zu beginnen. Die wichtigsten Projektmanagement-Dokumente dieser Phase zeigt die nachstehende Abbildung:

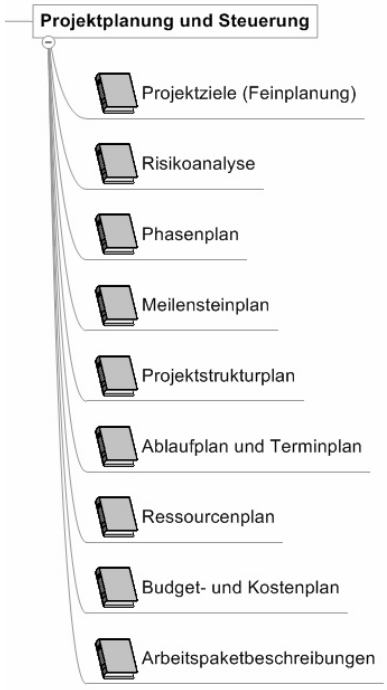


Abbildung 6.5: Gliederung der Projektmanagement-Dokumente der Planungsphase

6.2.2.3 Dokumente der Entwicklungs- und Realisierungsphase

In dieser Phase findet die eigentliche Projektdurchführung statt. Die durchzuführenden Aufgaben sind dabei von der Art des Projekts abhängig. Typische Aufgaben in dieser Phase sind:

- Erstellung der Konzepte (Grob- und Feinkonzepte)
- Modellierung der Prozesse
- Entwicklung der erforderlichen Software
- Entwicklung und Einrichtung der erforderlichen Systeminfrastruktur

Während bei Projekten, deren Ziel eine Organisationsänderung ist (beispielsweise die Einführung von ITIL) die Entwicklung der Prozesse im Vordergrund steht, hat bei Software-Entwicklungsprojekten die Programmierung der erforderlichen Software den größten Anteil. Dementsprechend unterscheiden sich auch die in dieser Phase zu erstellenden Dokumente.

Ergebnisdokumente In der Projektdurchführungsphase liegt das Hauptaugenmerk auf den Ergebnisdokumenten und hier schwerpunktmäßig auf den *Konzepten.* Eine detaillierte Beschreibung von Ziel und Aufbau eines Konzepts können Sie Abschnitt 6.3.5 entnehmen.

Weitere typische Ergebnisdokumente dieser Phase sind:

- Änderungsanforderungen
- Lasten- und Pflichtenhefte für externe Leistungsersteller
- Testberichte und Testprotokolle
- Entscheidungsvorlagen und Ergebnisse
- Prozessbeschreibungen für die Implementierungsprozesse

Sehr häufig zeigen Konzepte Alternativlösungen auf. In diesem Fällen sollten Entscheidungen von den dafür verantwortlichen Stellen eingefordert und die Ergebnisse dokumentiert werden. Hierfür sollten standardisierte *Entscheidungsvorlagen* verwendet werden.

Testdokumente

Unabhängig von der Art der zu erstellenden Lösung müssen die in die Produktivumgebung zu überführenden Systeme getestet und die Dokumente freigegeben werden. Bei Software-Entwicklungsprojekten beispielsweise muss die funktional vollständige Lösung getestet werden. Der Fokus liegt auf dem Beheben von Fehlern und der Vorbereitung der endgültigen Implementierung. Gelegentlich werden sogenannte Release Candidates (RCs) erstellt, die an Pilot-Benutzer verteilt werden. Die Tests erfolgen dabei möglichst realitätsnah und in einer der Produktivumgebung verwandten Infrastruktur.

Für die Durchführung der Tests sollte es notwendigerweise ein *Testkonzept* mit Beschreibungen zu Testorganisation, Testplan, Testablauf, konkreten Testfällen, und Testtools geben. Außerdem ist eine Dokumentation der Testdurchführung (Ergebnisse, Fehler, Mängel, unerwartete Ereignisse usw.) erforderlich.

hinweis

Alternativ zur Durchführung der Tests innerhalb der Entwicklungs- und Realisierungsphase ist es auch möglich, eine gesonderte Testphase als eigenständige Projektphase einzurichten. Bei einigen Vorgehensmodellen, wie beispielsweise dem Microsoft Solution-Framework ist eine solche Phase fester Bestandteil.

Änderungsanforderungen

Kein Projekt läuft exakt so ab, wie es ursprünglich geplant wurde. Bei vielen Projekten ändern sich noch während des Projekts die Inhalte, Ziele, Rahmenbedingungen oder Kundenanforderungen. Eine wesentliche Rolle spielt deshalb das Änderungsmanagement. Das Änderungsmanagement ist verantwortlich für die Organisation, Verwaltung und Abwicklung von *Änderungsanforderungen* während des Projektablaufs.

Projektmanagement-Dokumente Aber auch im Bereich der Projektmanagement-Dokumente passiert in dieser Phase sehr viel. Zum einen müssen die in der Startphase erstellten Planungs- und Steuerungsdokumente im Rahmen der Projektsteuerung fortgeschrieben werden. Zum anderen ist diese Phase durch ein intensives *Berichtswesen (Reporting)* geprägt.

Berichtswesen ist ein wesentlicher Bestandteil des PM

Das Berichtswesen ist ein wichtiger Bestandteil des Projektmanagements. Hierbei ist es die Aufgabe des Berichtswesens, Informationen über das Projekt komprimiert und aussagefähig darzustellen. Es bildet damit die Basis für Abstimmungs- und Entscheidungsprozesse im Projekt. Berichte sollen den aktuellen Stand des Projekts festhalten – sowohl im Hinblick auf das bisher Erreichte als auch im Hinblick auf künftige Entwicklungen. Hierzu stellen Projektstatusberichte eines der wichtigsten Instrumente dar. Daneben gibt es eine Reihe weiterer Berichte (siehe nachstehende Abbildung), zu denen beispielsweise der Projektabschlussbericht gehört.

Sinnvoll ist es für das Projekt, einen Berichtsplan zu erstellen, der alle zu erstellenden Berichte zusammengefasst und schnell Auskunft darüber gibt, wer welche Information wann und an wen weiterleiten muss. Die folgende Tabelle zeigt exemplarisch einen solchen Berichtsplan.

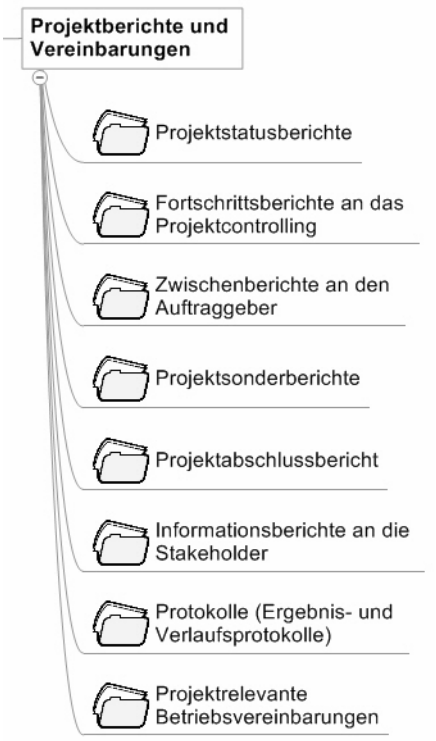


Abbildung 6.6: Gliederung der Projektmanagement-Dokumente der Entwicklungs- und Realisierungsphase

Bericht	Ersteller	Empfänger	Rhythmus
Statusberichte der Teilprojekte	Teilprojektleiter	Projektleitung	wöchentlich
Statusberichte für das Gesamtprojekt	Projektleiter	Lenkungsausschuss, Betriebsrat, Revision	monatlich
Projektsonderberichte	Projektmitarbeiter oder Projektleiter	Betroffene Organisationseinheiten Lenkungsausschuss	Bei Bedarf, wenn unerwartete Situationen eintreten, die weitere Maßnahmen und Entscheidungen erfordern
Meeting- und Ergebnisprotokolle	Protokollant	alle Teilnehmer, Projektleitung	bei Bedarf
Projektabschlussbericht	Projektleiter	Lenkungsausschuss, Geschäftsleitung	am Ende des Projekts

Tabelle 6.2: Für jedes Projekt sollte es einen Berichtsplan geben.

6.2.2.4 Dokumente der Implementierungsphase

In der Phase wird die getestete Lösung in der Produktivumgebung implementiert. Die Lösung erfüllt dabei die definierten Anforderungen und wird für den Betrieb freigegeben. Neue Prozesse werden in den Betrieb übernommen, evaluiert und abgenommen. Ein formaler Projektabschluss beinhaltet die Erstellung eines Projektabschlussberichts und die Übergabe der Dokumentationen. Typische Aufgaben in dieser Phase sind:

- Bereitstellung aller Systeme für den IT-Betrieb
- Überführung der Systeme in den IT-Betrieb und ihre Abnahme
- Implementierung der Prozesse und Freigabe der Prozesse
- Erstellung der Dokumente für den IT-Betrieb
- Abnahmedokumente

Dokumente für den IT-Betrieb

Auch in dieser Phase werden Ergebnisdokumente erstellt. So müssen für alle in den IT-Betrieb zu übernehmenden Systeme die Dokumente bereitgestellt werden, die später in die Betriebsdokumentation überführt werden. Hierzu gehören sowohl die Prozessbeschreibungen als auch die Systemakten für die neu implementierten Systeme. Zusätzlich muss gegebenenfalls das Notfallhandbuch angepasst werden.

6.3 Wichtige Ergebnisdokumente im Detail

Das vorliegende Kapitel stellt die aus Sicht der Dokumentation wichtigsten Ergebnisdokumente eines Projekts vor und erläutert deren Einsatzzweck und Inhalt.

Die Beschreibung der Dokumente an dieser Stelle beschränkt sich auf die fachlichen Inhalte. Zusätzlich sollten die Hinweise und Erläuterungen in Abschnitt 7.1.1 für den formalen Aufbau von Dokumenten beachtet werden.

hinweis

Die Projektmanagement-Dokumente werden im Weiteren nicht ausführlicher betrachtet, da detaillierte Beschreibungen und Anleitungen zur Erstellung, Nutzung und Pflege der Projektmanagement-Dokumente in der zahlreich vorhandenen Literatur zum Thema Projektmanagement zu finden sind.

6.3.1 Lastenheft und Pflichtenheft

Bei genauer Betrachtung der in den vorstehenden Abbildungen gezeigten Gliederungen fällt auf, dass Lasten- und Pflichtenhefte sowohl im Bereich der Ergebnisdokumente als auch unter den Projektmanagement-Dokumenten zu finden sind. Dies ist richtig.

Bekannt sind Lasten- und Pflichtenhefte vor allem aus dem Bereich der Software-Entwicklung. Mithilfe des Lastenheftes wird dem Entwickler mitgeteilt, was er zu programmieren hat. Dieser entwickelt aus den Anforderungen des Kunden (Lastenheft) die genaue Produktspezifikation. Damit stellt das Lastenheft die Problemstellung des Auftraggebers dar und geht dem Pflichtenheft voraus. Das Pflichtenheft liefert den Lösungsvorschlag des Auftragnehmers.

Lasten- und Pflichtenheft auch für das Projekt

Nun werden diese beiden Dokument aber nicht nur für die (innerhalb des Projekts) zu entwickelnden Produkte benötigt, sondern auch für das übergeordnete Projekt selbst. Die Anforderungen, die an ein Projekt gestellt werden, und dessen Ziele müssen schriftlich festgehalten werden. In diesem Fall beschreibt das Lastenheft das angestrebte Projektergebnis und das Pflichtenheft, wie dieses umzusetzen ist.

Beispielsweise soll ein Projekt zur Migration auf ein neues Betriebssystem durchgeführt werden, und die Projektdurchführung soll extern vergeben werden. In diesem Fall ist ein Lastenheft für das Projekt vom Auftraggeber zu erstellen und das Pflichtenheft vom Auftragnehmer. Beide Dokumente werden Bestandteil des Projektvertrags. Im Rahmen des Projekts sind dann die Anforderungen für die neu anzuschaffenden Server zu definieren. Auf der Basis dieser Ergebnisse wird das Lastenheft für die Beschaffung der Serversysteme erstellt. Zusätzlich werden noch Lastenhefte für einzelne Programmieraufträge erstellt, die ebenfalls zu beauftragen sind. Die anschließend auf Basis der Lastenhefte zu erstellenden Pflichtenhefte beschreiben die erarbeiteten Realisierungsvorgaben (für das Serversystem und die zu erstellende Software).

Lasten- und Pflichtenheft in DIN normiert

Sowohl das Lastenheft als auch das Pflichtenheft sind in der DIN 69905 „Projektmanagement, Begriffe“ folgendermaßen normiert:

Nach der DIN 69905 ist das Lastenheft die *„Gesamtheit der Forderungen an die Lieferungen und Leistungen eines Auftragnehmer“*. Zugleich dient das Lastenheft auch als Grundlage beim Einholen von Angeboten. Das Pflichtenheft hingegen enthält entsprechend der DIN die *„vom Auftraggeber erarbeiteten Realisierungsvorgaben aufgrund der Umsetzung des Lastenheftes“* [PJMGR].

6.3.1.1 Lastenheft

Grundsätzlich kann das Lastenheft als ein Anforderungskatalog beschrieben werden, der die Zielsetzungen, Aufgabenstellungen, Anforderungen des Auftraggebers und weitere Leistungsdaten des zu entwickelnden Produkts spezifiziert. Bei Bauprojekten wird das Lastenheft auch als *Leistungsverzeichnis (LV)* bezeichnet. Außerdem wird in der Praxis manchmal auch der Begriff *Fachkonzept* und *Sollkonzept* gleichbedeutend mit Lastenheft verwendet.

Im Lastenheft definiert der Auftraggeber demnach das „Was“ und das „Wofür“. Es beschreibt jedoch nicht wie etwas gemacht werden soll. Zusätzlich enthält es eine Beschreibung des Ist-Zustands. Wichtig ist, dass die Anforderungen qualifizierbar und nachprüfbar sind.

Gliederung

Die Gliederung des Lastenhefts ist nicht verbindlich geregelt und hängt insbesondere von der zu erstellenden Lösung ab. Für die Grobgliederung bieten die folgenden Punkte eine Vorlage:

- Allgemeines (Titel, Auftraggeber, terminlicher Rahmen)
- Zielsetzung (Anlass und Zielsetzung, Priorisierung, Begrenzung des Vorhabens)
- Produktfunktionen bzw. Aufgabenstellung (Beschreibung des Ist-Zustands, geforderte Hauptfunktionen, fachliche Anforderungen, Schnittstellen)
- Leistungsanforderungen (Leistungsumfang, Leistungs- Sicherheits- und Qualitätsanforderungen)
- Produkteinsatz bzw. Umgebung, in der das Produkt eingesetzt werden soll (technisches Umfeld, Standards, Einschränkungen)
- Ergänzungen und Randbedingungen

Hinweise zur Erstellung

Auch wenn die Gliederung etwas anderes vermuten lässt, soll das Lastenheft nur eine grobe Produktskizze für ein zu erstellendes Produkt darstellen. Es sollte daher nicht zu detailliert sein und kann häufig auf nur wenige Seiten begrenzt werden. Zusätzlich sollte auf eine übersichtliche Darstellung geachtet werden. So empfiehlt es sich, Abläufe in Zeichnungen zu verdeutlichen und Zahlenreihen in grafischen Darstellungen zu visualisieren.

Wird allerdings das Lastenheft als Grundlage für eine Ausschreibung verwendet, ist durchaus eine umfassendere Ausgestaltung erforderlich. In diesem Fall kann das Lastenheft durchaus die Qualität eines Pflichtenheftes haben.

6.3.1.2 Pflichtenheft

Aufgabe des Pflichtenheftes ist es, aus den Anforderungen des Kunden (Lastenheft) eine möglichst vollständige konsistente und eindeutige Produktdefinition als Basis für das zu erstellende Produkt zu liefern. Während im Lastenheft der Auftraggeber das „Was“ und das „Wofür“ beschreibt, definiert das Pflichtenheft das „Was“ und das „Womit“.

In der Praxis wird das Pflichtenheft manchmal auch als *fachliches Feinkonzept*, *Sollkonzept*, *Anforderungsspezifikation* oder *Funktionsspezifikation* bezeichnet.

Inhalt eines Pflichtenheftes

Der Aufbau und Inhalt eines Pflichtenheftes muss sich noch stärker als das Lastenheft daran orientieren, für welchen Zweck das Pflichtenheft benötigt wird. So unterscheidet sich ein Pflichtenheft zur Erstellung von Software zwangsläufig deutlich von einem Pflichtenheft für die Bereitstellung von Komponenten für ein Rechenzentrum. Auch in anderen Bereichen wie beispielsweise im Maschinenbau und der Fertigung gibt es die Form des Pflichtenheftes als Vorgabe für bestimmte Arbeiten.

In der Literatur finden sich Beschreibungen für Pflichtenhefte zu fast allen Bereichen, sodass an dieser Stelle auf eine detaillierte Beschreibung verzichtet werden soll. Ein Muster-Pflichtenheft einschließlich einer Word-Vorlage ist beispielsweise hier zu finden [HDVO]. Einen umfassenden Gliederungsvorschlag liefert beispielsweise Balzer in seinem Buch [SWTECHNIK]. Ein detaillierte Darstellung einschließlich einer Gliederung ist auch unter [STBAUR] zu finden.

Auf einen Punkt sollte bei der Erstellung des Pflichtenheftes aber immer geachtet werden: Wird das Pflichtenheft aus der Sicht der später zu erstellenden Dokumente erstellt, können meist sehr viele Inhalte aus dem Pflichtenheft in die spätere Betriebsdokumentation (beispielsweise die Systemakte) übernommen werden. Dies kann im nachhinein viel Arbeit sparen.

hinweis

Das Lasten- sowie das Pflichtenheft sind wichtige Dokumente der IT-Dokumentation, insbesondere wenn Aufträge extern vergeben werden. Sie dienen als Nachweis für das, was vereinbart wurde, und können vor allem bei Streitfällen von hoher Wichtigkeit sein. Sie sollten daher mit der entsprechenden Sorgfalt erstellt und verwaltet werden.

6.3.2 Änderungsanforderungen

Aufgrund neuer Anforderungen, entdeckter Fehler oder neu gewonnener Erkenntnisse wird es sich im Laufe des Projekts immer wieder als erforderlich erweisen, einmal aufgestellte Planungen anzupassen. Wichtig ist, das erforderliche Änderungen in definierten Prozessen erfolgen und nachvollziehbar dokumentiert werden.

In der Praxis zeigt es sich immer wieder, dass Änderungen, die sich in einem Projekt ankündigen, zu Beginn oftmals einfach ignoriert werden. Dies wird auch dadurch begünstigt, dass es in Projekten keine standardisierten Prozesse wie im IT-Betrieb gibt, die zwangsläufig zu einem Anstoß von Änderungsprozessen führen. Dies rächt sich aber fast zwangsläufig in einer späteren Projektphase. Zeichnen sich dann Probleme ab, wird häufig überstürzt gehandelt. Und an eine Dokumentation denkt in der Hektik niemand mehr, was eine Nachvollziehbarkeit unmöglich macht. Treten dann Konflikte ein, oder kommt es zu Rechtsstreitigkeiten, wird es aufgrund mangelnder Nachweisbarkeit besonders schwierig.

Änderungen dürfen nur kontrolliert erfolgen

Es ist daher wichtig, erforderliche Änderungen nicht aufzuschieben und den Änderungsprozess so zu gestalten, dass nur kontrolliert geändert wird. Dazu sollte der Änderungsprozess die folgenden Schritte umfassen:

- Änderungen identifizieren und beschreiben (Änderungsanforderung)
- Änderungen klassifizieren nach der Dringlichkeit und dem Grad ihrer Auswirkung

- Änderungen bewerten und eine Entscheidung vorbereiten in Bezug auf die Risiken, die entstehen, wenn die Änderung nicht durchgeführt wird, und in Bezug auf die Risiken, die durch die Änderung entstehen
- Änderungen genehmigen
- Änderungen veranlassen
- Änderungen durchführen, testen und freigeben
- Die genannten Schritte dokumentieren
- Änderungen verifizieren (Ist der erwartete Nutzen eingetreten?)

Änderungsanforderung

Ein wichtiges Dokument in diesem Prozess ist die *Änderungsanforderung*. In der Praxis wird diese auch als *Änderungsantrag*, *Change Request (CR)* oder *Request For Change (RFC)* bezeichnet.

Im Wesentlichen handelt es sich bei der Änderungsanforderung um einen standardisierten Antrag zur Durchführung einer Änderung. Jede Änderungsanforderung sollte mindestens die folgenden Informationen beinhalten:

- Eindeutige RFC-ID
- Datum der Erstellung
- Name des Erstellers
- Begründung für die Änderung
- Bekannte Auswirkungen auf andere Systeme oder Prozesse sowie mögliche Risiken
- Bekannte Auswirkungen und Risiken, sofern die Änderung nicht durchgeführt wird
- Datum der gewünschten Umsetzung
- Geschätzter Zeitaufwand für die geforderte Änderung
- Kostenschätzung der Änderung (gegebenenfalls getrennt nach internen und externen Kosten, Lizenzkosten, Personalkosten usw.)
- Beteiligte Organisationseinheiten
- Ergebnis der Genehmigungsprüfung (Begründung, Auflagen)
- Detaillierte Beschreibung der erforderlichen Änderung
- Rollback-Pläne
- Einfluss auf vorhandene Notfallpläne

cd-rom

In Abschnitt 8.9 und auf der beigefügten CD-ROM befindet sich ein Bespiel für eine Änderungsanforderung, das als Muster verwendet werden kann.

Änderungen können hinsichtlich ihres Umfangs und ihrer Auswirkungen sehr unterschiedlich sein. Während bei vielen Änderungen die Genehmigung durch den Projektleiter oder einen Fachverantwortlichen ausreicht, sollten umfangreiche Änderungen im Projekt zusätzlich durch ein Gremium wie den Lenkungsausschuss freigegeben werden.

Änderungsklassen

Die folgende Klassifizierung stellt ein Beispiel dar. Es ist aber auch eine stärkere Detaillierung mit weiteren Änderungsklassen möglich. Allerdings wachsen mit einer stärkeren Unterteilung auch die Abgrenzungsprobleme.

- Die *Änderungsklasse 1* umfasst alle Anträge, die nicht in die Klasse 2 fallen bzw. keine Standard-Änderungen sind. Diese Änderungen haben Auswirkungen auf den Leistungsumfang des Projekts. Sie müssen den Änderungsprozess komplett durchlaufen und in der Änderungskonferenz des Lenkungsausschusses genehmigt werden.
- Die *Änderungsklasse 2* umfasst alle Änderungen, die nur geringe Auswirkungen und geringe Risiken haben. Sie müssen ebenfalls den Änderungsprozess durchlaufen, können aber vom Projektleiter, einem Fachverantwortlichen oder dem Change-Koordinator freigegeben werden.

Standardänderungen sind projektuntypisch

Zusätzlich zu den beiden Klassen gibt es zumindest im Betrieb die Klasse der *Standard-Änderungen*. Hierbei handelt es sich um wiederkehrende Änderungen, die den Änderungsprozess bereits durchlaufen haben, einem dokumentierten Ansatz folgen und für die keine erneute Freigabe erforderlich ist. In einem Projekt, das ja durch seine Einmaligkeit gekennzeichnet ist, wird es nur bei sehr langfristigen Projekten derartige Änderungen geben.

Zu beachten ist, dass auch ein Abbruch oder die Ablehnung einer Änderung einen formalen Prozess durchlaufen und dokumentiert werden muss. Beispielsweise ist zu klären, ob der Antrag ganz oder teilweise abgelehnt wird und ob eine Alternative zwingend erforderlich ist.

6.3.3 Entscheidungsvorlagen

Auch wenn alle Rahmenbedingungen im Projektvertrag festgelegt sind, wird es in einem Projekt immer wieder Situationen geben, in denen Entscheidungen auf der Leitungsebene erforderlich sind. Außerdem ist es nicht unüblich, in Konzepten alternative Lösungswege aufzuzeigen über die dann auf Leitungsebene entschieden werden muss. Derartige Entscheidungen können beispielsweise erforderlich sein, wenn damit auch die Freigabe finanzieller Mittel sowie personeller Ressourcen verbunden ist.

Für diese Zwecke werden Entscheidungsvorlagen benötigt. Mit der Entscheidungsvorlage sind den Verantwortlichen alle notwendigen Informationen bereitzustellen, um entscheiden zu können, ob und welcher der beschriebenen Lösungsansätze weiterverfolgt werden soll.

Wesentliche Inhalte

Dazu sollte die Entscheidungsvorlage folgende Informationen liefern:

- *Kontext:* Kurze Beschreibung des Kontexts, in dem die Entscheidung zu treffen ist.
- *Zielsetzungen:* Managementorientierte Beschreibung der mit dem Einsatz der beschriebenen Lösungen verbundenen Ziele
- *Lösungsansätze:* Skizzierung aller alternativen Lösungsansätze einschließlich zu erwartender Kosten und personeller Aufwende
- *Diskussion der Lösungsansätze:* Benennung von Vor- und Nachteilen der einzelnen Lösungsansätze und Vergleich der Lösungsansätze. Falls sinnvoll bzw. möglich, sollte auch eine Gegenüberstellung von Kosten und Nutzen erfolgen.
- *Empfehlung:* Begründete Empfehlung eines Lösungsansatzes und Darstellung der zu erwartenden Kosten und Aufwende.

Wichtig ist eine prägnante und auf die wesentlichen Informationen reduzierte Darstellung. Diese Anforderungen können am besten durch eine entsprechende Dokumentvorlage sichergestellt werden.

cd-rom

In Abschnitt 8.10 und auf der beigefügten CD-ROM befindet sich ein Bespiel für eine Entscheidungsvorlage, die als Muster verwendet werden kann.

6.3.4 Testdokumentation

Tests sind ein unverzichtbares Element der Qualitätssicherung sowie der Entscheidungsfindung, nicht nur in einem Projekt. Für alle Änderungsprozesse gilt grundsätzlich: Änderungen an Systemen oder Neuentwicklungen dürfen ohne ausreichende Tests in den Produktivbetrieb nicht übernommen werden. Hierbei müssen in der Regel mehrere Teststufen durchlaufen werden: Funktionstests, Integrationstests, Lasttests, Abnahmetests usw. Alle Tests müssen systematisch und klar definiert durchgeführt werden, was nur mit einer entsprechenden Dokumentation möglich ist. Diese Forderung gilt grundsätzlich und unabhängig davon, ob Änderungsprozesse im Rahmen eines Projekts oder im Regelbetrieb umgesetzt werden. Sowie für alle Entwicklungen, egal ob es sich dabei um eine neu entwickelte Softwarelösung oder um einen neu zu implementierenden Server handelt.

Industriestandard IEEE 829

Beachtenswert, insbesondere für die Durchführung von Softwaretests, ist der vom IEEE (Institute of Electrical and Electronic Engineers) veröffentlichte Standard 829 für die Softwaretestdokumentation. Dieser Standard beschreibt in acht Dokumenten den inhaltlichen Aufbau von Testdokumenten und liefert wichtige Anhaltspunkte für die Dokumentation von Softwaretests [IEEE].

Die nachstehende Beschreibung der Testdokumente lehnt sich an diesen Standard an.

6.3.4.1 Testkonzept

Für alle Tests, die in einem Projekt durchzuführen sind, ist zu gewährleisten, dass die Testfälle umfänglich und vollständig sind, einen definierten Testprozess durchlaufen und dass dieser einen revisionssicheren Ablauf gewährleistet. Es werden daher Dokumente für die Testplanung benötigt. Dies ist die Aufgabe des Testkonzepts. Bezogen auf den IEEE-Standard 829 entspricht dieses Dokument dem dort benannten *Testplan*.

Das Testkonzept bildet den inhaltlichen Leitfaden: Also sozusagen das Drehbuch für die Testdurchführung und beinhaltet sowohl die Testziele sowie Abgrenzung, Vorgehensweise, Mittel und Ablaufplan der Testaktivitäten und Beschreibungen der Testprozesse.

In der Regel werden innerhalb eines Projekts unterschiedliche Teststufen durchlaufen. Hierbei handelt es sich mindestens um die nachfolgenden Teststufen. In Abhängigkeit vom Projekt können zusätzlich noch Last- und Stresstests erforderlich sein.

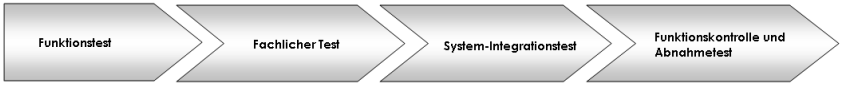


Abbildung 6.7: Mehrstufiges Testverfahren

beispiel

Die Einführung einer neuen Software erfordert zunächst einen *Funktionstest*, in dem die zugesicherten Eigenschaften der Software getestet werden.

Wurde der Funktionstest erfolgreich abgeschlossen, muss die neue Software von Seiten der Fachabteilung getestet werden. Während beim Funktionstest nur geprüft wird, ob alle Funktionen der Software fehlerfrei arbeiten, geht es beim *fachlichen Test* vor allem darum zu bewerten, ob die Software auch die korrekten Ergebnisse liefert. Die kann nur durch von den Fachverantwortlichen bzw. den späteren Anwendern bewertet werden.

Auf der nächsten Teststufe wird das Zusammenspiel der neuen Software mit den anderen Systemkomponenten (*System-Integrationstest*) der Systemumgebung erprobt. Im Vordergrund steht hier die Überprüfung der Funktionalitäten des Software-Systems im Zusammenspiel mit dem Gesamtsystem und die Untersuchung möglicher Beeinträchtigungen des Gesamtsystems. Dies gewährleistet eine formalisierte Überprüfung, wie gut Änderungen mit dem produktiven System zusammenarbeiten werden.

Abhängig von der einzuführenden Software kann es nach dem Integrationstest erforderlich sein, weitere Tests zur Verifikation und Einschätzung der Systemkapazitäten und des Systemsverhaltens unter Last durchzuführen. Während beim Integrationstest die Funktionen der Software nur anhand weniger Testdaten geprüft werden, dienen diese Tests dazu, das Verhalten der Software bei der Verarbeitung von Massendaten zu testen. Unterschieden werden kann noch zwischen *Lasttests*, die ein System an den (geforderten) Grenzen der Leistungs-

fähigkeit testen, und *Stresstests*, die das Verhalten bei Überlast, d. h. bei einem temporären Überschreiten der Grenzen, prüfen. Weiter kann es auf dieser Teststufe sinnvoll sein, *Robustheitstest* durchzuführen. Diese Tests überprüfen das Systemverhalten bei einem Ausfall einzelner Teile oder unter anormalen Umgebungsbedingungen und schließen den provozierten Ausfall spezifischer Teilkomponenten ein.

Hat die neu entwickelte Software auch diese Teststufe erfolgreich durchlaufen, erfolgt die Implementierung in der Produktivumgebung. Nach einer nochmaligen ausführlichen *Funktionskontrolle* können dann die Übergabe und Abnahme erfolgen (Abnahmetest). Der formelle *Abnahmetest* soll sicherstellen, dass das System die Forderungen des Pflichtenheftes in dem Verständnis des Auftraggebers erfüllt. Mit der Abnahme gehen schließlich auch die Gefahren auf den Auftraggeber; die Gewährleistung beginnt.

Inhalt des Testkonzepts

Das Testkonzept sollte Vorgaben für alle Teststufen enthalten und für jede Stufe die folgenden Punkte beschreiben:

- Zielsetzung der Tests und erwartete Ergebnisse
- Voraussetzungen für die Testdurchführung
- Hinweise zur Testorganisation
- Testinhalt und Testabgrenzung (zu testende Leistungsmerkmale und Leistungsmerkmale, die nicht getestet werden)
- Testinfrastruktur (Systemumgebung, Testtools)
- Testablaufplanung (Zeitplanung , Testteilnehmer)
- Prozessbeschreibung für den Testablauf
- Verantwortlichkeiten und Zuständigkeiten
- Kriterien für einen Testabbruch und eine Testfortsetzung
- Testdokumentation (Was ist zu dokumentieren, welche Dokumente werden benötigt?)
- Abnahmekriterien und Freigabeverfahren
- Risikoanalyse

Einheitliches Verständnis schaffen

Dem Testkonzept kommt aber noch eine weitere wichtige Aufgabe zu. Es verwundert nicht allzu sehr, dass in der Literatur die Definition der Begriffe rund um das Thema „Testen“ nicht einheitlich ist. So sprechen die einen von Integrationstest, während andere diesen als Systemtest oder als System-Integrationstest (als Abgrenzung zum Fachtest) bezeichnen.

Wichtig ist aber, dass innerhalb eines Projekts eine einheitliche Verwendung der Begriffe herrscht. Was ein Integrationstest ist, muss für das Projekt verbindlich definiert werden, um im Team ein einheitliches Verständnis dafür zu erzielen. Diese Festlegungen können im Testkonzept erfolgen.

6.3.4.2 Dokumente für die Testdurchführung

Gemäß IEEE-Standard 829 untergliedern sich die Dokumente für die Testdurchführung wie folgt: *Test-Design-Spezifikation, Testfall-Spezifikation* und *Test-Ablauf-Spezifikation*.

Unabhängig davon, ob man sich an dieser Unterteilung ausrichtet oder nicht: Es werden Dokumente benötigt, die die einzelnen Testfälle spezifizieren. Ein Testfall ist eine Kombination von Eingabedaten, Bedingungen und erwarteten Ausgaben, die einem bestimmten Zweck dienen. Daher müssen für jeden Testfall die zu benutzenden Eingaben und zu erwarteten Ausgaben benannt und alle Schritte zur Durchführung des jeweiligen Testfalls beschrieben werden.

Mindestens die folgenden Abschnitte sollte jede Testfallbeschreibung enthalten:

- Eindeutige Nummerierung
- Verantwortlicher
- Testdurchführender
- Beschreibung der Testfallumgebung
- Testfallbeschreibung und zu testende Funktionen
- Test-Input
- Test-Output
- Qualitätsmerkmale und Testkriterien
- Schnittstellen zu anderen Tests

cd-rom

In Abschnitt 8.11 und auf der beigefügten CD-ROM finden Sie ein Beispiel für eine Testfallbeschreibung, die als Muster verwendet werden kann.

6.3.4.3 Test-Ergebnisdokumente

Besonders wichtige Dokumente liefert natürlich die Testdurchführung. Hier müssen Ergebnisse, Fehler, Mängel und unerwartete Ereignisse dokumentiert werden.

Der Standard IEEE 829 unterscheidet vier verschiedene Dokumente für die Testbeschreibung: *Testfall-Übertragungsbeschreibung*, *Testprotokoll*, *Test-Störfall-Beschreibung* und die *Test-Zusammenfassung*. Die Testfall-Übertragungsbeschreibung wird in den Fällen benötigt, in denen getrennte Entwicklungs- und Testteams an der Entwicklung beteiligt sind.

Von besonderer Wichtigkeit ist das Testprotokoll. Dieses dient zur Aufzeichnung der Ereignisse während eines Tests und enthält Angaben über alle ausgeführten Testfälle, deren Ergebnisse und aufgetretene Abweichungen vom erwarteten Ergebnis.

Wichtig als Nachweis

Das Protokoll dient in erster Linie dazu, die korrekte Arbeit des Testteams zu dokumentieren. Aufgetretene Fehlersituationen sollten besser in einem eigenen Dokument ausgeführt werden. Denn treten später Probleme auf, ist es in der Regel an dem Testteam nachzuweisen, warum der Fehler nicht früher erkannt wurde. Anhand eines vollständigen Testprotokolls kann dann ermittelt werden, ob für die fragliche Situation ein Testfall existierte, ob er ausgeführt wurde und was das Ergebnis war.

Ein Testprotokoll sollte daher mindestens die folgenden Informationen enthalten:

- Eindeutige Nummerierung
- Verantwortliche, beteiligte Personen
- Beschreibung aller durchgeführten Testfälle einschließlich Testumgebung und Testdurchführung
- Beschreibung der Testergebnisse einschließlich des Systemverhaltens und der Systemmeldungen und einer fachlichen und technischen Bewertung der Testergebnisse durch die am Test beteiligten Stellen

cd-rom

In Abschnitt 8.12 und auf der beigefügten CD-ROM befindet sich ein Beispiel für ein Testprotokoll, das als Muster verwendet werden kann.

Neben den Testprotokollen ist die Testzusammenfassung wichtig, die gleichzeitig eine Freigabebescheinigung beinhaltet, beispielsweise für das Erreichen der nächsthöheren Teststufe (siehe dazu nachfolgenden Abschnitt).

Testzusammenfassung = Freigabebescheinigung

Folgende Punkte sollten in der Testzusammenfassung daher enthalten sein:

- Geprüftes System und geprüfte Verfahren
- Anlass für Test und Freigabe
- Genaue Bezeichnung der freigegebenen Komponenten, Dokumente, Programme usw. (mit Versionsnummern)
- Bestätigung, dass die vorgeschriebenen Prüfungen erfolgreich durchgeführt wurden
- Freigabeerklärung

6.3.4.4 Hinweise zur Testumgebung

Unabhängig davon, ob ein neues System in einem Projekt oder innerhalb des laufenden Betriebs entwickelt wird, muss immer Folgendes gelten: Bevor Änderungen in eine Produktionsumgebung eingebracht werden dürfen, müssen sie getestet und freigegeben sein. Demzufolge ist die Vorhaltung einer Testumgebung zwingend erforderlich.

Empfehlenswert ist ein mehrstufiges Testverfahren. Hierbei ist der Übergang in die nächst höhere Systemumgebung nicht ohne ein erfolgreiches Durchlaufen der Tests der tieferen Teststufe und ohne entsprechende Freigaben möglich.

Entwicklungstestumgebung

Bei diesem dreistufigen Verfahren gibt es mit der Entwicklungstestumgebung eine Testumgebung in der die Funktionstests stattfinden. Die Testumgebung sollte möglichst die gleichen Kernkomponenten bereitstellen, wie sie in der produktiven IT-Infrastruktur verwendet werden.

Die Entwicklungstestumgebung unterliegt nicht den gleichen Betriebsprozessen wie die Produktionsumgebung. Die Umgebung sollte schnell auf einem definierten Ausgangszustand wieder herstellbar sein (beispielsweise durch Nutzung von Imageverfahren), weshalb eine Datensicherung typischerweise nur für ausgewählte Systeme durchgeführt wird. Außerdem muss die Entwicklungstestumgebung zwingend in einem isolierten Netzwerk betrieben werden, um keinerlei Rückwirkungen auf die produktive Umgebung zu haben.

Integrationstestumgebung

Die Integrationstestumgebung stellt idealerweise das komplette Abbild der Produktionsumgebung dar und beinhaltet die gleichen Technologien (Infrastruktur, Applikationen, Überwachungssysteme usw.) wie diese, sodass produktionsnahe Tests möglich sind. Sie muss ebenfalls zwingend in einem isolierten Netzwerk betrieben werden, um Rückwirkungen auf die Produktionsumgebung auszuschließen.

Damit die Integrationstestumgebung jederzeit die Produktionsumgebung widerspiegeln kann, muss sie den gleichen Betriebsprozessen unterliegen und auch entsprechend dokumentiert werden. In der Praxis werden hierzu häufig mit Hilfe von Synchronisations-Skripten beispielsweise Konten und Richtlinien von der Produktionsumgebung in die Integrationstestumgebung hinein synchronisiert.

Datenschutz beachten

Bei der Übernahme von Daten aus der Produktionsumgebung ist aber Vorsicht geboten. Denn sobald es sich dabei um personenbezogene Daten handelt, steht eine solche Vorgehensweise im Widerspruch zum Datenschutz. Dies ist darin begründet, dass in der Testumgebung aufgrund anderer Zugriffsberechtigungen möglicherweise unberechtigte Personen auf schützenswerte Daten Zugriff erlangen. Richtigerweise sollten daher in der Integrationstestumgebung produktionsnahe, anonymisierte Testdaten verwendet werden.

In der Integrationstestumgebung werden vor allem Integrationstests durchgeführt. Aber auch die fachlichen Tests sowie Belastungs- und Robustheitstests finden hierin statt. Um einen konsistenten Zustand mit der Produktionsumgebung aufrechtzuerhalten, dürfen Änderungen niemals erfolgen, ohne gleichzeitige Vorkehrungen zu planen, wie diese wieder rückgängig zu machen sind. Hierbei muss vor allem betrachtet werden, ob die Änderungen nur ein einzelnes

oder mehrere Systeme umfassen. Deshalb sind Rollback-Strategien immer inklusive der erforderlichen Wiederherstellungsschritte zu dokumentieren.

Die gesamte Testumgebung sollte in einer gesonderten Systemakte dokumentiert werden (siehe hierzu Abschnitt 4.2.2). Besondere Dokumentationsanforderungen aber gelten für die Integrationstestumgebung. Hierfür müssen alle Änderungen konsequent dokumentiert werden. Nur wenn jederzeit der Zustand der Integrationstestumgebung bekannt ist, ist eine verlässliche Durchführung und Bewertung von Integrationstests möglich. Die Dokumentation kann mit Hilfe von Logbüchern und Übersichtstabellen erfolgen, in denen die wichtigsten Änderungen festgehalten werden. Wird für die Produktionsumgebung eine Inventardatenbank (CMDB) geführt, sollte idealerweise auch die Integrationstestumgebung in diese mit einbezogen werden.

Tests auch im IT-Betrieb

Natürlich wird eine solche Testumgebung nicht nur von Seiten der Projektteams genutzt. Zu den Aufgaben des IT-Betriebs gehört eine regelmäßige Funktionskontrolle und eine Reihe von Aufgaben, die ebenfalls Tests erfordern. So sollten beispielsweise Service Packs vor dem Einspielen auf ihre Auswirkungen hin getestet werden, was sinnvollerweise ebenfalls in der Integrationstestumgebung erfolgt.

Zu den typischen Tests des Regelbetriebs gehören unter anderem die folgenden:

- *Service Pack- und Hot-Fix-Installationstest:* Prüfung von Service Packs und Hot-Fixes im Hinblick auf Installationsverfahren, Anforderungen, beabsichtigte sowie unvorhergesehener Auswirkungen. Auch Tests aufgrund eines Release-Wechsel können dieser Kategorie zugerechnet werden.
- *Sicherheitstests:* Hierbei handelt es sich zum einen um Tests, die der Verifikation dienen, dass ausschließlich Benutzer mit korrekter Autorisierung die Funktionalitäten des betrachteten Systems nutzen können. Zum anderen zählen hierzu Auditierungstests (zum Beispiel Penetrationstests), die die korrekte Umsetzung sicherheitsrelevanter Systemkonfigurationen verifizieren sollen.
- *Backup- und Recovery-Tests*: Bei diesen Tests handelt es sich um systemspezifische Prüfungen zur Unterstützung des IT-Betriebes, um die Sicherung und Wiederherstellung von Daten und kompletten Systemen zu verifizieren.
- *Robustheitstests:* Diese Tests überprüfen das Systemverhalten bei einem Ausfall einzelner Teile oder unter anormalen Umgebungsbedingungen und schließen den provozierten Ausfall spezifischer Teilkomponenten ein. Diese Tests werden vor allem bei Systemen durchgeführt, die der Verfügbarkeit dienen, wie beispielsweise Cluster-Systeme.
- *Überwachungstests:* Bei diesen Tests werden die Systeme auf korrekte und effiziente Überwachungs- und Alarmfunktionaliäten hin überprüft. Typischerweise wird hierbei auch die Fernüberwachung von Systemen verifiziert.
- *Skalierungstests:* Hierbei handelt es sich um typische Tests des Änderungsmanagements, die dazu dienen, die Skalierungsfähigkeit und die Erweiterbarkeit der Systeme einzuschätzen.

6.3.5 Konzepte

Wie an so mancher Stelle im vorliegenden Buch, könnte man auch an dieser Stelle wieder ein munteres „Begriffe-JoJo“ einfügen, denn wie die Ausführungen bereits gezeigt haben, gibt es zahlreiche Ausprägungen und Verwendungen des Begriffs „Konzept“ (Fachkonzept, DV-Konzept, Sollkonzept, Systemkonzept usw.), unter denen fast jeder etwas anderes versteht.

Es wurde daher schon mehrfach auf die Notwendigkeit hingewiesen, beim Aufbau der eigenen IT-Dokumentation die Verwendung der Dokumentenbezeichnungen für das eigene Unternehmen zu definieren und diese deutlich voneinander abzugrenzen. Weiter muss die verbindliche Verwendung der Begriffe kommuniziert und sichergestellt werden, dass jeder, der Dokumente erstellt, die Bezeichnungen dementsprechend verwendet. Dies gilt insbesondere für die Definition der zu erstellenden Konzepte.

Hier als „Technische Konzepte“ bezeichnet

Bei den hier betrachteten Konzepten handelt es sich um Dokumente, die auf der Grundlage der Ausgangsituation und der Anforderungsanalyse die technisch zu realisierende Lösung für eine definierte Aufgabe liefern und planerischen Charakter haben. Zur Abgrenzung anderer Konzepte, wie dem Testkonzept oder den zu den Rahmendokumenten zählenden Konzepten wie beispielsweise dem Rollenkonzept, werden derartige Konzepte im vorliegenden Buch als „Technische Konzepte“ bezeichnet.

Technische Konzepte gehören zu den wichtigsten Dokumenten eines jeden Projekts. Unabhängig davon, ob es sich um ein Organisationsprojekt handelt, das die Veränderung bestehender Organisationsstrukturen zum Ziel hat, oder um ein Projekt zur Migration auf ein neues Betriebssystem: Es wird mindestens ein technisches Konzept benötigt, das die geplante Lösung vorstellt und die erforderlichen Schritte aufzeigt. Wie viele technische Konzepte in einem Projekt benötigt werden, hängt natürlich in erster Linie von seinem Inhalt und seiner Größe ab.

beispiel

Handelt es sich beispielsweise um ein Projekt zur Einführung eines Ticket-Systems für den Helpdesk, können durchaus alle Aspekte in einem technischen Konzept behandelt werden. In einem solchen Fall wird der Lösungsgegenstand sehr häufig mit dem Projekt gleichgesetzt. Daher kommt es, dass man in der Literatur sehr häufig einem „Konzept für das Projekt“ begegnet. Soll in einem großen Unternehmen jedoch eine komplette Migration auf ein neues Serversystem einschließlich der Umstellung aller Clientrechner durchgeführt werden, können sogar sehr viele technische Konzepte für die einzelnen Komponenten (Migration der Server, Active Directory-Migration, Update Exchange, Client-Rollout) erforderlich sein.

Grobkonzept und Feinkonzept

Zwei Begriffe, die im Zusammenhang mit Konzepten immer wieder genannt werden lauten: *Grobkonzept* und *Feinkonzept*. Allerdings werden diese beiden Begriffe in unterschiedlichster Art verwendet.

Wird das Grobkonzept eher aus Projektmanagement-Sicht betrachtet, ist es bereits in der Projektinitialisierungsphase zu erstellen und zeigt die Inhalte sowie die wichtigsten Meilensteine des geplanten Projekts auf. Aus Sicht der Software-Entwicklung wird das Grobkonzept hingegen eher im Zusammenspiel mit dem Fachkonzept und dem DV-Konzept gesehen.

Die Beispiele zeigen, dass die Verwendung der beiden Begriffe in der Praxis ganz verschieden ist. Im vorliegenden Buch werden die Begriffe Grob- und Feinkonzept ausschließlich am Detaillierungsgrad ausgerichtet. Es kann nämlich in vielen Fällen durchaus sinnvoll sein, ein dem endgültigen technischen Konzept vorlaufendes Konzept mit einem geringeren Detaillierungsgrad zu erstellen.

In einem solchen Grobkonzept können beispielsweise auch alternative Lösungswege aufgezeigt werden. Diese Vorgehensweise minimiert das Risiko, mit einem direkt erstellten „Feinkonzept“ in die falsche Richtung zu laufen, und bietet frühzeitige Umkehrmöglichkeiten. Auf der Basis eines derart abgestimmten Grobkonzepts kann anschließend das Feinkonzept entwickelt werden.

6.3.5.1 Aufbau und Inhalt technischer Konzepte

Der formale Aufbau eines technischen Konzepts unterscheidet sich nicht wesentlich von dem, wie er in Abschnitt 7.1.1 ausführlich beschrieben ist. Einzig das Management Summary ist bei einem Konzept nicht als optionale Komponente zu behandeln. Da Konzepte immer auch von Entscheidern gelesen werden, sollte jedes Konzept diese Zusammenfassung enthalten.

Der inhaltliche Teil eines technischen Konzepts sollte mit einer Beschreibung der Ausgangssituation bzw. des Ist-Zustands der Umgebung beginnen, für die das Konzept eine Lösung liefern soll. Daran anschließen kann sich ein Überblick über die Anforderungen und Ziele, die mit der beschriebenen Lösung erreicht werden sollen. Den Schwerpunkt bildet die Beschreibung der möglichen Lösung sowie eine Beschreibung der geplanten Prozesse. Die Darstellung der Prozesse kann hier noch auf einem hohen Abstraktionsgrad erfolgen.

Handelt es sich bei dem Konzept um ein vorausgehendes Grobkonzept, sind die bestehende Struktur und – wie der Name bereits aussagt – grob die angestrebte Lösung zu beschreiben. Das heißt, die wichtigsten Funktionen werden definiert und im Überblick beschrieben. Das Feinkonzept hingegen umfasst die genauen Anweisungen für die Umsetzung. Hier werden die ermittelten Funktionen weiter analysiert und dargestellt. Dies kann eine Beschreibung der benötigten Infrastruktur (Hardware, Netzwerk, Support, Lizenzen usw.) sowie erste Erläuterungen für den Betrieb des neuen Systems einschließen.

Aufzeigen von Lösungsalternativen möglich

Gibt es Lösungsalternativen zum Erreichen der angestrebten Ziele, ist es sinnvoll, diese im technischen Konzept gegenüberzustellen. Dies schließt eine Benennung von Vor- und Nachteilen der einzelnen Lösungsansätze und einen Vergleich der Lösungsansätze untereinander ein. Auch eine Wirtschaftlichkeitsbetrachtung kann durchaus Gegenstand des technischen Konzepts sein. Den Abschluss sollte in diesem Falle eine kurze Zusammenfassung mit einer abschließenden Empfehlung (insbesondere für die Geschäftsleitung) bilden.

Sofern für das spezifische System sinnvoll, sollte das technische Konzept auch Aussagen zu Rollen und Berechtigungen enthalten. Außerdem ist es hilfreich, wenn das technische Konzept bereits Aussagen zu personal- und datenschutzrechtlichen Erfordernissen enthält.

Den Abschluss kann eine Darstellung der Schnittstellen und Zulieferleistungen bilden. Hier sollten Verbindungen zu Schnittstellen aufgezeigt werden, die folgende Fragen beantworten: Welche Lieferleistungen müssen durch andere Projekte bzw. Bereiche erbracht werden? Welche Vorgaben und Anforderungen ergeben sich aus der Lösung für andere Projekte bzw. Bereiche?

hinweis

Erfolgt eine vollständige Darstellung der Lösungsalternativen im Konzept, muss mit der Abnahme die gewählte Lösung benannt werden. Alternativ oder auch zusätzlich kann eine Entscheidungsvorlage ausgefüllt werden (siehe hierzu Abschnitt 6.3.3).

Die nachstehende Abbildung zeigt exemplarisch eine Gliederung für ein technisches Konzept. Selbstverständlich muss diese in Abhängigkeit vom Konzeptgegenstand angepasst und gegebenenfalls erweitert werden.

cd-rom

Eine Dokumentvorlage für ein technisches Konzept finden Sie auf der beigefügten CD-ROM

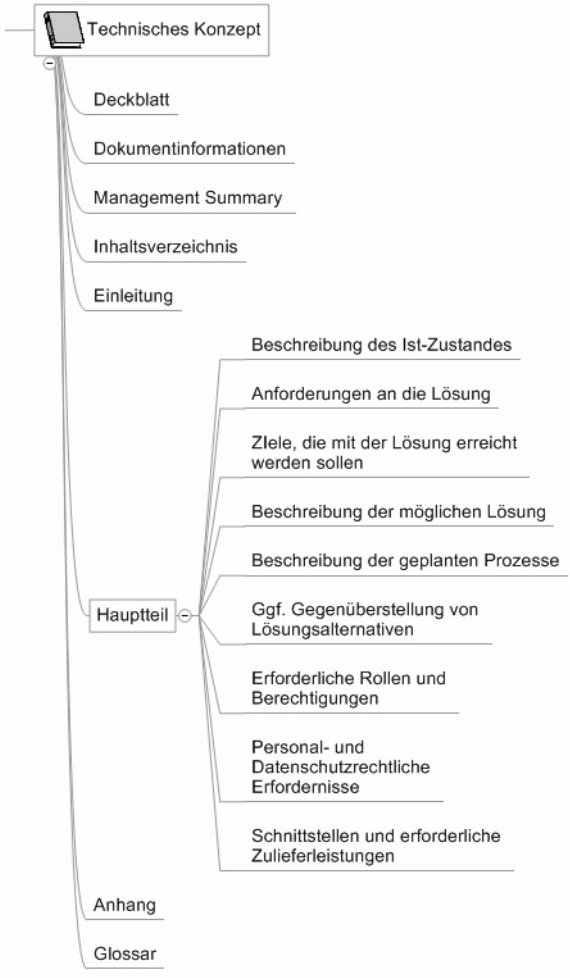


Abbildung 6.8: Gliederungsvorschlag für ein technisches Konzept

6.3.5.2 Freigabeprozess für ein technisches Konzept

Wie zuvor ausgeführt wurde, beschreiben Konzepte einen Lösungsweg für eine definierte Aufgabe und liefern damit die Basis für alle weiteren Aufgaben. Daher kommt der Qualitätssicherung und der Freigabe von technischen Konzepten ein hoher Stellewert zu.

Gilt für alle Dokumente

Generell sollte gelten, dass eine Verwendung eines Dokuments erst erfolgen darf, wenn dieses den Status „freigegeben" erreicht und damit den Qualitätssicherungs- und Freigabeprozess erfolgreich durchlaufen hat. Bei Dokumenten, für die kein Abnahmeprozess erforderlich ist, entspricht dies dem Status „endgültig (final)". Siehe hierzu Abschnitt 7.1.1.3.

Technische Konzepte sollten immer einen Freigabeprozess durchlaufen. Und sofern es sich nicht um ein reines Organisationsprojekt handelt, stellt die Freigabe eines Konzepts insofern eine Besonderheit dar, dass die Freigabe eng verzahnt ist mit dem Testprozess. So darf es in der Praxis natürlich nicht passieren, dass ein Konzept zur Implementierung eines Anwendungsservers abgenommen wird, obwohl die Tests, mit denen die Funktionen des Servers getestet werden, noch gar nicht abgeschlossen sind.

Anforderungen an die Prüfung

Der Freigabeprozess ist ein mehrstufiger Prozess. Bei jeder Stufe sollten die folgenden grundsätzlichen Punkte überprüft werden:

- Übereinstimmung mit den in der Dokumentationsrichtlinie definierten formalen Anforderungen
- Übereinstimmung mit den Anforderungen des Auftraggebers
- Formale und inhaltliche Vollständigkeit
- Technische Angemessenheit und Durchführbarkeit
- Sachliche Richtigkeit
- Schnittstellen zwischen dem zu prüfenden Dokument und bereits bestehenden Dokumenten

Wichtig und eigentlich selbstverständlich ist bei jeder Qualitätssicherung und Freigabe außerdem die Einhaltung der Regel: Der Qualitätssicherer eines Dokuments darf nicht gleichzeitig der Ersteller sein.

---

cd-rom

Ein Muster für eine Checkliste zur Qualitätssicherung und Freigabe von Dokumenten finden Sie in Abschnitt 8.7 und auf der beigefügten CD-ROM.

Stufen des Freigabeprozesses

Wie bereits erwähnt, sind beim Freigabeprozess meist die Ergebnisse des Testprozesses einzubeziehen. Hierbei kann die folgende Vorgehensweise sinnvoll sein:

- Das technische (Fein-)Konzept wird erstmalig in der Version 0.1 zur Qualitätssicherung eingereicht. Detaillierte Erläuterungen zur Versionierung finden Sie in Abschnitt 7.1.1.4. Wurde zuvor ein Grobkonzept erstellt, muss dieses bereits freigegeben sein.
- Die Freigabe in der Version 0.1 beinhaltet gleichzeitig die Zulassung zu den erforderlichen Funktionstests.
- Die Funktionstests müssen erfolgreich abgeschlossen sein, bevor der gegebenenfalls überarbeitete und angepasste Entwurf in der Version 0.5 auf der nächsten Stufe erneut zur Qualitätssicherung vorgelegt werden kann.
- Die Freigabe in der Version 0.5 beinhaltet wiederum gleichzeitig die Zulassung zum fachlichen Test und zum System-Integrationstests.

- Auch diese Tests müssen erfolgreich abgeschlossen sein, bevor für das technische Konzept die endgültige Freigabe in der Version 1.0 beantragt werden kann.
- Sind ergänzende Tests, wie beispielsweise Last- oder Robustheitstests erforderlich, kann noch eine weitere Abnahmestufe mit der Versionsnummer 0.8 eingefügt werden.

Änderungen an freigegebenen Dokumenten

Müssen später noch Änderungen an einem freigegebenen technischen Konzept erfolgen, so sollten diese mittels einer Änderungsanforderung beantragt werden. Dieser formale Weg ist erforderlich, da mit der Änderung gegebenenfalls erneute Tests verbunden sind. In diesem Fall sind bei einer Änderung dieselben Schritte wie bei der Neuerstellung zu durchlaufen.

Änderungen an technischen Konzepten (RFCs) können nur bis zur Implementierung der im Konzept beschriebenen technischen Lösung und dessen Abnahme für den Betrieb erfolgen, danach sind darauf bezogene RFCs nicht mehr zulässig. Mit der Abnahme hat das technische Konzept seine Aufgabe erfüllt. Sind später noch Änderungen am System erforderlich, so müssen diese den betrieblichen Änderungsprozess durchlaufen. Die Dokumentation erfolgt dann in den Dokumenten für den IT-Betrieb.

6.3.6 Dokumente für den IT-Betrieb

Die letzte Gruppe der hier zu betrachtenden Ergebnisdokumente beinhaltet alle Dokumente, die innerhalb des Projekts zwar erstellt werden, bei denen es sich aber um Dokumente für den IT-Betrieb handelt.

Kein Betrieb ohne Dokumente

Auch wenn dies in der Praxis nicht immer durchzuhalten ist, sollten Neuerungen und Änderungen an Systemen erst dann in die Produktionsumgebung übernommen werden, wenn auch die fertige Dokumentation dafür vorliegt. Das bedeutet: Die Systemakten müssen erstellt und die Prozessdokumentation muss erstellt und freigegeben sein. Nur so kann die Dokumentation in die Abnahme einbezogen werden – und was noch wichtiger ist: nur so kann mit dem neuen System vorgabengerecht gearbeitet werden. Ein weiteres wichtiges Argument für eine Erstellung der Dokumente parallel zur Implementierung ist, dass zu diesem Zeitpunkt alle Informationen noch präsent sind und aktuell vorliegen. Ebenso ist derjenige, der das System entwickelt und gegebenenfalls implementiert hat, noch greifbar.

Soll beispielsweise eine neu entwickelte Software in den Betrieb übernommen werden, so wird der Aufwand für die Erstellung der Systemakte reduziert, wenn derjenige, der das System programmiert hat, es auch zu dem Zeitpunkt, an dem die Information anfällt, dokumentiert. Dies ist insbesondere wichtig, wenn die Erstellung der Software extern erfolgte. Hierbei ist die neue Software so zu dokumentieren, dass zu einem späteren Zeitpunkt Wartung sowie Einarbeitung in das System effektiv und fehlerfrei möglich sind.

Ebenfalls sollten bis zum Zeitpunkt der Übernahme eines Systems in den Betrieb alle erforderlichen Änderungen an den bestehenden Betriebsdokumenten (beispielsweise Anpassungen im Rollenkonzept) erfolgt sein.

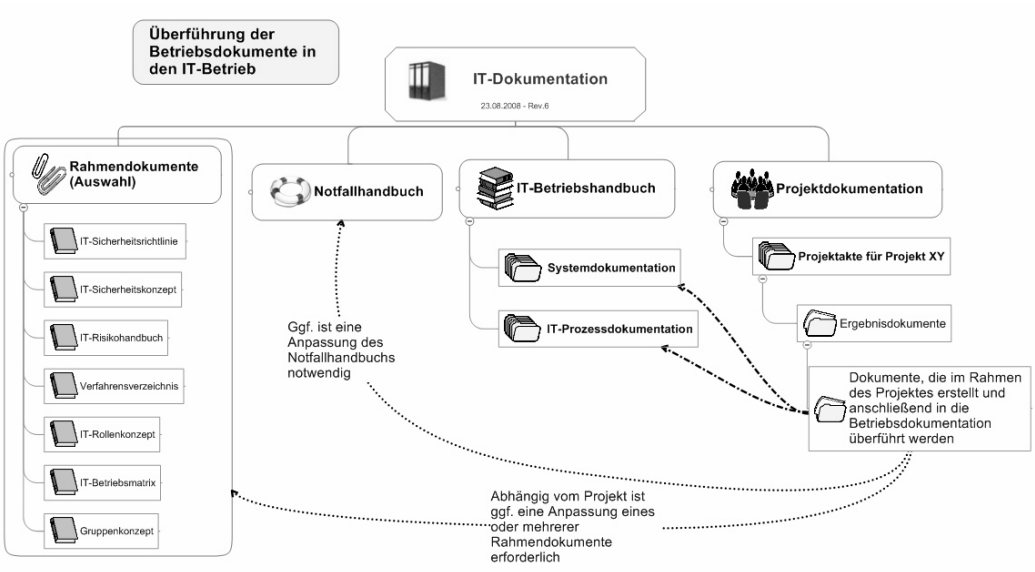


Abbildung 6.9: Erweiterung bzw. Anpassung der Betriebsdokumentation nach Projektabschluss

Praxis weicht von der Theorie ab

Das, was sich in der Grafik, also in der Theorie, noch recht einfach darstellt, klappt erfahrungsgemäß in der Praxis nur selten oder gar nicht. Gerade die Dokumentenschnittstelle, also die Erstellung der Dokumente für die Betriebsdokumentation und die Anpassung vorhandener Betriebsdokumente funktioniert häufig nicht gut oder gar nicht. Während sich alle auf die Übergabe der Systeme und Prozesse konzentrieren, fällt die Erweiterung und Anpassung der Betriebsdokumentation häufig „hinten runter".

Ein Grund hierfür ist, dass die Verantwortung der Betriebsdokumente bei einer anderen Stelle liegt als im Projekt und zwischen den beiden Stellen keine oder wenig Kontakt besteht. Hinzu kommt, dass diejenigen Projektmitarbeiter, die die Dokumentation erstellen, häufig (weil extern beauftragt) keine Kenntnis vom Betrieb und dessen Anforderungen haben und auch nicht wissen können, welche Dokumente von Seiten des Betriebs benötigt werden. Diese Schwierigkeiten führen in der Praxis dann häufig zu dem Fehler, dass überhaupt keine Dokumente für den IT-Betrieb erstellt oder die im Projekt erstellten Betriebsdokumente als abgeschlossen betrachtet werden und eine Übergabe an den Betrieb nie erfolgt. In der Folge werden Änderungen am System nicht in der Dokumentation berücksichtigt – es gibt somit eine weitere, bald veraltete „Schrank-Dokumentation".

Wie kann diesen Problemen begegnet werden?

Der wichtigste Punkt ist eine gut strukturierte und gepflegte Dokumentation für den IT-Betrieb. Denn wie sollen die Projektmitarbeiter geeignete Dokumente an den Betrieb übergeben, wenn es keine adäquate Betriebsdokumentation gibt?

Von Seiten des Betriebs müssen klare Anforderungen an die zu übergebenen Dokumente gestellt werden. Das heißt, die Dokumentationsanforderungen sollten Bestandteil des Lastenhefts sein. Diese Aufgabe ist vorzugsweise beim Änderungsmanagement anzusiedeln, das die wesentliche Schnittstelle zwischen dem IT-Betrieb und den IT-Projekten bildet (siehe hierzu Abschnitt 4.3.1.3).

Die Erstellung der Betriebsdokumente muss als Arbeitspaket in den Projektaufgaben verankert werden. In vielen Projekten wird viel Aufwand auf die Erstellung der Projektdokumente verwandt, der Erstellung der Betriebsdokumentation aber kaum Raum eingeräumt. An dieser Stelle machen sich die immer noch vorhandenen Akzeptanzprobleme gegenüber der Betriebsdokumentation bemerkbar. Viele Auftraggeber sind bereit, für ein technisches Konzept viel Geld zu bezahlen; aber von der Systemdokumentation wird erwartet, dass diese im Preis eingeschlossen ist.

6.4 Die Organisation der Projektdokumentation

In den vorstehenden Kapiteln wurden die Struktur und der Inhalt der Projektdokumentation vorgestellt. Zur Projektdokumentation gehören alle Dokumente, die „offiziell" als Dokumente existieren, sprich einen offiziellen Bearbeitungsstatus haben. Hierbei kann es sich sowohl um die Dokumente des Projektmanagements als auch um Ergebnisdokumente handeln.

Nicht gemeint ist damit der Bereich der Arbeitsdokumente, in dem die Projektmitarbeiter ihre Arbeitsversionen verwalten und möglicherweise eine eigene Informationssammlung aufbauen. Ein Dokument, in dem der Projektmitarbeiter gerade ein paar Informationen durch einfaches Kopieren zusammengestellt hat, und das noch keinen offiziellen Bearbeitungsstand hat, existiert aus Sicht der Projektdokumentation nicht. Auch Dokumente, die er als Informationsbasis aus dem Internet heruntergeladen hat, sind keine Dokumente im Sinne der IT-Dokumentation. Nichtsdestotrotz spielt aber gerade die Verwaltung des Arbeitsbereichs bei Projekten eine wichtige Rolle und ist Anlass für manches Problem bei der Projektdokumentation, sodass sie an dieser Stelle, neben den Anforderungen an die Projektdokumentation, ebenfalls betrachtet werden soll.

6.4.1 Anforderungen an die Projektdokumentation

Die im ersten Kapitel definierten Anforderungen an die Dokumentation gelten nicht nur für die Betriebsdokumentation, sondern selbstverständlich auch für die Projektdokumentation. Die Festlegung von Richtlinien und Vorgaben für die Erstellung, Änderung und Speicherung von Dokumenten ist die Voraussetzung zur Durchsetzung einheitlicher Qualitätsstandards und für die Sicherstellung von Dokumentationsanforderungen. Eine unternehmensweite Dokumentationsrichtlinie ist hierfür der beste Weg.

Welche Inhalte eine solche Dokumentationsrichtlinie haben sollte und worauf grundsätzlich bei der Erstellung von Dokumenten zu achten ist, damit diese bei-

spielsweise die Anforderung an die Revisionssicherheit erfüllen, können Sie in Abschnitt 7.1 nachlesen.

Wichtige Grundsätze

Auf einige wichtige Punkte soll aber bereits an dieser Stelle hingewiesen werden:

1. Der Projektverlauf muss nachvollziehbar über alle Projektphasen revisionssicher dokumentiert werden. Alle dafür erforderlichen Dokumente sind zudem entsprechend den gesetzlichen Regelungen aufzubewahren. Dies umfasst zwingend alle Dokumente der Projektinitiierungs- und der Projektplanungsphase wie beispielsweise den Projektauftrag. Aber auch die Ergebnisdokumentation einschließlich aller Konzeptarbeiten sowie die Test- und Abnahmeergebnisse sind zu dokumentieren und zu archivieren.
2. Alle Dokumente sind einer Versionierung zu unterziehen.
3. Änderungen an Dokumenten dürfen nur im Rahmen standardisierter Änderungsprozesse erfolgen und müssen nachvollziehbar sein.
4. Das Löschen von Projektdokumenten sollte eine Ausnahme darstellen und ist stets zu dokumentieren. Dem Löschen immer vorzuziehen ist das Setzen des Bearbeitungsstatus „ungültig".
5. Nach dem Abschluss des Projekts dürfen keine Änderungen mehr an den Projektdokumenten erfolgen. Nur die in den Betrieb überführten Dokumente werden innerhalb des IT-Betriebs weitergepflegt. Die gesamte Projektdokumentation sollte deshalb mit der Beendigung des Projektes „eingefroren", das heißt, als kompletter Dokumentensatz unveränderbar archiviert werden.

Richtlinien der Landesverwaltungen

In diesem Zusammenhang haben einige Landesverwaltungen Dokumentationsrichtlinien für IT-Projekte verabschiedet, die auf den *Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informations- und Kommunikationstechnik (IuK-Mindestanforderungen)* vom 26.09.2001 beruhen und für die landeseigenen Behörden gelten [IUK-MINDEST].

6.4.2 Typische Problemfelder der Projektdokumentationen

Die meisten Projekte weisen im Hinblick auf den täglichen Umgang mit den Projektdokumenten ähnliche Probleme auf.

6.4.2.1 Herausforderungen der täglichen Projektarbeit

Projektleiter als Dokumentenverwalter

Eine der Anforderungen an die Ordnungsmäßigkeit von Dokumenten lautet, dass die Lesbarkeit während der gesamten Aufbewahrungsdauer zu gewährleisten sowie die Datensicherheit in Bezug auf den Zugriffschutz und die Unveränderbarkeit der Daten sicherzustellen ist. Um diese und die übrigen oben genannten Anforderungen zu erfüllen, ist insbesondere eine entsprechende Dokumentenverwaltung erforderlich.

Aber auch in Unternehmen mit einer gut organisierten IT-Betriebsdokumentation wird häufig die Projektdokumentation außen vor gehalten und die Verwaltung der Projektdokumente dem Projektleiter, gegebenenfalls in Zusammen-

arbeit mit dem PMO, überlassen. Wie die Erfahrungen zeigen, ist dies aber nur bei kleinen Projekten ein gangbarer Weg. Bei größeren Projekten bleibt dem Projektleiter im täglichen Projektgeschäft meist kein Freiraum dafür. Und in diesen Fällen entwickeln sich im praktischen (hektischen) Projektalltag häufig individuell strukturierte Dokumentationsablagen, die die Verständlichkeit und Nachvollziehbarkeit der erarbeiteten Ergebnisse erheblich erschweren, massiv behindern oder so gut wie unmöglich machen.

Problemfeld: Externe Mitarbeiter

Aber auch die Projektmitarbeiter bekommen es zu spüren, wenn die Projektdokumentation derart stiefmütterlich behandelt wird. Dies gilt insbesondere, wenn in einem Projekt externe Mitarbeiter beschäftigt werden. Um externen Mitarbeitern die erforderlichen Zugriffe – und nur diese (womöglich auch mit dem eigenen Notebook) – zu ermöglichen, ist aus Sicherheitsgründen einiger Aufwand erforderlich, der vielfach gescheut wird.

Im positivsten Fall wird den externen Mitarbeiter ein Ordner für die eigenen Arbeitsdokumente zugewiesen. Darüber hinaus gibt es noch einen Gruppenordner, in dem ebenfalls Arbeitsversionen und Dokumente mit wichtigen Informationen gespeichert werden. Häufig aber arbeiten externe Mitarbeiter mit dem eigenen Notebook und speichern die Dokumente lokal. Bei Bedarf werden die Dokumente dann per E-Mail versendet (allerdings versenden auch interne Mitarbeiter Dokumente häufig per E-Mail). Änderungen und Abstimmungen erfolgen ebenfalls per E-Mail und sind somit für Dritte aufgrund der Ablage in lokalen Mail- und Datei-Verzeichnissen in keiner Weise mehr nachvollziehbar. Und wohl jeder Berater ist in derartigen Umgebungen schon in die Situation geraten, dass im vermeintlich letzten Stand eines Dokuments „plötzlich" die Anmerkungen des Kollegen fehlten. Abgesehen davon, dass durch die Mehrfachspeicherung unnötigerweise wertvoller (Postfach-)Speicher belegt wird.

Problem: Redundante Datenhaltung

Aus der unstrukturierten oder sogar lokalen Speicherung der Projektdokumente erwachsen aber noch andere Probleme: Ein Grundsatz bei der Dokumentenerstellung muss lauten, dass Informationen grundsätzlich nur in einem Dokument stehen dürfen. Die häufig angewandte Methode, Informationen mittels Kopieren und Einfügen in ein anderes Dokument zu übernehmen, anstatt auf das Dokument zu verweisen, führt zwangsläufig zu Inkonsistenzen und erhöhtem Pflegeaufwand. Die gleichen Folgen hat die Erfassung von Informationen in einem Dokument, ohne die Inhalte anderer Dokumente zu berücksichtigen.

Um diesem Problem zu begegnen, muss sichergestellt werden, dass allen Projektmitgliedern die Inhalte der für sie relevanten Dokumente bekannt sind und ein Verweis auf diese Dokumente möglich ist. Zusätzlich ist zu gewährleisten, dass Änderungen an Dokumenten immer an der gültigen aktuellen Version eines Dokuments erfolgen.

Mit einer typischen wild wachsenden „Projektteam-Dokumentenablage", in der in Dutzenden von Ordnern mindestens zehn Arbeitsversionen eines Dokuments liegen, und die aktuelle Version sich auf dem lokalen Notebook des Beraters befindet, ist diese Forderung allerdings nicht durchzusetzen.

Problem: Verweise auf Inhalte, die es gar nicht gibt

Und noch ein weiteres Phänomen steht mit dem vorgenannten in ummittelbaren Zusammenhang und ist typisch für Projektdokumente. In einem Projekt werden häufig verschiedene Dokumente parallel von unterschiedlichen Personen erstellt. Mangels genauer Kenntnis der Dokumente und der Tatsache, dass das andere Dokument ebenfalls noch in der Erstellung ist, wird vielfach „blind" auf andere Dokumente verwiesen. Es wird hierbei davon ausgegangen, dass der andere Projektmitarbeiter dieses Thema in sein Dokument noch aufnehmen wird. So kommt es, dass man in Dokumenten Verweise auf Inhalte oder sogar auf Dokumente findet, die es gar nicht gibt.

6.4.2.2 Mögliche Lösungsansätze

Um den genannten typischen Problemen der Dokumentation in Projekten zu begegnen, sind sowohl organisatorische wie auch technische Maßnahmen erforderlich.

Projekteigener Dokumentenverwalter

Wie die Ausführungen zeigen, ist es ohne eine zentrale Verwaltung der Projektdokumente kaum möglich, den Problemen zu begegnen. Bei umfangreichen oder langfristigen Projekten ist daher eine projekteigene Dokumentenverwaltung dringend zu empfehlen. Diese sollte nach Möglichkeit bereits zu Projektbeginn implementiert werden; sie kann dann auch den Aufbau und die Pflege einer zentralen Dokumentenablage übernehmen.

Typischerweise übernimmt eine solche Dokumentenstelle folgende Aufgaben:

- Registrieren aller Dokumente (sofern kein Dokumentenmanagement-System eingesetzt wird)
- Kennzeichnen aller Projektdokumente mit einer eindeutigen ID (auch diese Aufgabe könnte ein Dokumentenmanagement-System übernehmen)
- Einrichten einer geeigneten Ablagestruktur und sicherstellen, dass diese auch eingehalten wird
- Bereitstellen aller Dokumente der IT-Dokumentation in der jeweils aktuellen Version und sicherstellen, dass die Projektmitarbeiter jederzeit Zugriff auf die von ihnen benötigten Dokumente haben
- Überwachen von Dokumentenänderungen und Bereitstellung der geänderten Dokumente
- Informieren der Projektmitarbeiter über wichtige Änderungen an Dokumenten
- Vorbereiten und Durchführen von Dokumentenübergaben an den IT-Betrieb

Ohne DMS nur schwer umsetzbar

Realistischerweise sind die genannten Anforderungen und Aufgaben auch beim Einsatz einer zentralen Dokumentenverwaltung nur in kleinen Projekten ohne den Einsatz eines elektronischen Dokumentenmanagement-Systems (DMS) umsetzbar. Die Hauptaufgabe des DMS liegt darin, die definierten Dokumentationsprozesse automatisiert zu steuern. Für die Projektdokumentation sind insbesondere die Funktionen zum Erstellen und Ändern von Dokumenten wichtig. Das Versionsmanagement eines DMS beispielsweise kann die Bearbeitung von Dokumenten kontrollieren. Das heißt, Dokumente müssen zur Bearbeitung aus

dem System ausgecheckt werden und können während der Bearbeitungszeit von anderen Benutzern nur angezeigt, jedoch nicht geändert werden. Nach der Bearbeitung wird das Dokument wieder eingecheckt. Das DMS vergibt dann eine neue Versionsnummer. Hierdurch wird verhindert, dass zwei oder mehrere Projektmitarbeiter gleichzeitig an einem Dokument arbeiten und ihre Arbeitsergebnisse im schlimmsten Fall gegenseitig vernichten. Abhängig vom eingesetzten System sind diese Abläufe mehr oder weniger anpassbar und durch Workflows zu erweitern.

Außerdem stellt ein DMS sicher, dass immer die aktuell gültige Version eines Dokuments greifbar ist. Dies erst macht die Verwendung von Verknüpfungen auf andere Dokumente und von Objektverknüpfungen möglich. Objektverknüpfungen sind außerordentlich hilfreich und ermöglichen es beispielsweise, eine Excel-Tabelle in ein Word-Dokument so einzubinden, dass Änderungen am Excel-Dokument automatisch in das Word-Dokument übernommen werden. Ebenso lässt sich angeben, für welche Dokumente derartige Verknüpfungen eingesetzt werden können. Hierfür aber müssen die Zugriffe auf die entsprechenden Dokumente sichergestellt sein. Wichtige Hinweise zum Einsatz von Verweisen finden Sie in Abschnitt 7.2.2.1.

Wird im Untenehmen kein DMS eingesetzt, oder ist es nicht möglich bzw. gewünscht, die Projektdokumentation in das DMS für den IT-Betrieb zu integrieren, kann der Einsatz der Windows SharePoint Services eine mögliche Lösung bieten. Mit den *Windows SharePoint Services 3.0* stellt Microsoft kostenlos ein Groupware-System bereit, dessen integrierte Funktionen zur Verwaltung von Dokumenten in vielen Fällen durchaus ausreichend sein können, und das darüber hinaus noch nützliche Workflows bietet. Einen ersten Eindruck von den Möglichkeiten der Windows SharePoint Services 3.0 erhalten Sie in Abschnitt 7.4.3.1.

6.5 Fazit

IT-Projekte dienen in der Mehrzahl dazu, Neuerungen, Anpassungen und Optimierungen des IT-Betriebs zu realisieren, die aufgrund ihres Umfangs oder ihrer Ausprägung nicht im IT-Regelbetrieb durchführbar sind. Projekte sind gekennzeichnet durch eine eigene Projektstruktur und das Merkmal der Einmaligkeit. Dementsprechend unterscheidet sich die Dokumentation des IT-Betriebs von der Projektdokumentation. Dies manifestiert sich auch, wie das Kaptitel gezeigt hat, an typischen Problemen, die in Bezug auf die Organisation der Dokumentation in Projekten bestehen.

Bei Projekten sind die Planung, die Durchführung, das Testen und die Implementierung bedarfsgerecht zu dokumentieren. Neben den Projektmanagement-Dokumenten spielen deshalb vor allem Konzepte und Testdokumente eine wichtige Rolle.

Lösungen, die in einem Projekt entwickelt werden, müssen nach dem Testen in den IT-Betrieb überführt werden. Nicht nur hierfür muss es dokumentierte Prozesse geben. Wichtig ist, dass nur Systeme in den Betrieb überführt werden, für die auch Betriebsdokumente erstellt wurden. Eine Betriebsüberführung muss also auch die Überführung der Dokumente in den IT-Betrieb einschließen.

7 Dokumente erstellen und verwalten in der Praxis

In diesem Kapitel steht nicht mehr die Frage „Was ist zu Dokumentieren?“ im Vordergrund, sondern die Frage „Wie erstelle ich ein Dokument?“ bzw. „Welche Punkte müssen beachtet werden, um anforderungsgerechte Dokumente zu erstellen?“.

Die Ausführungen der vorangegangenen Kapitel haben gezeigt, dass die Notwendigkeit, Dokumentationen zu erstellen und zu pflegen, immer größer werden. Ebenso steigen auch die Anforderungen an die Qualität der Dokumentation. Und damit sieht sich mancher Administrator, der bislang die Dokumentation „seiner Systeme“ weitgehend nur „im Kopf“ hatte, mit dem häufig ungeliebten Thema Dokumentation konfrontiert.

Dabei ist es unter Beachtung einiger wichtiger Punkte durchaus auch für weniger Geübte möglich, anforderungsgerechte Dokumente zu erstellen. Dies zeigt dieses Kapitel und liefert unter anderem konkrete Hilfen für die Arbeit mit Microsoft Word. Die Erstellung eines Dokuments darf aber nicht nur aus formaler Sicht betrachtet werden.

Viele Fehler passieren im organisatorischen Bereich. Wurden beispielsweise bei der Informationssammlung wichtige Vorläuferdokumente übersehen und daher nicht berücksichtigt, kann auch ein perfektes formales Dokument die inhaltlichen Mängel nicht ausgleichen. Das Kapitel bietet deshalb auch Hilfen und Anregungen zur Optimierung der Vorgehensweise bei der Erstellung von Dokumenten, beispielsweise durch Einsatz von Mind Maps.

Gute Dokumente können aber nicht ohne die Einbindung in ein Regelwerk entstehen. Benötigt werden Vorgaben, die die Dokumentation standardisieren und den Erstellern von Dokumenten als Leitfaden dienen. Einen Schwerpunkt des Kapitels bilden daher die Erläuterungen zum Erstellen einer Dokumentationsrichtlinie. Eine solche Dokumentationsrichtlinie darf nicht nur Vorgaben für die Einzeldokumente enthalten, sondern muss auch die Verwaltung und Speicherung der Gesamt-Dokumentation regeln. Je mehr Dokumente entstehen, desto wichtiger ist es, diese so abzulegen, dass alle schnell gefunden werden können und jeder Mitarbeiter auf die von ihm benötigten Dokumente Zugriff hat. Auch hierzu möchte das Kapitel Anregungen liefern.

7.1 Einführung von Dokumentationsstandards

Das Festlegen von Richtlinien und Vorgaben für die Erstellung, Änderung und Speicherung von Dokumenten ist die Voraussetzung zur Durchsetzung einheitlicher Qualitätsstandards und für die Sicherstellung der Revisionssicherheit für die unternehmensweite Dokumentation.

Ohne verbindliche Regelungen ergeben sich im praktischen IT-Betriebs- und Projektalltag häufig individuell strukturierte Dokumentationsablagen, die die Verständlichkeit und Nachvollziehbarkeit der erarbeiteten Inhalte erheblich erschweren. Und wer schon Erfahrung mit „wild gewachsenen" IT-Dokumentationen gemacht hat, weiß, welche Schwierigkeiten entstehen können, wenn die Einzeldokumente keinerlei Standards in Bezug auf Benennung, formalen Aufbau und inhaltliche Ausgestaltung aufweisen und Abhängigkeiten zwischen den Dokumenten nicht nachvollziehbar sind.

Mit wachsender Unternehmensgröße wird daher die Erstellung und Durchsetzung einer Dokumentationsrichtlinie zunehmend wichtiger. Diese wird sinnvollerweise übergeordnet auf der Unternehmensebene definiert. Wo eine solche übergeordnete Richtlinie fehlt, sollte sie zumindest für die Ebene der IT-Dokumentation entwickelt werden.

Welche Punkte sollte eine Dokumentationsrichtlinie regeln?

Sinnvollerweise schreibt die Dokumentationsrichtlinie Regelungen für die folgenden Bereiche fest:

- Richtlinien und Klassifizierungen, die für alle Dokumente gelten (Namenskonventionen, Bearbeitungsstatus, Nummerierungssystem usw.)
- Formaler Aufbau der Einzeldokumente
- Dokumentationsprozesse (Freigabeprozesse, Beauftragungsprozesse, Qualitätssicherungsverfahren usw.)
- Regelungen zur Speicherung der Dokumente im Dateisystem bzw. im Dokumentenmanagement-System
- Regelungen zur Archivierung

Generell sollte eine Dokumentationsrichtlinie darauf ausgerichtet sein, dass die folgenden Einzelanforderungen an die Dokumente erfüllt werden:

- Verständlichkeit
- Aktualität
- Vollständigkeit
- Richtigkeit

Kriterien für Revisionssicherheit

Diese Kriterien entsprechen auch der geforderten Revisionssicherheit. Ein Dokument kann dann als revisionssicher betrachtet werden, wenn es aktuell, vollständig und für einen sachverständigen Dritten nachvollziehbar ist. Weiter muss die Aufbewahrungsform die Lesbarkeit während der gesamten Aufbewahrungsdauer gewährleisten; und die Datensicherheit in Bezug auf den Zugriffschutz und die Unveränderbarkeit der Daten sicherstellen.

7.1.1 Richtlinien für alle Dokumente

Schwerpunkt einer Dokumentationsrichtlinie ist die Festlegung von Richtlinien und Klassifizierungen, die beim Erstellen und Ändern von Dokumenten verbindlich einzuhalten sind.

7.1.1.1 Festlegung von Dokumentenklassen

Es ist sinnvoll, Dokumente in Klassen zu unterteilen. Die Zuordnung zu einer Dokumentenklasse definiert ein Dokument im Hinblick auf seinen Informationsinhalt und seine Darstellungsform. Benutzer des Dokuments erhalten damit Hinweise auf den Inhalt. Ebenso können auch Suchvorgänge bei einer entsprechenden Verschlagwortung nach Dokumentenklassen erfolgen.

Welche und wie viele Dokumentenklassen gebildet werden, liegt in der Entscheidung des Unternehmens. Legt man die in den vorangegangenen Kapiteln definierten Strukturen zugrunde, ergeben sich daraus auch folgerichtig die wichtigsten Dokumentenklassen: Systemakten, Prozessbeschreibungen, Konzepte, Richtliniendokumente, Arbeitsanweisungen, Testdokumente usw.

In der Dokumentationsrichtlinie sollten alle Klassen benannt und spezifiziert werden, wobei eine Begrenzung auf die unbedingt notwendige Anzahl unterschiedlicher Dokumentenklassen zu empfehlen ist. Werden zu viele Klassen ausgewiesen, sind diese oft schwer voneinander abzugrenzen. Bei der Verwendung nur weniger Klassen treten weniger Grenzfälle auf; der Ermessensspielraum wird kleiner.

Zusätzliche Hinweise und Anregungen zur Festlegung der Dokumentenklassen liefert die DIN EN 61355. Die Norm DIN EN 61355 „Klassifikation und Kennzeichnung von Dokumenten für Anlagen, Systeme und Einrichtungen“ regelt die einheitliche und herstellerübergreifende Klassifikation und Identifikation von Dokumentenklassen. Der Anwendungsbereich der Norm dient zwar vorrangig als Grundlage zur Erstellung strukturierter Dokumentationen für den Anlagenbau, sie kann aber trotzdem Anregungen für die IT-Dokumentation liefern.

hinweis

In der Literatur findet man anstelle des Begriffs *Dokumentenklasse*, der im vorliegenden Buch verwendet wird, häufig auch den Begriff *Dokumentenart* oder *Dokumentart*. Die DIN EN 61355 verwendet sogar den Begriff *Dokumentenartenklasse*. Selbstverständlich ist auch die Verwendung eines dieser Begriffe möglich; er muss lediglich in der Dokumentationsrichtlinie eindeutig definiert werden.

7.1.1.2 Eindeutige Dokumentennummer

Es ist sinnvoll, dass jedes Dokument eine eindeutige Nummer trägt, die es unveränderbar während seines gesamten Lebenszyklus behält. Dies ermöglicht es, zweifelsfrei auf Dokumente zu referenzieren.

Ein solches Nummerierungssystem muss immer im Kontext bestehender Nummerierungsstrukturen im Unternehmen betrachtet werden. So kann die Nummerierung von Dokumenten beispielsweise nicht isoliert von der Nummerierungsstruktur der Prozesse betrachtet werden,

Automatische Nummerierung bei Einsatz eines DMS

Hinzu kommt, dass Dokumentenmanagement-Systeme in der Regel eine eigene Systematik mitbringen, zumal die automatisierte eindeutige Kennzeichnung von Dokumenten ein wesentlicher Bestandteil dieser Systeme ist.

An dieser Stelle soll der Hinweis auf die Notwendigkeit einer eindeutigen Dokumentennummer daher ausreichen.

7.1.1.3 Bearbeitungsstatus

Um die Arbeitsabläufe zu unterstützen, ist es sinnvoll, jedem Dokument einen Status zuzuordnen, der den aktuellen Arbeitsstand dokumentiert. Diese Status können frei definiert werden, sollten aber möglichst einfach gehalten sein. Als sinnvoll hat sich die Unterscheidung der folgenden Bearbeitungszustände erwiesen:

- *In Bearbeitung (Draft):* Das Dokument befindet sich in der Erstellung oder in der Überarbeitung.
- *Abgeschlossen (Ready):* Das Dokument ist fertiggestellt und steht zur Freigabe bereit. Dieser Status wird vom Dokumentersteller vergeben.
- *Endgültig (Final):* Das Dokument ist endgültig. Es unterliegt jedoch keinem Abnahmeprozess und kann daher vom Dokumentersteller diesen Status erhalten.
- *Freigegeben (Released):* Das Dokument wurde von einem Verantwortlichen abgenommen und freigegeben. Damit ist jedes freigegebene Dokument gleichzeitig auch „endgültig".
- *Ungültig (Invalid):* Das Dokument ist nicht mehr gültig. Den Status „ungültig" kann ein Dokument zu jeder Zeit erhalten. Dies kann beispielsweise geschehen, wenn die Freigabe verweigert wurde oder wenn ein Dokument funktionale Teile beschreibt, die die außer Betrieb gestellt wurden. Die Vergabe des Status „ungültig" muss einem gesonderten Prozess unterliegen.

Die nachstehende Tabelle zeigt den Ablauf der Aktivitäten und Statusänderungen während eines Freigabeprozesses im Überblick.

Tätigkeit und Durchführender	Bearbeitungsstatus
Ein neues Dokument wird durch den Dokumentersteller erstellt.	In Bearbeitung
Das Dokument wurde qualitätsgesichert, und die Änderungen werden vom Dokumentersteller eingearbeitet.	In Bearbeitung
Das Dokument wurde vom Dokumentersteller zur Freigabe eingereicht. Dokumente im Status „abgeschlossen" dürfen nicht mehr verändert werden.	Abgeschlossen
Das Dokument wurde freigegeben.	Freigegeben
Ein freigegebenes Dokument muss angepasst werden.	In Bearbeitung
Das geänderte Dokumente wird erneut zur Freigabe eingereicht.	Abgeschlossen
Das Dokument wird mit neuer Versionsnummer freigegeben.	Freigegeben

Tabelle 7.1: Bearbeitungsstatusänderungen während eines Freigabeprozesses

7.1.1.4 Versionierung

Ein wichtiger Punkt, der unbedingt in der Dokumentationsrichtlinie geregelt werden sollte, betrifft die Versionierung. Dies umfasst sowohl die Versionsnummerierung als auch die damit verbundenen Prozesse. Gibt es hierzu keine verbindlichen Regeln, führt dies erfahrungsgemäß – zumindest dann, wenn kein Dokumentenmanagement-System eingesetzt wird – innerhalb kurzer Zeit dazu, dass jeder seine „eigenen Versionsnummern" verwendet und keiner das Wirrwarr der Zahlen mehr interpretieren kann.

Anforderung an die Versionierung

Die Notation der Version sollte zwei Aspekte erkennen lassen:

- Den Freigabestatus des Dokuments
- Den derzeitigen Bearbeitungsstatus des Dokuments

Typischerweise werden für Dokumente bis zur Abnahme Nummern bis 0.99 vergeben. Das finale bzw. abgenommene Dokument erhält die Versionsnummer 1.0. Sind daran später Änderungen erforderlich, wird entsprechend hoch gezählt. Zwischenabnahmen im Rahmen der Qualitätsprüfung können dabei mit der Versionsnummer 0.5 oder 0.8 gekennzeichnet werden.

Bearbeitungsnummer schafft Klarheit

Der Nachteil bei einer alleinigen Verwendung der Freigabenummer ist, dass Bearbeitungsstände nicht oder nur unzureichend dargestellt werden können. Häufig wird dafür die zweite Nachkommastelle verwendet, was aber zu Verwir-

rungen führen kann. Besser ist es daher, eine zusätzliche Bearbeitungsnummer zu verwenden. Für die Versionsnummerierung wird daher folgende Methode vorgeschlagen:

Die *Versionsnummer* besteht aus zwei Teilen, die durch einen Bindestrich getrennt sind.

- Freigabenummer (FN)
- Bearbeitungsnummer (BN)

Es handelt sich hierbei um eine laufende Nummer im Format *FN-BN,* die sich mit jeder Änderung ändert. Der Dokumentersteller verwendet bis zur ersten Abnahme ausschließlich die BN und zählt diese hoch. Bei der ersten Prüfung im Rahmen der Qualitätssicherung erhält das Dokument die FN = 0.1. Gleichzeitig wird die Bearbeitungsnummer BN wieder auf die BN = 00 zurückgesetzt. Jede erneute Bearbeitung und nachfolgende Abnahme erhöht die FN um eins. Mit der Abnahme, sprich mit der Freigabe erhält das Dokument die FN 1.0.

Die nachstehende Tabelle zeigt dazu einige Beispiele:

Version 0.0-06	Sechste Arbeitsversion des Dokuments. Es ist noch keine Abnahme bzw. noch keine Prüfung erfolgt.
Version 0.2-02	Das Dokument ist noch nicht abgenommen. Es handelt sich um die zweite Arbeitsversion nach der zweiten Prüfung.
Version 1.0-01	Das Dokument ist final, wird aber derzeit in der ersten Arbeitsversion überarbeitet.

Tabelle 7.2: Beispiel: Versionsnummern und ihre Bedeutung

Während der Erstellung und Bearbeitung des Dokuments durch den Dokumentersteller wird also ausschließlich der zweite Nummernbereich (BN) für die Versionierung der Arbeitsversionen des Dokuments genutzt. Diese wird mit jeder Qualitätsprüfung zurückgesetzt. Die Freigabenummer FN hingegen erhöht sich fortlaufend über die ganze Lebenszeit des Dokuments.

Wird ein Dokumentenmanagement-System eingesetzt, kann damit auch die Versionierung automatisiert werden. Häufig verwenden Dokumentenmanagement-Systeme eigene Versionierungsregeln. Inwiefern diese geeignet sind, muss im Einzelfall geprüft werden. Nach Möglichkeit sollten die Regeln an die eigenen Bedürfnisse anpassbar sein, sodass die beschriebene Notation auch beim Einsatz eines DMS verwendet werden kann.

7.1.1.5 Vertraulichkeitsstufen

Sollen Dokumente Hinweise zur Vertraulichkeit enthalten, ist es notwendig, Vertraulichkeitsstufen in der Dokumentationsrichtlinie zu definieren. Derartige Sperrvermerke regeln Restriktionen hinsichtlich der Weiterverbreitung des

Dokuments. In vielen Unternehmen existieren hierfür unternehmensweit gültige Regeln. Fehlen diese, sollten sie unbedingt definiert werden. Als mögliche Vertraulichkeitsstufen können ausgewiesen werden:

- Offen
- Projektintern
- Nur für den internen Gebrauch
- Vertraulich
- Geheim (gegebenenfalls noch „Streng geheim" als weitere Vertraulichkeitsstufe)

7.1.1.6 Regelungen für Dokumentenformate

Auch Regelungen beispielsweise zum Dokumentenlayout und zu den Speicherformaten können in der Dokumentationsrichtlinie festgelegt werden. Sinnvoll sind beispielsweise die Festlegungen zu folgenden Aspekten:

- Die Sprache, in der Dokumente zu verfassen sind
- Layoutvorschriften (Schriftgröße, Schriftart, Anforderungen an Barrierefreiheit u. Ä.). Die Umsetzung sollte durch ein Bereitstellen von Dokumentvorlagen, deren Verwendung verbindlich vorgeschrieben wird, sichergestellt werden. (Siehe hierzu Abschnitt 7.2.1.)
- Elektronische Formate (einzusetzende Office-Version, Format, in dem Dokumente zu erstellen, zu veröffentlichen und abzulegen sind). Empfehlenswert ist, dass Entwürfe, Zwischenschritte und alle anderen Dokumente, die weiterverarbeitet werden müssen, im jeweiligen Bearbeitungsformat (zum Beispiel *.doc*, *.xls*, *.ppt*, *.mpp*) abgespeichert werden. Zusätzliche Kopien sollten in einem nicht bearbeitbaren Format (beispielsweise als PDF-Dokument) abgespeichert werden. Dokumente, die den Bearbeitungsstatus *endgültig* oder *freigegeben* erreicht haben, müssen zusätzlich revisionssicher archiviert werden. (Siehe hierzu Abschnitt 7.4.2.2)
- Auch sollte festgelegt werden, welche Dokumentenform (Papierausdruck oder elektronisches Dokument) die jeweils gültige ist. Um die Aktualität der Dokumente zu gewährleisten, wird empfohlen, dass nur die elektronischen Dokumente im PDF-Format gültig sind.

7.1.2 Formaler Aufbau der Einzeldokumente

Die Dokumentationsrichtlinie sollte auch die formale Grobstruktur der Dokumente festlegen. Die Gliederung der Dokumente im Detail ist dann von der jeweiligen Dokumentenklasse abhängig und kann durch das Bereitstellen von Dokumentvorlagen vorgegeben werden.

7.1.2.1 Gliederung der Basis-Dokumentvorlage für alle Dokumente

Die nachstehende Abbildung stellt einen möglichen formalen Aufbau dar, der als Basis für alle Dokumente gelten kann. Einige Komponenten sind als optional zu betrachten, da nicht alle Dokumentenklassen alle Bestandteile benötigen. So werden verständlicherweise Berichtsdokumente keine der aufgeführten Verzeichnisse enthalten; und ein Checklisten-Dokument erfordert kein Management Summary.

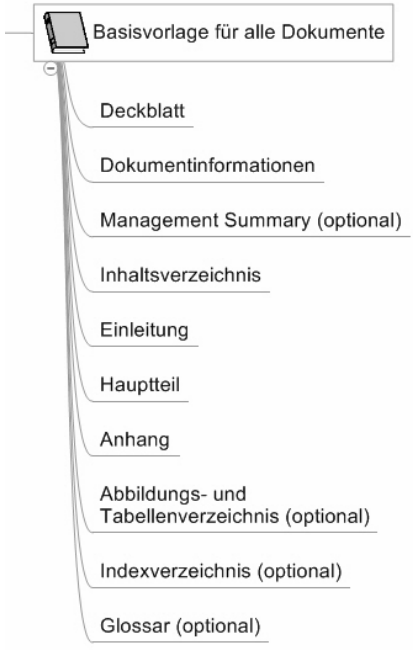


Abbildung 7.1: Basisgliederung für alle Dokumente

cd-rom

In Abschnitt 8.6 und auf der beigefügten CD-ROM befindet sich die in der Abbildung dargestellte Dokumentvorlage, die als Basis für alle Dokumente verwendet werden kann.

Deckblatt Grundsätzlich ist ein Deckblatt nicht zwingend erforderlich, wird aber üblicherweise verwendet, um Dokumente optisch ansprechend zu gestalten. Insofern steht beim Deckblatt die optische Gestaltung im Vordergrund. Inhaltlich sollte das Deckblatt neben dem hervorgehobenen Titel (in Verbindung mit der Dokumentenklasse) die wichtigsten Informationen zum Dokument enthalten. Hierzu zählen unter anderem die Dokumentennummer, die Version, der Bearbeitungsstatus, der verantwortliche Autor sowie das Datum der letzten Bearbeitung.

Informationen zum Dokument Die erste Seite nach dem Deckblatt enthält alle formalen Informationen zum Dokument.

Dokumentinfobox

Ein bewährte Möglichkeit ist die Verwendung einer Tabelle, die alle wesentlichen Dokumentinformationen einschließlich des aktuellen Bearbeitungsstands beinhaltet (im Folgenden als „Dokumentinfobox" bezeichnet). In der Praxis haben sich folgende Felder als sinnvoll erwiesen:

Sinnvolle Angaben in der Infobox

- *Dokumentenklasse:* Die Art des Dokuments gemäß den in der Dokumentationsrichtlinie ausgewiesenen Klassen (zum Beispiel Konzept, Systemakte oder Arbeitsanweisung)
- *Dokumententitel:* Titel bzw. Thema des Dokuments
- *Dokumentennummer:* Eindeutige Nummer des Dokuments
- *Verantwortlicher Autor:* Name der Person, die für die Erstellung des Dokuments und für das Einpflegen von Änderungen verantwortlich ist
- *Dateiname:* Name des elektronischen Dokuments
- *Erstellung begonnen am:* Hier ist das Datum einzutragen, an dem mit der Erstellung des Dokuments begonnen wurde. Dieses Datum wird bei der Erstellung eingetragen und nicht mehr geändert.
- *Letzte Bearbeitung:* Automatische Einfügung des letzten Speicherdatums
- *Letztes Druckdatum:* Automatische Einfügung des letzten Druckdatums
- *Seitenzahl:* Die Gesamtanzahl der Seiten des Dokuments. Wird in der Fußzeile eine Dokumentennummerierung verwendet, aus der jeweils die Gesamtseitenzahl hervorgeht, kann die Angabe an dieser Stelle entfallen.
- *Vertraulichkeitsstufe:* Angabe von Restriktionen bezüglich der Weiterverbreitung und gegebenenfalls auch des Zugriffs gemäß den in der Dokumentationsrichtlinie ausgewiesenen Stufen.
- *Versionsnummer:* Die Versionsnummer ist damit eine laufende Nummer im Format *FN-BN,* die sich mit jeder Änderung ändert.
- *Bearbeitungsstatus:* Zeigt den aktuellen Bearbeitungsstatus des Dokuments. Die Bearbeitungsstatus sind gemäß den Festlegungen der Dokumentationsrichtlinie zu verwenden.
- *Freigegeben am und durch:* Ist das Dokument freigeben, muss das Freigabedatum und zusätzlich der Name des Freigebers eingetragen werden.

Wichtige Informationen zum Dokument	
Dokumentenklasse:	Dokumentvorlage
Dokumententitel:	Titel des Dokuments
Dokumentennummer:	123
Verantwortlicher Autor:	Manuela Reiss
Dateiname:	basis-dokumentvorlage.dot
Erstellung begonnen am:	01.07.2008
Letzte Bearbeitung am:	11. Oktober 2008
Letzter Ausdruck erfolgt am:	05. Okt. 2008
Seitenzahl:	11
Vertraulichkeitsstufe:	Offen
Versionsnummer:	Version: 0.0-03
Bearbeitungsstatus:	In Bearbeitung
Freigabe am:	
Freigegeben durch:	

Abbildung 7.2: Infobox mit allen wichtigen Angaben zum Dokument

Redundante Informationen zum Deckblatt

Einige Informationen stehen damit redundant sowohl auf dem Deckblatt, als auch in der Dokumentinfobox. Diese Vorgehensweise kann sinnvoll sein, da in der Praxis nicht alle Dokumente ein Deckblatt erhalten. Konzepte und Richtliniendokumente weisen aus optischen Gründen in der Regel ein Deckblatt auf. In öffentlichen Unternehmen ist es darüber hinaus üblich, dass Unterschriften auf der Deckblattseite stehen. Hingegen ist ein Deckblatt beispielsweise bei Checklisten oder Hardware-Systemakten durchaus entbehrlich, hier kann das Dokument mit der Dokumentinfobox beginnen. Alternativ ist es auch möglich, die Dokumentinfobox direkt auf das Deckblatt zu setzen. Wichtig ist jedoch, dass alle Dokumente eine Dokumentinfobox enthalten.

Um einen erhöhten Pflegeaufwand und Inkonsistenzen beim Eintragen redundanter Informationen zu verhindern, ist es erforderlich, alle Informationen als sich automatisch aktualisierende Felder einzutragen. Erläuterungen, wie hierbei vorzugehen ist, können Sie dem Abschnitt 7.2.1.2 entnehmen.

Änderungsnachweis

Zusätzlich zur hoch gezählten Versionsnummer sollte jedes Dokument eine Tabelle enthalten, in der der Status, der jeweilige Bearbeiter, das Bearbeitungsdatum und eine (knappe) Beschreibung der wesentlichsten Änderungen fortgeführt werden.

Änderungsnachweis				
Versions-nummer	Bearbeitungs-status	Datum	Bearbeiter	Änderung/Bemerkung

Abbildung 7.3: Tabelle zur Pflege des Änderungsnachweises

Mitgeltende Dokumente

Erfahrungsgemäß führt diese Tabelle bei Erstellern von Dokumenten immer wieder zu Verwirrungen und wird daher häufig nur sehr stiefmütterlich gepflegt. Dies liegt häufig daran, dass der Bearbeiter nicht weiß, welche Dokumente er hier einzutragen hat.

Betrachtet man den Begriff der mitgeltenden Dokumente eher eng, handelt es sich bei ihnen vor allem um Richtliniendokumente, die Regelungen enthalten, die für dieses Dokument Gültigkeit besitzen, die aber im Dokument nicht explizit genannt werden (hierzu zählen typischerweise Namenskonventionen).

Meist wird der Begriff aber eher weit gefasst und beinhaltet dann auch alle *ergänzenden Dokumente*. Ergänzende Dokumente können auch externer Herkunft sein und enthalten Informationen, die in irgendeiner Form für das Dokument relevant sind bzw. es ergänzen. Auf ergänzende Dokumente wird an relevanter Stelle im Dokument verwiesen. Typischerweise sind alle Arbeitshilfen-Dokumente ergänzende Dokumente.

Erläuterungen sind wichtig

Hier muss also im Einzelfall festgelegt werden, welche Dokumente einzutragen sind. Sollen auch ergänzende Dokumente in die Tabelle aufgenommen werden, sollte sie besser den Titel *Mitgeltende und ergänzende Dokumente* tragen. Der Tabelle sollte außerdem eine kurze Erklärung beigefügt werden, die erläutert, welche Dokumente der Dokumentersteller einzutragen hat.

tipp

Der zweite Weg, also das Eintragen aller mitgeltenden und ergänzenden Dokumente, bietet in der Praxis einige Vorteile und ist daher zu empfehlen. Möchte jemand für das vorliegende Dokument alle relevanten Dokumente zusammenstellen und als Dokumentensatz mitnehmen, kann er dies sehr schnell anhand der Tabelle tun. Weiter liefert die Tabelle die Möglichkeit, Verweise auf andere Dokumente innerhalb des Dokuments auf die Dokumentennummer als eindeutige Referenz zu beschränken. Alle anderen Informationen sind in der Tabelle der mitgeltenden Dokumente zu erfassen und somit an nur einer Stelle zu pflegen.

Außerdem ist es sinnvoll zu vereinbaren, dass nur gültige Dokumente mit einer gültigen Dokumentennummer eingetragen werden dürfen. Dies verhindert unter anderem, dass auf Dokumente verwiesen wird, die es (noch) gar nicht oder nicht mehr gibt.

Ergänzende Dokumente/Mitgeltende Unterlagen*				
Dokumentennummer	Dokumentenklasse und Titel des Dokuments	Version	Datum letzter Bearbeitung	Verantwortlicher Autor

*In der Tabelle sind alle Dokumente einzutragen, die für dieses Dokument Gültigkeit besitzen, die aber im Dokument nicht explizit genannt werden (beispielsweise Namenskonventionen). Einzutragen sind auch alle Dokumente, auf die im nachfolgenden Dokument explizit verwiesen wird.

Abbildung 7.4: Tabelle zur Pflege der mitgeltenden Dokumente

Management Summary Das sogenannte Management Summary soll Führungskräften und Entscheidern alle wichtigen Fakten liefern, sodass diese unter Berücksichtigung der Unternehmensstrategie und aller anderen Randbedingungen möglichst schnell die richtige Entscheidung treffen können. Es sollte daher in jedem an die Unternehmensleitung gerichteten größeren Dokument enthalten sein.

Grundsätzlich empfiehlt es sich, dass das Management Summary die Gliederung des Hauptdokuments aufgreift und alle Hauptaussagen des Dokuments benennt (jeweils ein Satz). Wichtig ist außerdem, Entscheidungsalternativen und ihre jeweiligen Konsequenzen aufzuführen.

Inhaltsverzeichnis Nicht alle Dokumente enthalten ein Inhaltsverzeichnis. Hierzu gehören in der Regel Checklisten, Protokolle oder kleinere Arbeitsanweisungen. Auf ein Inhaltsverzeichnis sollte aber nur bei sehr kurzen Dokumenten verzichtet werden, zumal es nicht nur dazu dienen kann, schnell auf das gewünschte Kapitel zuzugreifen, sondern auch, um sich sehr schnell einen Überblick über das Dokument zu verschaffen.

Einleitung Jedes Dokument sollte einen Einführungsteil haben. Hier sind der Zweck und die Zielsetzung des Dokuments zu benennen. Außerdem sollten die Rahmenbedingungen erläutert und Abgrenzungen getroffen werden.

In der Praxis begegnen den Autoren des vorliegenden Buches immer wieder Einleitungsteile, die sehr stark und auch nicht immer sinnvoll untergliedert sind – da folgt beispielsweise im Einleitungsteil noch ein Vorwort. Da die Abgrenzung zwischen den einzelnen Teilen häufig nicht klar ist, verfahren die Ersteller eines Dokuments dann erfahrungsgemäß nach dem Grundsatz: *„Irgendwas muss ich da ja eintragen."* Da zu den einzelnen Unterpunkten häufig nur noch wenig Wesentliches geschrieben wird, fehlt dem Einleitungsteil häufig die Struktur.

Besser ist es daher, den Einleitungsteil so wenig wie möglich zu untergliedern. Als sinnvoll hat sich in der Praxis die folgende Unterteilung erwiesen:

- Zweck des Dokuments
- Geltungsbereich und Abgrenzung

Hauptteil Der Hauptteil beinhaltet den eigentlichen Gegenstand des Dokuments. Die Gliederung des Hauptteils wird im Wesentlichen durch die Dokumentenklasse bestimmt.

Anhänge Umfangreiche oder ergänzende Dokumententeile, die den Fluss des Dokuments stören, sollten als Anhänge (häufig auch als *Anlagen* bezeichnet) an das Ende des Dokuments verschoben werden. Typischerweise gehören Auswertungen und umfangreiche Tabellen in den Anhang.

Niemals Inhalte aus anderen Dokumenten einfügen

In der Praxis werden vielfach Inhalte aus anderen gültigen Dokumenten als Anhänge eingefügt. Diese Vorgehensweise bringt gleich eine ganze Reihe von Nachteilen mit sich und sollte unbedingt unterbleiben. So sollten grundsätzlich Informationen immer nur an einer (einzigen) Stelle stehen und dort auch gepflegt werden. Werden beispielsweise Teile eines Dokuments in den Anhang eines anderen Dokuments kopiert, müssen bei einer Änderung immer beide Dokumente geändert werden. Da dies dann aber meist nicht erfolgt, entstehen nicht nur Inkonsistenzen, sondern wird im schlimmsten Fall mit veralteten Informationen gearbeitet.

Soll auf Informationen bestehender Dokumente verwiesen werden, darf dies immer nur mittels Verweis auf das Dokument geschehen. Ob hierzu eine Verknüpfung in das Dokument eingefügt wird oder nur auf das Dokument textlich verwiesen wird, kann individuell entschieden werden. Wichtig ist, dass der Verweis auf das richtige Dokument zeigt, was mit Verwendung einer eindeutigen Dokumentennummer sichergestellt werden kann.

Tabellen- und Abbildungsverzeichnisse Typischerweise enthalten umfangreiche Dokumente ein Abbildungs- und ein Tabellenverzeichnis.

Notwendigkeit sorgfältig prüfen

In welchen Dokumenten Abbildungs- und Tabellenverzeichnisse erforderlich sind, sollte einheitlich geregelt werden. Dabei sollte die jeweilige Notwendigkeit kritisch hinterfragt werden, denn der damit verbundene Arbeitsaufwand bei der Erstellung eines Dokuments ist nicht zu unterschätzen.

In einem umfangeichen Richtliniendokument oder einem Konzept, dass nur wenige Abbildungen und Tabellen enthält, die zudem sehr wichtig sind, kann es durchaus sinnvoll sein, diese mit Hilfe eines Verzeichnisses schnell finden zu können.

Betrachtet man aber einmal das eigene Leseverhalten und stellt sich die Frage, wie häufig man schon Abbildungs- oder Tabellenverzeichnisse verwendet hat, lautet bei vielen die Antwort wohl: Noch nie. Abbildungs- und Tabellenverzeichnisse gehören zu den Dokumententeilen, die häufig erstellt werden, ohne dass deren Sinnhaftigkeit ernsthaft hinterfragt wird. Zwar verursacht die eigentliche Erstellung der Verzeichnisse kaum Aufwand – vorausgesetzt die entsprechenden Funktionen des Textverarbeitungsprogramms wurden genutzt –, doch kosten sie in jedem Fall Platz und blähen Dokumente unnötig auf. Die Empfehlung kann daher nur lauten, sehr kritisch zu prüfen, bei welchen Dokumentenklassen diese Verzeichnisse benötigt werden.

Tabellen und Abbildungen beschriften

Die Frage, die es aber eigentlich zu beantworten gilt, ist, ob und wie Abbildungen und Tabellen zu beschriften sind. Sind in einem Dokument (beispielsweise in einem Installationshandbuch oder in einer Arbeitsanweisung) sehr viele Abbildungen zu beschriften, verursacht dies einen erheblichen Arbeitsaufwand. Um diesen einzuschränken, werden dann oftmals von den Dokumenterstellern nichtsagende Beschriftungen erstellt. Nicht nur einmal haben die Autoren dieses Buches unter einer Grafik den Beschriftungstext „Eigenschaftendialogbox" gelesen. Derartige Beschriftungen aber helfen niemanden – sie kosten nur Platz und Zeit.

Beschriftungen können Zusatzinfos liefern

Dabei macht die Beschriftung von Abbildungen und Tabellen durchaus Sinn. So können hier beispielsweise Erklärungen geliefert werden, die man im Fließtext mühsam suchen müsste. Auch ist es möglich, zusätzliche Informationen anzubieten.

In Anleitungen, die Abbildungen von Dialogboxen oder Funktionen enthalten, kann es beispielsweise sinnvoll sein, mit der Beschriftung die Menühierarchie, das heißt den Pfad zur Dialogbox, zu benennen. Diese Vorgehensweise bietet einen wirklichen Zusatznutzen. So könnte die Beschriftung einer Abbildung beispielsweise folgendermaßen lauten:

Schrift in Großbuchstaben Menü FORMAT \ ZEICHEN

Indexverzeichnis In einem Index sind die im Dokument behandelten Begriffe und Themen sowie die dazugehörigen Seitenzahlen aufgelistet. Die in den Index aufzunehmenden Begriffe müssen einzeln vom Dokumentersteller festgelegt und für den Indexeintrag markiert werden.

Wann sollte ein Index erstellt werden

Auch hier stellt sich die Frage, wann es sinnvoll ist, ein Indexverzeichnis in ein Dokument einzufügen. Das Indexverzeichnis dient dazu, ein gewünschtes Thema oder einen Begriff schnell im Dokument zu finden. Insofern ist bei Dokumenten, die nur wenige Seiten umfassen, die Erstellung eines Index kaum sinnvoll.

Zusätzlich muss das vorrangige Ausgabemedium betrachtet werden. Werden die Dokumente in einem Dokumentenmanagement-System verwaltet und bearbeitet, das die Dokumente automatisch indexiert und auch die Fundstellen anzeigt, und werden die Dokumente überwiegend am Bildschirm gelesen, so ist ein manuell erstelltes Indexverzeichnis wenig sinnvoll. Und selbst wenn kein unterstützendes System eingesetzt wird, ist man mit der Suchfunktion des Textverarbeitungsprogramms bzw. des PDF-Readers meist immer noch schneller. Zudem ist man nicht darauf angewiesen, dass der Dokumentersteller genau den gesuchten Begriff in das Indexverzeichnis aufgenommen hat.

Handelt es sich hingegen um umfangreiche Dokumente, mit denen auch oder sogar vorrangig in gedruckter Form gearbeitet wird, ist ein Indexverzeichnis allerdings erforderlich.

Glossar Ein Glossar erläutert die im Dokument verwendeten Fachbegriffe und Abkürzungen. Es soll den richtigen Gebrauch der Fachausdrücke und deren eindeutiges Verständnis sicherstellen.

Wichtig ist, dass das Glossar definiert, wie die Begriffe im betreffenden Dokument verwendet werden. Wie das vorliegende Buch eindrucksvoll beweist, gibt es viele Fachbegriffe, die nicht eindeutig definiert sind. Für diese Fälle ist es zwingend erforderlich, im Glossar deren jeweilige Verwendung im Dokument zu erläutern.

7.1.2.2 Bereitstellung von Dokumentvorlagen

Zur Durchsetzung der formalen Richtlinien sollten für die Erstellung neuer Dokumente Vorlagen bereitgestellt werden, die das Layout und eine Strukturierung vorgeben. Dabei kann es sinnvoll sein, zumindest für die wichtigsten Dokumentenklassen gesonderte Dokumentvorlagen zu erstellen. In mehrsprachigen Umgebungen sollten außerdem die Dokumentvorlagen in den benötigten Sprachversionen vorliegen.

Dokumentvorlagen schaffen Standards

Sinnvollerweise enthalten diese Vorlagen neben Layoutvorgaben auch Hinweise zur inhaltlichen Erstellung. Demzufolge sollten Dokumentvorlagen Folgendes vorgeben:

- Deckblatt mit den wichtigsten Dokumentinformationen (Autor, Vertraulichkeitsklassen Dokumentstatus usw.)
- Änderungsnachweis mit Hinweisen zur dessen Führung
- Ergänzende Dokumente bzw. mitgeltende Unterlagen mit Hinweisen zur dessen Verwendung
- Gliederung des Dokuments einschließlich Management Summary, Hauptteil, Glossar, Abbildungs- und Tabellenverzeichnisse, Index
- In Abhängigkeit von der Dokumentenklasse gegebenenfalls Vorgaben für die Inhalte einzelner Kapitel

cd-rom

An dieser Stelle sei noch einmal auf den Abschnitt 8.6 und die der CD-ROM beigefügte Dokumentvorlage verwiesen, die als Muster verwendet werden kann.

7.1.2.3 Regelungen für Dokumentationsprozesse

Auch für die Dokumentationsprozesse können allgemeinverbindliche Regelungen getroffen werden. Die erforderlichen Prozesse ergeben sich aus dem Dokumentenlebenszyklus (siehe Abschnitt 7.4.1). Hierzu gehören unter anderem die folgenden Prozesse:

- Prozesse zur Erstellung eines Dokuments
- Freigabeprozessse

- Prozesse zur Bereitstellung von Dokumenten
- Prozesse zur Nutzung von Dokumenten (Regelung von Berechtigungen)
- Prozesse zur Änderung von Dokumenten mit dem Status *endgültig* oder *freigegeben* (beispielsweise Vergabe des Status *ungültig*)
- Prozesse zur Archivierung von Dokumenten
- Prozesse zur Entsorgung von Dokumenten

Die nachfolgenden Richtlinien gelten für die genannten Prozesse. Sie sollen lediglich einige Möglichkeiten aufzeigen und müssen entsprechend ergänzt bzw. angepasst werden.

- Nur Dokumente, die den Status *endgültig* oder *freigegeben* tragen, dürfen als Arbeitsgrundlage für Aufgaben verwendet werden.
- Jeder Verantwortliche für ein Projekt, Teilprojekt bzw. Arbeitspaket oder einer betrieblichen Organisationseinheit ist für die Erstellung und Pflege der eigenen Dokumente selbst verantwortlich.
- Alle Dokumente müssen in Übereinstimmung mit geltenden Normen und Gesetzen und gegebenenfalls Vertragsinhalten, internen Anweisungen und spezifischen Anforderungen des Auftraggebers erstellt werden.
- Der Qualitätssicherer eines Dokuments darf nicht gleichzeitig der Ersteller eines Dokuments sein.
- Die Prüfung eines Dokuments erfolgt unter folgenden sachlichen und fachlichen Gesichtspunkten:
  - Übereinstimmung mit den definierten Prüfkriterien
  - Technische Angemessenheit und Durchführbarkeit
  - Übereinstimmung mit den Anforderungen des Auftraggebers
  - Schnittstellen zwischen dem zu prüfenden Dokument und bereits bestehenden Dokumenten
  - Wirtschaftliche und qualitative Gesichtspunkte

hinweis

Zur Umsetzung einer Dokumentationsrichtlinie empfiehlt es sich in der Praxis, einen Dokumentationsverantwortlichen einzusetzen. Sinnvoll ist es, diesen möglichst frühzeitig einzusetzen und bereits in die Erstellung der Dokumentationsrichtlinie mit einzubeziehen.

7.2 Empfehlungen für die Dokumentenerstellung mit Microsoft Office

Ein im Administrationsumfeld häufig gehörter Satz lautet: „Mit Office kenne ich mich nicht so gut aus". Dementsprechend wird beispielsweise Word immer noch als eine bessere Schreibmaschine eingesetzt. Das ist schade, denn in aller Regel stellen die Office-Produkte das wichtigste Handwerkszeug für jeden dar, der in irgendeiner Weise Dokumente zu erstellen hat. Und Dokumente zu erstellen, ohne die wichtigsten Funktionen von Office zu beherrschen, erschwert nicht nur die Erstellung, sondern vor allem auch die Pflege der Dokumente bei erforderlichen Änderungen.

Insbesondere Word bietet eine Vielzahl an Funktionen, die nicht nur dem Dokumentersteller, sondern auch dem Nutzer von Dokumenten das Leben sehr erleichtern können. Zwar will das nachstehende Kapitel kein Word-Seminar darstellen, doch kann erfahrungsgemäß die Kenntnis einiger nützlicher Funktionen, aber auch das Wissen um einige Stolpersteine das Erstellen und Nutzen von Word-Dokumenten deutlich vereinfachen.

Natürlich lassen sich Dokumente für die IT-Dokumentation auch mit anderen Textverarbeitungsprogrammen (zum Beispiel mit Hilfe der Bürosuite von OpenOffice) erstellen. Ebenso können auch DTP-Programme wie beispielsweise Adobe FrameMaker verwendet werden, die umfangreichere Layoutmöglichkeiten bieten. So findet man in FrameMaker unter anderem eine integrierte Buchfunktion, die es erlaubt, mehrere Dokumente zu einem Dokument (dem sogenannten Buch) zusammenzufassen.

hinweis

Die nachstehend vorgestellten Beispiele zu den Office-Produkten wurden mit Office Professional 2003 und Visio 2003 erstellt. Alle dargestellten Funktionen gelten in gleicher oder ähnlicher Weise auch für die anderen derzeit aktuellen Office-Versionen.

Die folgenden Ausführungen bieten sowohl Unterstützung bei der Erstellung von Dokumentvorlagen als auch bei der Dokumentenerstellung auf Basis einer solchen Vorlage.

Dem Aufbau der nachstehenden Kapitel liegt die Annahme zugrunde, dass Dokumentvorlagen eingesetzt werden, die dem Dokumentersteller einige Aufgaben, wie beispielsweise die Erstellung eines Inhaltsverzeichnisses, abnehmen. Alle Aufgaben, die sinnvollerweise im Rahmen der Erstellung einer Dokumentvorlage durchgeführt werden (Formatvorlagen erstellen, Verzeichnisse konfigurieren, Index einrichten usw.) werden im ersten Abschnitt behandelt. Die daraus resultierenden Aufgaben im Rahmen der Dokumentenerstellung schließen sich daran an.

Die aus den nachstehenden Beschreibungen abgeleitete Dokumentvorlage finden Sie in Abschnitt 8.6.

7.2.1 Eine Dokumentvorlage erstellen

Die folgenden Kapitel wenden sich in erster Linie an diejenigen, die eine Dokumentvorlage erstellen wollen. Es werden alle wichtigen Komponenten und deren Einsatz vorgestellt und die Vorgehensweise beim Einbinden in eine Dokumentvorlage beschrieben.

Aber auch diejenigen, die „nur" Dokumente erstellen, werden den ein oder anderen nützlichen Hinweis finden. Speziell an Ersteller von Dokumenten wendet sich der anschließende Abschnitt 7.2.2, der Hilfen, Tipps und Tricks für die Erstellung von Dokumenten mit Word liefert.

7.2.1.1 Masterlayout festlegen

Ein gutes Layout erleichtert die Lesbarkeit

Wie in den vorstehenden Kapiteln beschrieben, dienen Dokumentvorlagen vor allem auch der Layoutvorgabe. Gerade beim Erstellen technischer Dokumentationen wird der Faktor Layout aber oftmals vernachlässigt, was dazu führt, dass die fachlich ausgerichteten und damit oftmals nicht leicht zu lesenden Texte für den Leser noch schwerer zu erfassen sind.

Mit einem guten Layout kann viel für die Lesefreundlichkeit erreicht werden. Daher gilt es im ersten Schritt, den Satzspiegel und die Druckformate (d. h. die Schriftart und die Schriftgrößen) festzulegen.

Überlegungen zur Standardschriftart

Als gar nicht so einfach kann sich die Wahl der Standardschrift erweisen. Üblicherweise werden hierfür die beiden Schriftarten Times oder Arial gewählt.

Bei Times bzw. Times New Roman (TNR) handelt es sich um eine Serifenschrift. Gedacht sind die Serifen als haarfeine Akzente, die den lesenden Blick unaufdringlich unterstützen, daher gelten sie bei gedrucktem Text als besser lesbar. Längere Texte werden deshalb üblicherweise in einer Serifenschrift gedruckt. Serifenlose Schriften, wie beispielsweise Arial oder Helveticia, werden dagegen eher für kurze Texte und Überschriften eingesetzt. Gut kombinieren lässt sich eine serifenlose Schrift für Überschriften und Bildunterschriften mit einer Serifenschrift für den Haupttext und die Marginalspalte.

Leider verkehren sich die Vorteile der Serifenschrift bei der Betrachtung am Bildschirm in Nachteile: Buchstaben und Wortbilder fransen aus und verschwimmen, das Schriftbild wird undeutlich, das Lesen anstrengend. Selbst ein guter Bildschirm kann nichts am Grundproblem jeder Serifenschrift beim Bildschirm ändern. Für die Betrachtung am Bildschirm sind serifenlose Schriften wie Arial daher besser geeignet, dies gilt insbesondere für kleine Schriftgrößen. Einige Schriftarten wurden speziell für die Betrachtung am Bildschirm entwickelt bzw. verbessert. Hierzu zählen unter anderem Verdana, Tahoma, Trebuchet, Georgia und einige Lucida-Schnitte. Bei der Auswahl der Standardschrift sollte daher beachtet werden, welches Medium hauptsächlich zum Lesen der Dokumente eingesetzt wird.

Beachtung verdient auch die Wahl der Schriftgrößen. Hier können folgende Werte als Anhaltspunkte dienen:

- Überschriften: 13 – 17 Punkt. Werden mehrere Überschriftenebenen benötigt, ist natürlich eine zusätzliche Abstufung nötig.
- Haupttext: 10 – 12 Punkt.
- Bild- und Tabellenunterschriften 7 – 9 Punkt.

hinweis

Ein Mix aus zu vielen Schriftarten und Schriftgraden sollte vermieden werden, da dies das Dokument unruhig macht und die Lesbarkeit erschwert. Weniger ist hier oftmals mehr.

7.2.1.2 Dokumenteigenschaften sinnvoll nutzen

Die meisten Dokumente haben ein Deckblatt, das die wichtigsten Dokumentinformationen (Dokumentenklasse, Titel, Autor, Version, Dokumentstatus usw.) enthält. Diese Information dürfen aber nicht nur auf dem Deckblatt stehen, sondern sollten, neben der Seitennummerierung, in der Kopf- bzw. Fußzeile jeder Seite zu finden sein.

Eindeutigkeit jeder einzelnen Seite ist wichtig

Hintergrund dabei ist, dass es bei einem revisionssicheren Dokument möglich sein muss, jede einzelne Seite eindeutig dem Dokument zuzuordnen. Das hierfür üblicherweise zitierte Beispiel ist ein Windstoß, der mehrere Dokumente durcheinander wirbelt. Alle Einzelseiten müssen sich anschließend wieder zweifelsfrei den verwirbelten Dokumenten zuordnen lassen.

Dies aber bedeutet, dass einige Attribute, wie beispielsweise der Bearbeitungsstatus, an verschiedenen Stellen im Dokument gepflegt werden müssen, was erfahrungsgemäß unweigerlich zu Inkonsistenzen führt. Abhilfe schafft die Verwendung der *Feldfunktion*.

Arbeiten mit Feldern

Word bietet die Möglichkeit, eine Vielzahl von Informationen als Felder einzufügen, die automatisch aktualisiert werden. Auch beim „Aktuellen Datum“ oder der „Seitenzahl“ handelt es sich um derartige Felder.

Darüber hinaus können aber auch alle in den Dokumenteigenschaften verfügbaren Attribute als Felder eingefügt werden. Hierzu ist es erforderlich, die Dokumenteigenschaften (diese werden auch als Metadaten bezeichnet) in der gleichnamigen Dialogbox zu pflegen.

Zu beachten ist, dass nicht nur in der Registerkarte ZUSAMMENFASSUNG Informationen zum Dokument eingetragen werden können, sondern viel umfassender in der Registerkarte ANPASSEN.

Definition von Metadaten

Als Metadaten („Daten über Daten“) bzw. Metainformationen werden Daten bezeichnet, die Informationen über andere Informationsressourcen enthalten und diese damit besser auffindbar machen. Metadaten liefern also Grundinformationen über ein Dokument, wie zum Beispiel Angaben über den Autor, den Titel, die ISBN-Nummer oder den Zeitpunkt der Veröffentlichung. Sie erleichtern das Auffinden von Dokumenten, weshalb sie insbesondere in Dokumentenmanagement-Systemen eine wichtige Rolle spielen.

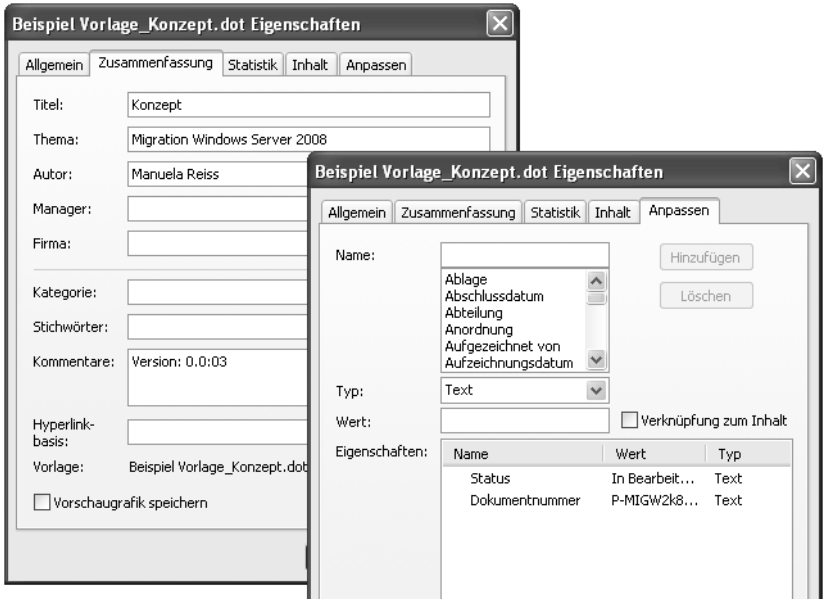


Abbildung 7.5: Fast alle Dokumentinformationen können in den Dokumenteigenschaften verwaltet werden.

Alle in der Eigenschaftendialogbox gepflegten Dokumentinformationen können anschließend als Feld an beliebiger Stelle im Dokument eingefügt werden. Hierzu ist die Kategorie DocProperty in der Feld-Dialogbox zu verwenden.

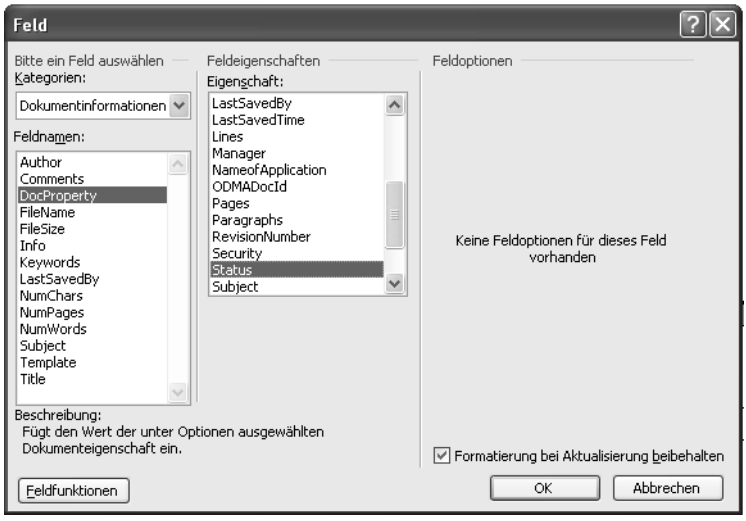


Abbildung 7.6: Alle Dokumenteigenschaften können als Feld eingefügt werden.

Beispiel

Die folgenden beiden Abbildungen zeigen das Deckblatt und die Kopf- bzw. Fußzeilen bzw. die Dokumentinfobox der Beispielvorlage. Das Beispiel zeigt, dass fast alle Informationen als Felder (grau unterlegt) verwendet werden können. Diese aktualisieren sich entweder automatisch (Datumsfelder, Seitenzahlen) oder müssen in den Dokumenteigenschaften gepflegt werden. Werden zusätzlich konsequent alle manuell einzutragenden Daten nur an einer Stelle verwendet, vermeidet man mit dieser Vorgehensweise Inkonsistenzen.

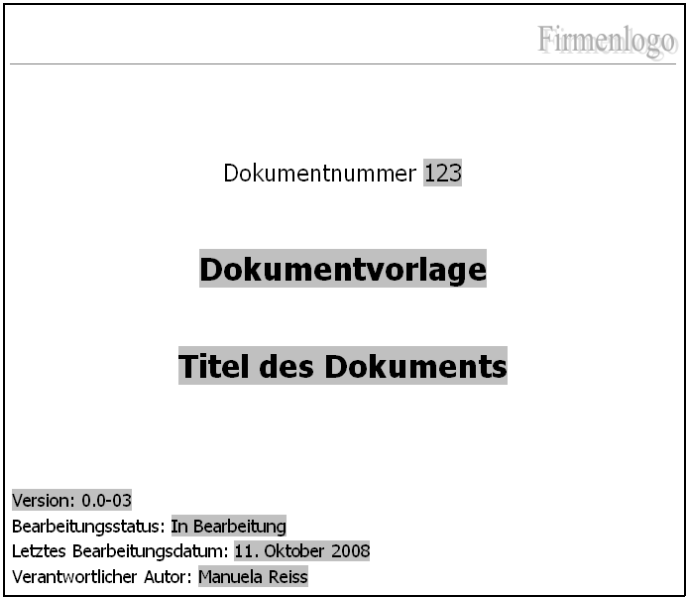
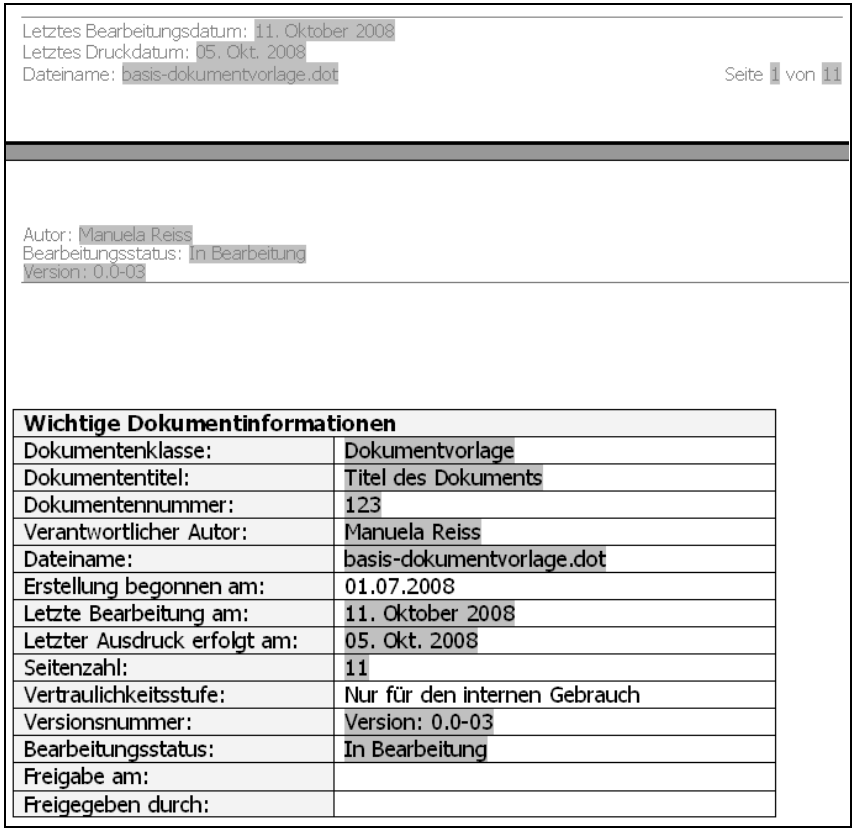


Abbildung 7.7: Deckblatt einer Dokumentvorlage unter Verwendung von Feldfunktionen



Wichtige Dokumentinformationen	
Dokumentenklasse:	Dokumentvorlage
Dokumententitel:	Titel des Dokuments
Dokumentennummer:	123
Verantwortlicher Autor:	Manuela Reiss
Dateiname:	basis-dokumentvorlage.dot
Erstellung begonnen am:	01.07.2008
Letzte Bearbeitung am:	11. Oktober 2008
Letzter Ausdruck erfolgt am:	05. Okt. 2008
Seitenzahl:	11
Vertraulichkeitsstufe:	Nur für den internen Gebrauch
Versionsnummer:	Version: 0.0-03
Bearbeitungsstatus:	In Bearbeitung
Freigabe am:	
Freigegeben durch:	

Abbildung 7.8: Beispiel für die Verwendung von Feldern in der Kopf- und Fußzeile und in der Dokumentinfobox

Deckblatt kann gegebenenfalls entfallen

Wie die beiden Abbildungen zeigen, sind einige Informationen redundant sowohl auf dem Deckblatt als auch in der Dokumentinfobox zu finden. Diese Vorgehensweise ist sinnvoll, da nicht alle Dokumente ein Deckblatt benötigen, Während beispielsweise Konzepte und Richtliniendokumente aus optischen Gründen in der Regel ein Deckblatt aufweisen, ist dies beispielsweise bei Checklisten oder Hardware-Systemakten entbehrlich. In diesem Fall würde die zweite Seite das Deckblatt darstellen. Selbstverständlich ist es alternativ auch möglich, die Dokumentinfobox direkt auf das Deckblatt zu setzen.

tipp

Noch komfortabler kann man die Eingabe der Metadaten gestalten, indem man mit Hilfe eines Makros beim Öffnen des Dokuments alle erforderlichen Eingaben in einer Dialogbox abfragt. Der damit verbundene Programmieraufwand macht sich schnell bezahlt, da mögliche Eingabefehler minimiert werden.

7.2.1.3 Formatvorlagen erleichtern die Standardisierung

Ein Thema, um das man weder als Ersteller einer Dokumentvorlage noch als dessen Nutzer herumkommt, betrifft den Bereich der *Formatvorlagen*. Hinter einer Formatvorlage (nicht zu verwechseln mit der Dokumentvorlage!) verbirgt sich eine Gruppe von Formatierungsmerkmalen, die auf einfache Weise Text, Tabellen oder Listen im Dokument zugewiesen werden kann. Der zuvor markierte Bereich übernimmt in einem Schritt alle in der Formatvorlage hinterlegten Formatierungen. Anstatt beispielsweise alle Überschriften in drei Einzelschritten zentriert und in 16 Punkt Arial zu formatieren, kann mit Hilfe einer zuvor erstellten Formatvorlage das gleiche Ergebnis durch Zuweisen einer Formatvorlage in einem Schritt erzielt werden.

Vereinfachen nachträglicher Änderungen

Fast noch entscheidender aber sind die Möglichkeiten, die Formatvorlagen in Bezug auf nachträgliche Änderungen bieten. Soll in dem zuvor gewählten Beispiel die Schriftgröße aller Überschriften auf 18 Punkt geändert werden, genügt eine Anpassung der Formatvorlage, um die Änderung durchzuführen.

Formatvorlagen gehören somit zu den wichtigsten Werkzeugen, um Dokumente komfortabel zu formatieren. Außerdem ermöglichen sie es, und dieser Umstand ist mindestens genauso entscheidend, einen Standard im Layout durchzusetzen.

Allerdings machen die vielschichtigen Einsatzmöglichkeiten von Formatvorlagen diese zu einem sehr komplexen Thema. Die nachstehenden Ausführungen beschränken sich daher auf die wichtigsten Aspekte und Stolperfallen im Umgang mit Formatvorlagen. Für eine eingehende Beschäftigung mit dem Thema kann hier nur auf die zahlreiche Literatur und auf die umfassenden Erläuterungen in der Word-Hilfe verwiesen werden.

Die Standard-Formatvorlage bestimmt das Layout Öffnet man ein neues Dokument ohne Auswahl einer Dokumentvorlage, so erstellt man automatisch ein Dokument, dass auf der Standard-Dokumentvorlage NORMAL.DOT basiert. In dieser Dokumentvorlage befindet sich die Formatvorlage STANDARD, die unter anderem die standardmäßig verwendete Schriftart und Schriftgröße festlegt.

Standardschrift ändern

Soll nun die beispielsweise die Standardschrift für alle Dokumente auf Arial 11 Punkt festgelegt werden, gilt es, diese Formatvorlage zu ändern. Dies ist am einfachsten möglich, indem in der Zeichendialogbox zunächst die gewünschte Schriftart und Größe festgelegt und anschließend die Option STANDARD gewählt wird.

Mit dieser Vorgehensweise wird die Standardschriftart für alle Dokumente geändert, für deren Erstellung nicht explizit eine Dokumentvorlage ausgewählt wird.

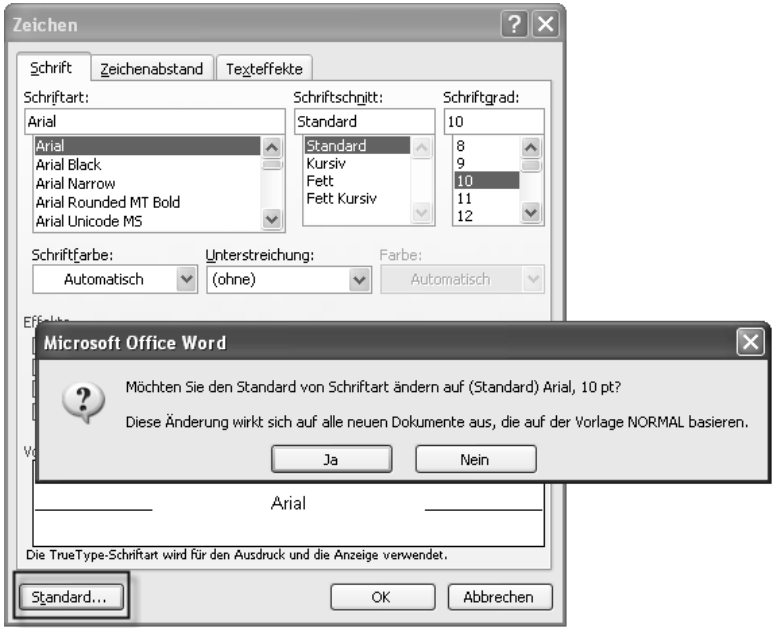


Abbildung 7.9: Standardschriftart für die Vorlage Normal.dot ändern

Werden, wie empfohlen Dokumentvorlagen für die verschiedenen Dokumentenklassen eingesetzt, muss die Standardschriftart in jeder Dokumentvorlage einmalig geändert werden. Dazu ist entweder die Vorlage oder ein neues Dokument auf der Basis der gewünschten Vorlage zu öffnen. Die weitere Vorgehensweise ist dann identisch mit der zuvor beschriebenen.

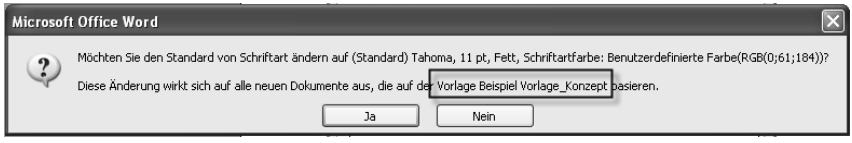


Abbildung 7.10: Für jede Dokumentvorlage kann die Standardschrift festgelegt werden.

Formatvorlagen erstellen und anpassen Zur Erstellung und Anpassung der in diesem Kapitel vorgestellten Formatvorlagen gibt es mehrere Möglichkeiten.

Als eine Möglichkeit, die nachstehend gezeigte Dialogbox zur Verwaltung von Formatvorlagen zu öffnen, kann die Option FORMATVORLAGEN UND FORMATIERUNG im Menü FORMAT verwendet werden. Im daraufhin angezeigten Aufgabenbereich werden alle mitgelieferten und selbsterstellten Formatvorlagen aufgelistet und können dort auch verwaltet werden. Auch das Erstellen neuer Formatvorlagen ist dort möglich.

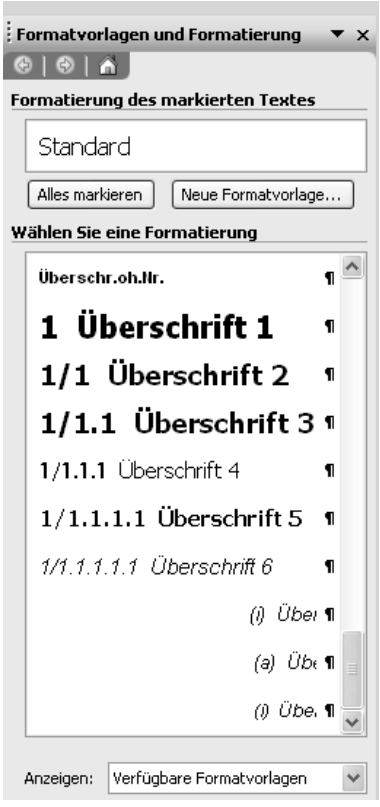


Abbildung 7.11: Formatvorlagen verwalten im Aufgabenbereich

Neue Formatvorlage erstellen

Zum Erstellen einer neuen Formatvorlage ist die Option NEUE FORMATVORLAGE zu wählen. Hier muss zunächst festgelegt werden, für welchen Bereich (Absatz, Zeichen, Tabelle, Liste) die Vorlage gelten soll, auf welcher Vorlage sie basieren soll und welche Formatvorlage für den Folgeabsatz Anwendung findet. Anschließend können die Formatierungen festgelegt werden, die mit der zu erstellenden Formatvorlage zukünftig zugewiesen werden sollen.

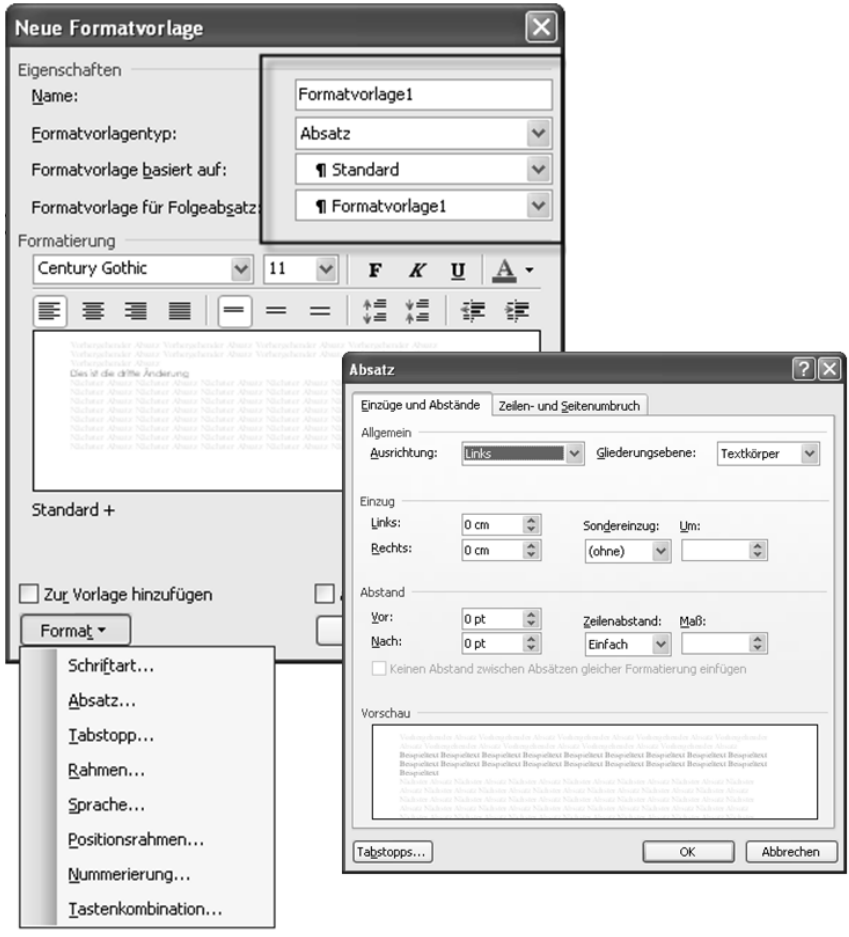


Abbildung 7.12: Eine neue Formatvorlage erstellen

Automatisches Aktualisieren verursacht Probleme

In der Dialogbox FORMATVORLAGE ÄNDERN bzw. NEUE FORMATVORLAGE gibt es mit der Option AUTOMATISCH AKTUALISIEREN eine Funktion, die mit Bedacht eingesetzt werden sollte, da sie ein hohes Fehlerpotential birgt. Ist die Funktion aktiviert, führt jede Änderung im Text, dem diese Formatvorlage zugewiesen ist, zu einer Änderung der Vorlage, das heißt, sie wird durch die Änderung automatisch ebenfalls verändert. Das damit das betreffende Dokument innerhalb kürzester Zeit keinem Layoutstandard mehr entspricht, ist eine fast zwangsläufige Folge.

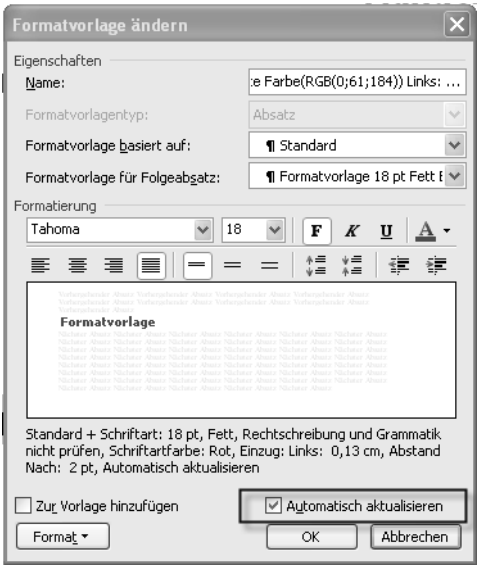


Abbildung 7.13: Die automatische Aktualisierung von Formatvorlagen kann ungewollte Auswirkungen haben.

Mit Marginalien „Lesestraßen" schaffen Bei Marginalien handelt es sich um Randbemerkungen, die am Rand des Textes stehen. Sie sind ein wichtiges Gestaltungselement, das die Verständlichkeit des Textes deutlich fördern kann. Inhaltlich kann es sich um kurze Stichwörter zum daneben stehenden Textblock, aber auch um ergänzende Informationen handeln. Richtig eingesetzt schaffen sie in Kombination mit den Überschriften sogenannte Lesestraßen, an denen sich der Leser entlang hangeln kann. Da diese Bemerkungen einiges an Platz brauchen, muss der Außenrand genügend breit sein. Es sollte daher vor der Erstellung der Dokumentvorlage geklärt sein, ob Marginalien verwendet werden. Dies ist dann bei der Festlegung des Seitenformats zu berücksichtigen.

Formatvorlage für Marginalien erstellen

Technisch können in Word Marginalien mit Hilfe eines Positionsrahmens in den Randbereich gesetzt werden. Die erste Zeile der Marginalie muss dabei in der gleichen Zeile stehen wie der dazugehörige Textteil. Konsequenterweise sollte auch hierfür eine Formatvorlage bereitgestellt werden. Recht einfach möglich ist dies, indem eine neue Formatvorlage erstellt und unter FORMAT die Option POSITIONSRAHMEN gewählt wird. Durch Auswahl der Position AUSSEN wird immer dann, wenn einem Absatz diese Formatvorlage zugewiesen wird, der Text in einem Positionsrahmen im Randbereich platziert.

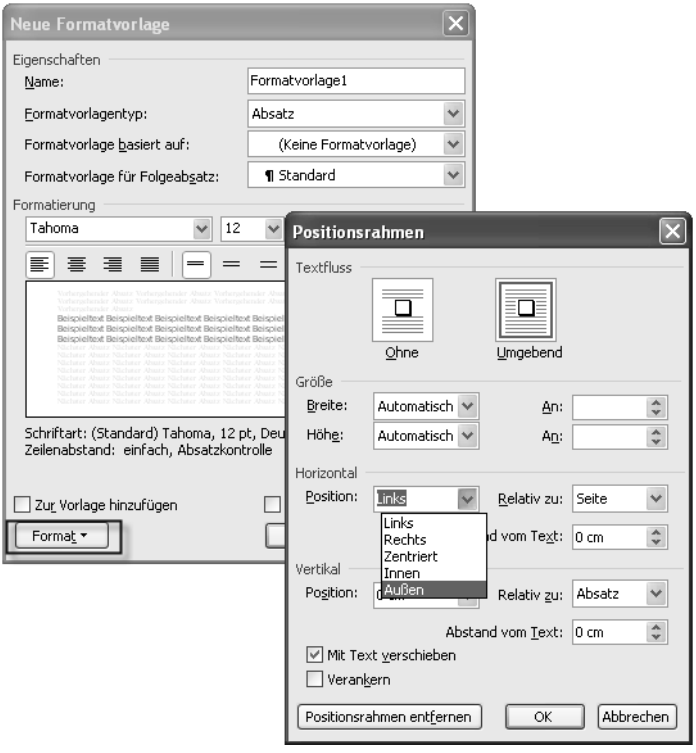


Abbildung 7.14: Formatvorlage für das Setzen von Marginalien erstellen

Überschriften-Formatvorlagen besser verstehen Die mit Word mitgelieferten vordefinierten Formatvorlagen ÜBERSCHRIFT 1 BIS 9 stellen eine Besonderheit dar. Werden diese zum Formatieren von Überschriften in einem Dokument verwendet, werden sie automatisch mit dem gewählten Nummerierungsformat nummeriert. Damit ist es möglich, Überschriften nicht nur herausgehoben zu formatieren, sondern auch entsprechend der Gliederungsebene zu nummerieren. Außerdem kann ohne weitere Anpassungen das Inhaltsverzeichnis aus den so ausgezeichneten Überschriften generiert werden.

Verknüpfung zwischen Überschrift und Nummerierung

Möchte man die Gliederungsfunktion mit benutzerdefinierten Formatvorlagen verknüpfen, ist es notwendig zu verstehen, wie Gliederungsebenen mit Formatvorlagen verknüpft sind. Und auch im Fehlerfall ist es wichtig, diese Einstellungen überprüfen zu können, denn erfahrungsgemäß bereitet gerade die Nummerierung in Überschriftenformaten immer wieder Probleme.

Um die Verknüpfung anzuzeigen bzw. zu konfigurieren, ist im Menü FORMAT zunächst die Option NUMMERIERUNG UND AUFZÄHLUNGSZEICHEN und dann die Registerkarte GLIEDERUNG zu wählen. Hier muss ein Nummerierungsformat, das „Überschrift 1“, „Überschrift 2“ usw. enthält, ausgewählt werden. Nach Auswahl der Option ERWEITERT wird die nachstehende Dialogbox angezeigt. In der angezeigten Dialogbox kann nicht nur die Nummerierung für die einzelnen Gliederungsebenen geändert werden. Vielmehr ist es auch möglich, die Gliederungsebenen mit anderen Formatvorlagen zu verbinden.

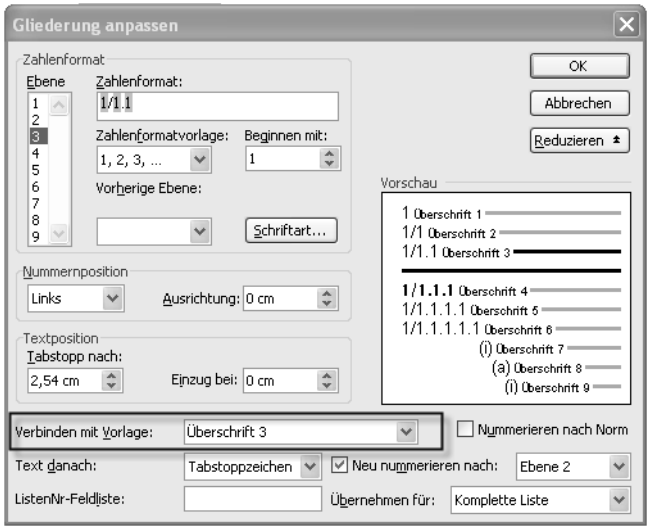


Abbildung 7.15: Die Gliederungsebenen müssen mit Formatvorlagen verknüpft werden.

Auch das Inhaltsverzeichnis basiert auf Formatvorlagen Nicht alle Dokumente benötigen ein Inhaltsverzeichnis. Hierzu gehören in der Regel Checklisten, Protokolle oder kleinere Arbeitsanweisungen. Bei umfangreichen Dokumenten aber ist das Inhaltsverzeichnis ein Pflichtelement. Es sollte sinnvollerweise bereits im gewünschten Layout in die Dokumentvorlage integriert werden. Die richtige Anwendung der Überschriftenformatvorlagen vorausgesetzt, enthält damit das Dokument ohne weitere Benutzereingriffe ein jederzeit aktuelles Inhaltsverzeichnis.

Inhaltsverzeichnis erstellen

Das Einbinden eines Inhaltsverzeichnisses kann mit Hilfe der Option INDEX- UND VERZEICHNISSE erfolgen, die bei Word 2003 im Menü EINFÜGEN unter REFERENZ versteckt ist. Auf der Registerkarte INHALTSVERZEICHNIS kann hier das Layout festgelegt werden. Ein Inhaltsverzeichnis lässt sich am einfachsten mit den integrierten Formatvorlagen für Gliederungsebenen oder Überschriften erstellen.

Wird als Format VON VORLAGE ausgewählt, wird das Layout verwendet, das in den vordefinierten Verzeichnis-Formatvorlagen für die verschiedenen Ebenen konfiguriert ist. Zu wählen ist dieses Format, wenn die vordefinierten Gliederungsebenen-Formate KLASSISCH, ELEGANT usw. nicht die Anforderungen erfüllen. Die Verzeichnis-Formatvorlagen entsprechen vollständig den übrigen Formatvorlagen und können genauso konfiguriert werden.

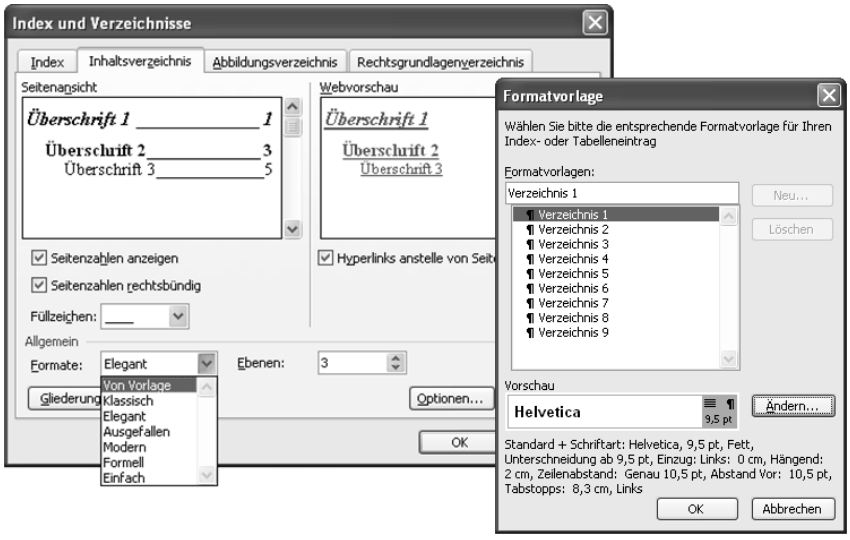


Abbildung 7.16: Sind keine Anpassungen erforderlich, ist das Inhaltsverzeichnis schnell erstellt.

Werden im Dokument für die Formatierung von Überschriften die vordefinierten Überschriften-Formatvorlagen verwendet, gibt es an dieser Stelle weiter nichts zu tun. Wurden jedoch eigene Formatvorlagen für Überschriften erstellt, muss Word noch mitgeteilt werden, dass diese für das Inhaltsverzeichnis zu verwenden sind. Hierzu wird die Schaltfläche OPTIONEN verwendet. In der angezeigten Dialogbox erfolgt die Zuordnung. Werden ausschließlich eigene Formatvorlagen verwendet, müssen die standardmäßig gesetzten Zuordnungen gelöscht werden.

tipp

Beim Inhaltsverzeichnis oder auch bei Anhängen ist es häufig nicht gewünscht, dass diese ebenfalls eine Nummerierung erhalten. Andererseits sollen sie ebenfalls der Überschriftenebene zugewiesen werden, was standardmäßig zur Formatierung mit einer Überschriftennummer führt.

Um für einzelne Überschriften die Nummerierung zu entfernen, ist in der Dialogbox NUMMERIERUNG UND AUFZÄHLUNG (im Menü FORMAT) die Auswahl OHNE zu verwenden. Auch das direkte Löschen der Nummerierung in der Überschrift funktioniert in der Regel, verlangt aber eine sehr exakte Markierung der Nummerierung.

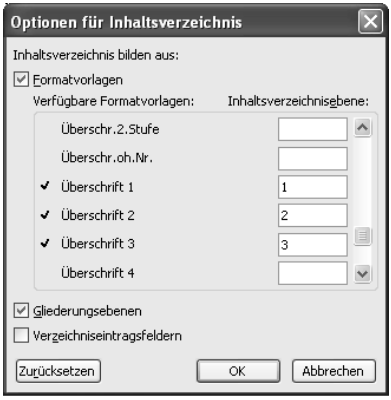


Abbildung 7.17: Auch benutzerdefinierte Formatvorlagen können für das Inhaltsverzeichnis verwendet werden.

tipp

Wie die kurzen Ausführungen gezeigt haben, ist das Zusammenspiel von Formatvorlagen, Gliederungsebenen und Verzeichnissen sehr komplex. Sofern möglich, sollten daher die integrierten Formatvorlagen für Gliederungsebenen und Überschriften verwendet werden. Ist dies nicht möglich, ist dringend anzuraten, sich vor der Bereitstellung der ersten Dokumentvorlage näher mit der Thematik zu beschäftigen. Unabdingbar ist es neu erstellte Dokumentvorlagen ausgiebig zu testen. Erfahrungsgemäß steckt hier die Tücke im Detail. Funktioniert das beschriebene Zusammenspiel nämlich nicht richtig, führt dies zu fehlerhaften Formatierungen und einem sehr eigenwilligen Verhalten der Vorlagen, das oftmals nicht nachvollziehbar ist.

Angepasste Symbolleisten bereitstellen Dokumentvorlagen ermöglichen es, das Layout und eine Strukturierung für zu erstellende Dokumente vorzugeben. Es sollte daher verbindlich vorgeschrieben werden, Dokumente ausschließlich unter Verwendung der entsprechenden Dokumentvorlagen zu erstellen. Natürlich sollten dann auch Formate ausschließlich mittels den darin enthaltenen Formatvorlagen zugewiesen werden. Direkte (sogenannte „harte“) Formatierungen sollten soweit wie möglich unterbleiben, da diese bei nachträglichen Änderungen erheblichen manuellen Aufwand verursachen.

Einfacher Zugriff erhöht die Akzeptanz

Vielfach aber ist das Vorhandensein der Formatvorlagen gar nicht bekannt oder sie werden nur halbherzig angewandt. Es hat es sich als hilfreich erwiesen, in einer Dokumentvorlage alle relevanten Formatierungen in einer speziellen Symbolleiste oder einem zusätzlichen Menü bereitzustellen. Sind alle einsetzbaren Formate übersichtlich am Bildschirmrand zu finden, werden diese in der Regel auch eher benutzt. Zusätzlich können den Symbolleisten Funktionen (beispielsweise die Querverweisfunktion) hinzugefügt werden, die häufig benötigt werden und standardmäßig nur über einen Menüzugriff verfügbar sind.

Es hat sich bewährt, die folgenden Funktionen auf einer Symbolleiste bereitzustellen:

- Überschriftenebenen
- Aufzählungen
- Nummerierungen
- Marginalien
- Tabellen
- Tabellen- und Bildunterschriften
- Grafiken einfügen und formatieren
- Text in Index aufnehmen
- Felder aktualisieren
- Standardformatvorlage zum Zurücksetzen aller Formatierungen
- Querverweise (siehe Abschnitt 7.2.2.1)
- Text unformatiert einfügen (siehe Abschnitt 7.2.2.6)

Reglementierung ist schwierig

In diesem Zusammenhang wird häufig die Frage gestellt, wie sichergestellt werden kann, dass die Ersteller von Dokumenten nicht trotzdem manuell direkte (harte) Formatierungen vornehmen.

Die Erfahrungen zeigen, dass dies kaum verhindert werden kann. Eine Reglementierung – beispielsweise durch das Entfernen des Menüs FORMAT und aller anderen Zugriffsmöglichkeiten darauf – ist zwar möglich, schränkt aber so stark ein, dass dies erfahrungsgemäß einen erhöhten Supportaufwand zur Folge hat. Außerdem müssen dann wirklich alle erforderlichen Formate über benutzerdefinierte Symbolleisten oder Menüs zur Verfügung gestellt werden, was wiederum erheblichen Aufwand für die Erstellung der Dokumentvorlage nach sich zieht. Eine entsprechende Unterweisung ist daher meist der bessere Weg.

tipp

Eine Formatvorlage, die als Symbolleistenbefehl (siehe Abbildung 7.18) auf keinen Fall fehlen sollte, ist die bereits beschriebene Standard-Formatvorlage. Mittels dieser Vorlage können mit einem Mausklick alle Formatierungen (Zeichen- und Absatzformatierungen) eines Absatzes oder aller markierten Absätze auf die Standardformatierung zurückgesetzt werden.

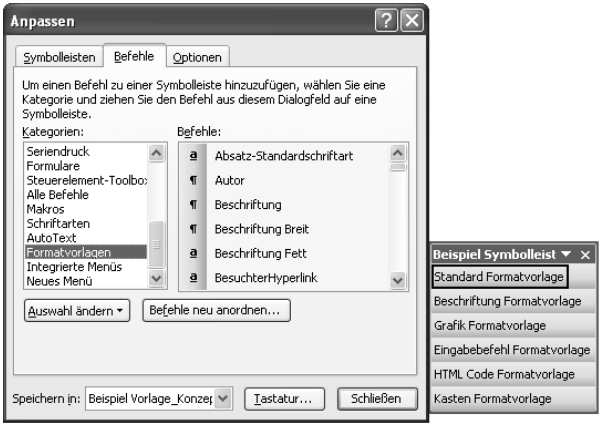


Abbildung 7.18: Formatvorlagen können in einer gesonderten Symbolleiste bereitgestellt werden.

7.2.1.4 Abbildungs- und Tabellenverzeichnisse einfügen

Soll eine Dokumentenklasse ein Abbildungs- bzw. Tabellenverzeichnis erhalten, können beide bereits in die dafür zu erstellende Dokumentvorlage integriert werden. Die Verzeichnisse enthalten solange keine Inhalte, bis vom Anwender Tabellen oder Grafiken mit den entsprechenden Beschriftungen hinzugefügt werden. Gibt es in einem Dokument keine Abbildungen oder Tabellen, kann das überflüssige Verzeichnis einfach gelöscht werden.

Abbildungs- und Tabellenverzeichnisse erstellen

Das Einbinden von Abbildungs- bzw. Tabellenverzeichnissen kann mit Hilfe der Option INDEX- UND VERZEICHNISSE erfolgen, die sich bei Word 2003 im Menü EINFÜGEN unter REFERENZ befindet. Auf der Registerkarte ABBILDUNGSVERZEICHNIS können sowohl das Abbildungsverzeichnis als auch Tabellen- und Formelverzeichnisse erstellt werde. Das Layout der Verzeichnisse basiert, genauso wie das Inhaltsverzeichnis, auf Formatvorlagen. Es kann, wie dort bereits beschrieben, angepasst werden.

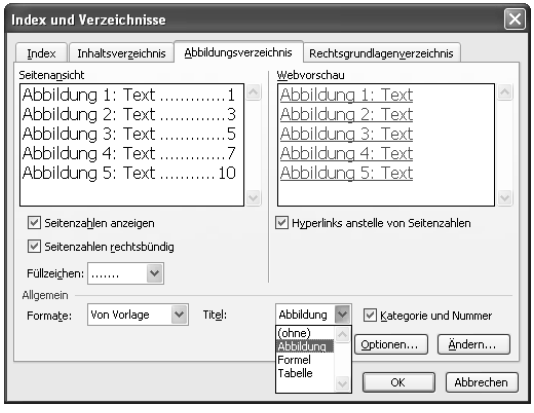


Abbildung 7.19: Mit der Registerkarte „Abbildungsverzeichnis“ können auch Tabellen- und Formelverzeichnisse erstellt werden.

Sinnvolle Beschriftungen für Abbildungen

In Anleitungen, die Screenshots von Dialogboxen oder Funktionen enthalten, kann es sinnvoll sein, mit der Beschriftung die Menü-Hierarchie zu benennen, in der die beschriebene Funktion zu finden ist. Die nachstehende Abbildung zeigt dazu ein Beispiel.

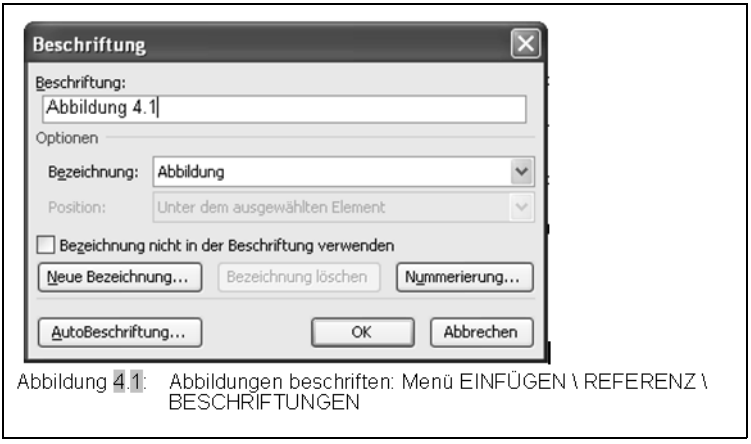


Abbildung 7.20: Abbildungsbeschriftung unter Einbeziehung der Menü-Hierarchie

7.2.1.5 Indexverzeichnis einfügen

In einem Index sind die im Dokument behandelten Begriffe und Themen sowie die dazugehörigen Seitenzahlen aufgelistet. Die in den Index aufzunehmenden Begriffe sollten einzeln vom Dokumentersteller festgelegt und als Indexeintrag markiert werden. Für diesen fügt Word ein Feld „Indexeintrag" (XE) in das Dokument ein. Ist für ein Dokument ein Indexverzeichnis erforderlich, kann dieses ebenfalls in die dafür zu erstellende Dokumentvorlage integriert werden.

Indexverzeichnis erstellen

Das Einbinden des Indexverzeichnisses kann mit Hilfe der bereits vorgestellten Option INDEX- UND VERZEICHNISSE erfolgen. Auf der Registerkarte INDEX kann das gewünschte Layout für das Indexverzeichnis gewählt werden Das Layout basiert genauso wie das Inhaltsverzeichnis bzw. andere Verzeichnisse auf Formatvorlagen und kann ebenso angepasst werden.

cd-rom

In Abschnitt 8.7 und auf der beigefügten CD-ROM finden Sie eine Checkliste, die alle erforderlichen Schritte zur Bereitstellung von Dokumentvorlagen zusammenfasst und die neben der Muster-Dokumentvorlage das Erstellen von Vorlagen unterstützt.

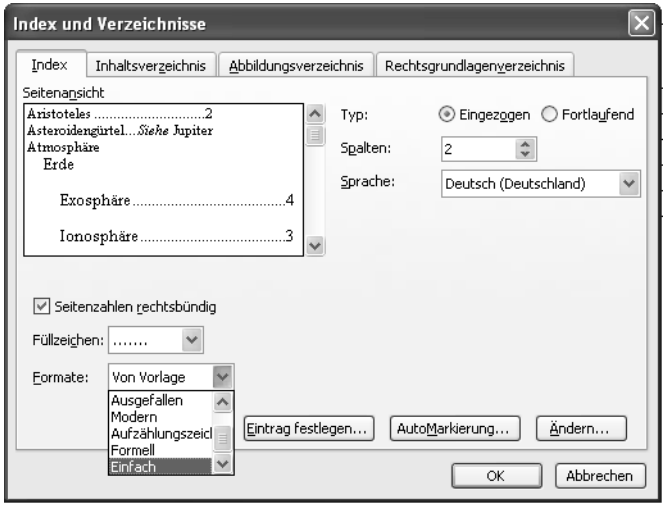


Abbildung 7.21: Dank vordefinierter Formate kann das Indexverzeichnis meist ohne weitere Konfiguration verwendet werden.

7.2.2 Word-Funktionen sinnvoll bei der Dokumentenerstellung nutzen

Word bietet eine Vielzahl Funktionen an, die nicht nur die Erstellung, sondern vor allem auch die spätere Pflege der Dokumente sehr erleichtern. Dieses Kapitel stellt einige wichtige Funktionen vor, die Ersteller von Dokumenten kennen sollten, um die in der Dokumentationsrichtlinie definierten Anforderungen im Rahmen einer standardisierten IT-Dokumentation optimal umzusetzen.

7.2.2.1 Ohne Querverweise geht es nicht

Ein immer noch weit verbreitetes Vorgehen sind manuell eingefügte Verweise – beispielsweise auf Überschriften, Abbildungen oder Tabellen. Bei Änderungen am Dokument, die einen der genannten Punkte betreffen, müssen in diesem Fall alle Verweise manuell geändert werden. Dass dies ein immense Fehlerquelle darstellt, muss kaum erwähnt werden. Als eine Grundregel sollte daher gelten:

> *Keine manuellen Verweise auf andere Seiten, Überschriften, Abbildungen, Tabellen oder Formeln!*

Die Querverweisfunktion von Word bietet die Möglichkeit, Verweise auf Überschriften, Abbildungen und Tabellen mit und ohne Seitenzahlen einzufügen. Die Querverweise werden automatisch aktualisiert, sodass man sich später nicht mehr darum kümmern muss.

Einen Querverweis erstellen

Soll beispielsweise auf eine Überschrift in einem anderen Kapitel verwiesen werden, muss zunächst die nachstehend gezeigte Dialogbox geöffnet werden. Die Funktion QUERVERWEIS ist bei Word 2003 im Menü EINFÜGEN unter REFERENZ zu finden. Anschließend wird als Verweistyp ÜBERSCHRIFT gewählt. Danach kann festgelegt werden, worauf verwiesen werden soll.

Abbildung 7.22: Die Querverweisfunktion unterstützt Verweise auf eine Reihe von Elementen.

Mittels des Verweistyps ÜBERSCHRIFT kann beispielsweise auf den Überschriftentext und die Überschriftennummer oder auch auf die Seitenzahl verwiesen werden. Selbstverständlich können auch mehrere Verweise miteinander kombiniert werden:

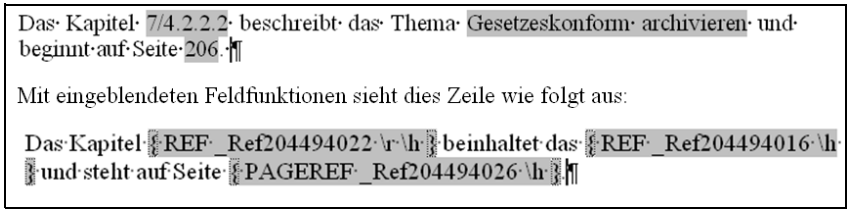


Abbildung 7.23: Anzeige eines Verweises

7.2.2.2 Arbeiten mit Überschriftenformatvorlagen

Dokumente werden mit Hilfe von Überschriften strukturiert. Diese sollen sich durch Schriftauszeichnungen, wie fette Schrift oder größere Schriftgrade hervorheben. Es wäre nun aber fatal, jede Überschrift manuell zu gestalten. Auch für die Gestaltung von Überschriften sollten stets Formatvorlagen verwendet werden.

Formatvorlagen müssen zwingend verwendet werden

Werden zentral erstellte Dokumentvorlagen bereitgestellt, sollten diese auch die erforderlichen Formatvorlagen enthalten. Anderenfalls sind die standardmäßig vorhandenen Überschriften-Formatvorlagen ÜBERSCHRIFT 1 BIS 9 zu verwenden. Werden diese zum Formatieren von Überschriften verwendet, werden sie automatisch mit dem gewählten Nummerierungsformat nummeriert. Damit ist es möglich, Überschriften nicht nur herausgehoben zu formatieren, sondern auch entsprechend der Gliederungsebene zu nummerieren. Außerdem kann bei Verwendung von Überschriften-Formatvorlagen ohne weitere manuelle Eingriffe das Inhaltsverzeichnis aus den so ausgezeichneten Überschriften generiert werden.

Der Zugriff auf die Formatvorlagen ist davon abhängig, ob speziell aufbereitete Dokumentvorlagen verwendet werden. Diese können zum Beispiel zusätzliche Symbolleisten für die Zugriff auf die Formatvorlagen beinhalten. Standardmäßig sind alle Formatvorlagen in der Symbolleiste FORMAT zu finden.

Abbildung 7.24: Vordefinierte Überschriften-Formatvorlagen erleichtern das Erstellen gegliederter Dokumente.

Es ist auch möglich, eigene Formatvorlagen als Überschriftenformatvorlagen zu erstellen. Erläuterungen hierzu können Sie Abschnitt 7.2.1.3 entnehmen. Im Sinne einer Dokumentenstandardisierung kann es aber nicht die Aufgabe des Dokumenterstellers sein, eigene Formatvorlagen zu erstellen.

7.2.2.3 Tabellen und Abbildungen richtig beschriften

In den meisten Fällen werden eingefügte Grafiken oder Tabellen eine Beschriftung erhalten, die auch einen Nummerierung einschließt. Besonders nützlich ist es, wenn ein Teil der Nummer auf das Kapitel verweist. Hinsichtlich der Nummerierung gilt das Gleiche wie bei Verweisen, beispielsweise auf Seitennummern. Sie dürfen niemals manuell erstellt werden, da jede Umstellung im Dokument eine manuelle Anpassung der Grafik- und Tabellennummern nach sich ziehen würde. Außerdem ist es bei manuell erstellten Grafik- und Tabellenbeschriftungen nicht möglich, automatisch ein Verzeichnis zu generieren.

Eine Grafik oder Tabelle beschriften

Um eine Grafik, Tabelle oder Formel zu beschriften, muss die Option BESCHRIFTUNG verwendet werden, die bei Word 2003 im Menü EINFÜGEN unter REFERENZ zu finden ist. Auf der Registerkarte BESCHRIFTUNG ist zunächst festzulegen, was (Abbildung, Tabelle oder Formel) beschriftet werden soll. Anschließend kann das Format der Beschriftung festgelegt werden.

Die genannten Schritte müssen für jede Grafik oder Tabelle wiederholt werden. Da dies recht aufwendig ist, enthalten angepasste Dokumentvorlagen meistens einen zusätzlichen Befehl auf einer Symbolleiste, hinter dem sich ein entsprechendes Makro verbirgt. Fehlt ein solcher, ist es am einfachsten, die Beschriftung einmalig zu erstellen und im Bedarfsfall die Beschriftungszeile zu kopieren und anzupassen.

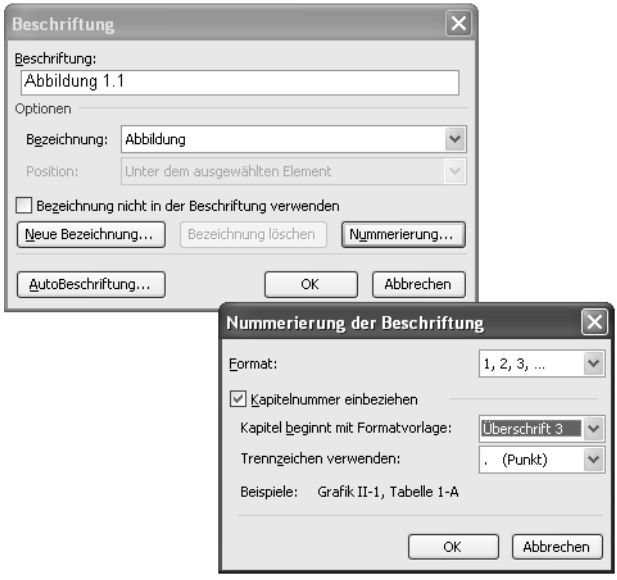


Abbildung 7.25: Abbildungen und Tabellen automatisch nummerieren mit der Beschriftungsfunktion

tipp

Die Beschriftungen dürfen aber nicht nur formal richtig sein, sondern sollten auch einen sinnvollen Text enthalten, der die dargestellte Abbildung bzw. Tabelle näher erläutert. Bei Abbildungen in Arbeitsanweisungen, die Screenshots darstellen, kann die Beschriftung beispielsweise den Pfad zur Dialogbox beschreiben. (Beachten Sie hierzu die Hinweise in Abschnitt 7.2.2.1).

Abbildungs- bzw. Tabellenverzeichnis erstellen

Aus den so erstellten Grafik- und Tabellenbeschriftungen kann sehr einfach ein Abbildungs- bzw. Tabellenverzeichnis erstellt werden. Bei Einsatz standardisierter Dokumentvorlagen sind diese Verzeichnisse wahrscheinlich bereits im Dokument erhalten und müssen nur noch aktualisiert werden. Anderenfalls können die Verzeichnisse, wie in Abschnitt 7.2.1.4 beschrieben, in das Dokument aufgenommen werden.

7.2.2.4 Einen Index erstellen

In einem Index sind die im Dokument behandelten Begriffe und Themen sowie die dazugehörigen Seitenzahlen aufgelistet. Die in den Index aufzunehmenden Begriffe sollten einzeln festgelegt und als Indexeintrag markiert werden. Zur Aufnahme von Begriffen in den Index ist wie folgt vorzugehen:

Begriffe in den Index aufnehmen

Benötigt wird die Option INDEX- UND VERZEICHNISSE, die sich bei Word 2003 im Menü EINFÜGEN unter REFERENZ befindet. Die Option EINTRAG FESTLEGEN öffnet eine weitere Dialogbox, die die Aufnahme des aktuell markierten Wortes in den Index ermöglicht. Für diesen fügt Word ein Feld für den Indexeintrag (XE) in das Dokument ein. Die Dialogbox bleibt geöffnet, sodass in einem Arbeitsgang mehrere Einträge festgelegt werden können.

Für die folgenden Elemente können Indexeinträge erstellt werden:

- Für einzelne Wörter, Wortgruppen oder Symbole
- Für Themen, die sich über mehrere Seiten erstrecken (unter Verwendung von Textmarken).
- Ein Bezug auf einen anderen Eintrag

Kommt ein Begriff mehrfach im Dokument vor, können mit Hilfe der Funktion ALLE FESTLEGEN in einem Arbeitsschritt alle Vorkommen in den Index aufgenommen werden.

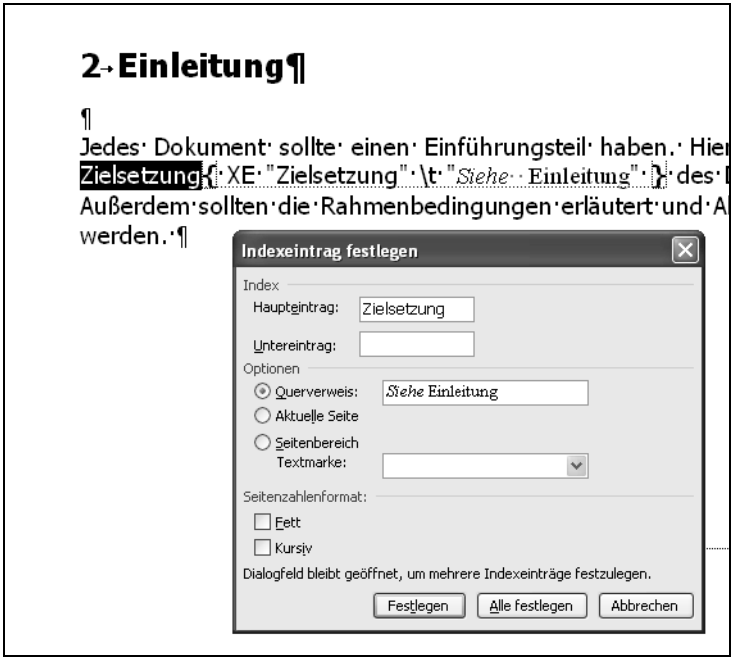


Abbildung 7.26: Ein Indexeintrag kann auf einen anderen Begriff verweisen.

Indexverzeichnis erstellen

Nachdem alle Indexeinträge festgelegt sind, kann das Indexverzeichnis erstellt werden. Beim Einsatz standardisierter Dokumentvorlagen ist das Indexverzeichnis wahrscheinlich bereits im Dokument enthalten und muss nur noch aktualisiert werden. Anderenfalls kann das Indexverzeichnis, wie in Abschnitt 7.2.2.4 beschrieben, in das Dokument aufgenommen werden.

Während der Erstellung sammelt Word alle festgelegten Indexeinträge, ordnet sie alphabetisch, verweist auf ihre jeweiligen Seitenzahlen und sucht und entfernt mehrfache Einträge auf derselben Seite. Sonderzeichen (wie z. B. @) werden dabei am Anfang des Index eingefügt. Wurde ein Format für das Indexverzeichnis gewählt, das Überschriften für alphabetisch sortierte Gruppen enthält, werden die Sonderzeichen unter der Überschrift # eingeordnet (# steht für das Nummernzeichen).

7.2.2.5 Daten aus anderen Anwendungen einfügen

Word spielt bei der Erstellung von Dokumenten die zentrale Rolle. Es gibt aber einige Elemente, die sich besser in anderen Anwendungen erstellen lassen. Für die Erstellung komplexer Tabellen beispielsweise ist Excel weitaus besser geeignet. Und Prozess- und Arbeitsablaufdiagramme werden mit Visio oder einem speziellen Programm zur Modellierung von Prozessen erstellt.

Das Hauptdokument ist in den meisten Fällen jedoch ein Word-Dokument, in das Inhalte aus anderen Anwendungen eingefügt werden müssen. Für das Einfügen von Daten aus anderen Anwendungen gibt es mehrere Möglichkeiten. Diese sollen hier zunächst kurz vorgestellt werden, bevor gezeigt wird, welche Methode für welchen Einsatzzweck geeignet ist.

Daten kopieren Die einfachste und am häufigsten angewendete Methode besteht darin, Daten aus anderen Anwendungen mit den Optionen KOPIEREN und EINFÜGEN (standardmäßiges Kopieren mit Strg + C und anschließendes Einfügen mit Strg + V) nach Word zu übernehmen. Dabei werden die Daten vollständig in Word integriert. Ändert sich etwas an den Daten in der Quelldatei, bekommt das Word-Dokument davon nichts mit. Änderungen im Quelldokument können nur durch erneutes Kopieren übernommen werden. Es muss also organisatorisch sichergestellt werden, dass die Inhalte in den Dokumenten aktuell gehalten werden

Wichtige Option: Inhalte einfügen

Daten als Objekte einbetten Häufig unbekannt sind die Möglichkeiten der Option INHALTE EINFÜGEN, die im Menü BEARBEITEN zu finden ist. Hierüber ist es möglich, Inhalte aus anderen Anwendungen als Objekte einzubetten.

Wurden zuvor Inhalte in der Quelldatei in die Zwischenablage kopiert, erkennt Word die Ursprungsanwendung (im nachstehend gezeigten Beispiel ist dies Excel) und erlaubt, die Inhalte als Excel-Arbeitsblatt-Objekt einzufügen. Wird dabei die Standardeinstellung EINFÜGEN beibehalten, werden die Daten als Objekt in Word eingebettet. Eingebettete Objekte werden nach dem Einfügen zum Bestandteil der Zieldatei. Daher werden die Informationen in der Zieldatei bei einer Änderung der Daten in der Quelldatei nicht aktualisiert.

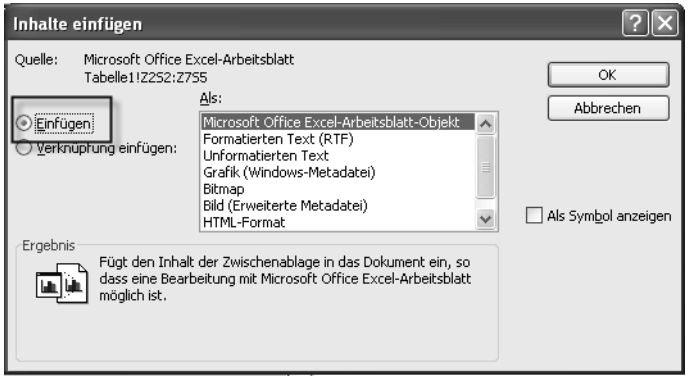


Abbildung 7.27: Daten aus Excel als Objekt einbetten

Eingebettete Objekte bearbeiten

Im Gegensatz zu „normal" eingefügten Daten, kann ein eingebettetes Objekt aus dem Zielprogramm heraus in der Ursprungsanwendung geändert werden. Ein Doppelklick auf das Objekt öffnet dieses im Quellprogramm.

Abbildung 7.28: Ein eingebettetes Objekt kann in Excel bearbeitet werden.

Daten als Objekt verknüpfen Es gibt noch eine dritte Möglichkeit, um Daten aus einer anderen Anwendung in Word zu übernehmen: Als Objekt verknüpfen. Auch hierfür ist die Option INHALTE EINFÜGEN im Menü BEARBEITEN zu wählen. Zusätzlich muss anstelle der Standardeinstellung EINFÜGEN die Option VERKNÜPFUNG EINFÜGEN gewählt werden.

Verknüpfte Objekte bearbeiten

Wird ein Objekt verknüpft, so werden die Informationen im Word-Dokument in der Standardeinstellung automatisch jedes Mal aktualisiert, wenn das Dokument geöffnet wird oder wenn die Quelldatei bei geöffnetem Word-Dokument geändert wird. Grund dafür ist, dass die verknüpften Daten in der Quelldatei gespeichert werden. Die Zieldatei speichert nur den Speicherort der Quelldatei und zeigt eine Darstellung der verknüpften Daten an. Demzufolge werden Daten verknüpfter Objekte zwangsläufig immer in der Quelldatei bearbeitet.

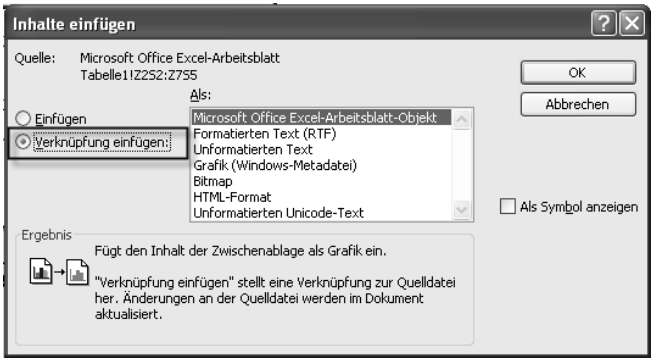


Abbildung 7.29: Daten aus Excel als Objekte einfügen

hinweis

Beim Verknüpfen eines Excel-Objekts können wahlweise die Text- und Zahlenformatierungen von Excel oder die von Word bereitgestellten Formate verwendet werden. Werden die Word-Formate benutzt, so wird die in Word durchgeführte Formatierung beibehalten, sobald die Daten aktualisiert werden.

Um alle Verknüpfungen im Dokument anzuzeigen und deren Einstellungen zu bearbeiten, ist im Menü BEARBEITEN die Option EINFÜGEN zu verwenden. In der Dialogbox VERKNÜPFUNGEN werden alle verknüpften Objekte aufgelistet. Da auch Querverweise als Verknüpfungen realisiert sind, listet Word diese ebenfalls auf.

In der nachstehend gezeigten Dialogbox können die Einstellungen für die verknüpften Objekte bearbeitet werden. Um beispielsweise eine Aktualisierung zu verhindern, können einzelne verknüpfte Objekte von einer Aktualisierung ausgeschlossen werden. In diesem Fall erwendet Word die zuletzt verfügbaren Informationen der Quelldatei.

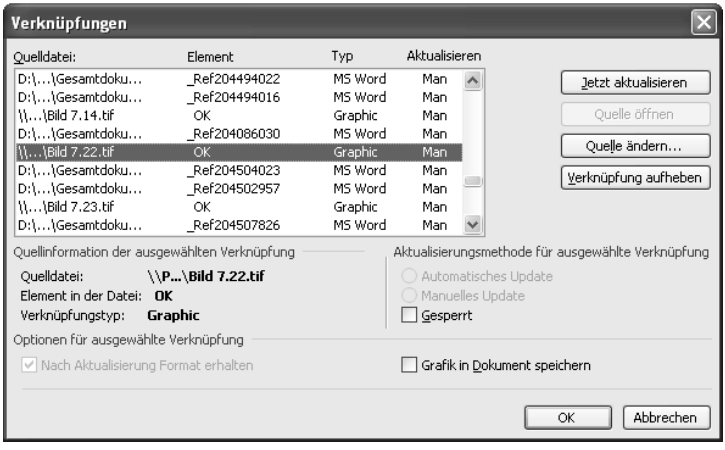


Abbildung 7.30: Dialogbox zum Bearbeiten von Verknüpfungen

Sinnvoller Einsatz der Methoden Selbstverständlich bietet auf den ersten Blick das Verknüpfen von Objekten die meisten Vorteile: Die Informationen sind immer aktuell, die Daten werden nicht redundant gespeichert und die Dateigröße der Word-Datei bleibt überschaubar.

Zugriff muss gewährleistet sein

Einschränkend zu beachten ist aber, dass Verknüpfungen nur funktionieren, wenn die Zugriffe auf die verknüpften Dateien gewährleistet sind. Und das ist durchaus nicht immer der der Fall. Wurden beispielsweise von dem Dokumentersteller alle Abbildungen als Objekte eingefügt, und hat er diese auf einem Netzlaufwerk gespeichert, auf das andere Benutzer keinen Zugriff haben, sehen diese nur leere Kästen anstelle der Abbildungen. Um also Fehlermeldungen und frustrierte Anwender zu vermeiden, die keinen Zugriff auf das verknüpfte Objekt haben, muss genau geprüft werden, ob und für welche Dokumente derartige Verknüpfungen eingesetzt werden können.

hinweis

Auch bei Verweisen auf andere Dokumente muss darauf geachtet werden, dass derjenige, der mit dem Dokument arbeitet, Zugriff auf verwiesene Dokumente hat. Selbstverständlich ist es komfortabel, wenn mit einem Mausklick auf einen Hyperlink das Dokument, auf das verwiesen wird, geöffnet werden kann. Wird ein Dokument beispielsweise im Intranet veröffentlicht, darf nicht vergessen werden, auch alle verwiesenen Dokumente ebenfalls dort zu veröffentlichen.

Ein Alternative kann das Einbetten von Objekten bieten. Da die gesamte Information in dem Word-Dokument enthalten ist, eignet sich das Einbetten besonders, wenn das Dokument Personen zur Verfügung gestellt werden soll, die keinen Zugang zu den unabhängig verwalteten Quelldateien der Daten haben. In diesem Fall können sie mit einem Doppelklick das Objekt öffnen und in der Quellanwendung bearbeiten.

Nachteile der Objekteinbettung

Nachteilig hierbei ist, dass alle Änderungen an einem eingebetteten Objekt nicht in die Quelldatei übernommen werden. Bei dieser Methode „wissen" das Quelldokument und das Word-Dokument nichts voneinander. Hier muss organisatorisch geregelt werden, an welchem Dokument Änderungen erfolgen dürfen. Außerdem muss der Bearbeiter des eingebetteten Objekts Zugriff auf das Quellprogramm haben, falls er eingebettete Objekte bearbeiten will. Die Frage, wie mit Daten, die in anderen Anwendungen erstellt wurden, umgegangen werden soll, lässt sich nicht generell beantworten und muss im Einzelfall entschieden werden.

tipp

Manchmal weisen eingefügte Grafiken ein recht merkwürdiges „Sprungverhalten" auf. Da kann es passieren, dass man eine eingefügte Grafik nach einem Verschiebevorgang zwischen zwei Seiten wiederfindet. Dieses Verhalten kann eintreten, wenn Grafiken nicht mit einem Absatz verknüpft sind, sondern als unverankertes Bild eingefügt wurden. Hier hilft die Verankerung der Grafik im Absatz, was mit der Option MIT TEXT IN ZEILE möglich ist. Diese Option ist in der Dialogbox LAYOUT (Option GRAFIK FORMATIEREN im Kontextmenü der Grafik) zu finden.

Sinnvollerweise sollte diese Option als Standard für alle Dokumente festgelegt werden. Möglich ist dies in den allgemeinen Optionen. Hier kann auf der Registerkarte BEARBEITEN unter BILD EINFÜGEN ALS festgelegt werden, in welchen Modus Bilder standardmäßig in Word eingefügt werden sollen.

7.2.2.6 Einfügen ist nicht gleich Einfügen

Wie die zuvor vorgestellte Option INHALTE EINFÜGEN gezeigt hat, gibt es beim Einfügen durchaus einige Punkte zu beachten. Das gilt auch für die Übernahme von Textpassagen aus anderen Dokumenten oder aus Webseiten. Beim standardmäßigen Kopieren mit Strg + C und anschließenden Einfügen mit Strg + V werden nicht nur alle Formierungen des Quelltextes, sondern auch ausgeblendete Steuerzeichen (beispielsweise Indexeinträge) und Links mit übernommen, was durchaus nicht immer gewünscht ist und lästige Nacharbeiten nach sich zieht. Wird ein Text hingegen mit der Option INHALTE EINFÜGEN als unformatierter Text eingefügt, übernimmt er beim Einfügen die Formatierung des aktuell gewählten Absatzes.

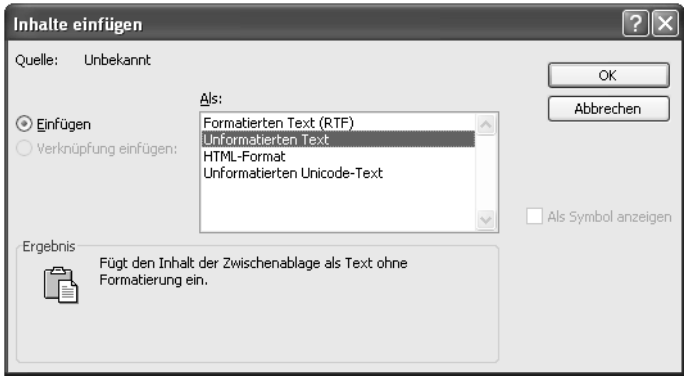


Abbildung 7.31: Text unformatiert einfügen

In den meisten Fällen ist es besser, Texte unformatiert einzufügen. Es macht daher Sinn, für diese Funktion zur schnelleren Verfügbarkeit ein Makro zu erstellen und dieses als Symbol in der Symbolleiste abzulegen oder ihm eine Tastenkombination zuzuweisen.

tipp

Das Einfügen von unformatierten Text kann nicht als Makro aufgezeichnet werden, sondern muss als VBA-Makro erstellt werden. Dieses muss lediglich die folgende Zeile enthalten:

```
Selection.PasteSpecial DataType:=wdPasteText
```

7.2.2.7 Textauszeichnungen sparsam einsetzen

Word bietet zwar zahlreiche Formatierungsmöglichkeiten an, doch sollten vor allem Textauszeichnungen sparsam eingesetzt werden. Eine Verwendung aller Möglichkeiten zwischen fett und farbig, verschiedenen Listenpunkten und Umrandungen macht einen Text nicht nur unruhig, sondern vermittelt auch schnell den Eindruck von Beliebigkeit. Dies gilt insbesondere für Doppelauszeichnungen, wie beispielsweise fett und unterstrichen. Textauszeichnungen sollten gezielt eingesetzt werden, damit sie ihren Zweck erfüllen. In diesem Fall ist wieder einmal weniger mehr.

7.3 Die Erstellung von Dokumenten optimieren

Nachdem zuvor die Erstellung von Dokumenten eher aus technischer Sicht betrachtet wurde, stehen im nachfolgenden Abschnitt die organisatorischen Abläufe bei der Erstellung eines neuen Dokuments im Vordergrund. Der Abschnitt bietet Hilfen und Anregungen zur Optimierung der Vorgehensweise beim Erstellen von Dokumenten.

Die nachfolgenden Ausführungen gelten im Prinzip für alle Dokumentenklassen, vorrangig allerdings für planungsintensive Dokumente wie Konzepte oder Prozessbeschreibungen. Beim Erstellen von Arbeitshilfen werden hingegen sicherlich nur einzelne Teilschritte zu berücksichtigen sein.

7.3.1 Planung und Vorbereitung der Erstellung

Die Erstellung eines Dokuments sollte immer mit einer Planungs- und Vorbereitungsphase beginnen. Bevor mit dem Schreiben begonnen wird, sollten die nachfolgenden Fragen beantwortet sein:

- Welchen Zweck soll das Dokument erfüllen?
- Wer ist die Zielgruppe?
- Welche Informationen liegen bereits vor?
- Wie ordnet sich das zu erstellende Dokument in die unternehmensweite IT-Dokumentation ein?
- Gibt es im Unternehmen Standards für die Dokumentation?
- Existieren Dokumentvorlagen?
- Gibt es definierte Dokumentationsprozesse und sind diese bekannt?

- Gibt es bereits Vorgängerdokumente oder mitgeltende Dokumente, die zu beachten sind?
- Gibt es inhaltliche Vorgaben?

Die Beantwortung der Fragen hilft, typische Fehler zu vermeiden. Erst nachdem alle Rahmenbedingungen geklärt sind, sollte mit dem Erstellen eines Dokuments begonnen werden.

7.3.1.1 Recherche und Aufbereitung von Informationen

Jedes Dokument hat eine Vorgeschichte. Sei es, dass beispielsweise im Rahmen eines Projekts ein Konzept zu erstellen oder ein Prozess zu dokumentieren ist. Im ersten Fall erzeugt bereits die Projektplanungsphase diverse Unterlagen. Im zweiten Fall wurden möglicherweise Interviews mit Mitarbeitern geführt, um die Prozessabläufe zu erfassen. Ist hingegen beispielsweise eine Installationsanleitung zu erstellen, stellt die vorhandene Dokumentation des Herstellers eine wichtige Informationsbasis dar. Wie die Beispiele zeigen, gibt es in aller Regel vorhandene Informationen, die erfasst und ausgewertet werden müssen. Sie bilden die Basis für neue zu erstellende Dokumente.

Die Erstellung eines Dokuments muss daher immer mit der Sichtung und der Dokumentation der vorhandenen Unterlagen, also mit der Erstellung der Stoffsammlung (auch als *Arbeitsdokumentation* bezeichnet) beginnen. Diese bildet nicht nur eine Informationsbasis, sondern dient auch als späterer Verwendungsnachweis, um Aussagen im Dokument zu belegen. In das Dokument werden diese Unterlagen in aller Regel nicht aufgenommen. Im Einzelfall kann es sinnvoll sein, dem Dokument einen Verweis auf bereits bestehende Unterlagen hinzuzufügen.

Arbeitsdokumentation einrichten

Zur Sammlung und Aufbereitung vorhandener Unterlagen und Dokumente sollte ein physischer Ordner angelegt werden, in dem alle vorhandenen Unterlagen eingeheftet werden können. Zusätzlich sollte ein schneller Zugriff auf die gespeicherten Informationen möglich sein. Dazu kann beispielsweise im Dateisystem ein gesonderter Ordner eingerichtet werden, in dem alle wichtigen Dateien gespeichert werden. Dies hat aber den Nachteil, dass Dateien redundant gespeichert werden. Außerdem liegen nicht alle Informationen in Form von Dateien vor. Auch Internetseiten und E-Mails können zu einer Arbeitsdokumentation zählen, was deren Verwaltung zusätzlich erschwert.

Infosammlung im Mind Map

Gute Dienste kann hier der Einsatz einer Mind Map bieten, die aufgrund der visuellen Darstellung einen schnellen Überblick über die vorhandenen Informationen bietet. Eine Mind Map kann mit wachsenden Kenntnisstand problemlos erweitert werden.

Bei Einsatz eines Mind Map-Tools, wie beispielsweise dem MindManager von Mindjet, können außerdem Verlinkungen auf Ordner und Dateien im Dateisystem, auf Internetseiten oder auf Outlook-Elemente hinterlegt werden. Damit ist es jederzeit leicht möglich, auf Dateien oder E-Mails zuzugreifen, ohne die Informationen zusätzlich abspeichern zu müssen. Auch Microsoft Visio stellt Funktionen zur Erstellung von Mind Maps bereit.

Was ist eine Mind Map

Eine Mind Map ist eine visuelle Darstellung von Informationen und Gedanken. Die Grundidee bzw. das Thema befindet sich als Titel in der Mitte der Map und ist Ausgang der zugehörigen Unterpunkte, die in strahlenförmiger, hierarchischer Anordnung abzweigen. Jeder Unterpunkt befindet sich auf einem Zweig. Die Hauptzweige einer Map beginnen auf der 1-Uhr-Position und werden im Uhrzeigersinn gelesen.

Die nachstehende Abbildung zeigt die möglichen Hauptzweige in einer Mind Map für die Verwaltung der Informationsquellen.

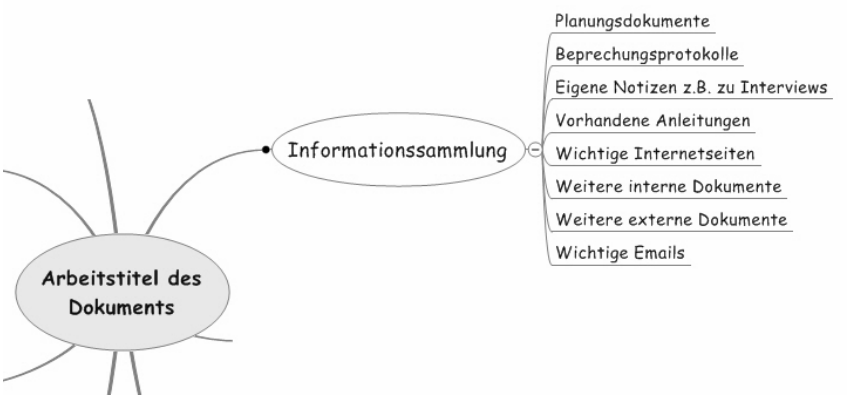


Abbildung 7.32: Die Erstellung beginnt mit der Informationssammlung.

hinweis

Mind Maps sind nicht nur ein gutes Werkzeug für die Informationssammlung, sondern können den gesamten Erstellungsprozess eines Dokuments wirkungsvoll unterstützen.

In Abschnitt 7.3.3 werden das Programm MindManager vorgestellt und seine Möglichkeiten für eine effektive Unterstützung der Dokumentenerstellung und der Dokumentenverwaltung erläutert.

Auf der beigefügten CD-ROM finden Sie eine mit MindManager erstellte Datei, die die in diesem Kapitel vorgestellte Erstellung eines Dokuments grafisch darstellt und eine Betrachtung der im Folgenden vorgestellten Einzelbereiche in einer Zusammenschau ermöglicht. Mit dem ebenfalls beigefügten MindManager Viewer kann diese Datei angesehen werden. Außerdem ist es möglich, Zweige zu öffnen, zu schließen und in sie hineinzuzoomen.

7.3.1.2 Vorgaben und Dokumentenumfeld klären

Bevor mit der Erstellung des Dokuments begonnen wird, muss Klarheit darüber bestehen, in welches Informations- und Dokumentationsnetz das zu erstellende Dokument eingebunden ist: Für wen wird es Informationsbasis sein?

Wer ist die Zielgruppe? Einer der häufigsten Fehler – nicht nur bei der Erstellung von Dokumenten im IT-Bereich – ist die Missachtung der Zielgruppe und des Zwecks, für den ein Dokument erstellt wird.

Dabei muss vor allem der Abstraktionsgrad des Dokuments an der Zielgruppe ausgerichtet werden. So interessiert sich die Unternehmensleitung selten für Schritt-für-Schritt-Anleitungen, während andererseits dem Anwender die beeindruckenden Speicherkapazitäten des neuen Speichersystems oder abstrakte Prozessdarstellungen bei seiner Arbeit wenig weiterhelfen. Nur wenn vorher die *Zielgruppe* und der *Zweck* des Dokuments genau identifiziert wird, kann das Dokument zielgruppenspezifisch erstellt werden und damit seinen Zweck erfüllen.

Auch im Hinblick auf die Fachsprache muss die Zielgruppe berücksichtigt werden. Zwar sollte nach Möglichkeit eine für Auftraggeber und Entwickler gleichermaßen verständliche Sprache verwendet werden, doch ist dies nicht immer umsetzbar. So wird es nur sehr schwer möglich sein, ein Pflichtenheft für Entwickler so abzufassen, dass dieses auch der Geschäftsleitung als Entscheidungsgrundlage dienen kann.

Einordnung in die IT-Dokumentation Im Vorfeld ist weiter zu klären, wie das zu erstellende Dokument in die bestehende IT-Dokumentation eingebunden ist. So sollten bereits in diesem Stadium alle ergänzenden und mitgeltenden Dokumente ermittelt werden. Insbesondere große Unternehmen verfügen zwangsläufig über eine umfangreiche IT-Dokumentation. Es ist wichtig zu klären, wie sich das zu erstellende Dokument in diese einfügen soll. Werden beispielsweise automatisiert mit einem Inventarisierungstool Systemakten für alle Rechner erstellt, ist es unnötig, im zu erstellenden Handbuch die IP-Konfiguration des Servers auszuführen. Dies schafft Redundanzen, die die Pflege der Dokumente später immens erhöhen. Es ist daher wichtig, sich im Vorfeld Kenntnis über alle Dokumente zu verschaffen, die Schnittstellen zum zu erstellenden Dokument haben und auf diese bei Bedarf zu verweisen.

Mitgeltende Dokumente ermitteln

Bei den mitgeltenden Dokumenten handelt es sich um eigenständige Dokumente, die Regelungen enthalten, die für das Dokument Gültigkeit besitzen, aber im Dokument nicht zwingend explizit genannt werden. Viele der Rahmendokumente gehören dazu. Beispielsweise kann in einer Arbeitsanweisung zur Einrichtung einer Verzeichnisfreigabe darauf verwiesen werden, dass für die Benennung der Freigabe die in der Namenskonvention benannten Regeln einzuhalten sind. In der Praxis bedeutet dies, dass der Ausführende Zugriff auf das mitgeltende Dokument haben und es bei seiner Tätigkeit bei Bedarf heranziehen muss. Weitere mitgeltende Dokumente können sein: Verträge, alle Richtliniendokumente, Service Level Agreements.

Mögliche Vorgängerversionen ermitteln

Weiterhin ist zu klären, ob Vorgängerdokumente oder Vorgängerversionen existieren. Diese zu kennen ist nicht nur in Bezug auf die inhaltliche Darstellung wichtig, sondern kann auch Zeit und Arbeit sparen. Gerade in großen Unternehmen werden häufig im Rahmen von Projekten Dokumente erstellt, die später aber nicht in die Betriebsdokumentation aufgenommen werden.

Inhaltliche Vorgaben und Richtlinien Dokumente entstehen nicht auf der grünen Wiese. Sie müssen daher Vorgaben und Richtlinien berücksichtigen. Hierbei kann es sich sowohl um externe als auch um interne Vorgaben handeln.

Soll in dem zu erstellenden Dokument beispielsweise die Archivierung von E-Mails konzipiert werden, müssen zwingend die gesetzlichen Datenschutzbestimmungen berücksichtigt werden. Auch aus Standards und Zertifizierungsanforderungen leiten sich inhaltliche Auflagen ab. Die zu berücksichtigenden Standards und Vorgaben zu ermitteln, ist eine der wichtigsten Aufgaben im Vorfeld.

Formale Standards und Vorgaben In vielen Unternehmen gibt es in irgendeiner Form Standards für die Dokumentenerstellung. Diese können beispielsweise den formalen Aufbau der Dokumente definieren oder Regeln für die Versionierung umfassen. Derartige formale Vorgaben und Vorschriften sind natürlich zu berücksichtigen. In vielen Fällen stehen auch Vorlagen zur Verfügung. Ist nicht klar, ob derartige Standards existieren, muss dies unbedingt vor Beginn der Dokumentation erfragt werden. Falls entsprechende Vorgaben fehlen, ist das zu erstellende Dokument ein guter Anlass, Standards für die IT-Dokumentation festzulegen.

Abhängigkeiten in einer Mind Map darstellen

Die aufgeführten Abhängigkeiten lassen sich ebenfalls gut in einer Mind Map darstellen. So können hier beispielsweise alle mitgeltenden Dokumente erfasst und später im Dokument in die Tabelle der mitgeltenden Dokumente übernommen werden. Die nachstehende Abbildung zeigt die möglichen Hauptzweige für die Verwaltung des Dokumentationsumfeldes in einer Mind Map.

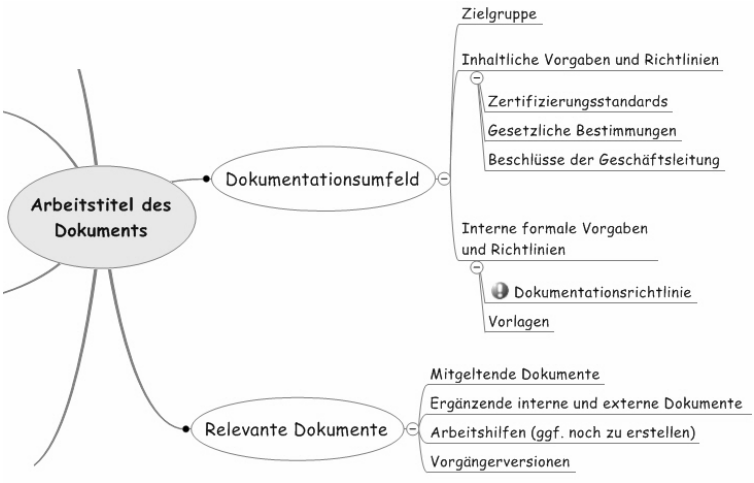


Abbildung 7.33: Das Sondieren des Dokumentenumfeldes gehört zu den wichtigsten Vorbereitungen

7.3.2 Erstellung des Dokuments

Nach dem Abschluss der Vorbereitungsarbeiten kann mit dem neuen Dokument begonnen werden.

7.3.2.1 Gliederung festlegen

Die Gliederung folgt in der Regel bestimmten Vorgaben. Gegebenenfalls gibt es auch eine Vorlage für die Dokumentenklasse, zu der das zu erstellende Dokument gehört. Ist dies nicht der Fall, müssen Hauptkapitel und Gliederungstiefe selbst festgelegt werden.

Gliederung in einer Mind Map abbilden

Auch beim Festlegen der Gliederung und beim Erstellen des Dokuments kann eine Mind Map gute Dienste leisten. Die Visualisierung der Gliederung ist eine gute Methode, um Fehler oder Brüche in der Strukturierung des Dokuments zu erkennen. Die Struktur sollte für jeden Leser nachvollziehbar sein. Kann sich der Leser an der Dokumentenstruktur wie an einem roten Faden entlang hangeln, werden sich ihm die Inhalte viel leichter erschließen. Deshalb sollten bei der Erstellung der Gliederung die folgenden Punkte beachtet werden:

- Inhalte, die gleichermaßen wichtig sind, haben die gleiche Gliederungsstufe.
- Die Gewichtung der Kapitel muss in sich stimmig sein. Stehen Kapitel auf der gleichen Ebene, von denen das eine Kapitel 20 Seiten Umfang hat und ein anderes Kapitel nur zwei Seiten lang ist, stimmt in der Regel etwas nicht.
- Eine Untergliederung eines Kapitels ist nur erforderlich, wenn es mindestens zwei Unterpunkte gibt.
- Es sollten so wenig Gliederungsstufen wie möglich verwendet werden. Mehr als fünf Gliederungsstufen sind selten sinnvoll und verringern eher die Übersichtlichkeit.

7.3.2.2 Inhaltliche Dokumentenerstellung

Aber auch bei der laufenden Erstellung des Dokuments kann eine Mind Map wertvolle Hilfe leisten. So können Erkenntnisse, die während der Erstellung des Dokuments gewonnen werden, und eintreffende Informationen jederzeit zugeordnet werden. Findet beispielsweise zu einem Thema des Dokuments eine Sitzung statt, kann das dazu erstellte Ergebnisprotokoll als Verknüpfung dem entsprechenden Zweig eingefügt werden. Auch wichtige E-Mails können jederzeit als Verknüpfung eingebunden werden. Damit kann eine Mind Map den gesamten Entstehungsweg des Dokuments begleiten und nach der Abnahme als Nachweisdokument archiviert werden.

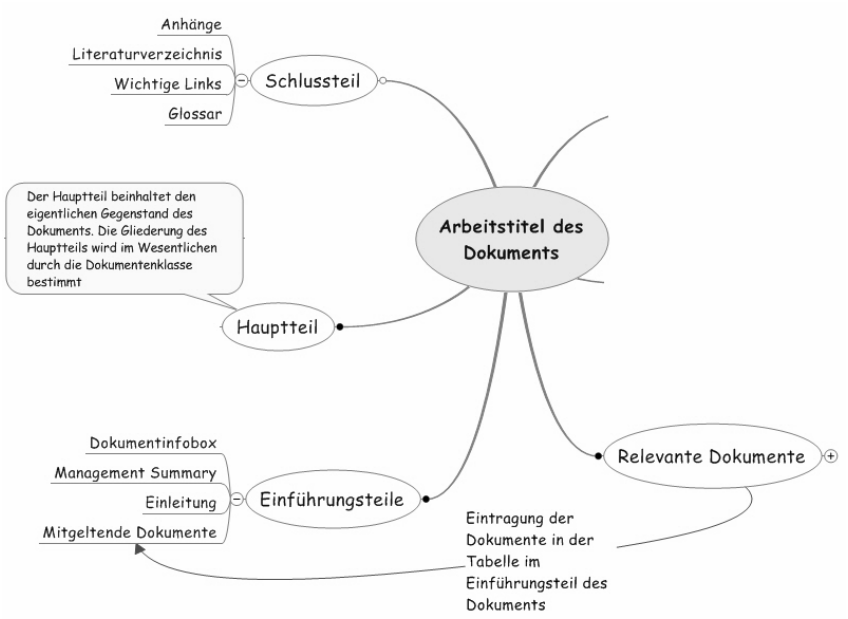


Abbildung 7.34: Die Gliederung des Dokuments kann in einer Mind Map entwickelt werden.

tipp

Nicht nur einmal haben die Autoren des Buches Dokumente im Entwurf zum Review erhalten, bei denen die Strukturierung noch nicht stimmte, die viele Rechtschreibfehler und unfertige Sätze enthielten, und bei denen die Formatierungen noch fehlten. Die Antwort der Verfasser solcher Dokumente war dann in der Regel: „Das ist ja nur der erste Entwurf."

Diese Haltung ist problematisch. Nicht nur, dass ein solches Dokument für denjenigen, der das Dokument lesen muss, eine Zumutung ist. Viel problematischer ist, dass der erste, negative Eindruck dieses Dokuments später nur schwer wieder revidierbar ist. Erfahrungsgemäß werden spätere Versionen eines solchen Dokuments viel kritischer betrachtet als Dokumente, die im ersten Entwurf einen professionellen Eindruck gemacht haben.

Deshalb gilt: Auch der erste Entwurf muss mit der gleichen Sorgfalt erstellt werden wie die endgültige Version – außer es ist ausdrücklich abweichend vereinbart worden. Schließlich gibt man mit jedem erstellten Dokument eine Visitenkarte ab.

Aufgaben in einer Mind Map visualisieren

In den meisten Fällen unterliegt die Erstellung eines Dokuments einem festen Zeitplan. Zumindest aber gibt es einen geplanten Abgabetermin. Werden Dokumente im Rahmen von Projekten erstellt, gibt es zumindest einen definierten Reviewprozess mit festgelegten Terminen.

Es kann daher sinnvoll sein, auch Aufgaben und Termine in einer Mind Map darzustellen. Die folgende Abbildung zeigt ein Beispiel.

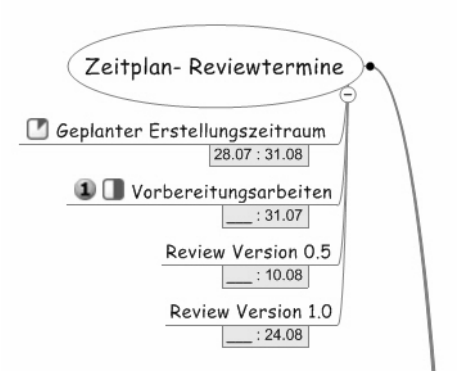


Abbildung 7.35: Nicht die Verwaltung, sondern die Visualisierung der Termine steht hier im Vordergrund.

7.3.3 Dokumentationsunterstützung mit MindManager

Die mit einem Mind Map-Tool erstellten Mind Maps können in vielen Bereichen der Dokumentation gute Dienste leisten. Nicht nur für eine strukturierte Informationssammlung bei der Dokumentenerstellung, sondern auch für eine visuelle Darstellung komplexer Inhalte bieten sie eine Reihe von Möglichkeiten.

Business Mapping gewinnt an Bedeutung

Dabei haben computergestützte Mind Maps (auch als *Business Maps* bezeichnet) nur noch wenig mit der klassischen Papier-und-Bleistift-Methode gemein. Die Mind Map-Tools erweitern die klassischen Mind Maps häufig um zusätzliche Funktionen, mit denen Verweise auf Dateien, Internetseiten oder andere Objekte hergestellt werden können. Sie bieten darüber hinaus Verwaltungsfunktionen wie beispielsweise Anzeigefilter. Außerdem erlauben sie oftmals die Zusammenarbeit mit den Office-Programmen. Es kann daher nicht verwundern, dass Business Maps nicht nur im hier betrachteten Segment des Wissensmanagement zunehmend an Bedeutung gewinnen.

Es gibt eine Reihe von Tools – von Freeware bis zu Geschäftsanwendungen –, die auf dem Mind-Map-Prinzip basieren. Neben klassischen Mind-Map-Werkzeugen für Einzelbenutzer existieren auch Lösungen, bei denen die Teilnehmer parallel an derselben Mind Map (auch in Echtzeit über das Web) arbeiten können.

MindManager von Mindjet

Die Autoren dieses Buches haben sich für den Einsatz des Tools MindManager Pro der Firma Mindjet entschieden, das sich durch eine besonders hohe Integration in die Office-Tools auszeichnet. So können beispielsweise Microsoft Outlook-Objekte (Kontakte, E-Mails, Aufgaben) eingefügt und regelmäßig synchronisiert werden.

MindManager Pro ermöglicht das Erstellen und Editieren von Mind Maps – verbunden mit vielen Funktionen zur Visualisierung (zahlreiche Text- und Zweigformatierungen, Icons, Beschriftungen oder Grafiken). Außerdem ist es möglich, Hyperlinks sowie Textnotizen zu Zweigen hinzuzufügen. Interessant ist auch die Multi-Map-Funktion, bei der Mind Maps mit anderen Mind Maps über Hyperlinks verknüpft und gemeinsam dargestellt werden können. Hilfreich sind auch die zahlreichen Filterfunktionen.

Im Hinblick auf die IT-Dokumentation ist wichtig, dass mit MindManager Pro erzeugte Mind Maps in eine Reihe von Formaten exportiert werden können: HTML, PDF, Bilddatei und als OLE-Objekt in alle gängigen Anwendungsprogramme. Fertige Projektpläne können nach Microsoft Project exportiert werden und dort als Vorlage für Projektmanagement-Aufgaben dienen.

Die folgenden Kapitel stellen die wichtigsten Funktionen von Mindjet MindManager Pro an einem Beispiel vor.

hinweis

Nähere Informationen zu Systemanforderungen, Bezugsmöglichkeiten und Preisen der aktuellen Version finden Sie im Steckbrief zu MindManager in Anhang D.5.

7.3.3.1 Einsatzmöglichkeiten und Arbeitsweise von MindManager

Nach dem Start von Mindjet MindManager Pro erscheint der nachstehend gezeigte Startbildschirm. Auf der rechten Seite erscheinen je nach Art der gewählten Funktion Befehle und Ressourcen, die das Erstellen von Mind Maps erleichtern. Für die Anzeige und Anordnung von Informationen in einer Map stehen verschiedene Elemente zur Verfügung, die überwiegend einfach per Drag & Drop in die Map hineingezogen werden können.

Eine neue Mind Map erstellen

Mit dem Befehl NEU kann eine neue Mind Map erstellt werden. Diese kann auf einer bereits erstellten eigenen Vorlage oder der Standardvorlage basieren. Jede Erstellung einer Mind Map beginnt mit der Benennung des Themas. Das Hautthema wird automatisch eingefügt und muss nur noch durch das Thema oder den Titel ersetzt werden (Abbildung 7.36).

Zweige und Anmerkungen einfügen

Im Beispiel wird eine neue Mind Map erstellt, die die Erstellung und Informationssammlung eines Abschnitts des Notfallhandbuches unterstützt. Vom Hauptthema ausgehend, können anschließend die benötigten Zweige und Unterzweige mit Hilfe der Tastatur oder der Taste in der Multifunktionsleiste hinzugefügt werden. Mit der Maus können die Zweige zu jedem Zeitpunkt per Drag & Drop umgruppiert werden. Eine rote Markierung zeigt an, wo der Zweig hinzugefügt wird.

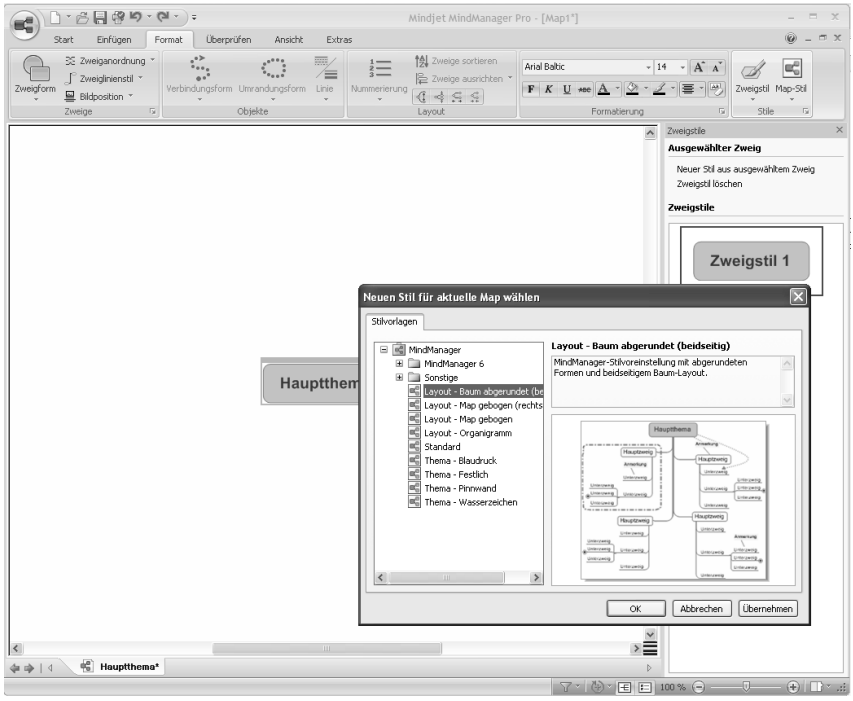


Abbildung 7.36: Eine neue Mind Map in Mind Manager Pro erstellen

Durch das Erweitern (Pluszeichen) oder Reduzieren (Minuszeichen) von Zweigen kann die Mind Map übersichtlich gehalten werden. Die Map wird so ausgedruckt, wie sie angezeigt wird – reduzierte Zweige werden vor dem Drucken nicht erweitert.

Allen Zweigen können weitere Elemente (Notizen, Bilder, Beschriftungen usw.) hinzugefügt werden. Weiterhin ist es möglich, freie Anmerkungen, die nicht mit einem bestimmten Zweig der Map verbunden sind, einzufügen und frei zu positionieren. Wie andere Zweige auch können freie Anmerkungen mit Unterzweigen ergänzt und jederzeit auf einen Zweig gezogen werden, um sie zu verankern.

Zweignotizen

Zusätzlich ist es möglich, einem Zweig oder einem anderen Element eine Notiz beizufügen. Darin kann beispielsweise auf die ursächliche Mail verwiesen werden. Zweignotizen können formatiert werden; sie dürfen Hyperlinks, Tabellen und Grafiken enthalten.

Map-Markierungen verwenden

In der nachstehenden Grafik (Abbildung 7.37) wurden sogenannte Map-Markierungen verwendet. Diese dienen dazu, Zweigen eine bestimmte Bedeutung zuzuweisen oder sie in Gruppen zu ordnen. Eine Markierung kann ein Icon, eine Textmarkierung oder eine Aufgabeninformation sein. Jede Markierung hat einen zugehörigen Namen oder eine Bedeutung. Zu finden sind die Map-Markierungen im Aufgabenbereich nach Gruppen geordnet, wobei die Bedeutung jeder Markierung angezeigt wird.

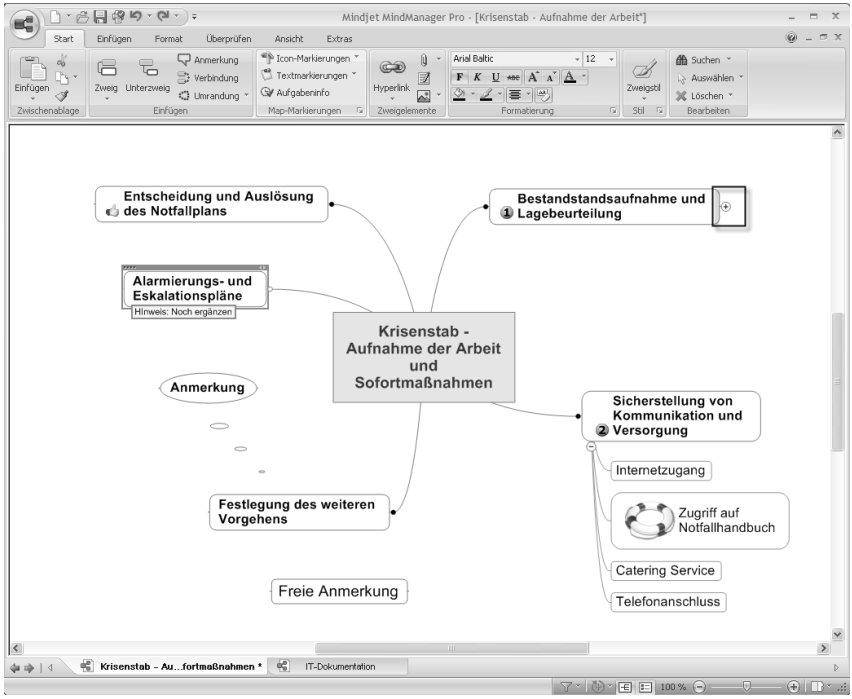


Abbildung 7.37: Zweige sind die wesentlichen Bestandteile einer Map.

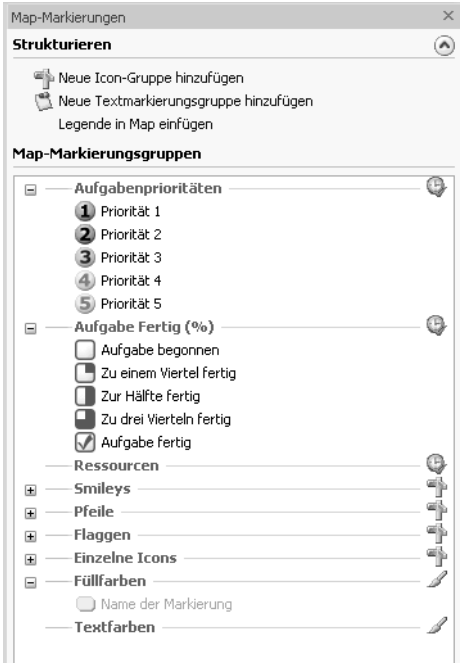


Abbildung 7.38: Map-Markierungen erleichtern die Übersicht.

Informationssammelbecken Postfach

Oft wird, insbesondere in der Phase der Stoffsammlung, eine neue E-Mail „sicherheitshalber“ zunächst in einer mehr oder weniger ausgeklügelten Postfach-Ordnerstruktur abgelegt. Man hofft, sich später noch daran zu erinnern, dass man diese E-Mail erhalten hat. Besser wäre es jedoch, die E-Mail direkt in die Arbeitsdokumentation einzubinden. Erfolgt die Planung mit MindManager Pro ist dies ohne Weiteres möglich. Alle Termine, E-Mails, Aufgaben, Kontakte und Notizen können direkt aus Outlook heraus in eine Mind Map eingefügt werden.

Während der Installation sucht MindManager alle installierten Office-Anwendungen und den Internet Explorer und erweitert deren Symbolleisten um zwei zusätzliche Symbole. Diese ermöglichen es, Elemente aus der betreffenden Anwendung direkt dem markierten Zweig in MindManager hinzuzufügen.

Damit ist es beispielsweise möglich, alle E-Mails zu einem bestimmten Thema in die Mind Map einzufügen. Das Symbol zeigt an, dass es sich um eine Mail handelt. Wird ein Element in Outlook bearbeitet, so erfolgt auch eine Aktualisierung in MindManager und umgekehrt. Außerdem kann hierüber die E-Mail jederzeit geöffnet werden. Zusätzlich kann die Mail auch im Aufgabenbereich angezeigt werden.

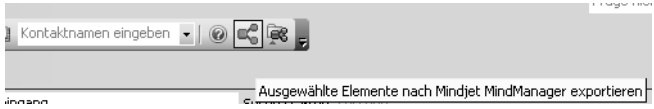


Abbildung 7.39: Outlook-Objekte in einer Mind Map verlinken

Enthalten Mails wichtige Anhänge, ist es jedoch besser, diese in der Dateistruktur zu speichern und die Datei in der Mind Map zu verlinken. Dies ist sehr einfach mit Drag & Drop möglich.

Anhänge und Hyperlinks anfügen

Wie bereits beschrieben, kann einem Zweig oder einer Notiz ein Hyperlink hinzufügt werden, der auf ein Dokument oder einen Ordner verweist. Darüber hinaus ist es auch möglich, dass Zweige mittels Hyperlinks auf eine andere Map, eine Internetadresse oder eine E-Mail-Adresse verweisen. Da auch dem Internet Explorer die in der vorstehend gezeigten Abbildung gezeigten Symbole hinzugefügt werden, ist es mit einem Klick möglich, Hyperlinks auf Internetseiten in eine Mind Map einzubinden. Damit kann eine Mind Map sogar die Favoritenliste des Internet Explorers ersetzen.

Textpassagen einfügen

Darüber hinaus können den Zweigen auch Anhänge hinzugefügt werden (pro Zweig kann ein Hyperlink hinzufügt werden). Statt die gesamte Datei als Anhang einzufügen, ist es auch möglich, in einer anderen Anwendung Text zu kopieren, ihn dann in eine Map einfügen und damit einen neuen Zweig zu erstellen. Damit sind wichtige Informationen direkt verfügbar, ohne dass die Gefahr besteht, dass sie beispielsweise in ausgedruckter Form in irgendeiner Ablage verschwinden. So können zum Beispiel Daten aus Excel in eine Mind Map eingefügt werden. Der neue Zweig ist mit seinen Quelldaten dynamisch verknüpft. Werden die Daten in Excel bearbeitet, so werden sie auch in MindManager aktualisiert.

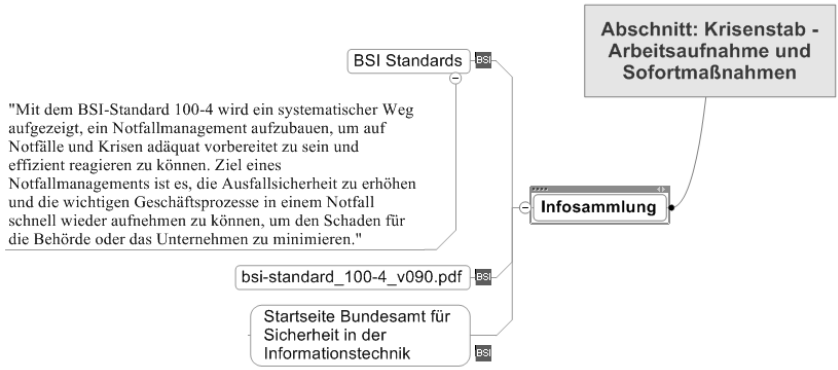


Abbildung 7.40: Textpassagen und Internet-Links werden als neue Zweige eingefügt.

7.3.3.2 Mind Maps bereitstellen

Falls Mind Maps nicht nur für das Sammeln und Verwalten von Informationen eingesetzt werden, sondern ihre Inhalte auch in die Dokumentation einfließen sollen, ist es entscheidend, in welcher Form Mind Maps bereitgestellt werden.

MindManager Pro unterstützt den Export von Maps (oder in einigen Fällen auch ausgewählter Zweige) in eine Reihe anderer Formate. Dazu zählen Grafikformate, Microsoft Office-Dokumente, PDF-Dateien und HTML-Dateien. Weiter lassen sich mit der Funktion Pack & Go die Maps und die dazugehörigen Dokumente zu einem .zip-Archiv schnüren.

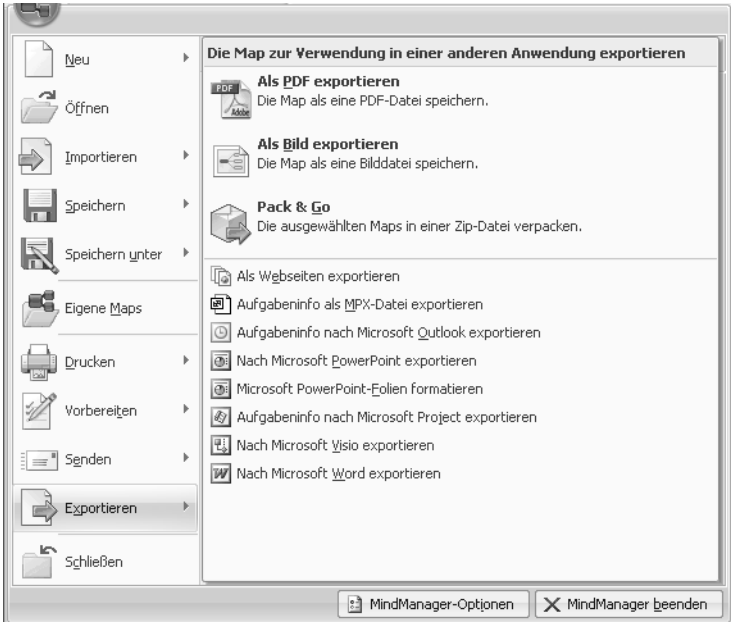


Abbildung 7.41: Verfügbare Exportmöglichkeiten in MindManager Pro

Hervorzuheben sind die Möglichkeiten bei dem Erstellen von Webseiten aus einer Map. Mindjet MindManager Pro bietet eine Vielzahl von Möglichkeiten für den Webexport: von der einfachen und schnellen Verwendung vorformatierter Vorlagen bis hin zur kompletten Steuerung durch den Benutzer. Damit können die Informationen in einer Mind Map auch beispielsweise im Intranet bereitgestellt werden. MindManager Pro verfügt über eine Reihe vordefinierter Webvorlagen, die für neue Webseiten unverändert übernommen oder auch angepasst werden können.

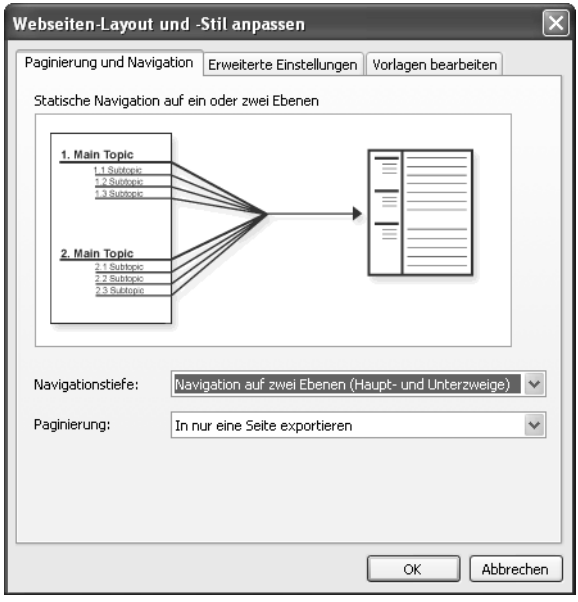


Abbildung 7.42: Mind Maps als Webseiten bereitstellen

Mindjet MindManager Viewer

Zusätzlich können mit dem kostenlosen Mindjet MindManager Viewer 7 MindManager-Maps komfortabel angezeigt werden, ohne die Vollversion der Anwendung installieren zu müssen. MindManager Viewer erlaubt eine problemlose Navigation in den Maps durch das Erweitern oder Reduzieren von Zweigen, das Vergrößern ausgewählter Zweige oder die Suche nach bestimmten Themen. Unter dem folgenden Link kann der Viewer kostenlos heruntergeladen werden [MIMAGER].

7.4 Dokumente sinnvoll organisieren

In der vorausgegangenen Kapiteln wurde ausführlich erläutert, was im Rahmen der IT-Dokumentation zu dokumentieren ist und wie sich Dokumente optimal erstellen lassen. Je mehr Dokumente aber entstehen, desto wichtiger ist es, diese so abzulegen, dass alle schnell gefunden werden und jeder auf die von ihm benötigten Dokumente Zugriff hat. Ebenso muss sichergestellt werden, dass Änderungen an einem Dokument immer an der aktuell gültigen Version des Dokuments erfolgen.

Das folgende Kapitel möchte hierzu ein paar Anregungen liefern. Darüber hinaus zeigt das Kapitel, welche Vorteile Dokumentenmanagement-Systeme (DMS) gegenüber der konventionellen Speicherung der Dokumente in einem Dateisystem bieten.

7.4.1 Aufgaben der Dokumentenverwaltung

Dokumentenlebenszyklus

Jedes Dokument durchläuft von der ersten Arbeitsversion bis zu seiner endgültigen (finalen) Version verschiedene Stufen. Alle Phasen lassen sich in einem *Dokumentenlebenszyklus* (engl. *Document Lifecycle*) darstellen. Dieser Zyklus beschreibt den Prozess, den ein Dokument von seiner Erstellung über die Verwendung bis zum Löschen bzw. bis zum Sichern in einem Langzeitarchiv durchläuft.

Die nachstehende Grafik zeigt den typischen Lebenszyklus für Dokumente der IT-Dokumentation.

hinweis

Im Zusammenhang mit Dokumentenmanagement-Systemen taucht in der Literatur auch immer wieder der Begriff *Document Lifecycle Management (DLM)* auf. DLM beschreibt die automatisierte Verwaltung und Kontrolle elektronischer Dokumente während ihrer gesamten Lebensdauer innerhalb einer Organisation – von ihrer Erstellung bis zu ihrer Löschung.

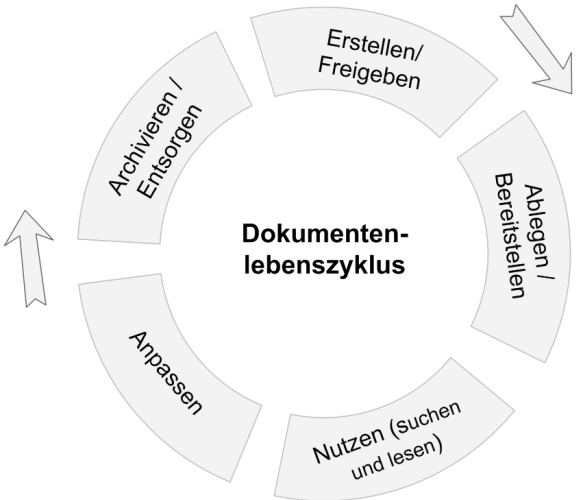


Abbildung 7.43: Der Dokumentenlebenszyklus eines Dokuments der IT-Dokumentation

Welche organisatorischen Anforderungen innerhalb jeder Phase zu beachten sind, wird im Folgenden erläutert.

7.4.1.1 Dokumentenerstellung

Der Lebenszyklus eines Dokuments beginnt mit dessen Erstellung. Die Notwendigkeit, Richtlinien und Vorgaben für das Erstellen und Freigeben von Dokumenten festzulegen, wurde bereits an verschiedenen Stellen behandelt. Die Basis in dieser Phase bildet die Dokumentationsrichtlinie (siehe Abschnitt 7.1). Diese sollte unter anderem Richtlinien für die Erstellung definieren und den formalen Aufbau der Einzeldokumente regeln.

7.4.1.2 Dokumentenablage und Dokumentenbereitstellung

Eine der größten Herausforderungen im Umgang mit der IT-Dokumentation stellt die Entwicklung einer sinnvollen Ablagestruktur für die Dokumente dar.

Diese Struktur muss sicherstellen, dass zu jedem Zeitpunkt allen Beteiligten bekannt ist, welchen Status ein Dokument aktuell hat und wo dieses gespeichert ist. Die Dokumente müssen also schnell gefunden werden können. Außerdem muss die Ablage die prozessorientierten Arbeitsabläufe durch eine einfache Bereitstellung aller erforderlichen Dokumente unterstützen. Gleichzeitig müssen Berechtigungen sicherstellen, dass nur berechtige Personen Zugriff auf die entsprechenden Dokumente erhalten.

Basis für neue Dokumente

Die Ablagestruktur muss aber nicht die Nutzung der Dokumente unterstützen. Sie stellt auch die Basis für die Erstellung weiterer Dokumente dar. Es wurde bereits darauf hingewiesen, dass Informationen grundsätzlich nur in einem Dokument stehen dürfen. Die häufig angewandte Methode, Informationen mittels Kopieren und Einfügen in ein anderes Dokument zu übernehmen, anstatt auf das Dokument zu verweisen, führt zwangsläufig zu Inkonsistenzen und einem erhöhten Pflegeaufwand. Ähnliche Folgen hat das Erfassen von Informationen in einem Dokument, ohne die Inhalte anderer Dokumente zu berücksichtigen. Gibt es beispielsweise Systemakten für alle Server, ist es unnötig, in der Installationsanleitung für eine Serveranwendung nochmals die IP-Konfiguration des Servers aufzuführen.

Es ist daher wichtig, sich im Vorfeld Kenntnis über alle Dokumente zu verschaffen, die Schnittstellen zum zu erstellenden Dokument haben, und auf diese bei Bedarf zu verweisen. Dies aber ist nur möglich, wenn die existierenden Dokumente bekannt sind und Zugriff auf sie besteht. In einer unstrukturierten IT-Dokumentation, bei der jede Organisationseinheit ihre eigenen Dokumente erstellt und verwaltet, ist diese Forderung schlicht nicht durchzusetzen.

Anforderungen an die Dokumentenablage

Wie die Ausführungen zeigen, ist es ohne eine zentral verwaltete Dokumentenablage kaum möglich, eine modulare, an den Prozessen orientierte IT-Dokumentation zu pflegen. Dabei können die einzelnen Dokumente durchaus dezentral gespeichert werden. Wichtig ist eine zentrale Verwaltung aller Metadaten und eine zentrale Vergabe der Dokumentennummern. Diese Informationen müssen allen Beteiligten zugänglich sein. Darüber hinaus muss sicher gestellt werden, dass jeder, der mit Dokumenten arbeitet, auch Zugriff auf die darin verwiesenen Dokumente hat. Das Gleiche gilt für Objektverknüpfungen.

7.4.1.3 Dokumentennutzung – Lesen und Suchen

In erster Linie müssen die Ersteller eines Dokuments einen schnellen Zugriff auf alle Dokumente haben, die sie zur Erledigung ihrer Aufgaben benötigen. Diese Anforderung kann bei einer entsprechenden Dokumentenstruktur und der Verwendung von Dokumentenverknüpfungen durchaus auch bei Speicherung der Dateien im Dateisystem befriedigend erfüllt werden.

Ergänzende Dokumente suchen

Schwieriger wird es mit der Suche von Textpassagen in den Dokumenten. Ist es beispielsweise für die Erstellung eines neuen Dokuments erforderlich, alle Dokumente zu erfassen, die dazu Schnittstellen aufweisen, sind entsprechende Suchfunktionen wünschenswert. Theoretisch sollten sich bei einer gut strukturierten IT-Dokumentation allein aus dem Thema und den definierten Merkmalen der verschiedenen Dokumentenklassen die ergänzenden Dokumente ableiten lassen, doch ist dies wohl eher wünschenswerte Theorie.

Wird zur Bereitstellung der IT-Dokumentation kein DMS bzw. keine Serveranwendung wie beispielsweise der *Microsoft Search Server* eingesetzt, bleibt manchmal nur die Verwendung der Windows Suchfunktion zum Durchsuchen der Dokumente.

7.4.1.4 Dokumentenänderung

In der IT-Dokumentation wird kaum ein Dokument zu finden sein, dass nach seiner Freigabe keinen Änderungen unterworfen ist. Wichtig ist, dass Änderungen standardisiert nach festen Vorgaben erfolgen. So darf es nicht passieren, dass ein Mitarbeiter Änderungen in einem Dokument vornimmt, während andere Mitarbeiter mit „ihrer" Arbeitsversion des Dokuments weiterarbeiten und von den Änderungen nichts mitbekommen. Auch darf es nicht passieren, dass ein Dokument gleichzeitig von mehreren Mitarbeitern bearbeitet wird und die Änderungen des einen überschrieben werden.

Auch ist es nicht empfehlenswert, nach jeder Änderung das Dokument per Mail an alle Beteiligten zur Begutachtung zu verschicken. Dies ist nicht nur eine „wirkungsvolle" Maßnahme, die Postfächer zu füllen, sondern führt zwangsläufig zu einer chaotischen Verbreitung von verschiedenen Arbeitsständen. Werden mehrere Instanzen von einer Datei bereitgestellt, muss klar erkennbar sein, welche das verbindlich gültige Dokument darstellt. Nur so lassen sich Fragen wie die die folgende vermeiden: „In welcher Version bzw. Kopie hast Du gestern eigentlich die Änderungen eingepflegt?"

Geänderte Dokumente erneut veröffentlichen

Sinnvollerweise sollten weitere Instanzen eines Dokuments nur in einem nicht veränderbaren Format, wie dem PDF-Format, bereitgestellt werden. Zum anderen muss es Regelungen geben, wann und in welcher Art durchgeführte Änderungen zu kommunizieren sind. Werden Dokumente geändert, die beispielsweise im Intranet veröffentlicht sind, darf die erneute Bereitstellung nicht vergessen werden.

7.4.1.5 Dokumentenarchivierung und Entsorgung

Das Archiv stellt die letzte Station im Dokumentenlebenszyklus dar. In den vergangenen Jahren wird das Thema Archivierung häufig unter dem Aspekt der *revisionssicheren elektronischen Archivierung* betrachtet. Abschnitt 7.4.2.2 können Sie hierzu weitere Informationen entnehmen.

Die elektronische Archivierung steht für die unveränderbare, sichere, geordnete und jederzeit zugreifbare langzeitige Aufbewahrung elektronischer Informationen. Diese Punkte sind wichtig, denn mit der Archivierung müssen die gesetzlichen Regelungen hinsichtlich der Aufbewahrungsfristen von Dokumenten umgesetzt werden.

Wenn ein Dokument nicht mehr länger in Bearbeitung ist oder in einem Prozess benutzt wird, sollte es archiviert werden. Dokumente, die archiviert wurden, können nicht mehr verändert werden. Gelöscht werden dürfen Dokumente aber erst (wenn überhaupt), nachdem ihre Aufbewahrungsfrist abgelaufen ist.

Für das Löschen von Dokumenten nach Ablauf der Aufbewahrungsfrist müssen ebenfalls Regelungen existieren. So kann es erforderlich sein, dass für das Löschen eine gesonderte Freigabe durch die fachverantwortliche Stelle erforderlich ist. In jedem Fall ist das Löschen von Dokumenten zu protokollieren. Außerdem sollte die Vernichtung nach den Vorschriften des BSI durchgeführt werden und.

7.4.1.6 Erforderliche Regelungen

Unabhängig von dem Einsatz eines Dokumentenmanagement-Systems sollten für alle Phasen des Dokumentenlebenszyklus Prozesse definiert werden. Hierzu zählen unter anderem die folgenden Prozesse:

- Prozess zur Erstellung eines Dokuments einschließlich der Arbeitsabläufe zur Qualitätssicherung
- Freigabeprozess
- Prozess zur Bereitstellung von Dokumenten
- Prozess zur Nutzung von Dokumenten (Regelung von Berechtigungen)
- Prozess zur Änderung von Dokumenten mit dem Status *endgültig* oder *freigegeben* (Informationen zum Dokumentenstatus (Siehe Abschnitt 7.1.1.3).
- Prozess zur Archivierung von Dokumenten
- Prozess zur Entsorgung von Dokumenten

Noch entscheidender als die Definition der Prozesse ist deren Durchsetzung. Hierzu müssen alle an der Erstellung von Dokumenten beteiligten Personen (hierzu gehören gegebenenfalls auch externe Berater) diese Regelungen kennen und einhalten. Ohne die Einhaltung verbindliche Regelungen entstehen schnell unstrukturierte Dokumentationsablagen die jede Menge Dokumente beherbergen, die keinerlei Standards in Bezug auf Benennung, formalen Aufbau und inhaltlicher Ausgestaltung aufweisen. Bei eines solchen Struktur ist es schwierig Bezüge zu anderen Dokumenten zu verwenden, so dass die Dokumente bezugslos nebeneinander stehen.

Immer noch wichtig: Miteinander reden

Darüber hinaus sollten auch die „klassischen" Kommunikationswege nicht vergessen werden. Anders als andere Bereiche mit ausschließlich definierbaren Arbeitsabläufe ist der Bereich der IT sehr stark von situationsbezogenem Handeln geprägt. Dies hat zwangsläufig auch Auswirkungen auf die Erstellung und Pflege der Dokumente. Daher können kaum alle Abläufe der Dokumentenerstellung und Pflege in verbindlichen Prozessen geregelt werden. Ist man gerade mit der Erstellung eines Dokuments zu einem übergreifenden Thema befasst, kann es beispielsweise wichtig sein, mit der entsprechenden Fachabteilung zu reden und damit sicherzustellen, das man nicht ein wesentliches ergänzendes Dokument unberücksichtigt lässt, weil sich dieses gerade ebenfalls in Erstellung befindet.

7.4.2 Einführung eines Dokumentenmanagement-Systems

Realistischerweise sind die genannten Anforderungen und die dazugehörenden Prozesse nur in sehr kleinen Unternehmen ohne den Einsatz eines Dokumentenmanagement-Systems (DMS) durchzusetzen.

7.4.2.1 Nutzen und Einsatzmöglichkeiten eines DMS

Dokumentenmanagement beschreibt die meist datenbankgestützte Verwaltung elektronischer Dokumente. Elektronische Dokumente sind entweder digital erzeugte bearbeitbare Dateien oder digitale Kopien eingescannter Papierdokumente.

Heute wird das Dokumentenmanagement häufig als eine Komponente des übergreifenden *Enterprise Content Management (ECM)* betrachtet. ECM ist ein modernes Kunstwort, das Produkte, Lösungen sowie eine ganze Branche beschreibt und Technologien zur Erfassung, Verwaltung, Speicherung, Bewahrung und Bereitstellung von Daten (Content) und Dokumenten zur Unterstützung von organisatorischen Prozessen im Unternehmen kombiniert.

Die Hauptaufgabe eines Dokumentenmanagement-Systems liegt darin, die definierten Dokumentationsprozesse über ein System abzubilden, zu steuern und zu überwachen. Das DMS organisiert dabei Entwurf und Erstellung, Weitergabe und Verteilung, Auffinden sowie die Ablage und Übergabe an ein Archiv oder Löschung der Dokumente. Dabei kann zwischen Dokumentenmanagement-Systemen im engeren und im weiterten Sinne unterschieden werden.

Eigenschaften klassischer Systeme

Unter „klassischen" Dokumentenmanagement-Systemen sind solche Lösungen zu verstehen, die die Erstellung, Nutzung und Änderung von Dokumenten unterstützen. Bei ihnen stehen folgende Funktionen im Vordergrund:

- Strukturierte Speicherung von Dokumenten
- Überwachung des Zugriffs auf Dokumente
- Indexgestützte Dokumentensuche
- Ein- und Auschecken von Dokumenten
- Versionsmanagement

Versionsverwaltung

Mit den beiden letztgenannten Funktionen unterstützt ein DMS die Erstellung und Änderung von Dokumenten. Das Versionsmanagement kontrolliert die Bearbeitung von Dokumenten, das heißt, Dokumente können zur Bearbeitung aus dem System ausgecheckt und während der Bearbeitungszeit von anderen Benutzern nur angezeigt, jedoch nicht geändert werden. Nach der Bearbeitung wird das Dokument wieder eingecheckt, und das DMS vergibt eine neue Versionsnummer. Hierdurch wird verhindert, dass zwei oder mehrere Personen gleichzeitig an einem Dokument arbeiten und ihre Arbeitsergebnisse im schlimmsten Fall gegenseitig löschen. Ebenso sind die Bearbeitungsschritte nachvollziehbar (Historie). Es gibt auch Systeme, die gleichzeitige Änderungen mehrerer Benutzer an einer Datei zulassen. Anschließend werden die Änderungen automatisch oder manuell zusammengeführt.

Index-gestützte Dokumentensuche

Die Suche in einem DMS kann über einen eigenständigen Software-Client oder über eine webbasierte Lösung erfolgen. Kennzeichnend für ein DMS ist die datenbankgestützte Metadatenverwaltung zur Index-gestützten Dokumentensuche. So gekennzeichnete Dokumente sind über weitaus mehr Informationsfelder recherchierbar, als sie ein Dateisystem zur Verfügung stellt. In der Regel ist auch eine Volltextsuche möglich.

beispiel

Bei der klassischen Ablage in Verzeichnissen wird in der Regel versucht, möglichst viele Dokumenteigenschaften durch Verwendung einer Ordnerhierarchie zu hinterlegen:

C:\Dokumente\Systemakten\Hardware\Server\Serv4711.doc

In einen DMS erhält das Dokument hingegen parallele Eigenschaften: Es wird der Dokumentenklasse der *Systemakten* zugeordnet, ist eine *Hardwareakte* der Kategorie *Server* mit dem Status e*ndgültig* und beschreibt den Server *Serv4711*. Gespeichert wird das Dokument in der Datenbank des DMS.

Damit kann dieser Server in beliebigen Suchanfragen gefunden werden:

- „Liste alle Systemakten“
- „Liste alle Systemakten der Kategorie *Server*“
- „Liste alle Hardwareakten mit dem Status *endgültig*“
- „Zeige die Systemakte für den Server *Serv4711*“

Virtuelle Akten

Eine wesentliche Funktion dabei ist die Möglichkeit, auswählbare Informationen zu „virtuellen Dokumenten“, sogenannten *virtuelle Akten* zusammenzufassen. Es handelt sich hierbei um eine zusammenhängende Sicht auf die Informationen, die aus den verschiedenen Quellen zusammengeführt werden. Nutzer des DMS können sich in einer virtuellen Akte genau das zusammenstellen, was sie bei Bedarf an Daten in der Dokumentenansicht sehen möchten. Die Inhalte einer Sicht werden dynamisch zur Laufzeit als Sicht erzeugt und in der gewünschten Form, zum Beispiel als tabellarische Darstellung oder in einer Ordnungsstruktur, visualisiert.

Gegenüber den Dokumentenmanagement-Systemen im engeren Sinne unterstützen erweiterte Systeme den vollständigen Lebenszyklus von Dokumenten von ihrer Entstehung bis zur ihrer Entsorgung. Erweiterte Systeme ergänzen die klassischen Funktionen eines Dokumentenmanagements mindestens um die beiden Komponenten *Workflow* und *Archivierung*. Dabei müssen nicht alle Komponenten zwangsläufig von einem Hersteller kommen.

Workflow-Komponente

Mit Hilfe der Workflow-Komponente werden die eigentlichen Prozesse und Arbeitsabläufe abgebildet. Beispielsweise können Review- und Freigabeprozesse mit Hilfe einer Workflow-Komponente gesteuert werden. Sind die Rollen, Ausführungsparameter und die Prozessteilnehmer definiert, kann die Workflow-Komponente den Transfer der Informationen zwischen den Prozessteilnehmern steuern, die Ausführung überwachen und warnen, wenn zum Beispiel Bearbeitungszeiten überschritten werden. Verbunden mit einem DMS ermöglicht das Workflow-Management die vollständige Bearbeitung eines Vorgangs in einem elektronischen Medium vom Anfang bis zum Ende. Die gesamte Vorgangsbearbeitung wird so elektronisch gesteuert. Technisch kann es sich bei der Workflow-Komponente um ein Workflow-Management-System oder ein Business Process Management System (BPMS) handeln.

Archivsystem

Die Archivierung stellt die letzte Station im Lebenszyklus eines Dokuments dar. Für die elektronische Archivierung werden zumeist spezielle Archivsysteme und in der Regel *WORM-Speichermedien* eingesetzt. WORM steht für „Write-Once, Read-Many" und beschreibt ein digital-optisches Speichermedium, das mit einem Laser berührungsfrei nur einmal beschrieben werden kann. Archivierte Dokumente sind damit gegenüber Änderungen geschützt.

Datensicherung ist keine Archivierung

Auch wenn im Zusammenhang mit Datensicherung der Begriff „Archiv" verwendet wird, ist eine Datensicherung keine Archivierung. Bei der Datensicherung werden im weitesten Sinne Dokumente auf einem Medium (Plattenspeicher, Magnetband usw.) gespeichert und für den Fall aufbewahrt, dass die gespeicherte Originaldokument wiederhergestellt werden muss. Archivierung hingegen ist an weitere Regeln gebunden wie: Unveränderbarkeit, langfristige Wiederauffindbarkeit, Wiedergabefähigkeit und jederzeitige Verfügbarkeit. Ein Archiv muss die Langzeitverfügbarkeit gewährleisten.

Die Funktionen eines DMS erleichtern die Durchsetzung von Richtlinien und Regelungen für die Dokumentation, sie machen sie aber nicht überflüssig. Seine Aufgabe kann ein DMS nur erfüllen, wenn alle Beteiligten ihre Dokumente entsprechend den Vereinbarungen erfassen und nicht an dem System „vorbei kommen".

Höherer Erfassungsaufwand

Der mögliche Widerstand der Anwender ist bei der Einführung eines DMS nicht zu unterschätzen. Der wesentliche Vorteil der leichteren und langfristigeren Wiederauffindbarkeit wird nicht allein durch das System sichergestellt, sondern durch Schlagwort-Wörterbücher, Dokumentenklassen und eine entsprechende Verschlagwortung bei der Ablage eines Dokuments. Damit verbunden ist zwangsläufig ein gegenüber der Dokumentenablage im Dateisystem höherer Aufwand bei der Ablage von Dokumenten im Dokumentenmanagement-System, der nicht selten zu einer Ablehnung des Systems durch die Benutzer führt.

7.4.2.2 Rechtliche Aspekte beim DMS-Einsatz

Bei der gesetzeskonformen Archivierung (hierbei spielt es keine Rolle, ob Dokumente oder E-Mails archiviert werden) müssen Unternehmen auf der einen Seite den Pflichten zur Aufbewahrung von handels- und steuerlich-relevanter Informationen nachkommen, auf der anderen Seite dürfen die dafür gewählten Maßnahmen den Datenschutz und die Privatsphäre der Mitarbeiter nicht verletzen. Vielen Unternehmen, die ein DMS einführen, ist nicht bewusst, dass sie damit im Hinblick auf den Datenschutz einige wesentliche Punkte beachten und entsprechende Maßnahmen umsetzen müssen.

Datenschutzrechtliche Aspekte Beim Einsatz eines Dokumentenmanagement-Systems sind die allgemeinen datenschutz-rechtlichen Grundsätze zu beachten:

> *Personenbezogene Daten dürfen nur erhoben, verarbeitet oder sonst genutzt werden, wenn und soweit das zur rechtmäßigen Erfüllung der Aufgaben der Daten verarbeitenden Stelle für den gesetzlich zugelassenen oder durch Einwilligung eröffneten Zweck erforderlich ist. Die Daten verarbeitende oder die in deren Auftrag arbeitende Stelle hat diejenigen technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um den Schutz des informationellen Selbstbestimmungsrechts zu gewährleisten.[DMS]*

Problembereiche aus Sicht des Datenschutzes

Aus Sicht des Datenschutzes und der Datensicherheit ist daher beim Einsatz eines DMS einiges zu beachten:

Generelle datenschutzrechtliche Gefahren In einem DMS werden Informationen meist fachübergreifend vorgehalten. Dies allein birgt Risiken in Bezug auf das Grundrecht auf informationelle Selbstbestimmung. So können mit Hilfe des DMS in automatisierter Weise aus einer Datensammlung durch vielfältige Datenverknüpfungen zusätzliche Informationen gewonnen werden. Die ausführlichen Such- und Auswertungsfunktionen eines DMS ermöglichen, falls eine Volltextrecherche zugelassen ist, quasi per Knopfdruck umfassende Recherchen zu einer bestimmten Person. Insbesondere die gezielte Zusammenführung von personenbezogenen Daten aus unterschiedlichen Datenquellen und ihre Auswertung sind gesetzeswidrig im Sinne des Datenschutzes, zumal sie überwiegend ohne Kenntnis der Betroffenen erfolgen.

Gefahren und eine Verletzung der informellen Selbstbestimmung ergeben sich auch aus der langen Aufbewahrungsfrist der Daten. Nach den Datenschutzgesetzen dürfen personenbezogene Daten nur solange aufbewahrt werden, wie ihre Kenntnis für die verantwortliche Stelle zur Erfüllung ihrer Aufgaben erforderlich ist.

Auswertung von Nutzerverhalten Dokumentenmanagement-Systeme können aber auch zur Ausforschung und zur Verhaltens- und Leistungskontrolle von Mitarbeitern genutzt werden. Insbesondere beim Einsatz eines Workflow-Management-Systems gibt es einige Aspekte, die die Daten verarbeitende Stelle berücksichtigen muss. Hierzu gehört beispielsweise die Abbildung des Bearbeitungsweges sowie die Leistungskontrolle durch eine Überwachung der Verweildauer. Durch die systemgesteuerte Vorgangsbearbeitung werden die Laufwege dokumentiert. Es entstehen eine Fülle zusätzlicher Protokoll- und Verfahrensdaten, die mitarbeiterbezogen ausgewertet werden können. Damit können ohne Weiteres permanente Verhaltens- und Leistungskontrollen der Beschäftigten erfolgen, was jedoch nicht zulässig ist.

Sicherstellung der Vertraulichkeit Es ist in jeder Phase der Datenverarbeitung sicherzustellen, dass nur befugte Personen die Daten zur Kenntnis nehmen können. Anwender dürfen nur die Rechte erhalten, die sie für die Erfüllung ihrer dienstlichen Aufgaben benötigen. Dies muss durch ein detailliertes Rollen- und Rechtekonzept sichergestellt werden. Der Einsatz eines DMS erfordert darüber hinaus von datenschutzrechtlicher Seite klare Festlegungen, wer für welche Aufgaben verantwortlich ist und wer die Verantwortung für die Vollständigkeit und Korrektheit der Daten trägt. Beim Einsatz eines DMS sollte deshalb ein gesondertes Datenschutzkonzept mit Bezug auf das DMS erstellt werden.

Weiterhin müssen Dokumente, an die hohe Vertraulichkeitsanforderungen gestellt werden, entsprechend sicher verschlüsselt werden. Die Verschlüsselung sollte sowohl bei der Übertragung der Daten erfolgen als auch eine verschlüsselte Speicherung der Daten umfassen.

Sicherstellung der Integrität Ein wichtiger Aspekt der gesetzeskonformen Datenhaltung ist der Schutz der Dokumente vor Veränderungen. Die Integrität und Echtheit der Dokumente muss jederzeit sichergestellt und notfalls auch nachzuweisen sein. Eine zentrale Bedeutung beim Einsatz eines DMS kommt daher dem Signieren von Dokumenten zu. Mit einer Signatur wird die Urheberschaft nachweisbar. Signaturen dienen damit der Authentizität, der Integrität, der Revisionsfähigkeit und der Rechtssicherheit. Hierbei ist jedoch zu beachten, das bei Ablage eines Dokuments verschiedene Daten anfallen, die gegebenenfalls auch unterschiedlich zu behandeln sind:

- Inhalt des Dokuments
- Metadaten, die formale und inhaltliche Eigenschaften des Dokuments bezeichnen

- Verfahrensdaten, die Eigenschaften der Organisation bzw. des Workflows, in denen das Dokument und Personen eingebunden sind, bezeichnen
- Protokolldaten, die systemtechnische Aktivitäten und Konfigurationsdaten enthalten

hinweis

Eine ausführliche Behandlung aller datenschutzrechtlichen Aspekte bei Einsatz eines DMS ist an dieser Stelle weder möglich noch sinnvoll. Die aufgezeigten Beispiele sollen lediglich auf die Problemfelder hinweisen, die bei der Einführung eines DMS zu beachten sind.

Einen guten Überblick über alle wichtigen Aspekte liefert die *Orientierungshilfe „Datenschutz bei Dokumentenmanagementsystemen" – des Arbeitskreises eGovernment der Konferenz der Datenschutzbeauftragten des Bundes und der Länder*. Die Orientierungshilfe stellt die datenschutzrechtlichen und -technischen Anforderungen, die zu beachtenden Sicherheitsaspekte und die Architektur des Dokumentenmanagement-Systems vor und gibt praktische Hinweise, wie die Anforderungen an ein DMS datenschutzgerecht umgesetzt werden können [DMS].

Gesetzeskonform archivieren Das Thema Archivierung und Langzeitspeicherung hat in den letzten Jahren besonders durch rechtliche Vorgaben an Bedeutung gewonnen. Standards wie der Sarbanes-Oxley Act und die Archivierung steuerrelevanter Daten entsprechend den GDPdU (siehe hierzu Abschnitt 1.1.1) machen revisionssichere Archiv- und Speichersysteme erforderlich.

Revisionssichere Archivierung

Eine elektronische Archivierung wird als revisionssicher betrachtet, wenn die Archivsystemlösung den Anforderungen des Handelsgesetzbuches sowie der Abgabenordnung und den GoBS an die sichere, ordnungsgemäße Aufbewahrung von kaufmännischen Dokumenten entspricht und die Aufbewahrungsfristen von sechs bis zehn Jahren erfüllt. Das HGB und die Abgabenordnung geben die Grundlagen für die Speicherung vor, ohne dabei herkömmliche Papierarchive von elektronischen Systemen zu unterscheiden.

Immer wieder wird die Frage nach dem „richtigen" Speichermedium zur Sicherstellung der gesetzlichen Anforderungen gestellt. Meist werden WORM-Medien verwendet, die physisch nur einmal beschreibbar sind. Allerdings hängt die Revisionssicherheit nicht nur von den Speichermedien ab. Vielmehr muss das gesamte Verfahren der Archivierung revisionssicher sein. Dies geht über die Frage der Speicherlaufwerke und Speichermedien hinaus und bezieht auch die organisatorischen Prozesse mit ein.

Zusätzliche Informationen zu diesem Thema und einen guten Leitfaden liefert der *VOI – Verband Organisations- und Informationssysteme e. V.* [VOI] auch mit seinen zehn Merksätzen zur revisionssicheren Archivierung:

1. *Jedes Dokument muss unveränderbar archiviert werden.*
2. *Es darf kein Dokument auf dem Weg ins Archiv oder im Archiv selbst verloren gehen.*
3. *Jedes Dokument muss mit geeigneten Retrievaltechniken wieder auffindbar sein.*
4. *Es muss genau das Dokument wiedergefunden werden, das gesucht worden ist.*
5. *Kein Dokument darf während seiner vorgesehenen Lebenszeit zerstört werden können.*
6. *Jedes Dokument muss in genau der gleichen Form, wie es erfasst wurde, wieder angezeigt und gedruckt werden können.*
7. *Jedes Dokument muss zeitnah wiedergefunden werden können.*
8. *Alle Aktionen im Archiv, die Veränderungen in der Organisation und Struktur bewirken, sind derart zu protokollieren, sodass die Wiederherstellung des ursprünglichen Zustandes möglich ist.*
9. *Elektronische Archive sind so auszulegen, dass eine Migration auf neue Plattformen, Medien, Softwareversionen und Komponenten ohne Informationsverlust möglich ist.*
10. *Das System muss dem Anwender die Möglichkeit bieten, die gesetzlichen Bestimmungen (BDSG, HGB/AO usw.) sowie die betrieblichen Bestimmungen des Anwenders hinsichtlich Datensicherheit und Datenschutz über die Lebensdauer des Archivs sicherzustellen.*

7.4.3 DMS am Beispiel der Windows SharePoint Services

Möchte man ein DMS einführen, hat man die Qual der Wahl. Es gibt eine Vielzahl möglicher Produkten und die Wahl des für das jeweilige Unternehmen passende DMS erfordert sorgfältige Analysen. Nicht immer aber muss es die „große" Lösung sein. Mit den *Windows SharePoint Services* stellt Microsoft kostenlos ein Groupware-System bereit, dessen integrierte Funktionen zur Verwaltung von Dokumenten in vielen Fällen durchaus ausreichend sein können, und das darüber hinaus einige nützliche Workflows bietet. Sei es, dass man eine kostengünstige Lösung für ein kleines Team sucht, sich erstmalig mit dem Thema beschäftigen möchte oder für eine temporär bestehende Projektgruppe eine DMS-Lösung sucht; nicht nur in diesen Fällen können die *Windows SharePoint Services (WSS) 3.0* eine Alternative darstellen.

Die folgenden Ausführungen sollen lediglich einen Eindruck von der Arbeitsweise und den Möglichkeiten der Windows SharePoint Services 3.0 vermitteln. Detaillierte Informationen sind in der zahlreichen Fachliteratur zu WSS zu finden.

7.4.3.1 Windows SharePoint Services 3.0 im Überblick

Die Windows SharePoint Services 3.0 (WWS 3.0) sind eine auf ASP.NET basierende Webanwendung und stellen ein Web- bzw. Wissensportal bereit, das dem Zusammenführen von Daten aus verschiedenen Informationsquellen dient. Dank erweiterbarer Listen und WebParts und einer weitgehend offenen Web-Infrastruktur, die von Entwicklern mit Hilfe von ASP.Net erweitert werden kann, bieten die Windows SharePoint Services vielfältige Anpassungs- und Erweiterungsmöglichkeiten.

Während Listen von den Portalbenutzern selber erstellt und erweitert werden können, handelt es sich bei den *WebParts* um ein modulares Bausteinkonzept, mit dem sich SharePoint-Seiten flexibel zusammenstellen lassen. Diese können für zahlreiche Funktionen, wie beispielsweise das Anzeigen von Informationen von externen Datenquellen (Datenbanken, Websites, RSS-Feeds), Navigationshilfen und Suchfunktionen, verwendet werden.

Es werden standardmäßig einige Vorlagen für Sites (Teamsites, Arbeitsbereiche für Meetings und die Dokumenterstellung) mitgeliefert sowie eine Reihe von vorbereiteten Listen und WebParts, die bereits die wichtigsten Funktionen für die Teamarbeit abdecken.

SQL Server erforderlich

Alle Informationen über die SharePoint-Konfiguration und die eingerichteten Sites werden in einer zentralen Konfigurationsdatenbank auf einem SQL Server gespeichert. Dabei kann wahlweise SQL Server 2000 oder WMSDE (Microsoft SQL Server 2000 Desktop Engine) verwendet werden. Die WMSDE gehört zum Lieferumfang der Windows SharePoint Services 3.0 und eignet sich insbesondere für Test- und Pilotumgebungen.

hinweis

Nähere Informationen zu Systemanforderungen, Bezugsmöglichkeiten und Preisen der aktuellen Version finden Sie im Steckbrief der *Windows SharePoint Services* in Anhang D.6.

Moss 2007 basiert auf WSS 3.0

Nicht zu verwechseln mit den Windows SharePoint Services ist Microsofts kostenpflichtiger *Microsoft Office SharePoint Server (MOSS) 2007*. MOSS setzt zwar auf den WSS auf, das die grundlegende Infrastruktur wie WebPart-Framework, Listen und Dokumentmanagement zur Verfügung stellt, bietet aber darüber hinausgehende Funktionen an. Die erweiterten Funktionen von MOSS liefern erweiterte Funktionen für die Teamarbeit und für die Implementierung von Geschäftsprozessen. Unterschiede gibt es beispielsweise bei den Suchfunktionen. Während die Suchfunktion der WWS 3.0 die Suche nur innerhalb der aktuellen Site und Subsites erlaubt, können mit MOSS alle SharePoint Services-Sites und alle Dateisysteme des Unternehmens in den globalen Suchindex eingebunden und als Volltext durchsucht werden.

Die WWS 3.0 können kostenlos bezogen werden, das heißt, es fallen keine über die Server- und CAL-Lizenzen hinaus gehenden Lizenzkosten an. Für einen unternehmensweiten Einsatz, bei dem Informationen für sämtliche Benutzer bereitgestellt werden sollen, ist hingegen der kostenpflichtige Microsoft Office SharePoint Server 2007 erforderlich.

7.4.3.2 Arbeitsweise und wichtige Funktionen

Die WWS 3.0 sind eine Workgroup-Lösung, bei der die gemeinsame Nutzung von Dokumenten und Informationen im Vordergrund steht. Ein wichtiger Bestandteil stellt dabei die Dokumentenverwaltung dar, die im wesentlichen folgende Funktionen bereitstellt:

- Ein- und Auschecken von Dokumenten
- Versionsmanagement
- Freigabeprozesse
- Dokumentensuche

Im Folgenden werden diese vier Bereiche der WWS 3.0 etwas näher betrachtet.

Initial-Konfigurationen erforderlich Einer der Vorteile der WSS 3.0 liegt darin, dass sie „Out-of-the-Box“ sehr viel mitbringen, was die Konfiguration erleichtert. Hierzu gehört beispielsweise eine Webanwendung, die eine einzelne SharePoint-Website bereitstellt. Nach dem Abschluss der Installation wird der Browser mit der „SharePoint Zentraldadministration“ geöffnet, für die auch ein Link im Startmenü unter dem Punkt VERWALTUNG angelegt. Hier müssen einige administrative Aufgaben durchgeführt werden, um die Bereitstellung abzuschließen.

Abbildung 7.44: Startseite der SharePoint-Zentraladministration nach der Installation

Gemeinsame Nutzung von Dokumenten In sogenannten *Dokumentbibliotheken* können Dokumente gespeichert und verwaltet werden. Dazu muss mittels einer Vorlage eine Website erstellt werden. Diese stellt eine Dokumentbibliothek zum Speichern der Haupt- und Begleitdokumente, eine Aufgabenliste zum Zuweisen von Einzelaufgaben sowie eine Hyperlink-Liste für zugehörige Ressourcen zur Verfügung.

Bibliotheken bilden die Basis

Nach dem Abschluss der Installation wird standardmäßig die Website TEAMWEBSITE eingerichtet. Diese beinhaltet die ebenfalls standardmäßig eingerichtete Dokumentbibliothek FREIGEGEBENE DOKUMENTE. Diese kann – wie alle Bibliotheken – individuell konfiguriert werden. So kann festgelegt werden, wie Dokumente angezeigt, verfolgt, verwaltet und erstellt werden sollen. Einen Eindruck der Möglichkeiten vermittelt die nachstehende Abbildung.

Abbildung 7.45: Zahlreiche Einstellungen ermöglichen eine individuelle Anpassung von Dokumentbibliotheken.

Für eine effektive Bearbeitung von Dokumenten im Team sind vor allem die beiden Funktionen zum Ein- und Auschecken von Dokumenten und die Versionsverwaltung wichtig, wobei beide Funktionen eng miteinander verzahnt sind.

Check-in/Check-out-System

Dokumente können durch Auschecken während der Zeit der Bearbeitung für andere Mitarbeiter gesperrt werden (nur Read-only-Zugriff möglich). Dies ist sinnvoll, damit sie nicht von anderen Benutzern versehentlich überschrieben oder bearbeitet werden. Nur der Benutzer, der ein Dokument auscheckt, kann es auch bearbeiten. Beim Einchecken wird die Eingabe eines Kommentars angefordert, sodass zu verfolgen ist, welche Änderungen in den einzelnen Versionen vorgenommen wurden.

Versions-management

Die Versionsverwaltung ermöglicht es, Änderungen an Dokumenten zu verfolgen. D.h., wann ein Element oder eine Datei geändert und von wem die Änderung vorgenommen wurde. Zudem wird dokumentiert, wenn Metadaten geändert wurden. Falls beispielsweise das Fälligkeitsdatum für ein Listenelement geändert wird, wird dies im Versionsverlauf angezeigt. Auch die beim Einchecken vergebenen Kommentare werden angezeigt.

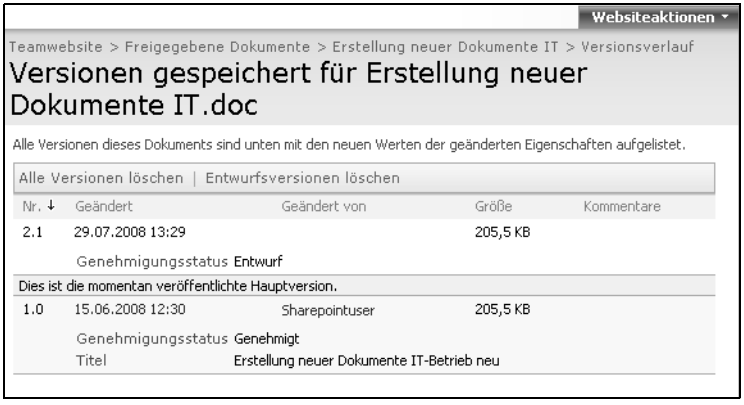


Abbildung 7.46: Zahlreiche Einstellungen ermöglichen eine individuelle Anpassung von Dokumentbibliotheken.

Für Bibliotheken können sowohl Hauptversionen als auch Nebenversionen betrachtet werden. Damit können beispielsweise genehmigungspflichtige Änderungen von kleineren Anpassungen (beispielsweise formale Änderungen) unterschieden werden. Zudem kann die Anzahl der gespeicherten Versionen beschränkt werden. Die Versionsverwaltung ist standardmäßig nicht aktiviert.

Freigabeprozesse verwenden WWS 3.0 verwendet für die Freigabe eines Dokuments den Begriff *Inhaltsgenehmigung*. Falls die Inhaltsgenehmigung erforderlich ist, behält ein Listenelement oder eine Datei den Status „Entwurf“ oder „Ausstehend“, bis es von jemandem genehmigt oder abgelehnt wurde, der über die Berechtigung zum Genehmigen verfügt. Nach erfolgter Genehmigung wird der Status „Genehmigt“ in der Liste oder Bibliothek zugewiesen, und das Element oder die Datei wird allen Benutzern angezeigt, die über die Berechtigung zum Anzeigen der Liste oder Bibliothek verfügen. Solange ein Dokument nicht genehmigt wurde, ist es nur für Personen mit der Berechtigung zum Anzeigen von Entwürfen sichtbar. Abhängig vom definierten Freigabeverfahren kann festgelegt werden, welche Personen im Freigabeprozess zu informieren sind. Diese können per E-Mail informiert werden, welche Aktivität ansteht.

Inhaltsgenehmigungen einrichten

Um den Freigabeprozess zu verwenden, müssen entsprechende Workflows erstellt und mit dem Genehmigungsprozess verknüpft werden. Insgesamt sind drei Schritte zur Einrichtung von Freigabeprozessen erforderlich:

1. Aktivieren der Inhaltsgenehmigung
2. Aktivieren der Verwaltung von Haupt- und Nebenversionen für die Bibliothek
3. Einrichten eines Workflows zum Verwalten der Inhaltsgenehmigung für eine Bibliothek

Die erforderlichen Einstellungen können in den Einstellungen der Dialogbox der Versionsverwaltung erfolgen, die in der nachstehenden Abbildung gezeigt wird.

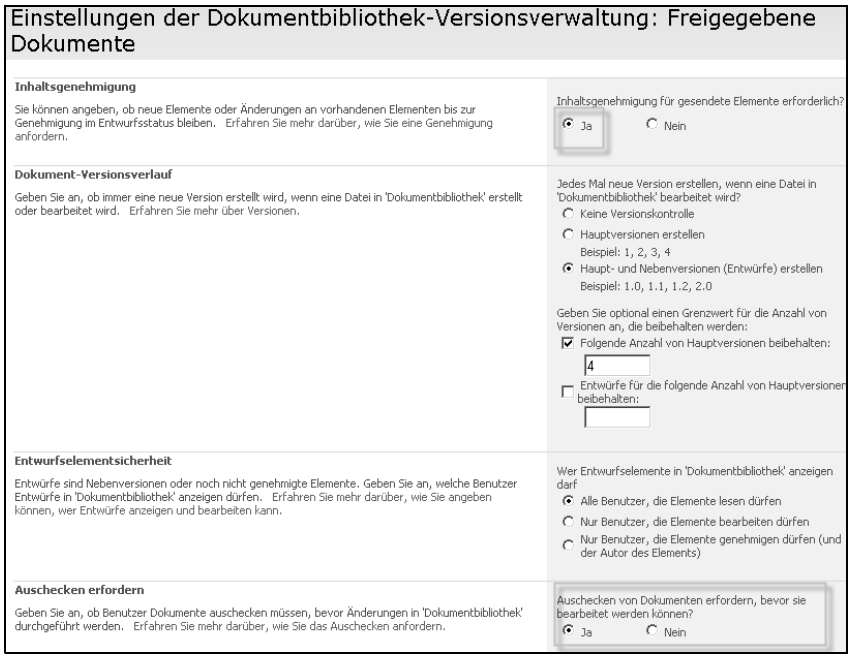


Abbildung 7.47: Die Versions- und Freigabeverwaltung kann konfiguriert werden

8 Beispiele, Muster und Checklisten für die Praxis

Dieses Kapitel liefert Beispiele, Musterdokumente und Vorlagen zu den im Buch vorgestellten Dokumenten. Die nachstehend beschriebenen Beispiele erheben nicht den Anspruch auf Vollständigkeit oder fachliche Richtigkeit, sondern dienen ausschließlich dazu die jeweiligen Dokumentationsmöglichkeiten vorzustellen und sind dahingehend optimiert.

cd-rom

Alle hier vorgestellten Beispiele und Muster befinden sich auf der beigefügten CD-ROM und können als Vorlage verwendet werden.

8.1 Beispiel – Rollenbeschreibung

Die folgende Tabelle zeigt exemplarisch ein Beispiel für die Beschreibung einer Rolle. Erläuterungen zur Nutzung von Rollenbeschreibungen finden Sie in Abschnitt 3.2.7.

Beispiel Service Desk-Koordinator

Der Service Desk wird im allgemeinen als Anlaufstelle definiert, an den sich die IT-Nutzer mit Problemen und Serviceanfragen wenden können. Der Service Desk-Koordinator stellt sicher, dass die im Rahmen des Service Desks definierten Aktivitäten durchgeführt werden. Eine Rollenbeschreibung für den Service Desk-Koordinator kann wie folgt aussehen:

Rollenbeschreibung: Service Desk-Koordinator	
Kurzbeschreibung:	Der Service Desk löst Support-Anfragen selbstständig oder koordiniert die Aktivitäten aller Beteiligten zur Service-Unterbrechungsbeseitigung. Weiter dokumentiert der Service Desk die Lösungen. Der Service Desk-Koordinator hat die Gesamtverantwortung für die definierten Service Desk-Leistungen. Er berichtet an den Service Desk-Eigner. Dieser wiederum ist zuständig für die Durchführung und Implementierung des Incident-Prozesses und die Einführung eines Service Desks. Der Service Desk-Koordinator repräsentiert und führt den Service Desk. Er ist Ansprechpartner für den operativen Betrieb aus Kundensicht.
Aufgaben/ Verantwortung:	• Gesamtverantwortung für den Service Desk • Ansprechpartner für alle Support-Themen aus dem Anwenderbereich • Ansprechpartner im Eskalationsfall • Verantwortlich für Qualitätsmanagement und Reporting • Liefert regelmäßige Statusberichte über Leistungen und Trends im Service Desk • Führt Reviews durch, welche die Effizienz und Effektivität des Service Desks periodisch untersuchen (Kostenmanagement) • Definiert und führt qualitätssichernde Maßnahmen durch • Informiert den Service Desk-Eigner über bevorstehende Maßnahmen und Aktivitäten • Verantwortlich für Ressourcen- und Infrastrukturmanagement • Organisation und Bereitstellung der notwendigen Technologien und Werkzeuge am Service Desk • Bereitstellung der benötigten Mitarbeiter und Organisation von Trainings
Befugnisse:	• Stellt die Personalplanung sicher und trägt fachliche Verantwortung für das Personal • Veranlasst Ausbildungs- und Bedarfsplanung • Führt Mitarbeiter- und Bewerbungsgespräche
Anforderungen: (technische Fähigkeiten)	• Kenntnisse über eingesetzte IT-Systeme (Hardware und Software) • Produktkenntnisse insbesondere des verwendeten Service Desk-Ticket-Systems
Anforderungen: (nicht-technische Fähigkeiten)	• Gute Kenntnisse über die IT-Infrastrukur des Unternehmens • Kundenorientierung und Kommunikationsfähigkeit • Sicheres Auftreten • Ausgeprägte Präsentationsfähigkeiten • Teamfähigkeit • Durchsetzungsvermögen • Selbständiges Arbeiten • Organisationsfähigkeit und Zeitmanagement
Unterstützung durch:	Alle Rollen aus dem Supportbereich

Tabelle 8.1: Beispiel für eine Rollenbeschreibung

8.2 Beispiel – Betriebsmatrix

Die nachstehende Tabelle zeigt beispielhaft an einem Auszug den Aufbau einer Betriebsmatrix für den IT-Betrieb.

Erläuterungen zu Nutzen und Einsatzzweck einer Betriebsmatrix finden Sie in Abschnitt 3.2.8.

Rolle	Name Rollenträger	Organisatorische Zuordnung	Anmerkungen
Rollen im Supportprozess			
Service Desk-Eigner	Mitarbeiter A	Betriebsleitung	Rollenzuständigkeit endet am 31.12.2008
Service Desk-Koordinator	Mitarbeiter B	Betriebsleitung	
Service Desk-Operator	Mitarbeiter K	Organisations-einheit XY	
Incident Analyst 1st Level	Mitarbeiter L	Organisations-einheit XY	
	Mitarbeiter M	Organisations-einheit XY	Zu 30% zugeordnet
	Mitarbeiter N	Organisations-einheit XY	
	Mitarbeiter O	Organisations-einheit XY	
Incident Analyst 2st Level	Mitarbeiter M	Organisations-einheit XY	Zu 70% zugeordnet
	N.N.	Externer Berater	
Rollen im Changemanagement-Prozess			
Changemanagement-Prozesseigner	Mitarbeiter A	Betriebsleitung	Rollenzuständigkeit endet am 31.12.2008
Changemanagement-Koordinator	Mitarbeiter C	Betriebsleitung	
Change-Implementierer	Mitarbeiter D		
	Mitarbeiter E		
	Mitarbeiter F		

Tabelle 8.2: Beispielhafter Aufbau einer Betriebsmatrix für den IT-Betrieb

8.3 Beispiel – Berechtigungsmatrix

Die folgende Tabelle zeigt eine Berechtigungsmatrix, in der beispielhaft einige administrative Tätigkeiten im Bereich der DHCP-Server-Verwaltung dargestellt sind. Gibt es beispielsweise eine Aufteilung zwischen zentraler IT und dezentralen Standorten, die von den eigenen Administratoren verwaltet werden, ist in der Regel auch die Verantwortung geteilt.

Erläuterungen zu einer Berechtigungsmatrix finden Sie in Abschnitt 4.2.2.

Berechtigungsmatrix: DHCP-Server-Verwaltung				
	Lokale Gruppe: DHCP-Administratoren	**Lokale Gruppe: DHCP-Benutzer**	**Domänen-Admins**	**Lokale Gruppe: Administratoren**
Anzeigen der DHCP-Serverdaten, einschließlich der DHCP-Serverkonfiguration	Lokaler Server	Lokaler Server	Alle DHCP-Server	Lokaler Server
Anzeigen der DHCP-Protokolldateien	Lokaler Server	Lokaler Server	Alle DHCP-Server	Lokaler Server
Erstellen und Löschen von Bereichen	Lokaler Server		Alle DHCP-Server	Lokaler erver
Ändern der Bereichskonfiguration	Lokaler Server		Alle DHCP-Server	Lokaler Server
Erstellen von Bereichsgruppierungen	Lokaler Server		Alle DHCP-Server	Lokaler Server
Verwalten von Reservierungen	Lokaler Server		Alle DHCP-Server	Lokaler Server
Änderung der DHCP Optionen	Lokaler Server		Alle DHCP-Server	Lokaler Server
Ändern der Konfiguration des DHCP-Serverdienstes			Alle DHCP-Server	Lokaler Server
Verwalten des DHCP-Servers, einschließlich des Exports und Imports der DHCP-Serverkonfiguration			Alle DHCP-Server	Lokaler Server
Ändern der DNS Konfiguration			Alle DHCP-Server	Lokaler Server
Berichten (Reporting)	Lokaler Server		Alle DHCP-Server	Lokaler Server

Tabelle 8.3: Berechtigungsmatrix zur Regelung der Verantwortlichkeiten am Beispiel der DHCP-Server-Verwaltung

In Einzelfällen kann es sinnvoll sein, für ein einzelnes Systemobjekt die Berechtigungen zu spezifizieren. Ein Beispiel für eine differenziertere Berechtigungsmatrix liefert die nachstehende Tabelle, die einen Auszug aus der zu konfigurierenden Sicherheitseinstellungen für eine neu einzurichtende Organisationseinheit (OU) zeigt.

Berechtigungsmatrix für eine neu einzurichtende Organisationseinheit (OU)			
Gruppe	**Geerbt von**	**Übernehmen für**	**Berechtigungen**
Konten-Operatoren	Explizit	Nur dieses Objekt	Computer erstellen oder löschen Benutzerkonto erstellen oder löschen Gruppen erstellen oder löschen Drucken erstellen oder löschen
Administratoren	Explizit	Dieses und alle untergeordneten Objekte	Inhalt auflisten Alle Eigenschaften lesen Alle Eigenschaften schreiben Löschen Berechtigungen lesen Berechtigungen ändern Besitzer ändern Alle erweiterten Rechte Alle untergeordneten Objekte erstellen
Authentifizierte Benutzer	Explizit	Nur dieses Objekt	Inhalt auflisten Alle Eigenschaften lesen Berechtigungen lesen
Domänen-Admins	Geerbt	Nur dieses Objekt	Vollzugriff
Organisations-Admins	Explizit	Dieses und alle untergeordneten Objekte	Vollzugriff
Exchange Enterprise-Server	Geerbt	Dieses und alle untergeordneten Objekte	Inhalt auflisten
		Benutzer-Objekte	Inhalt auflisten Alle Eigenschaften lesen Berechtigungen lesen
		Gruppen-Objekte	Inhalt aufliste Alle Eigenschaften lesen Berechtigungen lesen

Tabelle 8.4: Beispiel einer Berechtigungsmatrix für neu einzurichtende Organisationseinheiten

8.4 Beispiel – Hardware-Systemakte

Bei der folgenden Beispiel-Systemakte für ein Serversystem handelt es sich um Serverdatenblatt, das automatisiert mit dem Programm *DocuSnap* der Firma *itelio GmbH* (siehe hierzu Abschnitt 4.2.3) erstellt wurde.

Erläuterungen zum inhaltlichen Aufbau einer Systemakte finden Sie in Abschnitt 4.2.2.

Server-Datenblatt			
Stand	20.09.2008	Objektname:	2003DC.VMTestdom.de
Version	1.0	Autor:	M.Reiss
Firma	VMTESTDOM		
Dateiname	db-2003dc.doc		
Servername	2003DC		
IP-Adresse	VMware Accelerated AMD PCNet Adapter • DHCP: deaktiviert • IP: 10.50.10.50 • Subnetz:255.0.0.0 • Gateway: • DNS-Server: 127.0.0.1, 192.168.10.2 • Prim. WINS: • Sek. WINS: • MAC-Adresse: 07-5C-25-7B-C7-33		
Standort			
Installationszeitpunkt	16.05.2004		
Ansprechpartner beim Kunden, Telefonnr.			
Hersteller Typ / Modell	VMware, Inc. VMware Virtual Platform		
Seriennummer	VMware-56 44 66 79 g7fwe		
Garantie			

Hardwareausstattung	CPU Intel(R) Pentium(R) 4 CPU 3.00GHz, 2993 MHz
	RAM 252 MByte
	Pagefile C:\pagefile.sys (min. 384 MByte, max. 768 MByte)
	Laufwerke • (Removable Disk) A: • (Local Disk) C: 4087 MByte (Frei: 2184 MByte) FS: NTFS • (Compact Disk) D:
	SCSI-Controller keine Geräte registriert
	Netzwerkschnittstellen VMware Accelerated AMD PCNet Adapter (aktiviert)
	Backup-Laufwerk
BIOS	BIOS Version
	PTLTD - 6040000
	BIOS Build Number
	BIOS Release Date
	29.07.2005

Auto Update	Automatische Updates
	Automatische Updates Optionen
	Überprüfungsfrequenz
	Automatischer Neustart
	WSUS Server
Aufgabe	
Backup erfolgt durch	
Betriebssystem	Microsoft Windows Server 2003 Enterprise Edition
Service Pack	
Sprache	Deutsch
RAID-System	
Partitionen	• Datenträger Nr. 0, Partition Nr. 0 4087 MBytes • Datenträger Nr. 0, Partition Nr. 1 8 MBytes
Servermanagement	
SNMP Einstellungen	
Ereignisanzeige	• Anwendung (Max. Größe: 16384 KByte, Überschreiben: Bei Bedarf) • Sicherheit (Max. Größe: 131072 KByte, Überschreiben: Bei Bedarf) • System (Max. Größe: 16384 KByte, Überschreiben: Bei Bedarf) • DNS Server (Max. Größe: 16384 KByte, Überschreiben: Veraltet) • Verzeichnis (Max. Größe: 512 KByte, Überschreiben: Bei Bedarf) • Dateirepl. (Max. Größe: 512 KByte, Überschreiben: Bei Bedarf)
Systemfehler	Debugdatei: Vollständiges Speicherabbild, Automatischer Neustart nach Systemfehler

Installierte Software	VMware Tools, 3.00.0000, VMware, Inc. Windows Support Tools, 5.2.3790, Microsoft Corporation Acronis True Image Echo Enterprise Server, 9.5.8018, Acronis Acronis Universal Restore für Acronis True Image Echo Enterprise Server, 9.5.8018, Acronis WebFldrs, 9.00.3501, Microsoft Corporation
Installierte Hotfixes	
Redundanzen	Netzteile Lüfter Netzwerkinterfaces Festplatten/RAID externe Anschlüsse
Switchbox-Anschluss	Port-Nr. Tastenkombination
Freigaben	• ADMIN$= C:\WINDOWS • C$= C:\ • IPC$= • NETLOGON= C:\WINDOWS\SYSVOL\sysvol\VMTestdom.de\SCRIPTS • SYSVOL= C:\WINDOWS\SYSVOL\sysvol
Dienste	• Anbieter des Richtlinienergebnissatzes, nicht gestartet, Manual, LocalSystem • Anmeldedienst, gestartet, Auto, LocalSystem • Anwendungsverwaltung, nicht gestartet, Manual, LocalSystem • Arbeitsstationsdienst, gestartet, Auto, LocalSystem • Automatische Updates, gestartet, Auto, LocalSystem • Computerbrowser, gestartet, Auto, LocalSystem • Dateireplikationsdienst, gestartet, Auto, LocalSystem • DHCP-Client, gestartet, Auto, NT AUTHORITY\NetworkService • Dienst für Seriennummern der tragbaren Medien, nicht gestartet, Manual, LocalSystem • Dienst für virtuelle Datenträger (VDS), nicht gestartet, Manual, LocalSystem • Distributed Transaction Coordinator, gestartet, Auto, NT AUTHORITY\NetworkService • DNS-Client, gestartet, Auto, NT …….. …….. (Ausgabe gekürzt)
Drucker	
Druckerports	

USB-Geräte	USB-Root-Hub, (Standard-USB-Hostcontroller), OK, usbhub
Lokale Benutzer	• Administrator • Gast
Lokale Gruppen	• Administratoren • Benutzer • DHCP-Administratoren • DHCP-Benutzer • Gäste • Hauptbenutzer • Replikations-Operator • Sicherungs-Operatoren • WINS-Benutzer
Zeitzone	GMT +02:00
Freier physik. Speicher	108,34 MB
Freier Platz in Pagefile	481,57 MB
Freier virtueller Speicher	589,91 MB
Organisation	IT Training & Consulting
Windows-Verzeichnis	C:\WINDOWS
Lizenzkey Betriebssystem	PTGGGFZ- 6040000
Debuginfo speichern	Vollständiges Speicherabbild
Verzeichnis Speicherabb.	C:\WINDOWS\Minidump
Dateien überschreiben	ja
Remote Desktop	nicht aktiviert
Besonderheiten	
Benutzerdefinierte Werte der Datenbank	

8.5 Beispiel – Prozessbeschreibung

Das nachfolgende Kapitel zeigt eine Muster-Prozessbeschreibung am Beispiel: *Umzug eines IT-Mitarbeiters.* Ein bislang in einer Außenstelle eingesetzter IT-Mitarbeiter wechselt hierbei in die Zentrale des für das Unternehmen zuständigen IT-Betriebs. Die Personalabteilung teilt dies in einem Änderungsformular der Verwaltungsstelle des IT-Betriebs mit. Damit wird in der IT-Abteilung der genannte Prozess ausgelöst.

Die nachstehenden Beispiele dienen der Ergänzung der in Abschnitt 4.3.3 vorgestellten Anleitung zur Erstellung einer Prozessbeschreibung.

achtung

In der Praxis ist für den betrachteten Beispiel-Prozess selbstverständlich die individuelle Quell- und Zielumgebung des Unternehmens prozessbestimmend. Verfügen beispielsweise die dezentralen Stellen über eigene Domänen, sieht der Prozess anders aus, als in Fällen in denen die zentrale IT und die dezentralen Stellen lediglich als eigene Organisationseinheiten (OUs) abgebildet werden und bereits in einem gemeinsamen Exchange-Namensraum verwaltet werden.

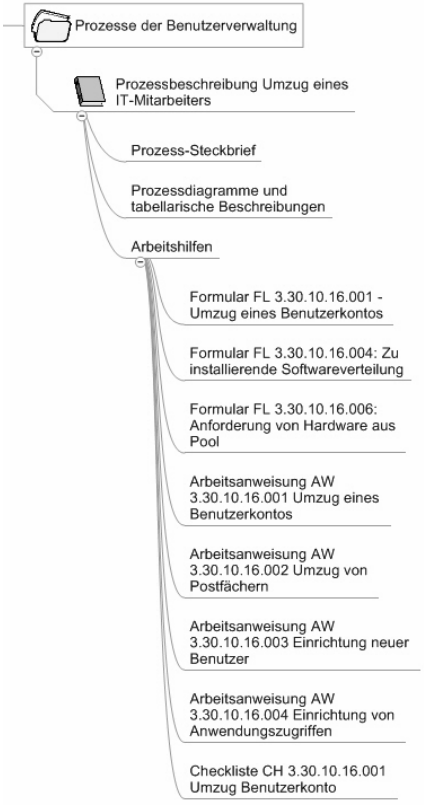


Abbildung 8.1: Struktur der Prozessbeschreibung des Beispielprozesses

8.5.1 Prozesssteckbrief

Wie in Abschnitt 4.3.3.1 beschrieben, ist es erforderlich, für jeden Prozess einen Prozesssteckbrief zu führen. Aus der folgenden Tabelle lassen sich die Struktur sowie wesentliche Inhalte eines Steckbriefes ableiten.

Prozesssteckbrief			
Prozessname	IT-Mitarbeiter umziehen	**Prozess-Nr.**	3.30.10.16.
Kurzbeschreibung	Die Personalabteilung beauftragt den Wechsel des IT-Mitarbeiters in die Zentrale.		
Prozessziel	Ziel ist, dass ein umziehenden IT-Mitarbeiter mit Beginn der neuen Tätigkeit über alle erforderlichen Ressourcen und Zugriffe am neuen Arbeitsplatz verfügt.		
Rollen			
Prozessverantwortlicher		**Prozessteam (Rollen)**	
Prozesseigner: Leiter IT-Verwaltung		Active Directory-Administrator Exchange-Administrator Clientsupport-Mitarbeiter Mitarbeiter IT-Verwaltung	
Prozessinput (Daten/Dokumente)	Anforderungsformular der Personalabteilung. Dieses regelt, welche Rollen der Mitarbeiter behält, welche er nicht mehr benötigt und welche er zusätzlich erhalten soll.		
Prozessoutput (Daten/Dokumente)	Checklisten		
Prozessauslösendes Ereignis	Die IT-Verwaltung erhält von der Personalabteilung den Auftrag für den Umzug eines IT-Mitarbeiters		
Schnittstellen zu anderen Prozessen	Facility-Managementprozess Konfigurationsmanagementprozess		
Risiken und Gefahren	Die Genehmigung zur Einrichtung der Rechte liegt zum angegebenen Termin nicht vor Der Rechner wird nicht rechtzeitig geliefert. Der Umzug des Arbeitsplatzes kann nicht zum genannten Termin erfolgen.		
Prozesskennzahlen Messgrößen	Der Termin wird um maximal einen Tag nicht überschritten.		
Prozess freigegeben am	12.11.2007	**Freigegeben durch**	Prozesseigner
Prozessbewertung durch	Qualitätsmanager	**Termin/Turnus**	01.11.2008

Prozesssteckbrief	
Arbeitshilfen	Formular FL 3.30.10.16.001: Umzug eines Benutzerkontos Formular FL 3.30.10.16.004: Zu installierende Softwareverteilung Formular FL 3.30.10.16.006: Anforderung von Hardware aus Pool Arbeitsanweisung AW 3.30.10.16.001 Umzug eines Benutzerkontos Arbeitsanweisung AW 3.30.10.16.002 Umzug von Postfächern Arbeitsanweisung AW 3.30.10.16.003 Einrichtung neuer Benutzer Arbeitsanweisung AW 3.30.10.16.002 Einrichtung von Anwendungszugriffen Checkliste CH 3.30.10.16.001

Tabelle 8.5: Prozesssteckbrief für den Beispielprozess „Umzug eines IT-Mitarbeiters“

Prozessnummerierung

Im Beispiel trägt der Prozess die Nummer 3.30.10.16. Wie beschrieben, sollte jeder Prozess eine eindeutige Nummer haben, die es beispielsweise ermöglicht in unterschiedlichen Dokumenten auf den Prozess zu referenzieren. Die Auflistung aller unternehmensweiten Prozesse kann grafisch in einer Prozesslandkarte mit einer unternehmensweit durchgängigen Prozessnummerierung und der Darstellung der Abhängigkeiten erfolgen. Wenn überhaupt eine Prozesslandkarte gepflegt wird, zeigt diese aber meist nur die Kernprozesse. Häufiger werden die Prozesse mit einer hierarchischen Notation in einer Tabelle gelistet.

Die nachfolgende Tabelle zeigt exemplarisch, wie eine solche Prozessnummerierung aussehen kann. Auch wenn die Nummerierung recht komplex wirkt, ist sie in der Praxis einfach umzusetzen, da den Verantwortlichen für übergeordnete Prozesskategorien (zum Bespiel für den IT-Betrieb) die Verantwortung für die Vergabe der untergeordneten Prozessnummern übertragen werden kann.

Prozessnummer	Prozesskategorie/Prozess (ganz oder teilweise ausgelagerte Prozesse)
1	**Managementprozesse**
1.10	Unternehmensziele
1.20	Organisation
1.20.10	Prozesse der Aufbauorganisation (z. B. Stellvertretungen)
1.20.20	Prozesse der Ablauforganisation (Prozessarchitektur und Aufbau des Management-Systems)
1.20.30	Informations- und Kommunikationsprozesse (intern, extern)
1.20.40	Grundlegende Prozesse der Dokumenten- und Datenlenkung, (Dokumentationsstruktur, Nachvollziehbarkeit, Archivierung, Datenschutz)
1.30	Unternehmensplanung (Budgetierung)

Prozessnummer	Prozesskategorie/Prozess (ganz oder teilweise ausgelagerte Prozesse)
1.40	Projektmanagement
2	**Kernprozesse**
2.10	Auftragsbearbeitung
2.10.10	Auftragseingang
2.10.20	Auftragserfassung
2.10.30	Auftragsabwicklung
2.10.40	*Versand*
2.20	Kundenbeziehungsprozesse
2.20.10	Marketing / Außendienst (Verkauf)
2.20.20	Kundenbindung
2.30.40	*E-Business*
2.30	….
3	**Serviceprozesse**
3.10	Personalwesen
3.10.10	….
3.20	…
3.30	**IT**
3.30.10	Betriebsprozesse
3.30.10.1	…
3.30.10….	…
3.30.10.16	Umzug eines IT-Mitarbeiters
3.30.20	Notfallprozesse

Tabelle 8.6: Beispiel für eine unternehmensweite Nummerierung von Prozessen

8.5.2 Prozessdiagramme und tabellarische Beschreibungen

Gemäß den Empfehlungen in Abschnitt 4.3.3.2 wird für den Prozessablauf die EPK-Notation verwendet, während die Arbeitsabläufe als Flussdiagramme dargestellt werden.

cd-rom

Auf der beigefügten CD-ROM finden Sie alle Prozessdiagramme als verlinkte HTML-Dokumentation. Alle Prozesse und Arbeitsabläufe wurden mit dem Programm SemTalk der Firma Semtation erstellt (siehe Abschnitt 4.3.4).

8.5.2.1 Beispiel: Hauptprozess „Umzug eines IT-Mitarbeiters"

Das nachstehende Diagramm zeigt den formalen Prozessablauf.

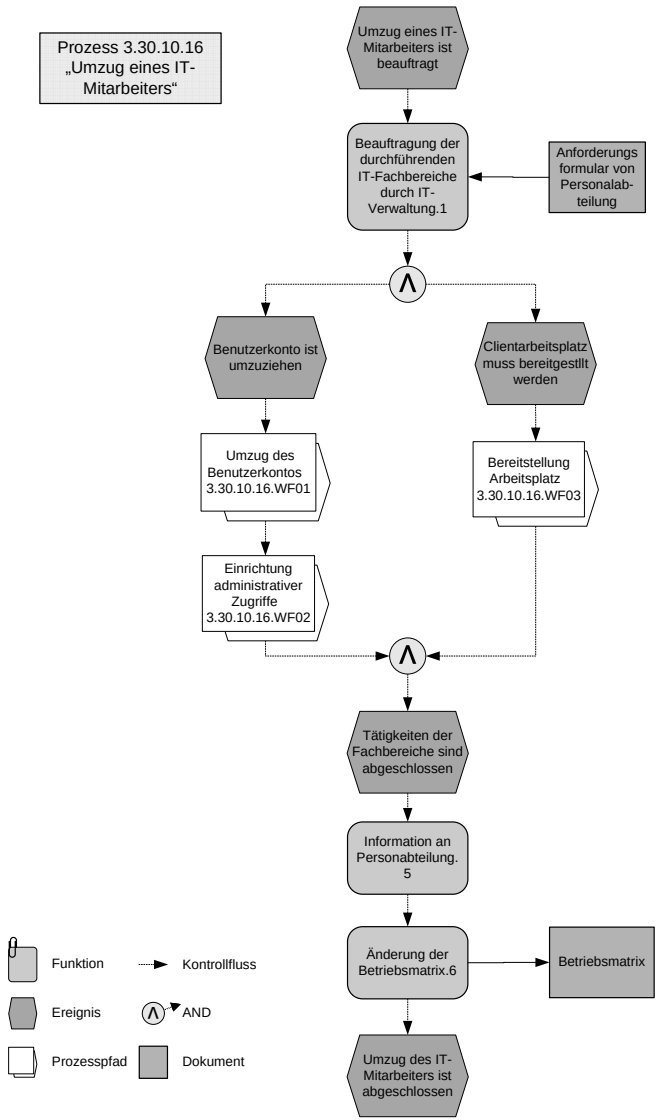


Abbildung 8.2: Hauptprozess des Beispielprozesses „Umzug eines IT-Mitarbeiters"

Tabellarische Prozessbeschreibung

Zusätzlich zur Diagrammdarstellung sollten alle Prozesse und Arbeitsabläufe in tabellarischer Form erläutert werden. Die nachstehende Tabelle zeigt hierfür wiederum ein Beispiel.

Hauptprozess: Umzug eines IT-Mitarbeiters - Prozessnummer 3.30.10.16			
Prozessschritt	**Bearbeiter**	**Aktivität**	**Anmerkungen**
1-Delegation der Aufgaben an Verantwortliche	IT-Verwaltung	Beauftragung der zuständigen Organisationseinheit mit dem Umzug des Benutzerkontos und der Einrichtung des Clientarbeitsplatzes.	Anforderungsformular der Personalabteilung
2-Arbeitsablauf 3.30.10.16.01 Umzug des Benutzerkontos	Zuständige Organisationseinheit	Dieser Teilprozess steuert den Umzug des Benutzerkontos einschließlich Postfachänderungen, Anpassung der Zugriffsberechtigungen und Datenübernahme. In diesem Prozess erfolgt noch keine Einrichtung administrativer Rollen.	
3-Arbeitsablauf 3.30.10.16.03 Einrichtung der administrativen Zugriffe	Zuständige Organisationseinheit	Nach gesonderter Freigabe erfolgt die Einrichtung administrativer Rollen (Gruppenzugehörigkeiten und Zugriffsberechtigungen).	
4-Arbeitsablauf 3.30.10.16.02 Bereitstellung des Clientarbeits-platzes	Zuständige Organisationseinheit	Der Teilprozess steuert die Einrichtung des Client-Arbeitsplatzes und initiiert im Falle des notwendigen Umzugs von Hardware den entsprechenden Teilprozess.	
5-Information an beauftragende Stelle	IT-Verwaltung	Nach Abschluss aller Teilprozesse ist die Personalabteilung über den Prozessabschluss zu informieren.	
6-Anpassung der Betriebmatrix	IT-Verwaltung	Rollen, die der neue IT-Mitarbeiter im IT-Betrieb übernimmt, werden in der Betriebsmatrix angepasst. Die Betriebsmatrix definiert die organisatorische Platzierung der Aufgaben und Rollen.	IT-Betriebsmatrix

Tabelle 8.7: Beschreibung des Hauptprozesses des Beispielprozesses „Umzug eines IT-Mitarbeiters“

8.5.2.2 Beispiel: Arbeitsablauf „Umzug und Anpassung des Benutzerkontos"

Die folgende Abbildung zeigt den ersten von drei Arbeitsabläufen in Flussdiagrammdarstellung. Diese beschreibt die erforderlichen Anpassungen des Benutzerkontos.

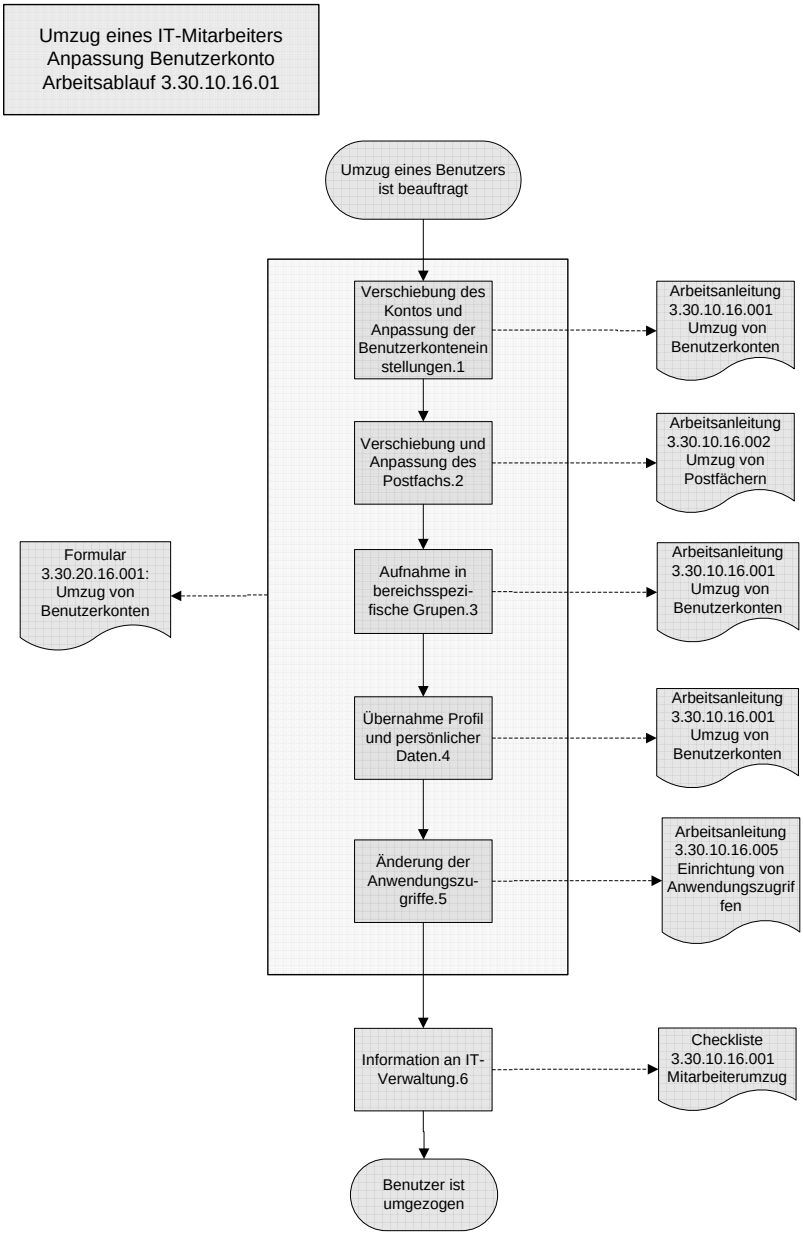


Abbildung 8.3: Arbeitsablauf „Umzug und Anpassung des Benutzerkontos"

Auch die Arbeitsabläufe sollten zusätzlich in einer Tabelle erläutert werden. Da bei den Arbeitsabläufen die operativen Tätigkeiten im Vordergrund stehen, ist auch die Erläuterung in den Tabellen an den Anforderungen der Prozessausführenden auszurichten. So ist beispielsweise hier der Verweis auf die entsprechenden Arbeitshilfen wichtig. Die nachstehende Tabelle zeigt hierfür wiederum ein Beispiel.

Umzug und Anpassung des Benutzerkontos - Arbeitsablauf 3.30.10.16.01

Arbeitsschritt	Bearbeiter	Aktivität	Arbeitshilfe
1-Verschiebung des Kontos und Anpassung der Benutzerkonteneinstellungen.1	zuständige Organisationseinheit	Das Benutzerkonto wird in die Organisationseinheit ZentraleIT verschoben, und die Kontoeinstellungen werden geändert. Damit erhält der Benutzer alle OU-spezifischen Berechtigungen und Einstellungen. Im Einzelfall kann es erforderlich bzw. gewünscht sein, zusätzlich ein lokales Benutzerkonto nicht zu verschieben, sondern neu in der OU ZentraleIT einzurichten.	*Formular FL 3.30.10.16.001: Umzug eines Benutzerkontos* Das Formular erhält alle benutzerspezifischen Anforderungen des umzuziehenden Benutzers. Es dient gleichzeitig als Nachweis und wird in die Dokumentation übernommen. *Arbeitsanweisung AW 3.30.10.16.001 zur Durchführung des Umzugs von Benutzern*. Diese enthält genaue Beschreibungen der durchzuführenden Tätigkeiten einschließlich Schritt-für-Schritt-Anleitungen. Ist eine Neueinrichtung des Benutzerkontos erforderlich, ist die *Arbeitsanweisung AW 3.30.10.16.003 zur Einrichtung neuer Benutzer zu verwenden.*
2-Verschiebung und Anpassung des Postfachs	zuständige Organisationseinheit	Das Postfach des Benutzers ist in die Speichergruppe der zentralen IT zu verschieben. Die Postfachinformationen sind dementsprechend zu konfigurieren.	Formular *FL 3.30.10.16.002: Umzug eines Benutzerkontos* und *Arbeitsanweisung AW 3.30.10.16.002 zur Durchführung des Umzugs von Benutzerpostfächern*
3-Aufnahme in bereichsspezifische Gruppen	zuständige Organisationseinheit	Aufnahme des Benutzers in die allgemeinen Gruppen für den IT-Betrieb	Formular *FL 3.30.10.16.001: Umzug eines Benutzerkontos* und *Arbeitsanweisung zur Durchführung des Umzugs von Benutzern*

Umzug und Anpassung des Benutzerkontos - Arbeitsablauf 3.30.10.16.01			
Arbeitsschritt	**Bearbeiter**	**Aktivität**	**Arbeitshilfe**
4-Übernahme Benutzerprofil und persönlicher Daten	zuständige Organisationseinheit	Das servergespeicherte Benutzerprofil ist auf den von der Zentrale IT verwalteten Server umzuziehen. Die Inhalte des persönlichen Ordners sowie gegebenenfalls PST-Dateien werden übernommen.	*Formular FL 3.30.10.16.001: Umzug eines Benutzerkontos* und *Arbeitsanweisung AW 3.30.10.16.001 zur Durchführung des Umzugs von Benutzern*
5-Änderung der Anwendungszugriffe	zuständige Organisationseinheit	Bei Anwendungen, die über eigene Benutzerverwaltungen verfügen, sind die Zugriffe mit Hilfe der entsprechenden Schnittstellen zu konfigurieren.	*Formular FL 3.30.10.16.001: Umzug eines Benutzerkontos* und *Arbeitsanweisung AW 3.30.10.16.005 zur Einrichtung von Anwendungszugriffen*
6-Information an IT-Verwaltung.	IT-Verwaltung	Nach Abschluss der Tätigkeiten des Teilprozesses ist die IT-Verwaltung über den Abschluss zu informieren. Hierzu ist der IT-Verwaltung die ausgefüllte Checkliste zu übergeben.	*Checkliste CH 3.30.10.16.001: Umzug eines Benutzerkontos*

Tabelle 8.8: Beschreibung „Umzug und Anpassung des Benutzerkontos“

hinweis

Die Auswahl der in der Tabelle zu beschreibenden Parameter ist bei Bedarf zu erweitern. So kann es insbesondere bei der Beschreibung der Arbeitsabläufe sinnvoll sein, zusätzlich noch das geforderte Ergebnis oder den Auslöser für den jeweiligen Arbeitsschritt zu dokumentieren.

Die beiden folgenden Arbeitsabläufe zur Einrichtung eines Client-Arbeitsplatzes und zur Einrichtung der administrativen Zugriffe werden der Vollständigkeit halber im Folgenden ebenfalls dargestellt Auf eine detaillierte Beschreibung in tabellarischer Form wird aber verzichtet.

8.5.2.3 Beispiel: Arbeitsablauf „Bereitstellung eines Client-Arbeitsplatzes"

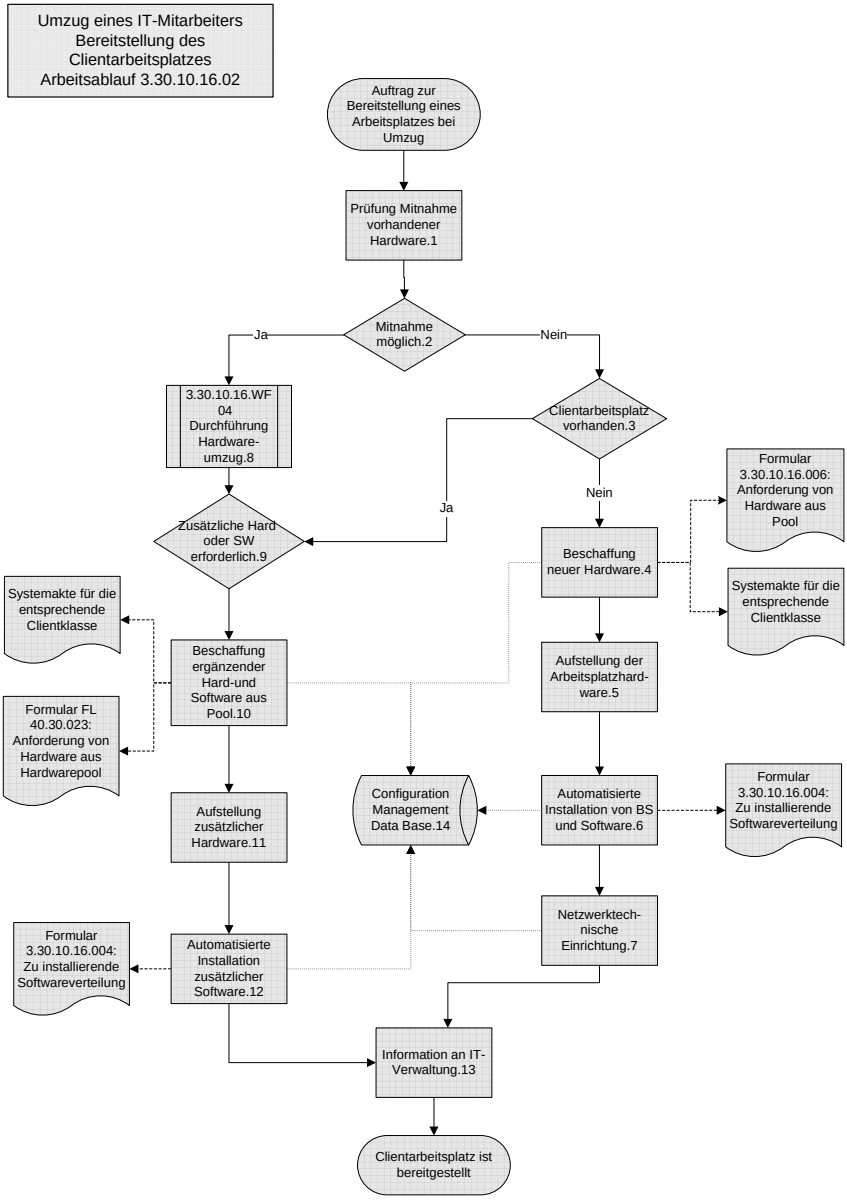


Abbildung 8.4: Der Arbeitsablauf „Bereitstellung eines Client-Arbeitsplatzes" in Flussdiagrammdarstellung

8.5.2.4 Beispiel: Arbeitsablauf „Einrichtung der administrativen Zugriffe"

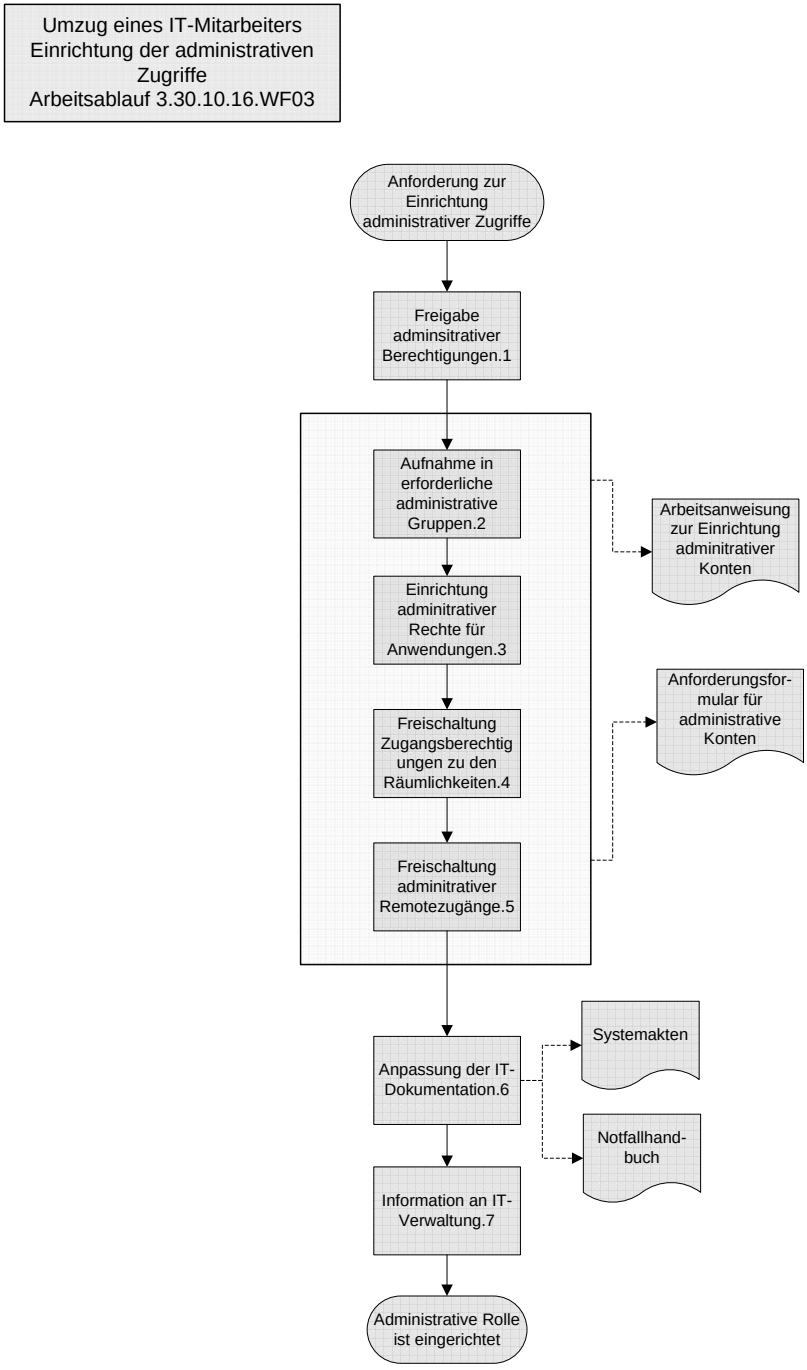


Abbildung 8.5: Arbeitsablauf „Umzug eines IT-Mitarbeiters""

8.5.3 Arbeitshilfen

Das nachstehende Kapitel zeigt Beispiele für die im Prozess benannten Arbeitshilfen

8.5.3.1 Arbeitsanweisung zum Erstellen neuer Benutzerkonten

Die folgende Arbeitsweise ist eine knapp gehaltene Anweisung, die sich eher an erfahrende Administratoren wendet. Zur Verdeutlichung kann die Anweisung durch Abbildungen der entsprechenden Dialogboxen ergänzt werden (siehe hierzu Abschnitt 4.3.3.3).

Die Einrichtung eines neuen Benutzers erfolgt im BENUTZERMANAGER FÜR DOMÄNEN. Im Einzelnen ist folgendermaßen vorzugehen:

1. *Ein neues Benutzerkonto anlegen (im Menü BENUTZER die Option NEUER BENUTZER verwenden)*
2. *Benutzername vergeben (siehe Formular FL 3.30.10.16.002). Der Benutzername muss den Namenskonventionen entsprechen. Siehe hierzu Dokument „Namenskonventionen“*
3. *Alle Benutzereigenschaften gemäß Formular FL 3.30.10.16.002 eintragen*
4. *Startkennwort eintragen. Das Startkennwort für die Domäne BEISPIELFIRMA ist: START123*
5. *Die Option BENUTZER MUSS KENNWORT BEI DER NÄCHSTEN ANMELDUNG ÄNDERN ist standardmäßig aktiviert. Diese Option ist nur in Ausnahmefällen zu deaktivieren (beispielsweise bei der Erstellung von systembezogenen Konten).*
6. *Die Gruppenzugehörigkeit festlegen (siehe Formular FL 3.30.10.16.002). Standardmäßig ist der neue Benutzer Mitglied der Gruppe „Domänenbenutzer“.*
7. *Abhängig von der Zugehörigkeit zu einer Abteilung, ist die Mitgliedschaft in der entsprechenden Gruppe Abtxxxxxx bzw. Refxxxxxx einzutragen. Standard-Domänenbenutzer müssen der Gruppe „Zertifikatsbenutzer“ hinzugefügt werden*
8. *Umgebungsprofil für den neuen Benutzer einrichten, Pfad für Benutzerprofil festlegen. Speicherort für die Profile sind die jeweiligen Basisverzeichnisse der Benutzer. Siehe Formular FL 3.30.10.16.002.*

Das Logon-Skript gemäß Formular FL 3.30.10.16.002 eintragen. Standard-Domänenbenutzer erhalten kein Logon-Skript.

Weitere Benutzerbeschränkungen sind zurzeit nicht vorgesehen. Bei den Optionen ZEITEN, ANMELDEN AN, KONTO und RAS sind die Standardeinstellungen zu übernehmen.

8.5.3.2 Formular: Mitarbeiterumzug

Eine gute Unterstützung können Formulare bieten. Das Beispielformular enthält alle Informationen, die der Mitarbeiter für die Einrichtung des Benutzerkontos benötigt.

FL 3.30.10.16.002 – Umzug eines Benutzers		
Objekteigenschaften		**Anmerkung**
Allgemeine Benutzerkonteninformationen		
Vorname	Gabi	Keine Änderung
Nachname	Muster	Keine Änderung
Titel	Dr.	Keine Änderung
Anzeigename	Muster, Gabi	Keine Änderung
Beschreibung	Mitarbeiter(in) zentraler IT-Betrieb	
Büro	Haupthaus, Zimmer 5, 4.Stock	
E-Mail	Gabi.Muster@beispielfirma.de	
Organisationseinheit (OU)	ITZentrale	
Domäne	Beispielfirma.de	
Abteilung	Zentraler IT-Betrieb	
Position	Administrator	
Strasse	Schubertstraße 5	
Postleitzahl	63528	
Benutzeranmeldename	Gabi.Muster@beispielfirma.de	
Benutzeranmeldename (Pre-Windows 2000)	Gabi.muster	
Telefonnummer	06045 1234567-8	
Handy-Nummer		Keine Änderung
Faxnummer	06045 1234567-9	
Private Telefonnummer		Keine Änderung
Profilpfad	\\beispielsrv\profile$\ gabi.muster$	
Anmeldeskript		Bestehendes Anmeldeskript löschen, OU-Anmeldeskript verwenden
Basislaufwerk	\\beispielsrv\basis\ gabi.muster	

Gruppenmitgliedschaften (Active Directory und Anwendungen)		
Active Directory-Gruppen, in die der Benutzer aufgenommen werden muss		
Active Directory-Gruppen, aus denen der Benutzer entfernt werden muss		
Anwendungen, für die der Benutzer Zugriffe benötigt (Gruppen, in die der Anwender aufzunehmen ist)	Anwendung und erforderliche Rechte	
Postfachinformationen		
Postfach		Keine Änderung
Abweichender Anzeigename		Keine Änderung
E-Mail-Adressen	FAX: 12345 SMTP: gabi.muster@beispiel-firma.de	X400-Adresse hinzufügen. Andere Adressen: keine Änderung
Terminalserverprofil		
Terminalserver: Benutzerprofil	\\terminalsrv\profile$\ gabi.muster$	
Terminalserver: Homelaufwerk	\\terminalsrv\basis$\ gabi.muster$	
Umzuziehende Daten		
Datei oder Ordner	Von	Nach
Einstellungen für sicherheitskritische Sicherheits- und Verteilergruppen (Zuweisen von Administratorrechten)		
Administratorengruppen, aus denen das Benutzerkonto entfernt werden muss		
Administratorengruppen, in die der Benutzer aufgenommen werden muss		
Freigabe der Administratorrechte	Freigegeben von	Am

Tabelle 8.9: Beispielformular: Umzug und Anpassung des Benutzerkontos

8.5.3.3 Checkliste: Mitarbeiterumzug

Eine Checkliste ist hilfreich, da in ihr alle erledigten Arbeiten abgehakt werden können und damit deren Erledigung sicher gestellt wird. Gleichzeitig können Checklisten als Arbeitsnachweis dienen und der betreffenden Organisationseinheit zur Unterschrift vorgelegt werden.

Checkliste CH 3.30.10.16.001 - Mitarbeiterumzug	
Aktivität	**Erledigt**
Das Benutzerkonto wurde umgezogen.	☐
Die Kontoinformationen wurden angepasst.	☐
Die Postfachinformationen wurden geändert.	☐
Das Terminalserverprofil wurde angepasst.	☐
Die persönlichen Daten des Benutzers wurden umgezogen.	☐
Das Benutzerkonto wurde aus nicht mehr benötigten Sicherheits- und Verteilergruppen entfernt.	☐
Das Benutzerkonto wurde in die erforderlichen Sicherheits- und Verteilergruppen aufgenommen.	☐
Das Benutzerkonto wurde aus nicht mehr benötigten Administratorengruppen entfernt.	☐
Das Benutzerkonto wurde in die erforderlichen Administratorengruppen aufgenommen.	☐
Zusätzlich benötigte Rechte wurden erteilt.	☐

Tabelle 8.10: Beispiel-Checkliste: Umzug und Anpassung des Benutzerkontos

8.6 Muster – Basisdokumentvorlage

Dieses Kapitel zeigt den formalen Aufbau eines Dokuments an Beispielen. Dieses kann als Muster unabhängig von der verwenden Dokumentenklasse verwendet werden. Informationen, die aus Feldfunktionen stammen sind grau unterlegt. Die Gliederung der Dokumente im Detail ist von der jeweiligen Dokumentenklasse abhängig und kann durch spezielle Dokumentvorlagen vorgegeben werden. In Abschnitt 7.1.2.1 finden Sie Erläuterungen zu den nachstehend gezeigten Komponenten der Beispieldokumentvorlage.

cd-rom

Auf der beigefügten CD-ROM befindet sich die im folgenden vorgestellte Dokumentvorlagendatei. Sie kann als Muster-Dokumentvorlage verwendet und angepasst werden.

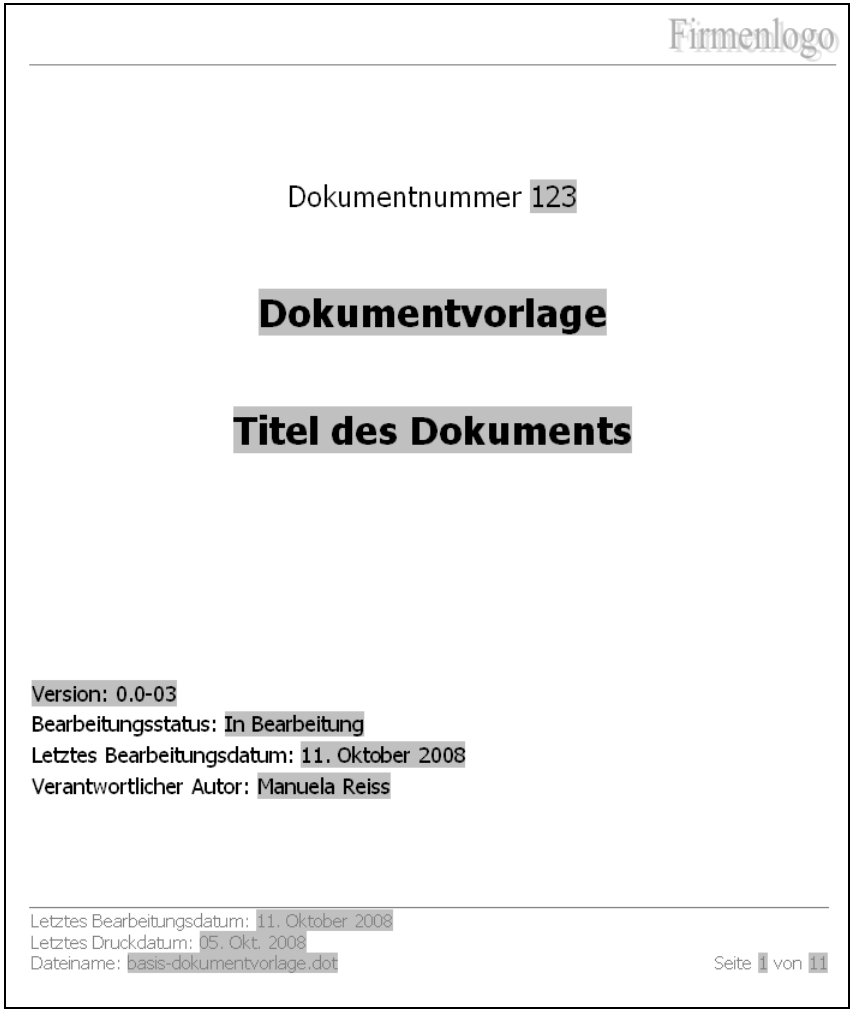
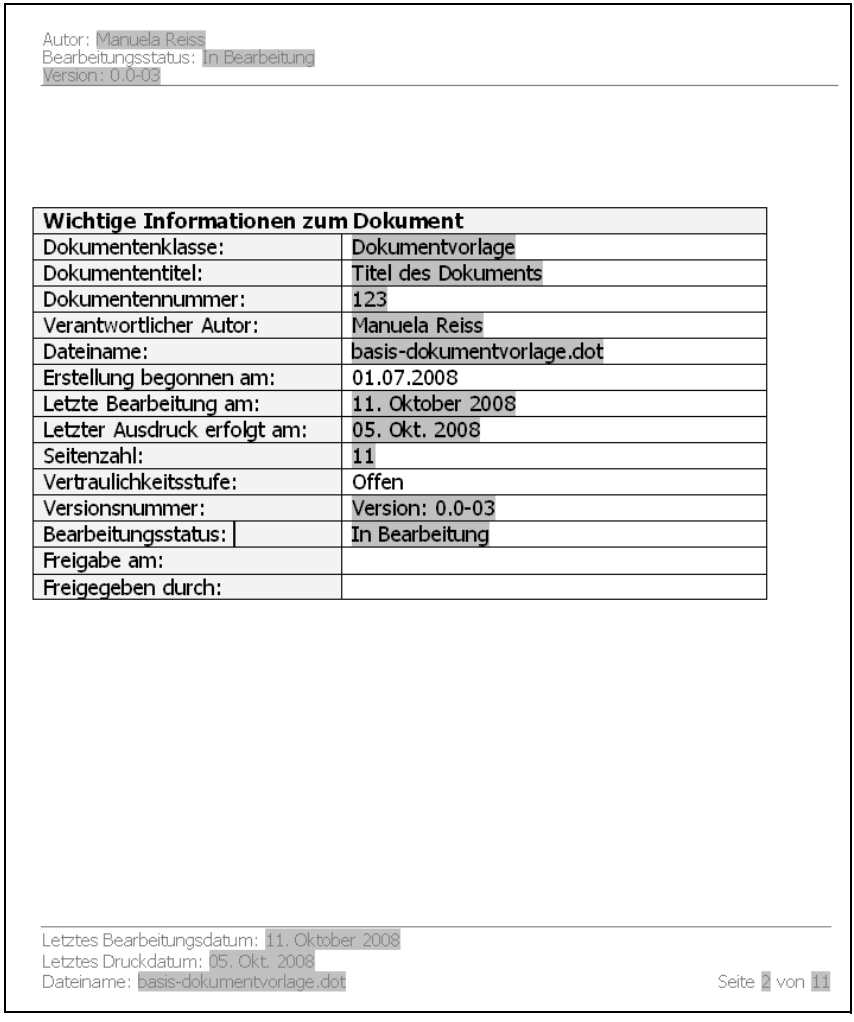


Abbildung 8.6: Muster-Dokumentvorlage: Deckblatt


Autor: Manuela Reiss
Bearbeitungsstatus: In Bearbeitung
Version: 0.0-03

Wichtige Informationen zum Dokument	
Dokumentenklasse:	Dokumentvorlage
Dokumententitel:	Titel des Dokuments
Dokumentennummer:	123
Verantwortlicher Autor:	Manuela Reiss
Dateiname:	basis-dokumentvorlage.dot
Erstellung begonnen am:	01.07.2008
Letzte Bearbeitung am:	11. Oktober 2008
Letzter Ausdruck erfolgt am:	05. Okt. 2008
Seitenzahl:	11
Vertraulichkeitsstufe:	Offen
Versionsnummer:	Version: 0.0-03
Bearbeitungsstatus:	In Bearbeitung
Freigabe am:	
Freigegeben durch:	

Letztes Bearbeitungsdatum: 11. Oktober 2008
Letztes Druckdatum: 05. Okt. 2008
Dateiname: basis-dokumentvorlage.dot Seite 2 von 11

Abbildung 8.7: Muster-Dokumentvorlage: Dokumentinfobox

Autor: Manuela Reiss
Bearbeitungsstatus: In Bearbeitung
Version: 0.0-03

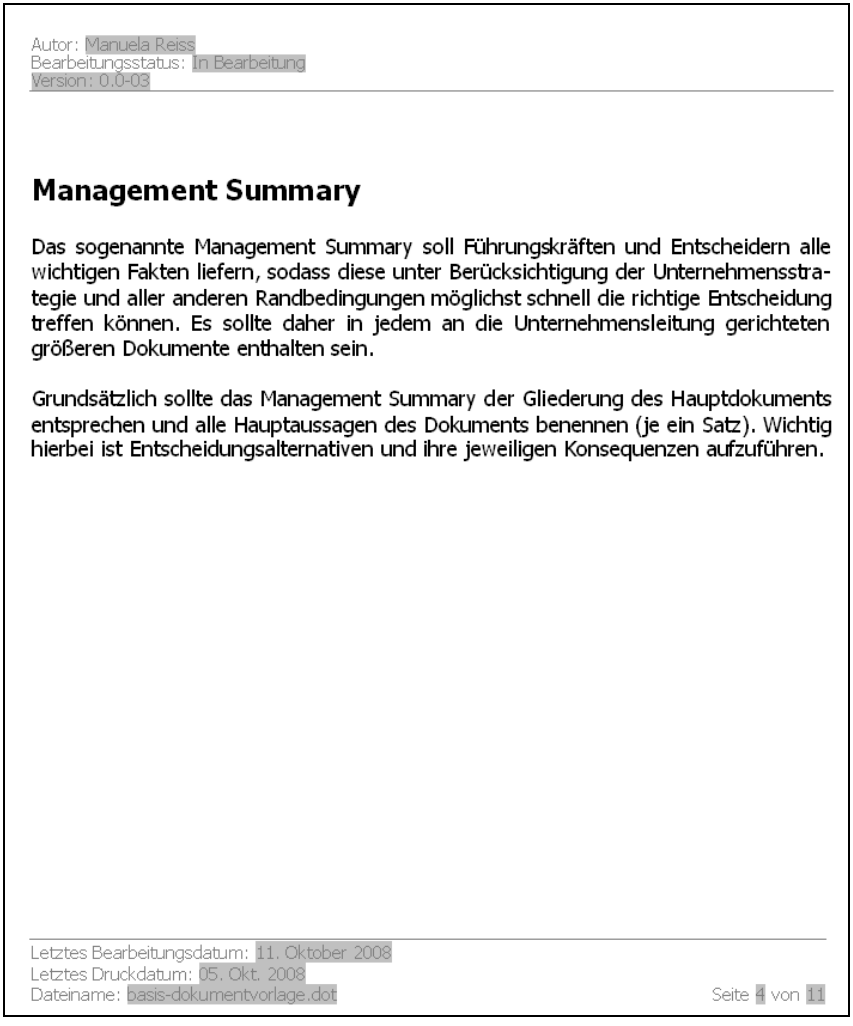
Änderungsnachweis				
Versions-nummer	Bearbeitungs-status	Datum	Bearbeiter	Änderung / Bemerkung

Ergänzende Dokumente/Mitgeltende Unterlagen*				
Dokumen-tennummer	Dokumentenklasse und Titel des Doku-ments	Version	Datum letz-ter Bearbei-tung	Verantwortlicher Autor

* In der Tabelle sind alle Dokumente einzutragen, die für dieses Dokument Gültigkeit besitzen, die aber im Dokument nicht explizit genannt werden (beispielsweise Namenskonventionen). Einzutragen sind auch alle Dokumente, auf die im nachfolgenden Dokument explizit verwiesen wird·

Letztes Bearbeitungsdatum: 11. Oktober 2008
Letztes Druckdatum: 05. Okt. 2008
Dateiname: basis-dokumentvorlage.dot Seite 3 von 11

Abbildung 8.8: Muster-Dokumentvorlage: Änderungsnachweis und mitgeltende Dokumente


Autor: Manuela Reiss
Bearbeitungsstatus: In Bearbeitung
Version: 0.0-03

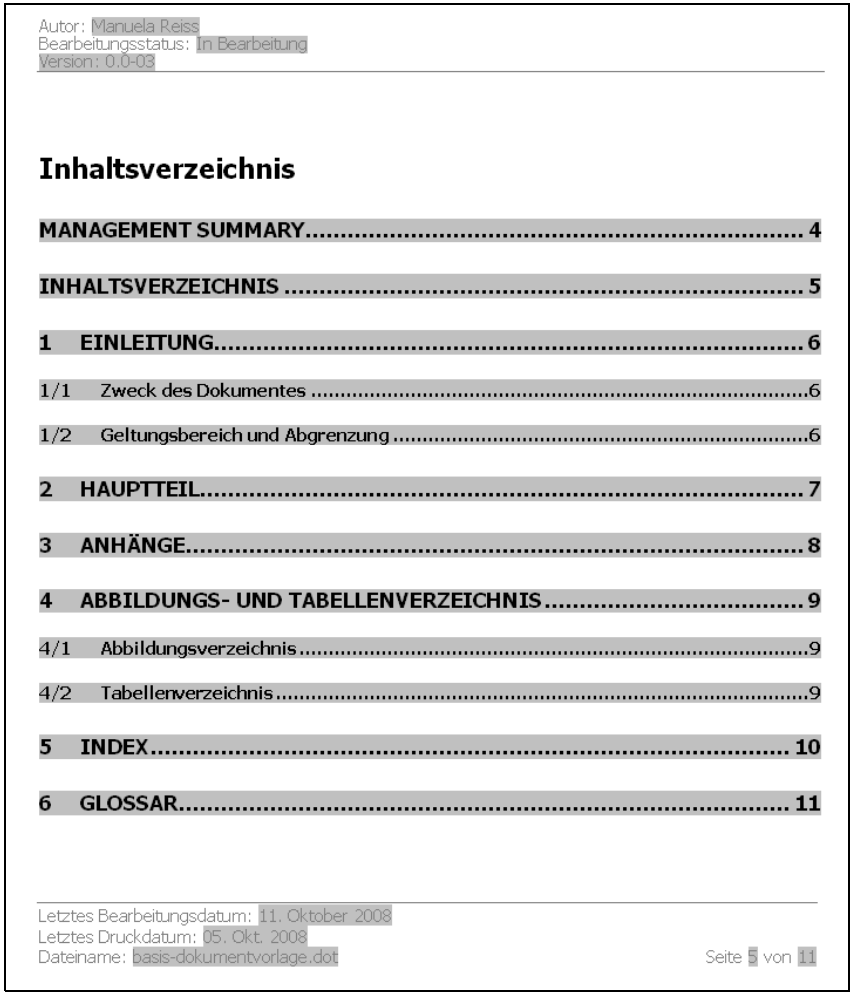
Management Summary

Das sogenannte Management Summary soll Führungskräften und Entscheidern alle wichtigen Fakten liefern, sodass diese unter Berücksichtigung der Unternehmensstrategie und aller anderen Randbedingungen möglichst schnell die richtige Entscheidung treffen können. Es sollte daher in jedem an die Unternehmensleitung gerichteten größeren Dokumente enthalten sein.

Grundsätzlich sollte das Management Summary der Gliederung des Hauptdokuments entsprechen und alle Hauptaussagen des Dokuments benennen (je ein Satz). Wichtig hierbei ist Entscheidungsalternativen und ihre jeweiligen Konsequenzen aufzuführen.

Letztes Bearbeitungsdatum: 11. Oktober 2008
Letztes Druckdatum: 05. Okt. 2008
Dateiname: basis-dokumentvorlage.dot Seite 4 von 11

Abbildung 8.9: Muster-Dokumentvorlage: Management Summary



Autor: Manuela Reiss
Bearbeitungsstatus: In Bearbeitung
Version: 0.0-03

Inhaltsverzeichnis

Letztes Bearbeitungsdatum: 11. Oktober 2008
Letztes Druckdatum: 05. Okt. 2008
Dateiname: basis-dokumentvorlage.dot Seite 5 von 11

Abbildung 8.10: Muster-Dokumentvorlage: Inhaltsverzeichnis

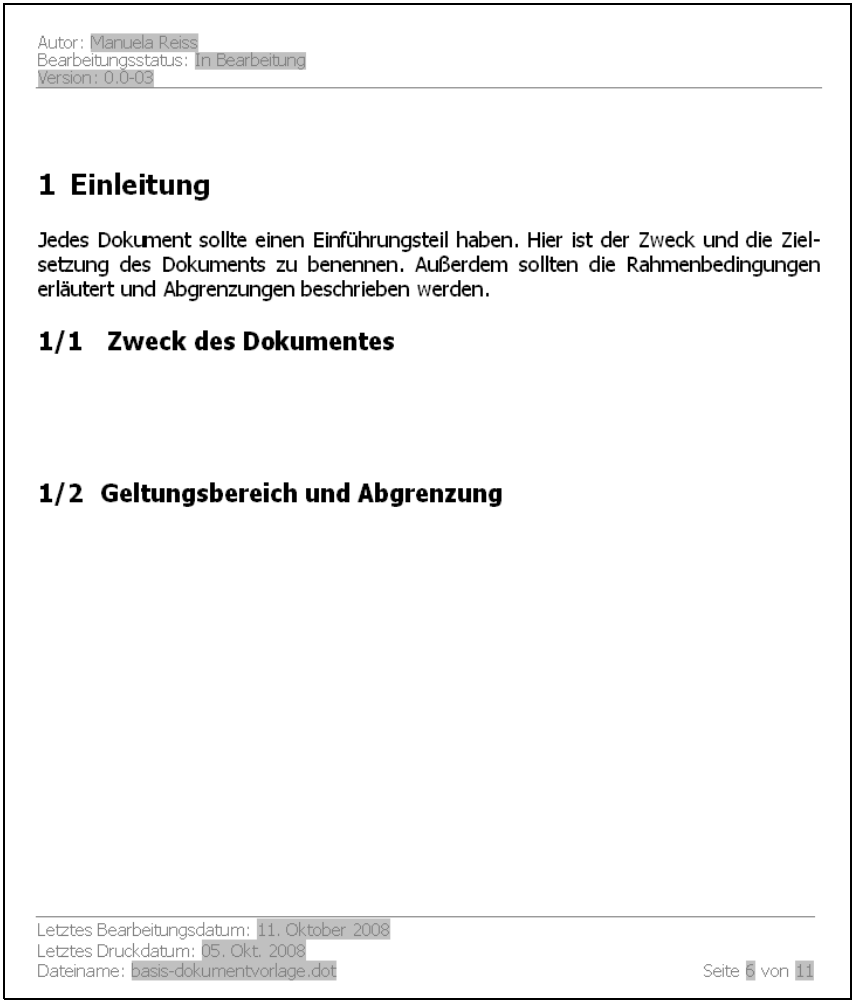


Abbildung 8.11: Muster-Dokumentvorlage: Einleitung

Autor: Manuela Reiss
Bearbeitungsstatus: In Bearbeitung
Version: 0.0-03

2 Hauptteil

An dieser Stelle ist der eigentliche Gegenstand des Dokuments zu beschreiben. Die Gliederung des Hauptteils ist abhängig von der Dokumentenklasse und dem zu beschreibenden System.

Hinweise zur Beschriftung von Abbildungen und Tabellen:

Abbildungen und Tabellen sind mit der Beschriftungsfunktion von Word zu beschriften. Die Beschriftung soll einen erläuternden Text zur dargestellten Abbildung bzw. Tabelle liefern. Bei Abbildungen in Arbeitsanleitungen, die Screenshots enthalten sollte (soweit möglich und sinnvoll) die Beschriftung die Menühierarchie beschreiben (siehe nachstehendes Beispiel).

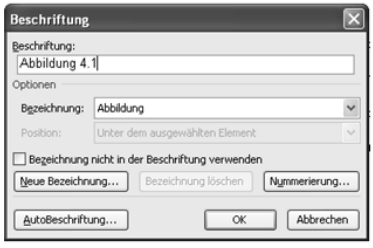


Abbildung 2.1: Abbildungen beschriften: Menü EINFÜGEN \ REFERENZ \ BESCHRIFTUNGEN

Letztes Bearbeitungsdatum: 11. Oktober 2008
Letztes Druckdatum: 05. Okt. 2008
Dateiname: basis-dokumentvorlage.dot Seite 7 von 11

Abbildung 8.12: Muster-Dokumentvorlage: Hauptteil

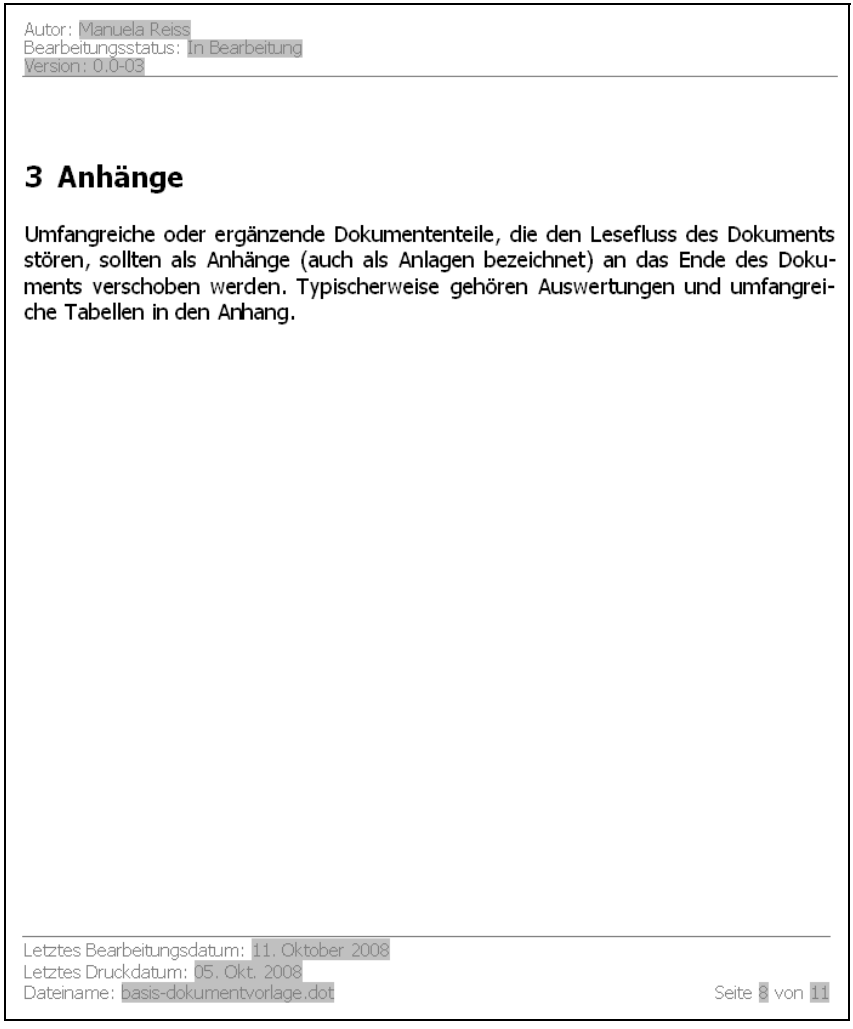
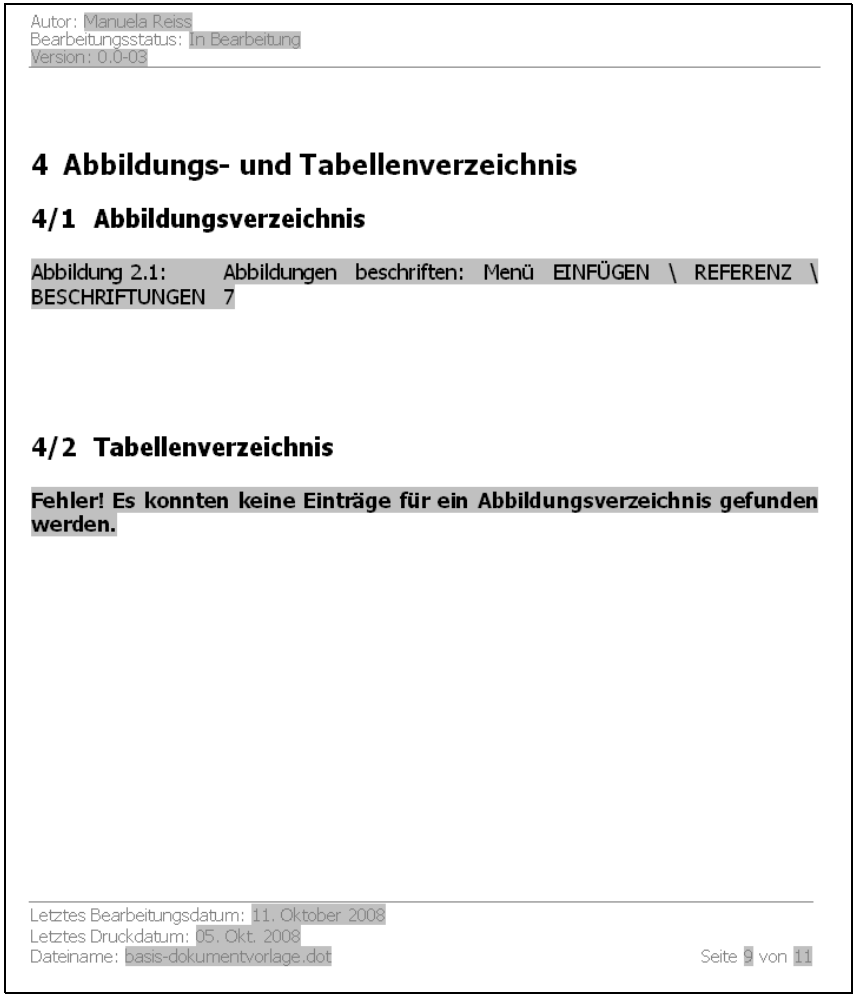


Abbildung 8.13: Muster-Dokumentvorlage: Anhänge


Autor: Manuela Reiss
Bearbeitungsstatus: In Bearbeitung
Version: 0.0-03

4 Abbildungs- und Tabellenverzeichnis

4/1 Abbildungsverzeichnis

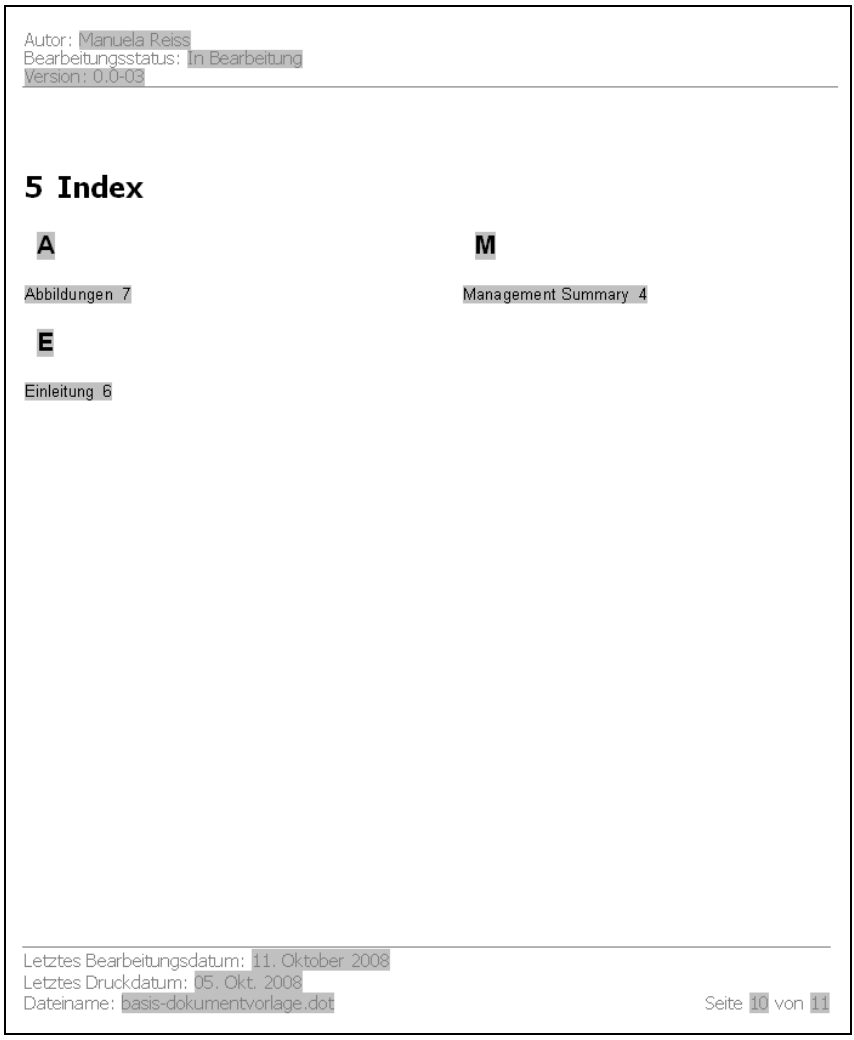
Abbildung 2.1: Abbildungen beschriften: Menü EINFÜGEN \ REFERENZ \ BESCHRIFTUNGEN 7

4/2 Tabellenverzeichnis

Fehler! Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.

Letztes Bearbeitungsdatum: 11. Oktober 2008
Letztes Druckdatum: 05. Okt. 2008
Dateiname: basis-dokumentvorlage.dot Seite 9 von 11

Abbildung 8.14: Muster-Dokumentvorlage: Abbildungs- und Tabellenverzeichnis


Autor: Manuela Reiss
Bearbeitungsstatus: In Bearbeitung
Version: 0.0-03

5 Index

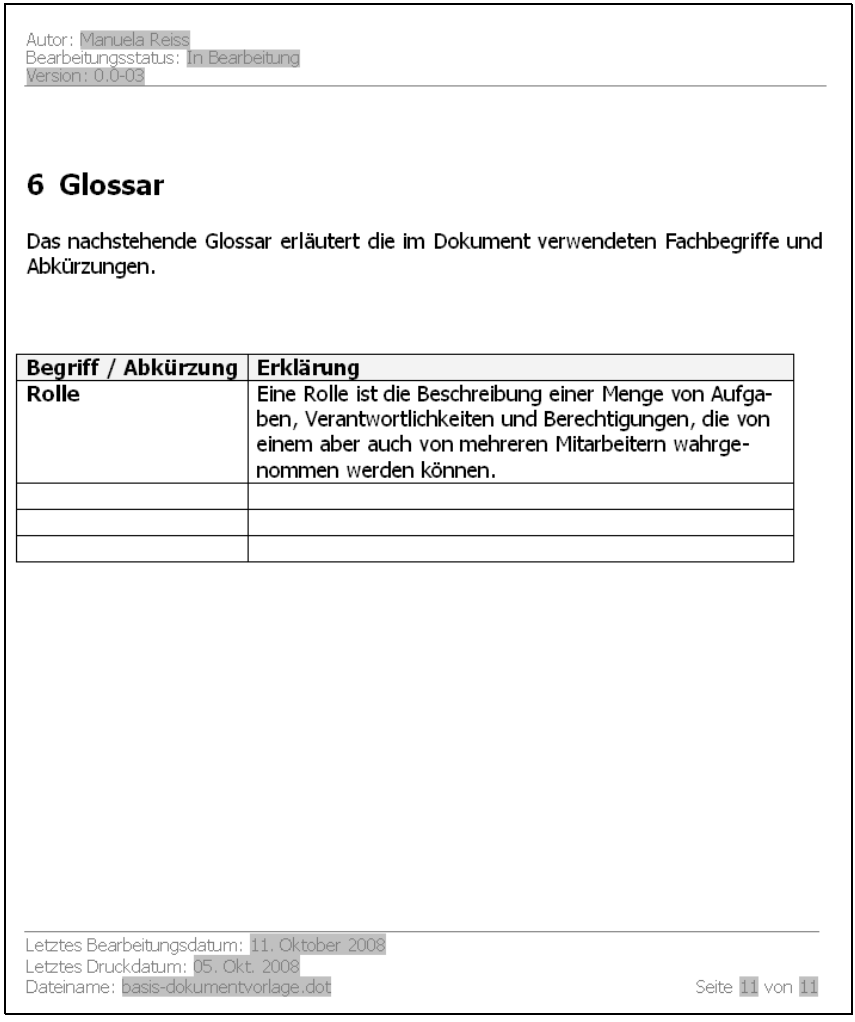
A

E

M

Letztes Bearbeitungsdatum: 11. Oktober 2008
Letztes Druckdatum: 05. Okt. 2008
Dateiname: basis-dokumentvorlage.dot
Seite 10 von 11

Abbildung 8.15: Muster-Dokumentvorlage: Index



Autor: Manuela Reiss
Bearbeitungsstatus: In Bearbeitung
Version: 0.0-03

6 Glossar

Das nachstehende Glossar erläutert die im Dokument verwendeten Fachbegriffe und Abkürzungen.

Begriff / Abkürzung	Erklärung
Rolle	Eine Rolle ist die Beschreibung einer Menge von Aufgaben, Verantwortlichkeiten und Berechtigungen, die von einem aber auch von mehreren Mitarbeitern wahrgenommen werden können.

Letztes Bearbeitungsdatum: 11. Oktober 2008
Letztes Druckdatum: 05. Okt. 2008
Dateiname: basis-dokumentvorlage.dot Seite 11 von 11

Abbildung 8.16: Muster-Dokumentvorlage: Glossar

8.7 Checkliste – Erstellen einer Dokumentvorlage

Die folgende Tabelle enthält eine Checkliste, die bei der Erstellung einer Dokumentvorlage unterstützt.

Erläuterungen zu den in der Checkliste aufgeführten Punkten finden Sie in Abschnitt 7.2.1.

Aufgabe	Anmerkung	
Masterlayout festlegen	Beinhaltet das Festlegen der Standardschrift und der Schriftgrade für Überschriften sowie Bild- und Tabellenunterschriften.	☐
Verwaltung der Metadaten festlegen	Im ersten Schritt ist festzulegen, wie die erforderlichen Metadaten in den auf der Vorlage basierenden Dokumenten erfasst werden sollen (beispielsweise in den Dokumenteneigenschaften). Gegebenenfalls ist ein entsprechendes Makro zu erstellen.	☐
Benötigte Formatvorlagen erstellen	Für alle erforderlichen Formatierungen (wie beispielsweise Marginalien) sollten Formatvorlagen erstellt werden.	☐
Zusätzliche Symbolleisten für Formatierungen bereitstellen	Alle wichtigen Formatierungen und Funktionen, auf die häufiger Zugriff erforderlich ist, sollten als Befehle auf Symbolleisten bereitgestellt werden. Hierzu gehören mindestens die Folgenden: • Alle Überschriftenebenen • Aufzählungen • Nummerierungen • Marginalien • Tabellen • Tabellen- und Bildunterschriften • Grafiken einfügen und formatieren • Text in Index aufnehmen • Felder aktualisieren • Standardformatvorlage zum Zurücksetzen aller Formatierungen • Text unformatiert einfügen • Querverweisfunktion aufrufen	☐
Deckblatt erstellen	Dies umfasst das Erstellen des Deckblattlayouts und die Aufnahme der zuvor festgelegten Informationen auf das Deckblatt. Handelt es sich um eine dokumentenklassenspezifische Vorlage, für die kein Deckblatt erforderlich ist, entfällt dieser Schritt.	☐
Dokumentinfobox erstellen	Die Dokumentinfobox sollte so weit wie möglich aus Feldern aufgebaut werden, deren Inhalt automatisch aus den Dokumenteigenschaften entnommen wird.	☐
Tabelle für Änderungsnachweis erstellen	Es muss festgelegt werden, welche Informationen im Änderungsnachweis zu erfassen sind.	☐

Aufgabe	Anmerkung	
Tabelle für mitgeltende Dokumente erstellen	Zusätzlich sollte ein Hinweis erläutern, welche Dokumente einzutragen sind.	☐
Management Summary einfügen	Handelt es sich um eine dokumentenklassenspezifische Vorlage, für die keine Zusammenfassung erforderlich ist, entfällt dieser Schritt.	☐
Inhaltsverzeichnis einfügen	Es ist das Layout für das Inhaltsverzeichnis festzulegen. Gegebenenfalls müssen die zugehörigen Formatvorlagen angepasst werden. Handelt es sich um eine dokumentenklassenspezifische Vorlage, für die kein Inhaltsverzeichnis erforderlich ist, entfällt dieser Schritt.	☐
Einleitung einfügen	Festlegen möglicher Unterkapitel der Einleitung (möglichst wenige Unterkapitel)	☐
Hauptteil einfügen	Die Gliederung für den Hauptteil sollte vorgegeben werden und Erläuterungen für die Erstellung der einzelnen Bereiche beinhalten. Die Gliederung ist abhängig von der Dokumentenklasse, für die die Vorlage gilt.	☐
Abbildungs- und Tabellenbeschriftungen definieren	Am Anfang des Hauptteils sollte darüber informiert werden, ob Grafiken und Tabellen zu beschriften sind und wie die Vorgaben dafür aussehen.	☐
Anhang einfügen	Gegebenenfalls sollte ein Hinweis eingefügt werden, der darauf hinweist, dass keine Informationen aus anderen Dokumenten in den Anhang eingefügt werden dürfen.	☐
Abbildungs- und/oder Tabellenverzeichnisse	Es sind die Verzeichnisse im gewünschten Layout in das Dokument einzufügen. Gegebenenfalls müssen die zugehörigen Formatvorlagen angepasst werden. Zusätzlich müssen entsprechende Beschriftungsvorgaben festgelegt werden. Handelt es sich um eine dokumentenklassenspezifische Vorlage für die kein Abbildungs- oder Tabellenverzeichnis erforderlich ist, entfällt dieser Schritt.	☐
Indexverzeichnis einfügen	Es ist das Verzeichnis im gewünschten Layout in das Dokument einzufügen. Handelt es sich um eine dokumentenklassenspezifische Vorlage für die kein Index erforderlich ist, entfällt dieser Schritt.	☐
Tabelle für das Glossar erstellen	Handelt es sich um eine dokumentenklassenspezifische Vorlage für die kein Glossar erforderlich ist, entfällt dieser Schritt.	☐

8.8 Checkliste – Qualitätssicherung eines Dokuments

Die folgende Tabelle enthält eine Checkliste, die bei der Qualitätssicherung eines Dokuments herangezogen werden kann. Durch die Unterschrift des Qualitätssicherers dient die Checkliste gleichzeitig als Nachweisdokument im Freigabeprozess.

Hinweise zu den aufgeführten formalen Anforderungen finden Sie in Abschnitt 7.1.1. Den Freigabeprozess eines Dokuments können Sie in Abschnitt 6.3.5.2 nachlesen.

Checkliste zur Qualitätssicherung eines Dokuments		
Dokumententitel		Dokumentennummer
Name des Qualitätssicherers	Unterschrift	Organisationseinheit / Telefon
Formalinhaltliche Anforderungen		
Ist die Dokumenteninfobox vorhanden?		☐
Ist die Dokumenteninfobox vollständig ausgefüllt?		
Dokumentenklasse		☐
Dokumententitel		☐
Dokumentennummer		☐
Verantwortlicher Autor		☐
Dateiname		☐
Erstellung begonnen am		☐
Letzte Bearbeitung		☐
Letztes Druckdatum		☐
Vertraulichkeitsstufe		☐
Versionsnummer		☐
Bearbeitungsstatus		☐
Ist die Vertraulichkeitsstufe korrekt angegeben?		☐
Ist der Bearbeitungsstatus richtig angegeben?		☐
Ist die Versionsnummer korrekt angegeben?		☐
Sind alle Seiten eindeutig als dem Dokument zugehörig zu identifizieren?		☐
Sind die mitgeltenden und ergänzenden Dokumente aufgelistet?		☐
Ist ein korrektes Inhaltsverzeichnis vorhanden?		☐
Gibt es eine Änderungshistorie?		☐
Existiert ein Management Summary?		
JA		☐
Nicht erforderlich		☐

Checkliste zur Qualitätssicherung eines Dokuments	
Existiert ein Glossar bzw. Abkürzungsverzeichnis? *JA* *Nicht erforderlich*	☐ ☐
Gibt es ein Indexverzeichnis (gegebenenfalls formalinhaltliche Prüfung)? *JA* *Nicht erforderlich*	☐ ☐
Wurde die richtige Dokumentvorlage verwendet?	☐
Entspricht das Layout den Dokumentationsstandards?	☐
Sind Tabellen und Bilder *eine sinnvolle Ergänzung des Textes?* *entsprechend den Standards erstellt?* *verständlich bzgl. der verwendeten Symbole (Legende vorhanden)?*	 ☐ ☐ ☐
Ist das Dokument vollständig, d. h., fehlen keine Textsteile, Seiten, Abbildungen?	☐
Wurden die Begriffe eindeutig definiert und durchgängig verwendet?	☐
Sind alle nicht allgemein bekannten bzw. spezifisch verwendeten Begriffe und Abkürzungen im Dokument oder im Glossar definiert?	☐
Ist das Dokument verständlich gegliedert und übersichtlich aufgebaut?	☐
Sofern Objektverknüpfungen verwendet wurden, besteht auf diese Zugriff?	☐
Inhaltliche Anforderungen (sachliche Richtigkeit, technische Angemessenheit und Durchführbarkeit)	
Stimmt der Inhalt mit den Anforderungen des Auftraggebers überein?	☐
Ist die textliche Darstellung der Zielgruppe entsprechend angemessen?	☐
Sind die Inhalte des Dokuments nachvollziehbar?	☐
Ist der Inhalt konsistent?	☐
Wurden Schnittstellen zwischen dem Dokument und bereits bestehenden Dokumenten berücksichtigt?	☐
Ist das Dokument inhaltlich vollständig? *JA* *JA, aber Ergänzungen erforderlich (siehe Erläuterungen im Dokument)*	 ☐ ☐
Sind die Inhalte sachlich richtig *JA* *JA, aber Anpassungen erforderlich (siehe Erläuterungen im Dokument)*	 ☐ ☐

8.9 Muster – Änderungsanforderung (Change Request)

Die nachfolgende Tabelle zeigt den möglichen Aufbau einer Änderungsanforderung. Erläuterungen zur Nutzung finden Sie in Abschnitt 6.3.2.

Änderungsanforderung (Change Request)			
1. Angaben des Antragstellers			
Allgemeine Angaben	RFC-ID (wird vergeben)		Datum der Antragstellung:
Antragsteller	Name	Organisations-einheit	Telefon
Ziel der Änderung	☐ Funktionale Systemänderung/-erweiterung ☐ Kapazitätserweiterung ☐ Außerbetriebnahme einer Systemkomponente ☐ Änderung oder Erweiterung eines Prozesses ☐ Andere		
Änderungswunsch: Was soll geändert werden?			
Grund der Änderung (Notwendigkeit beschreiben)			
Bekannte Auswirkungen auf andere Systeme / Prozesse inkl. bereits bekannter Risiken			
Risiken bei Nichtumsetzung			
Erforderlicher Zeitrahmen / Termin			
Unterschrift des Antragstellers			
2. Angaben des Bearbeiters			
Bearbeiter	Name	Organisations-einheit	Telefon
Machbarkeit/Nutzen (Ist die Änderung durchführbar und ist das Ziel der Änderung damit erreichbar?)	☐ ja ☐ ja, mit folgender Einschränkung: ☐ nein, weil:		
Zusätzlich zu beteiligende Organisationseinheiten?	☐ Keine ☐ Ja, folgende:		

Änderungsanforderung (Change Request)	
Erkannte Risiken (Welche Probleme können bei der Einführung oder danach auftreten?)	☐ Keine ☐ Folgende:
Detaillierte Beschreibung der Änderung. Was ist zu tun, um das Ziel zu erreichen? Was muss im Detail geändert werden?	
Erforderliche Rollbackmaßnahmen	
Auswirkungen auf Notfallpläne, deren erforderliche Anpassungen nach Umsetzung des RFC	
Geschätzte Kosten	_____EURO ☐ Finanzierung gesichert durch (Kontierung)
Aus den Risiken und dem Umfang abgeleitete Änderungsklasse	☐ Änderungsklasse A ☐ Änderungsklasse B
Erweitertes Genehmigungsverfahren (bei Änderungen der Klasse A zwingend erforderlich)	☐ Nein ☐ Ja
Empfehlung für erweitertes Genehmigungsverfahren	☐ Sollte umgesetzt werden ☐ Sollte mit Einschränkungen umgesetzt werden ☐ Ablehnung, Grund:
3. Angaben zur Umsetzung	
Bewilligung erteilt	☐ Erteilt ☐ Nicht erteilt, weil ☐ Mit Auflagen:
Geplanter Zeitrahmen / Termin	
Unterschrift des Bearbeiters	Datum:

8.10 Muster – Entscheidungsvorlage

Die nachfolgende Tabelle zeigt den möglichen Aufbau einer Entscheidungsvorlage bei Lösungsalternativen. Erläuterungen zu einer solchen Entscheidungsvorlage finden Sie in Abschnitt 6.3.3.

Entscheidungsvorlage			
Allgemeine Angaben	Lfd. Nummer: (wird vergeben)		Datum der Antragstellung:
Entscheidung wird benötigt durch: bis zum _____	☐ Unternehmensleitung ☐ IT-Leitung ☐ Projektleitung ☐ Lenkungsausschuss ☐ Andere:		
Angaben des Erstellers der Entscheidungsvorlage			
Antragsteller	Name	Organisationseinheit	Telefon
Allgemeine Angaben und Kontext in dem die Entscheidung zu treffen ist			
Beschreibung der mit den beschriebenen Lösungen verbundenen Ziele			
Lösungsvorschlag A			
Beschreibung Lösungsvorschlag A			
Vorteile und Nachteile von Lösungsvorschlag A	Vorteile:		Nachteile:
Bekannte Auswirkungen auf andere Systeme / Prozesse sowie bereits bekannte Risiken			
Geschätzte Kosten: (Investitions-, Implementierung- Schulungs- und Lizenz-Kosten) / geschätzter Ressourcenbedarf und Angabe Kostenträger			
Lösungsvorschlag B (optional)			
Beschreibung Lösungsvorschlag B			
Vorteile und Nachteile von Lösungsvorschlag B	Vorteile:		Nachteile:

Entscheidungsvorlage		
Bekannte Auswirkungen auf andere Systeme / Prozesse sowie bereits bekannte Risiken		
Geschätzte Kosten: (Investitions-, Implementierung- Schulungs- und Lizenz-Kosten) / geschätzter Ressourcenbedarf und Angabe Kostenträger		
Lösungsvorschlag C (optional)		
Beschreibung Lösungsvorschlag C		
Vorteile und Nachteile von Lösungsvorschlag C	Vorteile:	Nachteile:
Bekannte Auswirkungen auf andere Systeme / Prozesse sowie bereits bekannte Risiken		
Geschätzte Kosten: (Investitions-, Implementierung- Schulungs- und Lizenz-Kosten) / geschätzter Ressourcenbedarf und Angabe Kostenträger		
Empfehlung		
Empfohlener Lösungsweg	☐ A ☐ B ☐ C Bewertung der einzelnen Lösungsalternativen und Begründung der Entscheidung:	
Angaben zur Entscheidung		
Entscheidung durch: am _____	Name: Organisationseinheit: Telefon:	
Ausgewählte Lösungsalternative	☐ A ☐ B ☐ C ☐ Keiner der genannten Vorschläge	
Begründung		
Ergänzungen (Auflagen, erkannte Risiken usw.)	☐ Keine ☐ Folgende:	
Datum und Unterschrift des Entscheiders		

8.11 Muster – Testfallbeschreibung

Die nachfolgende Tabelle zeigt den möglichen Aufbau einer Testfallbeschreibung. Erläuterungen zur Nutzung befinden sich in Abschnitt 6.3.4.2.

Testfallbeschreibung			
Allgemeine Angaben	Name Testfall		Testfall-ID: (wird vergeben)
Verantwortlicher	Name	Organisationseinheit	Telefon
Testfall			
Umgebung			
Testfallbeschreibung und zu testende Funktionen			
Test durchzuführen von (Angabe der Rolle)			
Testinput			
Erwarteter Testoutput			
Qualitätsmerkmale und Testkriterien			
Schnittstellen zu anderen Tests, Arbeitspaketen			
Anmerkungen			

8.12 Muster – Testprotokoll

Die nachfolgende Tabelle zeigt den möglichen Aufbau eines Testprotokolls. Erläuterungen zur Nutzung sind in Abschnitt 6.3.4.3 enthalten.

Testprotokoll			
Allgemeine Angaben	Testumgebung	Testprotokoll-ID	
Name des Testfalls			
Datum und Uhrzeit		Von Uhrzeit Bis Uhrzeit	
Testpersonen			
Tester	Name	Organisationseinheit	Telefon
Testbegleitende Personen	Name	Organisationseinheit	Telefon
Testumgebung			
Testumgebung und betroffene Systeme			
Testdurchführung			
Testschritte			
Testergebnisse Ergebnisse bzw. Beschreibungen des Testdurchlaufes (Schritt für Schritt getrennt) dokumentieren			
1.			
2.			
3.			
Anmerkungen / Erläuterungen			
Änderungen an der Testumgebung aufgrund der Tests			
Änderung		Grund	
Erforderliche Wiederherstellungsaktionen			
Tester	Datum	Unterschrift	

A Abkürzungs-verzeichnis

APIPA	Automatic Private IP Adressing
AO	Abgabenordnung
AD	Active Directory
AktG	Aktiengesetz
AO	Abgabenordnung
BCM	Business Continuity Management
BCP	Business Continuity Plan
BDSG	Bundesdatenschutzgesetz
BfDI	Der Bundesbeauftragte für den Datenschutz und die Informations-freiheit
BIA	Business Impact-Analyse
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BPMN	Business Process Modeling Notation

BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz)
CAB	Change Advisory Board
CAFM	Computer Aided Facility Management
CI	Configuration Item
CMDB	Configuration Management Data Base
CMMI	Capability Maturity Model Integration
COBIT	Control Objectives for Information and Related Technology
COSO	Committee of Sponsoring Organizationsof the Treadway Commission
CR	Change Request
DHCP	Dynamic Host Configuration Protocol
DIIR	Deutsches Institut für Interne Revision e. V.
DIN	Deutsches Institut für Normung e. V.
DLM	Document Lifecycle Management
DMS	Dokumentenmanagement-System
DNS	Domain Name System
ECM	Enterprise Content Management
eEPK	Erweiterte Ereignisgesteuerte Prozessketten
EN	Europäische Norm
EPK	Ereignisgesteuerte Prozessketten
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GoB	Grundsätze ordnungsgemäßer Buchführung
GoBS	Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme
GPO	Group Policy Object
HGB	Handelsgesetzbuch
ICMP	International Control Message Protocol
IDW	Institut der Wirtschaftsprüfer in Deutschland e. V.
IEEE	Institute of Electrical and Electronics Engineers

IIA	Institute of Internal Auditors
IKS	Internes Kontrollsystem
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
ITSCM	IT Service Continuity Management
IuK	Informations- und Kommunikationstechnik
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KSA	Kommunikationsstrukturanalyse
KVP	Kontinuierlicher Verbesserungsprozess
MaRisk	Mindestanforderungen an das Risikomanagement
MOF	Microsoft Operations Framework
MS	Microsoft
MSF	Microsoft Solutions Framework
NAS	Network Attached Storage
OGC	Office of Government Commerce
OU	Organisational Unit (Organisationseinheit im Active Directory)
OWA	Outlook Web Access
PDA	Personal Digital Assistant
PDCA	Plan-Do-Check-Act (Deming-Kreis)
PKI	Public Key Infrastructure
PM	Project Management
PMBOK	Project Management Body of Knowledge
PRINCE2	PRrojects IN Controlled Environments
PS	Prüfungsstandard
QM	Qualitätsmanagement
RACI	Responsible, Accountable, Consulted und Informed
RASCI	Responsible, Accountable, Supportive, Consulted und Informed
RC	Release Candidate
RFC	Request For Change

SAN	Storage Area Network
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SOX	Sarbanes-Oxley Act
TK	Telekommunikation
TÜVIT	TÜV Informationstechnik GmbH
UML	Unified Modeling Language
VBA	Visual BASIC for Applications
VOI	Verband Organisations- und Informationssysteme e. V.
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WfMC	Workflow Management Coalition
WORM	Write-Once, Read-Many
WSS	Windows SharePoint Services
XML	Extensible Markup Language
MOSS	Microsoft Office SharePoint Server

B

Glossar

Wie im Buch ausgeführt wurde, dient ein Glossar der Erläuterung der im *betreffenden* Dokument bzw. Buch verwenden Fachbegriffe. Entsprechend liefert das nachstehende Glossar keine Auflistung und Erläuterung allgemeingültiger Begriffe, sondern beschreibt ausschließlich definitionswürdige Begriffe bzw. deren Verwendung im Buch.

Änderungsanforderung	Eine Änderungsanforderung (Change Request) beschreibt einen standardisierten Antrag zur Durchführung einer Änderung.
Änderungsmanagement	Das Änderungsmanagement umfasst alle Aufgaben, die einer geplanten, kontrollierten und standardisierten Einführung neuer oder geänderter IT-Systeme und IT-Verfahren dienen. Es definiert die Verantwortlichkeiten und plant die auszuführenden Arbeiten. In der Projektliteratur werden das Änderungsmanagement und das Veränderungsmanagement voneinander abgegrenzt. Auf das Erfordernis, die jeweiligen Anpassungen zu dokumentieren, hat diese Abgrenzung keinen Einfluss. Daher wird in dem vorliegenden Buch für beide Fälle von Änderungen bzw. Änderungsmanagement (Change Management) gesprochen.

Aktivität	Eine Aktivität bildet die kleinste Ausführungseinheit in einem Arbeitsablauf.
Arbeitsablauf	Ein Arbeitsablauf ist ein zusammenhängend ablaufender Teil eines Prozesses, bei dem die operative Sicht im Vordergrund steht. Arbeitsabläufe stellen operative Detailansichten eines Prozesses dar. Sie können, müssen jedoch nicht IT-unterstützt durchgeführt werden.
Arbeitsanweisungen	Hierbei handelt es sich typischerweise um Schritt-für-Schritt-Anleitungen. Die einzelnen Schritte müssen die auszuführende Tätigkeit, die betroffenen Objekte sowie die jeweiligen Randbedingungen (z. B. Ortsangaben) enthalten.
Arbeitshilfen	Arbeitshilfen sind alle Formen von Anleitungen und Beschreibungen, welche die in den Arbeitsabläufen benannten Tätigkeiten detaillieren. Hierbei kann es sich beispielsweise um Arbeitsanweisungen, Checklisten, Mustervorlagen, Formulare und Fragenkataloge handeln.
Berechtigungsmatrix	Eine Berechtigungsmatrix beschreibt eine tabellarische Zuordnung von Aktivitäten und Aufgaben bzw. von Berechtigungen zu den Systemgruppen.
Betriebsmatrix	Eine Betriebsmatrix ermöglicht die eindeutige Zuordnung von Personen und Rollen und hilft dabei, Doppelbesetzungen, unklare Zuständigkeiten und Überschneidungen zu verhindern. Dabei kann eine Person mehrere Rollen besetzen; es kann aber auch eine Rolle durch mehrere Personen besetzt werden.
Dokumentations-richtlinie	Die Dokumentationsrichtlinie enthält verbindliche Regelungen für den formalen Aufbau einzelner Dokumente und definiert die Dokumentationsprozesse. Sie enthält also nicht nur Vorgaben für die Einzeldokumente, sondern regelt auch die Verwaltung und Speicherung der Gesamtdokumentation.
Dokumentenklasse	Die Zuordnung zu einer Dokumentenklasse definiert ein Dokument im Hinblick auf seinen Informationsinhalt und die Darstellungsform. Dokumentersteller und Benutzer des Dokuments erhalten damit Hinweise auf den Inhalt und auch Suchvorgänge können bei entsprechender Verschlagwortung nach Dokumentenklassen erfolgen
Dokumentinfobox	Eine Tabelle, die alle wesentlichen Dokumentinformationen einschließlich des aktuellen Bearbeitungsstandes beinhaltet. Sie sollte in jedem Dokument stehen.

Entscheidungsvorlage	Entscheidungsvorlagen stellen den Verantwortlichen alle notwendigen Informationen bereit, um zu entscheiden, welcher Lösungsansatz weiterverfolgt werden soll.
Ergebnisdokumente	Als Ergebnisdokumente werden alle Dokumente bezeichnet, die im Rahmen eines Projekts während der Projektdurchführungsphase erstellt werden und das Projektergebnis dokumentieren. Von den Ergebnisdokumenten sind die Projektmanagement-Dokumente abzugrenzen.
Geschäftsfortführungsplan	Sie müssen gewährleisten, dass im Notfall zeitnah Ersatzlösungen zur Verfügung stehen und alle wichtigen Geschäftsprozesse nicht oder nur temporär unterbrochen werden.
Grob- und Feinkonzept	Im Buch werden die Begriffe Grob- und Feinkonzept ausschließlich am Detaillierungsgrad ausgerichtet. Es kann in vielen Fällen durchaus sinnvoll sein, ein dem endgültigen technischen Konzept vorlaufendes Konzept, mit einem geringeren Detaillierungsgrad zu erstellen.
IT-Betrieb	Der IT-Betrieb umfasst alle Aufgaben des Regelbetriebs, des Supportmanagements sowie des Notfallmanagements. Letzteres kommt bei einer schwerwiegenden Störung des Betriebs zum Einsatz und hat die Wiederherstellung des Betriebs zur Aufgabe.
IT-Betriebshandbuch	Das Betriebshandbuch umfasst alle für den IT-Betrieb erforderlichen Dokumente. Es handelt sich hierbei um eine modular aufgebaute Dokumentation, die sich aus Systemakten und Prozessbeschreibungen zusammensetzt.
IT-Dokumentation	Gesamtheitliche Dokumentation für alle IT Organisationseinheiten
IT-Gruppenkonzept	Das IT-Gruppenkonzept beschreibt die systemtechnischen Gruppen und definiert die Zuordnung zu den Rollen. Damit bildet es eine Schnittstelle zwischen der Prozessdokumentation und der Systemdokumentation.
IT-Konzept	Das IT-Konzept ist ein strategisches Dokument, das der grundsätzlichen Einordnung der IT in das Unternehmen dient und die übergeordnete strategische Ausrichtung des Unternehmens im Hinblick auf die IT festlegt.
IT-Projektmanagement-Handbuch	Das IT-Projektmanagement-Handbuch (PM-Handbuch) regelt die verbindlichen Sollvorgaben, die für alle IT-Einzelprojekte gelten. Bei der im Buch vorgestellten Struktur der IT-Dokumentation wird das Projektmanagement-Handbuch aufgrund des übergeordneten Charakters den Rahmendokumenten zugeordnet.

IT-Rollenkonzept	Das IT-Rollenkonzept definiert und beschreibt alle im Bereich der IT eingesetzten Rollen. Mit Hilfe der Rollenbeschreibungen können in der Betriebsmatrix die Mitarbeiter bzw. die Organisationseinheiten den Rollen zugeordnet werden.
IT-Sicherheitskonzept	Das IT-Sicherheitskonzept regelt die Struktur und die konkrete Umsetzung der IT-Sicherheit. Während die IT-Sicherheitsrichtlinie Schutzziele und allgemeine Sicherheitsmaßnahmen im Sinne offizieller Vorgaben des Unternehmens vorgibt, beschreibt das IT-Sicherheitskonzept detaillierte Sicherheitsmaßnahmen und Handlungsanweisungen zum Umgang mit IT-Sicherheit.
IT-Sicherheitsrichtlinie	Die IT-Sicherheitsrichtlinie schreibt die zentralen Richtlinien für die IT-Sicherheit in einem Unternehmen fest. Sie definiert die Sicherheitsziele und die Grundsätze für den Umgang mit Informationen sowie die Verantwortungsbereiche für die IT-Sicherheit.
Lastenheft	Das Lastenheft stellt einen Anforderungskatalog dar, in dem die Zielsetzungen, Aufgabenstellungen, Anforderungen des Auftraggebers und weitere Leistungsdaten des zu entwickelnden Produkts beschrieben werden. Im Lastenheft definiert der Auftraggeber demnach das „Was“ und das „Wofür“. Es beschreibt jedoch nicht, wie etwas gemacht werden soll. Dies ist Aufgabe des Pflichtenhefts.
Mitgeltende Dokumente	Bei den mitgeltenden Dokumenten handelt es sich um eigenständige Dokumente, die Reglungen enthalten, die für dieses Dokument Gültigkeit besitzen, aber im Dokument nicht zwingend explizit genannt werden müssen. Typischerweise sind Rahmendokumente mitgeltende Dokumente.
Modell	Zur Optimierung der IT-Organisation, also der Aufbau- und Ablauforganisation, haben sich verschiedene Modelle wie ITIL oder COBIT entwickelt. Sie stellen in der Regel ein Baukastensystem (Framework) zur Verfügung, in dem die IT-Organisation segmentiert und deren Hauptprozesse entsprechend der Ausrichtung der Modelle beschrieben sind.
Normentwurf	Ein Normentwurf wird der Öffentlichkeit mit seiner Herausgabe zur Prüfung und Stellungnahme vorgelegt. Nach Prüfung der Einsprüche und Stellungnahmen kann der Normentwurf durch eine endgültige Norm abgelöst werden oder in einen erneuten Entwurf münden.

Notfall	Ein Notfall tritt im Verständnis dieses Buches immer dann ein, wenn innerhalb einer fest definierten Zeit eine Wiederherstellung der Verfügbarkeit eines unternehmenskritischen Dienstes nicht gegeben ist und daraus ein das Unternehmen bedrohender Schaden droht oder eintritt.
Notfallhandbuch	Das Notfallhandbuch beschreibt die Gesamtheit aller für die Notfallbewältigung benötigten Dokumente, was unter anderem die Notfallpläne mit Beschreibungen aller erforderlichen Maßnahmen und Aktionen nach dem Eintritt eines Notfalles und die Testdokumente beinhaltet.
Notfallkonzept	Das Notfallkonzept umfasst alle für die Notfallvorsorge benötigten Dokumente und hat als Richtliniendokument übergeordneten Charakter.
Notfallplan	Der Notfallplan fasst die Gesamtheit aller Notfalldokumente für ein Schadensereignis zusammen. Dies schließt neben dem Geschäftsfortführungsplan und dem Wiederherstellungsplan auch beispielsweise die ereignisspezifischen Alarmierungspläne ein.
Pflichtenheft	Aufgabe des Pflichtenheftes ist es, aus den Anforderungen des Kunden (Lastenheft) eine möglichst vollständige konsistente und eindeutige Produktdefinition als Basis für das zu erstellende Produkt zu liefern.
Projekt	Bei einem IT-Projekt handelt es sich in Konkretisierung der DIN 69901 um ein zielgerichtetes, zeitlich, personell und sachlich abgegrenztes IT-Vorhaben. Das Projekt hat die Erweiterung bzw. den Umbau des IT-Betriebs zur Aufgabe.
Projektakte	Projektakten bezeichnen die Zusammenstellung aller auf ein Projekt bezogenen Dokumente. Hierbei kann es sich sowohl um Dokumente des Projektmanagements als auch um Ergebnisdokumente handeln. Für jedes Projekt ist innerhalb der Projektdokumentation eine Projektakte zu führen. Innerhalb der Projektakte ist eine Unterscheidung in Dokumente für das Projektmanagement und in Ergebnisdokumente sinnvoll.
Projektdokumentation	Die Projektdokumentation beinhaltet alle Dokumente, die Bestandteil der IT-Dokumentation sind und im Rahmen von Projekten erstellt werden oder dafür gelten. Sie steht auf einer Ebene mit dem Betriebshandbuch, das die entsprechende Aufgabe für den IT-Betrieb übernimmt.

Prozess	Ein Prozess ist eine Kette aufeinander aufbauender Aktivitäten und dient der Herstellung eines Produkts oder einer Dienstleistung. Ein Prozess hat einen definierten Anfang, einen beschriebenen Ablauf und ein definiertes Ende. Die einzelnen Aktivitäten sind dabei voneinander abhängig.
Prozessbeschreibung	Eine Prozessbeschreibung definiert die Dokumentation eines einzelnen Prozesses und enthält detaillierte Regelungen für diesen Prozess. Die Prozessbeschreibung kann in einem einzigen Dokument zusammengefasst sein, aber auch aus mehreren Einzeldokumenten bestehen.
Prozessdokumentation	Die Prozessdokumentation umfasst als Gesamtdokument alle einzelnen Prozessbeschreibungen.
Prozesslandkarte	In einer Prozesslandkarte werden alle wesentlichen Prozesse eines Unternehmens und deren logischer Zusammenhang dargestellt. Eine Prozesslandkarte beschreibt demnach die Struktur der Unternehmensprozesse und das Zusammenwirken der einzelnen Teilprozesse.
Prozesssteckbrief	Der Prozesssteckbrief enthält alle wichtigen Daten und Rahmenbedingungen eines Prozesses und liefert in tabellarischer Form einen schnellen Überblick über alle wichtigen Prozessmerkmale.
Rahmendokumente	Rahmendokumente regeln allgemeine Vorgaben und Normierungen und legen die aufbauorganisatorischen Zuordnungen und Funktionszuordnungen fest. Sie stellen somit die Klammer für die den drei anderen Bereichen (Betriebshandbuch, Projektdokumentation und Notfallhandbuch) zugeordneten Dokumente dar.
Review	Ein Review ist eine Begutachtung von Dokumenten, die der Beurteilung und Qualitätssicherung dient. Es ist Bestandteil von Dokumentenfreigabeprozessen.
Risikohandbuch	Das unternehmensweite Risikohandbuch bildet die Grundlage eines unternehmensweiten Risikomanagements. Es stellt organisatorische Maßnahmen und Regelungen dar, die zur Risikoerkennung, -quantifizierung, -kommunikation, -steuerung und -kontrolle zu beachten sind. Die IT-servicegefährdenden Risiken können in einem gesonderten IT-Risikohandbuch im Rahmen der IT-Dokumentation dokumentiert werden.
Rolle	Eine Rolle beschreibt die Menge von Aufgaben, Verantwortlichkeiten und Berechtigungen, die von einem aber auch von mehreren Mitarbeitern wahrgenommen werden.

Systemsakten	Systemakten dienen zur Beschreibung des Aufbaus des eines Systems sowie der Konfigurationsbeschreibung. Sie beinhalten alle relevanten Informationen für ein System; sie werden gesondert für jedes System angelegt und gepflegt. Als System werden beispielsweise sowohl einzelne Server (Hardware-Systemakten) als auch das Standard-Softwarepaket für die Rechner oder der Verzeichnisdienst Active Directory (Software-Systemakten) betrachtet.
Systemdokumentation	Die Systemdokumentation besteht aus den einzelnen Systemakten der eingesetzten Hard- und Softwaresysteme (Betriebssysteme, Datenbanksysteme, Cluster-Infrastruktur usw.) und stellt hierfür einen Sammelbegriff dar.
Technisches Konzept	Bei den hier betrachteten Konzepten handelt es sich um Dokumente, die auf der Grundlage der Ausgangsituation und der Anforderungsanalyse die technisch zu realisierende Lösung für eine definierte Aufgabe liefern und planerischen Charakter haben. Zur Abgrenzung anderer Konzepte, wie zu den Rahmendokumenten zählenden Konzepten (beispielsweise dem Rollenkonzept), werden derartige Konzepte im vorliegenden Buch als „Technische Konzepte“ bezeichnet.
Testfallbeschreibung	Ein Testfall ist eine Kombination von Eingabedaten, Bedingungen und erwarteten Ausgaben, die einem bestimmten Zweck dient. In der Testfallbeschreibung müssen für jeden Testfall die zu benutzenden Eingaben und zu erwarteten Ausgaben benannt und alle Schritte zur Durchführung des jeweiligen Testfalls beschrieben werden.
Testkonzept	Das Testkonzept bildet den inhaltlichen Leitfaden für die Testdurchführung und beinhaltet sowohl die Testziele als auch Abgrenzungen, Vorgehensweisen, Mittel und den Ablaufplan der Testaktivitäten und Beschreibungen der Testprozesse.
Testprotokoll	Das Testprotokoll dient zur Aufzeichnung der Ereignisse während einer Testausführung und enthält Angaben über alle ausgeführten Testfälle, deren Ergebnisse und aufgetretene Abweichungen vom erwarteten Ergebnis.
Verfahren	Der Begriff Verfahren wird im datenschutzrechtlichen Zusammenhang verwendet und bezeichnet hier Vorgänge, in denen personenbezogene Daten verarbeitet oder genutzt werden. Ein Beispiel für ein Verfahren ist die automatisierte Zeiterfassung.

Verfahrensanweisungen	Prozessbeschreibungen und Verfahrensanweisungen beschreiben im Grunde das Gleiche. Was unter der früheren ISO 9001:1994 als Verfahrensanweisung bezeichnet wurde, wird in der aktuellen Norm ISO 9001:2001 als Prozessbeschreibung geführt. Die Prozessbeschreibung kann als visuelle Verfahrensbeschreibung und damit als eine Weiterentwicklung der früher überwiegend textlich gestalteten Verfahrensanweisung betrachtet werden.. Im Buch wird ausschließlich der Begriff Prozessbeschreibung verwendet.
Virtuelle Akten	Bei einer virtuellen Akte handelt es sich um eine zusammenhängende Sicht auf die zusammengehörigen Informationen, die aus den verschiedenen Quellen zusammengeführt werden. Nutzer eines DMS können sich in einer virtuellen Akte genau das zusammenstellen, was sie in der Dokumentenansicht sehen möchten. Die Inhalte einer Sicht werden dynamisch zur Laufzeit als Sicht erzeugt und in der gewünschten Form als tabellarische Darstellung oder in einer Ordnungsstruktur visualisiert.
Wiederanlaufplan	Wiederanlaufpläne müssen innerhalb eines angemessenen Zeitraums die Rückkehr zum Normalbetrieb ermöglichen. Dazu müssen sie Handlungsanweisungen für spezielle Ereignisse enthalten, die beschreiben was in welcher Reihenfolge zu tun ist. Hierzu zählen auch Wiederbeschaffungsmaßnahmen und Ausweichmöglichkeiten.
Wiederherstellungsanleitung (Wiederherstellungsplan)	Ein Wiederherstellungsplan beschreibt die technische Seite der Wiederherstellung und enthält konkrete Arbeitsanweisungen zur Wiederherstellung eines Systems. Da dieser Begriff eine hohe Verwechslungsgefahr birgt, wird im Buch statt dessen der Begriff Wiederherstellungsanleitung verwendet.

C

Literatur und Links

Die nachfolgende Tabelle enthält – nach Kapitel geordnet – Internetlinks und Literaturhinweise. Diese verweisen auf die im Buch verwendeten Quellen und bieten zusätzliche Informationen zu den vorgestellten Themen.

Kapitel 1		
ASPRÜF	Richtlinie über die Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen vom 17.05.2006	*http://www.securitymanager.de/magazin/news_h19810_mit_euro-sox_wird_itk-auditierung_pflicht.html*
BDSG	Bundesdatenschutzgesetz BDSG vom 27.01.1977 Zuletzt geändert am 25.08.2006	*http://www.bfdi.bund.de/cln_027/nn_532042/SharedDocs/Publikationen/GesetzeVerordnungen/BDSG, templateId=raw,property=publicationFile.pdf/BDSG.pdf*
BSGI	Gesetz über die Einrichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Einrichtungsgesetz)	*http://www.gesetze-im-internet.de/*

BDSGKOM	Peter Gola, Rudolf Schomerus, Christoph Klug: BDSG – Bundesdatenschutzgesetz. Kommentar. 9. Auflage, Verlag C. H. Beck, München 2007, ISBN-13: 978-3406555442	
BFDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	*http://www.bfdi.bund.de/*
BSISTAND	BSI-Standards	*http://www.bsi.bund.de/literat/bsi_standard/index.htm*
COBIT	Control Objectives for Information and Related Technology	*http://www.cobit-isaca.de/* *http://www.isaca.org* *http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981* *http://www.risikomanagement-in-it-projekten.de/03COBIT/seite03.html* *http://www.conect.at/uploads/tx_posseminar/Mueller_04.pdf*
DIIR	Deutsches Institut für Interne Revision e. V.	*http://www.iir-ev.de/deutsch/default.asp* *http://www.iir-ev.de/deutsch/download/allgemeine_downloads.asp?navid=1* *http://www.revision-online.com/html/ron_b_verbaende.html*
GDPdU	„Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)“ BMF-Schreiben vom 16. Juli 2001	*http://www.markus-flamm.de/datenzugriff/gdpdu/index.html* *http://www.bundesfinanzministerium.de/nn_314/DE/Wirtschaft_und_Verwaltung/Steuern/Veroeffentlichungen_zu_Steuerarten/Abgabenordnung/003.html*
GESETZE	Aktiengesetz (AktG) vom 06.09.1965. Zuletzt geändert am 12.08.2008 Handelsgesetzbuch (HGB) vom 10.05.1897. Zuletzt geändert am 10.12.2007 Abgabenordnung (AO) vom 16.04.1976. Zuletzt geändert am 08.04.2008 „Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS)“ vom 07.11.1995	*www.juris.de* *http://www.gesetze-im-internet.de/* *http://www.bundesfinanzministerium.de*

GOBS	Henstorf, Karl-Georg; Kampffmeyer, Dr. Ulrich; Prochnow, Jan: Grundsätze der Verfahrensdokumentation nach GoBS – „Code of Practice" zur revisionssicheren Archivierung VOI-Schriftenreihe Kompendium Band 4 1999, ISBN 3-932898-04-4	
IDW	Institut der Wirtschaftsprüfer in Deutschland e.V.	*http://www.idw.de/idw/*
ZIR	ZIR – Zeitschrift Interne Revision Fachzeitschrift für Wissenschaft und Praxis Herausgeber: Deutsches Instituts für Interne Revision e. V. (IIR), Frankfurt am Main	*http://esv.info/z/ZIR/zeitschriften.html*
ISO	International Organization for Standardization	*http://www.iso.org/iso/home.htm*
ISOLIST	Liste der ISO-Normen	*http://de.wikipedia.org/wiki/Liste_der_ISO-Normen*
ISO9000	ISO 9000-Normenreihe	*http://www.zingel.de/pdf/08iso.pdf* *http://www.iso9001.qmb.info/*
ISO20000	ISO 20000 vom 15.12.2005	*http://www.ips-it-schulungen.de/media/doc/IPS_Arminius_080527_ISO20K.pdf und* *http://www.searchsecurity.de/index.cfm?pid=3898&pk=70326*
ISO27001	„Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz – Prüfschema für ISO 27001-Audits" Stand: 1. Februar 2006 Herausgeber: Bundesamt für Sicherheit in der Informationstechnik	*www.bsi.bund.de/gshb/zert/ISO27001/pruefschema06.pdf*
ITIL	Information Technology Infrastructure Library (ITIL)	*http://www.itil-officialsite.com/home/home.asp* *http://www.itil.org/de/* *http://www.bsi.bund.de/literat/studien/ITinf/index.htm* *http://www.ogc.gov.uk/guidance_itil.asp*

ITILB	Martin Kittel, Torsten J. Koerting, Dirk Schött Kompendium für ITIL-Projekte Books on Demand GmbH 2006 ISBN-10: 3-8334-5411-3 Böttcher, Roland IT-Servicemanagement mit ITIL V3 dpunkt.verlag GmbH 2007 ISBN 978-3-936931-50-1	
KONTRAG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) vom 05.03.1998	*http://www.wiwi.uni-regensburg.de/scherrer/edu/opi/kontrag.html* *http://62.157.187.34/data/revwelt_/PDF/kontrag.pdf*
MARISK	Mindestanforderungen an das Risikomanagementsystem (MaRisk) vom 20.12.2005 geändert am 30.10.2007	*http://www.bundesbank.de/bankenaufsicht/bankenaufsicht_marisk.php* *http://www.deutsche-sparkassenakademie.de/leitfaden/DSGV-MaRisk-Interpretationsleitfaden_Version_2.pdf*
PS330	IDW Prüfungsstandard 330, Abschlussprüfung bei Einsatz von IT vom 24.09.2002	*http://www.it-audit.de/html/ian_sch_ita_standard.html#Standards* *http://www.it-audit.net/unterstutzung_jahresabschlussprufung_audit_support_nach_idw_ps_330_.html*
PS850	Entwurf IDW Prüfungsstandard: Projektbegleitende Prüfung bei Einsatz von Informationstechnologie (IDW EPS 850) (Stand: 19.09.2007)	*http://www.idw.de/idw/generator/id=281116.html*
PSIDW	Verlautbarungen – IDW Prüfungsstandards	*http://www.idw.de/idw/portal/n281334/n281114/n302246/index.jsp*
SOX	Sarbanes-Oxley Act (SOX) vom 30.07.2002	*http://www.sarbanes-oxley.com/* *http://www.kpmg.de/Themen/1439.htm* *http://62.157.187.34/sox_inhalte-site-revwelt.html* *http://www.compliancemagazin.de/printable/produkte/dokumentation/stellent271106.html*
TÜVIT	TÜV Informationstechnik GmbH Unternehmensgruppe TÜV NORD IT-Grundschutz nach BSI-Standard 100	*http://www.tuvit.de/default.asp* *http://www.tuvit.de/IT-Grundschutz.asp*

Kapitel 2		
BSI	Bundesamt für Sicherheit in der Informationstechnik (BSI)	*http://www.bsi.de/*
BSI-1004	BSI-Standard 100-4 Notfallmanagement – Entwurf Version 0.9, Stand: 01. August 2008	*http://www.bsi.de/literat/bsi_standard/bsi-standard_100-4_v090.pdf*
BSI-GS	IT-Grundschutz-Kataloge des BSI	*http://www.bsi.de/gshb/deutsch/index.htm*
GPM	Deutsche Gesellschaft für Projektmanagement e. V. (offizielle Website)	*http://www.gpm-ipma.de*
GSTOOL	GSTOOL (Software des BSI zum IT-Grundschutz)	*http://www.bsi.de/gstool/index.htm*
INFODUDEN	Duden Informatik, Bibliographisches Institut & F. A. Brockhaus AG. Ein Sachlexikon für Studium und Praxis Auflage 4, 2006, ISBN 3411052341	
PJMGR	Heinz Schelle, Roland Ottmann, Astrid Pfeiffer: ProjektManager – GPM Deutsche Gesellschaft für Projektmanagement e. V., ISBN: 978-3-924841-26-3	
Kapitel 3		
BSI-1001	BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)	*http://www.bsi.de/literat/bsi_standard/standard_1001.pdf*
BSI-1003	BSI-Standard-100-3: Risikoanalyse auf der Basis von IT-Grundschutz	*http://www.bsi.de/literat/bsi_standard/standard_1003.pdf*
BITKOM	Verfahrensverzeichnis und Verarbeitungsübersicht nach BDSG – Ein Praxisleitfaden –	*http://www.bitkom.org/files/documents/BITKOM_Verfahrensverzeichnis_V_2.0.pdf*
EN ISO1	Qualität & Norm: Die Dokumentation eines QM-Systems	*http://www.iso9001.qmb.info/allgemein/dokuumstellung.htm*
EN ISO2	Qualität & Norm: Tabelle der DIN EN ISO 9001:2000	*http://www.iso9001.qmb.info/allgemein/norm_uebersicht.htm*
LFDI	Website des Landesbeauftragten für Datenschutz und Informationsfreiheit Saarland.	*http://www.lfdi.saarland.de*

Kapitel 4		
DOCUSNAP	DocuSnap (Inventarisierungstool)	*http://www.docusnap.de*
IDOIT	i-doit (Open-Source-Anwendung für eine ITIL-konforme IT-Dokumentation)	*http://www.i-doit.org*
MOF	MicrosoftTechnet-Artikel zum Thema Microsoft Operations Framework	*http://www.microsoft.com/germany/technet/datenbank/articles/495298.mspx*
PMBOK	PMI (Project Management Institute)	*http://www.pmi.org*
RIMACON	rimacon omniSuite (lizenzkostenfreies Software-Tool für den Aufbau einer CMDB)	*http://www.rimacon.de*
SEM	SemTalk (Tool für die Geschäftsprozess-modellierung in MS Visio)	*http://www.semtalk.de*
Kapitel 5		
BSI	Bundesamt für Sicherheit in der Informationstechnik	*http://www.bsi.de/*
BSI-ITIL	„ITIL und Informationssicherheit Möglichkeiten und Chancen des Zusammenwirkens von IT-Sicherheit und IT-Service-Management“ (Broschüre des BSI)	*http://www.bsi.bund.de/literat/studien/ITinf/itil.pdf*
BCMTOOL	Marktübersicht BCM- und Notfallplanungs-Tools	*http://bcm-news.de/tinc?key=ModQ0vfH&formname=BCM_Tools*
Kapitel 6		
HDVO	Anleitung und Tool zur Erstellung von Pflichtenheften	*http://www.hdvo.de/*
IEEE	IEEE-Standard 829 für Software Tests („ANSI/IEEE 829-1983 IEEE Standard for Software Test Documentation-Description“)	*http://standards.ieee.org/reading/ieee/std_public/description/se/829-1983_desc.html*
IUK-MINDEST	„IT-Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informations- und Kommunikationstechnik (IuK-Mindestanforderungen)“ vom 26.09.2001	*http://bundesrechnungshof.de/veroeffentlichungen/broschuere*

PRINCE	PRINCE2 (offizielle Website)	*http://www.ogc.gov.uk/methods_prince_2.asp*
PROMAGZIN	Projekt Magazin – Das Fachmagazin im Internet für erfolgreiches Projektmanagement	*http://www.projektmagazin.de/*
STBAUR	Webpräsenz von Stefan Karl Baur. Pflichtenheft: Abgrenzung und Inhalte	*http://www.stefan-baur.de/cs.se.pflichtenheft.html*
SWTECHNIK	Helmut Balzert: Lehrbuch der Software-Technik, Spektrum Akademischer Verlag GmbH, 1997, ISBN 3827400651.	
Kapitel 7		
DMS	Orientierungshilfe „Datenschutz bei Dokumentenmanagementsystemen“ (Publikation des BFDI)	*http://www.bfdi.bund.de/cln_027/nn_530436/DE/Themen/TechnologischerDatenschutz/TechnologischeOrientierungshilfen/Artikel/OrientierungshilfeDMS.html*
MIMAGER	Mindjet MindManager Viewer 7	*http://www.mindjet.com/de-DE/resources/downloads/mm_viewer.aspx?s=2*
SIGDOK	„Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente“ (Publikation des BMWI, Stand: August 2007)	*http://www.bmwi.de/BMWi/Navigation/Service/publikationen,did=218700.html*
VOI	Verband Organisations- und Informationssysteme e. V. (offizielle Website)	*http://www.voi.de/*
VOIMERK	Grundsätze der elektronischen Archivierung. „Code of Practice“ zum Einsatz von Dokumenten-Management- und elektronischen Archivsystemen, VOI 2. Auflage: (1. Januar 1997) ISBN-10: 3932898036	
WSS	Microsoft Windows SharePoint Services 3.0 (Webseite von Microsoft)	*http://office.microsoft.com/de-h/sharepointtechnology/default.aspx*

D Steckbriefe der vorgestellten Programme

Die folgenden Tabellen enthalten alle wichtigen Daten zu den im Buch vorgestellten Programmen. Die Angaben beziehen sich auf die jeweils mit Stand September 2008 aktuelle Version.

D.1 Steckbrief: GSTOOL

Steckbrief GSTOOL des BSI (aktuelle Version 4.5 , V 4.5 2082, DB 4.45045, MD 09)	
Hersteller:	Bundesamt für Sicherheit in der Informationstechnik (BSI).
Kontakt:	Godesberger Allee 185–189 53175 Bonn Telefon: 0228/99 9582-0 Fax: 0228/99 9582-5400 E-Mail: *bsi@bsi.bund.de* *Internet: www.bsi.de*

Steckbrief GSTOOL des BSI (aktuelle Version 4.5 , V 4.5 2082, DB 4.45045, MD 09)	
Systemanforderungen:	**Betriebssystem** Windows 2000, Windows XP, Windows Vista **Computer** Mindestens 256 MB RAM, für Vista mindestens 512 MB RAM empfohlen 150 MB Plattenspeicher und zusätzlich 50 MB zur Installation Für die Schnittstellen zu den Office-Programmen ist mindestens die Version Office 2002 erforderlich Browser-Software: Das GSTOOL nutzt den unter Windows eingestellten Standard-Browser und ist für den Internet Explorer optimiert.
Preise:	GSTOOL Lizenz-Preis (Upgrade-Preis von 4.0/4.1) 1 Lizenz 895,92 € (35,25 €) 2 Lizenzen 1.791,84 € (70,50 €) 3 Lizenzen 2.553,37 € (100,46 €) 4 oder 5 Lizenzen 4.027,16 € (158,45 €) 6 bis 10 Lizenzen 7.498,85 € (295,04 €) 11 bis 20 Lizenzen 13.707,58 € (539,33 €) 21 bis 40 Lizenzen 23.437,27 € (922,14 €) Firmenlizenz (bei mehr als 40 Lizenzen) auf Anfrage Jeweils zzgl. Mehrwertsteuer Die Abgabe an Bundes-, Landes- und Kommunalverwaltungen der Bundesrepublik Deutschland erfolgt kostenfrei.
Testversion:	Eine 30tägige Testversion kann kostenlos herunter geladen werden: *http://www.bsi.de/gstool/down.htm*

Tabelle D.1: Steckbrief: GSTOOL

D.2 Steckbrief: DocuSnap

Steckbrief DocuSnap (aktuelle Version 4.1)	
Hersteller:	Itelio GmbH
Kontakt:	Telefon: 08033/6978-0 Fax: 08033/6978-91 E-Mail: info@itelio.de Internet: www.itelio.de und www.docusnap.de
Systemanforderungen für den Rechner auf dem DocuSnap installiert ist:	Microsoft Windows XP/Windows Server 2003/Vista Microsoft Office 2003/2007 Microsoft Visio 2003/2007
Auslesbare Systeme und Netzwerkobjekte:	Windows Server 2003, 2003 R2, 2000 und Windows NT Clients: Windows NT, Windows 2000, Windows XP und Windows Vista Alle SNMP-fähigen Netzwerkgeräte (Drucker, Router usw.) Optional: MS Exchange 2003, MS SQL Server 2000/2005, Windows DHCP-Server Domänen/Strukturen: Active Directory Domänen (2000/2003), Windows NT 4.0-Domänen, Arbeitsgruppen, einzelne Hosts
Preise:	DocuSnap wird nach den im Active Directory Service registrierten Computerkonten lizenziert. Zusätzliche Geräte wie z. B. Drucker, Netzwerkkomponenten werden nicht in die Berechnung einbezogen. < 25: pauschal 200,00 € Darüber hinaus erfolgt eine Staffelung zwischen 3,50 € und 8,00 € abhängig von der Anzahl der benötigten Lizenzen. Für die Dokumentation von Linux-Systemen werden folgende Preise berechnet: < 10: pauschal 300,00 € Darüber hinaus pro System zwischen 25,00 € und 30,00 € Die Module Exchange Server, SQL Server, DHCP, Rechteanalyse und Lizenzverwaltung werden zusätzlich berechnet.
Testversion:	Eine 30tägige Testversion kann kostenlos herunter geladen werden. Zuvor ist eine Registrierung erforderlich.

Tabelle D.2: Steckbrief: DocuSnap 4.1

D.3 Steckbrief: SemTalk

Steckbrief SemTalk (aktuelle Version 3.0)	
Hersteller:	Semtation GmbH
Kontakt:	Telefon: 0331/581 39 36 Fax: 0331/581 39 29 E-Mail: sales@semtalk.com Internet: www.semtalk.de
Systemanforderungen für den Rechner auf dem SemTalk installiert ist:	Für SemTalk wird MS Visio 2003 oder Visio 2007 benötigt. Da SemTalk 3 Funktionen der .Net-Technologie verwendet, ist zusätzlich „.NET Framework Version 2.0 Redistributable Package“ erforderlich. Für die Schnittstellen zu Excel, PowerPoint und Projekt ist mindestens die Version 2003 erforderlich. Der Export zu MS Word kann mit Word 2007, Word 2003 und Word 2002 genutzt werden
Datenbankschnittstellen:	SemTalk verwendet Dokumente, die bei Bedarf mit einer zentralen Ablage abgeglichen werden. Ab der Version SemTalk 2.3 kann optional eine SQL Server-Datenbank eingesetzt werden.
Preise:	• Einzelplatzlizenz: 950,00 € • 5er-Lizenz: 3499,00 € • 10er-Lizenz: 6499,00 € Ohne MS Visio. Weitere Staffelungen auf Anfrage.
Testversion:	Eine 30tägige Testversion kann kostenlos herunter geladen werden. Dafür ist eine Registrierung erforderlich.

Tabelle D.3: Steckbrief: SemTalk 3.0

D.4 Steckbrief: FaciPlan

Steckbrief FaciPlan (aktuelle Version FaciPlan 2007)	
Hersteller:	FaciWare GmbH
Kontakt:	Telefon: 08031/7978338 E-Mail: info@faciware.com Internet: www.faciware.com
Systemanforderungen für den Rechner, auf dem DocuSnap installiert ist:	FaciPlan 2007 auf Basis von Microsoft Visio Professional 2007 benötigt als Betriebssystem Windows 2000 ab Service Pack 3 bzw. Windows XP. Zusätzlich erforderlich ist das .NET Framework 2.0. Auf der Installations-CD befindet sich im Verzeichnis *CD\Setup\dotnetfx* die Datei *dotnetfx.exe*.
Preise:	• FaciPlan Professional 2007 kostet pro Lizenz 990,00 € zuzüglich MwSt. • FaciPlan Enterprise 2007 mit erweiterten Funktionalitäten wie z. B. Datenbankexportmöglichkeiten kostet 1.490,00 € (inkl. einer Visio Professional 2003/2007-Lizenz).
Testversion:	Unter info@faciware.com kann eine kostenlose Demo-CD und eine Testversion von FaciPlan angefordert werden (Registrierung erforderlich). Es besteht die Möglichkeit, FaciPlan online zu testen.

Tabelle D.4: Steckbrief: FaciPlan 2007

D.5 Steckbrief: Mindjet MindManager

Steckbrief Mindjet MindManager Pro (aktuelle Version 7)	
Hersteller:	Mindjet GmbH
Kontakt:	Siemensstraße 30 63755 Alzenau Telefon: 06023/9645-12 E-Mail: info@mindjet.de Internet: www.mindjet.de
Systemanforderungen:	**Betriebssystem:** Microsoft Vista Ultimate oder Business Microsoft Windows XP Professional Home oder Tablet PC Editionen Microsoft Windows Server 2003 **Computer:** IBM oder kompatibler Pentium Prozessor (mindestens 700 MHz) Mindestens 256 MB RAM, für Vista mindestens 512 MB RAM empfohlen 150 MB Plattenspeicher und zusätzlich 50 MB zur Installation Für die Schnittstellen zu den Office Programmen ist mindestens die Version Office 2002.
Preise:	• Mindjet MindManager Lite 7 ist zum Preis von 79,00 € (zzgl. MwSt) erhältlich (als Einstiegsprodukt für Privatpersonen platziert). • Mindjet MindManager Pro 7 bietet den vollständigen Funktionsumfang und kostet in der Vollversion 299,00 € (zzgl. MwSt.) bzw. 149,00 € in der Upgrade-Version. • Mindjet MindManager 7 Mac für den Einsatz auf Macintosh Rechner. Die Vollversion kostet 129,00 € zzgl. MwSt. und die Upgrade-Version 69,00 €.
Testversion:	Eine 30tägige Testversion kann kostenlos herunter geladen werden. Dafür ist eine Registrierung erforderlich.
Mindjet MindManager Viewer:	Mit dem kostenlosen Mindjet MindManager Viewer 7 können MindManager Maps angezeigt werden, ohne die Vollversion der Anwendung installieren zu müssen. Unter dem folgenden Link kann der Viewer kostenlos heruntergeladen werden. *http://www.mindjet.com/de-DE/resources/downloads/mm_viewer.aspx?s=2*

Tabelle D.5: Steckbrief: MindManager 7.0

D.6 Steckbrief: Windows SharePoint Services

Steckbrief Windows SharePoint Services (aktuelle Version 3.0 mit Service Pack 1)	
Hersteller:	Microsoftt GmbH
Systemanforderungen:	**Betriebssystem** Windows Server 2003 Windows Server 2008 **Computer** Server mit einer Prozessorgeschwindigkeit von mindestens 2,5 GHz, 1 GB RAM Weiter wird Microsoft .NET Framework 3.0 benötigt.
Preise:	Microsoft stellt die Windows SharePoint Services 3.0 kostenlos im Microsoft Download Center zur Verfügung.

Tabelle D.6: Steckbrief: Windows SharePoint Services 3.0

Index

B

C

D

E

F

G

H

I

O

P

Q

R

S

T

U

V

W

Z

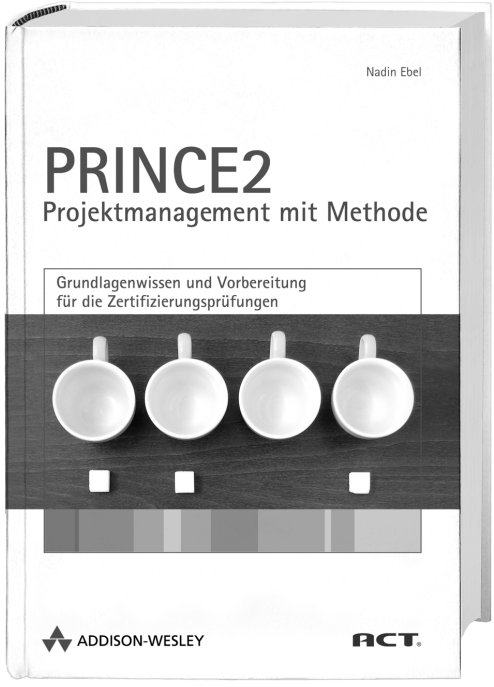
informit.de, Partner von Addison-Wesley, bietet aktuelles Fachwissen rund um die Uhr.

www.informit.de

In Zusammenarbeit mit den Top-Autoren von Addison-Wesley, absoluten Spezialisten ihres Fachgebiets, bieten wir Ihnen ständig hochinteressante, brandaktuelle deutsch- und englischsprachige Bücher, Softwareprodukte, Video-Trainings sowie eBooks.

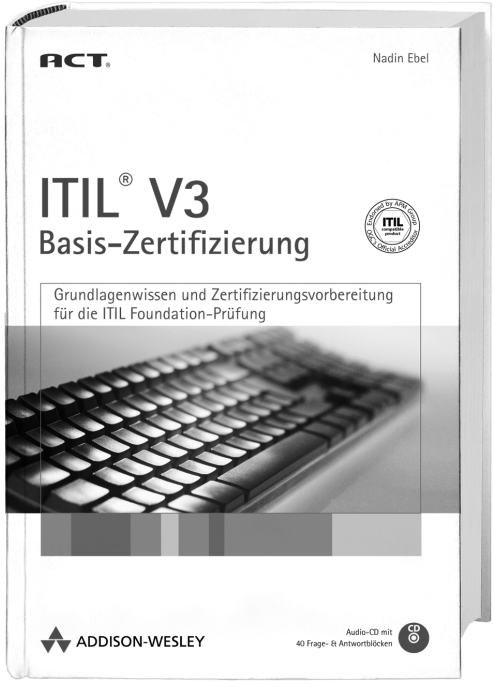
wenn Sie mehr wissen wollen …

www.informit.de



Dieses Buch macht Sie mit den Begrifflichkeiten, dem Prozessmodell und der PRINCE2-Philosophie sowie einem allgemeinen Verständnis für den Themenkomplex des Projektmanagements vertraut.
Wenn Sie sich als Projektleiter oder -mitarbeiter in PRINCE2 einarbeiten, hilft Ihnen das Buch, sich in einem (PRINCE2-)Projektumfeld zurechtzufinden und die Ihnen zugedachten Aufgaben wahrzunehmen.
Bei der Vorbereitung auf die Foundation-Prüfung unterstützt es Sie mit über 300 Beispielfragen samt kommentierten Lösungen bei der Überprüfung Ihres Wissenstandes.

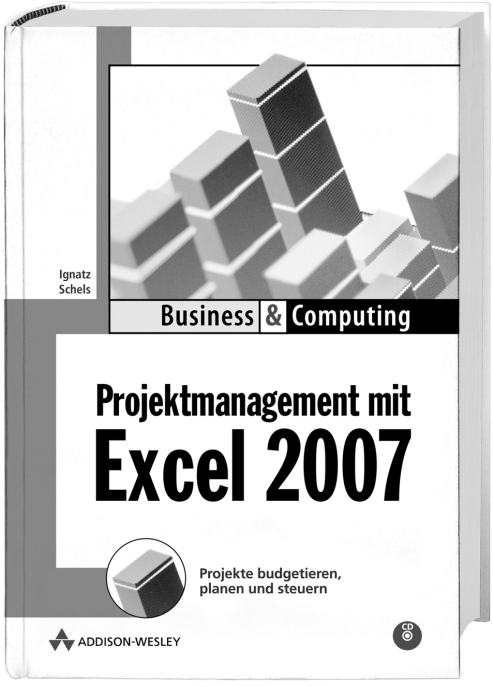
Nadin Ebel
ISBN 978-3-8273-2542-6
49.95 EUR [D]



Dieses Lern- und Nachschlagewerk vermittelt das notwendige Wissen zur Vorbereitung auf die ITIL-Basis-Zertifizierung zur Version 3.0. Im Mittelpunkt stehen die Grundlagenkenntnisse zum IT-Service-Management und den Inhalten des Service Lifecycle.
Sie lernen mithilfe dieses Buches die ITIL-Terminologie, -Funktionen und -Kernprozesse kennen. Die Erläuterung der Bereiche Service Strategy, Service Design, Service Transition, Service Operation und der Service-Verbesserung (Continual Service Improvement) schafft ein grundlegendes Verständnis über die Planung, Entwicklung, Implementierung und den Betrieb der Dienstleistungen in der IT-Organisation.

Nadin Ebel
ISBN 978-3-8273-2599-0
59.95 EUR [D]

THE SIGN OF EXCELLENCE



Professionelle und erfolgreiche Projektarbeit ist keine Hexerei! Allerdings scheitern viele Projekte am Einsatz der richtigen Software, denn teure Projektverfolgungs-Software ist nicht immer vonnöten. Hier zeigt der Autor, wie man diese Aufgabe mit Excel löst.

Ignatz Schels
ISBN 978-3-8273-2600-3
39.95 EUR [D]

www.addison-wesley.de

[The Sign of Excellence]
ADDISON-WESLEY