Informatik im Fokus

Herausgeber:

Informatik im Fokus

Rauber, T.; Rünger, G.
Multicore: Parallele Programmierung. 2008

El Moussaoui, H.; Zeppenfeld, K.
AJAX. 2008

Behrendt, J.; Zeppenfeld, K.
Web 2.0. 2008

Hoffmann, S.; Lienhart, R.
OpenMP. 2008

Steimle, J.
Algorithmic Mechanism Design. 2008

Stych, C.; Zeppenfeld, K.
ITIL. 2008

Bode, A.; Karl, W.
Multicore-Architekturen. 2008

Christof Stych · Klaus Zeppenfeld

ITIL

Springer

Christof Stych
Schürener Straße 99a
44269 Dortmund
christof.stych@gmx.net

Klaus Zeppenfeld
FH Dortmund
FB Informatik
Emil-Figge-Str. 42
44227 Dortmund
zeppenfeld@fh-dortmund.de

ISBN 978-3-540-73118-4 e-ISBN 978-3-540-73119-1

DOI 10.1007/978-3-540-73119-1

ISSN 1865-4452

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.

Einbandgestaltung: KünkelLopka Werbeagentur, Heidelberg

Gedruckt auf säurefreiem Papier

9 8 7 6 5 4 3 2 1

springer.com

Vorwort

Die Welt der Informationstechnik (IT) ist ständigen Änderungen unterworfen. Durch rapide Entwicklungen in der Informatik und die technischen Innovationen hält die IT Einzug bis in die oberste Managementebene. So spricht die ganze Welt scheinbar nur noch von Dienstleistungen und Services, die es anzuwenden und zu fördern gilt.

Das Interesse des Kunden kann nicht mehr mit einer Produktvielfalt, sondern mit der Qualität von Dienstsleistungen geweckt werden. Diskutiert wird derzeit über Web-Services, Software-as-a-Service (SaaS), Offshoring von Unternehmensbereichen, Service-Oriented-Architecture (SOA) und IT-Service-Management (ITSM).

In diesem Zusammenhang fällt auch sehr oft der Begriff ITIL: Die IT-Infrastructure-Library (ITIL) ist eine Bibliothek von so genannten Best-Practise-Erfahrungen, die sich mit den für ein Unternehmen wichtigen (Geschäfts-) Prozessen beschäftigt und stets die Optimierung des Ablaufs und der Wirtschaftlichkeit solcher Prozesse anstrebt. Es wird ein IT-Service-Management (ITSM) beschrieben, dessen Kernpunkt fortwährend ein Service bildet. Aus diesem Grund ist die aktuelle ITIL-Revision 3 in aller Munde. Diese Revision wurde im vergangenen Herbst in englischer Sprache veröffentlicht.

Das vorliegende Buch gehört zur Informatik im Fokus-Reihe des Springer-Verlags und gibt eine ausgiebige Einführung in ITIL und das gesamte Umfeld: das IT-Service-

Management. Wer sich für ITIL interessiert, ist mit dieser konstruktiven Einführung als Informationsquelle und Nachschlagewerk gut bedient. Begriffe werden definiert, viele Abbildungen helfen das Beschriebene besser zu behalten. Mit Hilfe von Checklisten und Aufgaben kann das Wissen nochmals gefestigt werden.

An dieser Stelle möchten wir uns ganz herzlich beim Springer-Verlag für die sehr gute Zusammenarbeit bedanken.

Darüber hinaus bedanken wir uns bei Uwe Kirchhoff und Martin Bömer von der Materna GmbH, die uns die nötigen ITIL-Materialien zur Verfügung gestellt haben.

Unser Dank gilt auch unseren Familien, die uns in dieser Zeit entbehrt und unterstützt haben.

Dortmund, im Mai 2008

Christof Stych
Klaus Zeppenfeld

Inhaltsverzeichnis

1 Einleitung

1.1 Beschreibung der Thematik

Unternehmen stehen heutzutage unter einem enormen Wettbewerbsdruck. Früher konnte der Mitbewerb durch Einsatz von Informationstechnologie (IT) ein- und überholt werden, in dem durch Effizienz Kosten gespart und auf Veränderungen relativ schnell reagiert werden konnte, wohingegen heute die IT in allen Unternehmen präsent ist. Es geht bereits schon soweit, dass mit Hilfe der IT komplexe Geschäftsprozesse unterstützt werden und nur durch ihre Optimierung der Wettbewerbsvorteil erreicht werden kann. Aus diesem Grund wird die IT an sich und die damit verwalteten Daten zu einer bedeutenden und für das Unternehmen überlebenswichtigen Ressource, die es vor Ausfall – vor dem Zugriff Dritter oder vor Katastrophen – zu schützen gilt [o01].

Es ist demnach der Fokus zunächst auf die Datenhaltung zu setzen. Wichtige Informationen sind verfügbar zu halten, am besten hochverfügbar mit 99,99%, die Rechtslage, die Datensicherheit und der Datenschutz müssen eingehalten, Kosten minimiert und die Produktivität gesteigert werden [o01]. Zu erreichen ist dies mit einer durchgängigen IT-Infrastruktur, die auch bei Ausfällen ihren Dienst erledigt.

Das traditionelle IT-Management wird durch den Servicegedanken zunehmend serviceorientierter [09]. Dabei stehen nicht unbedingt die Produkte im Vordergrund, sondern die Wünsche

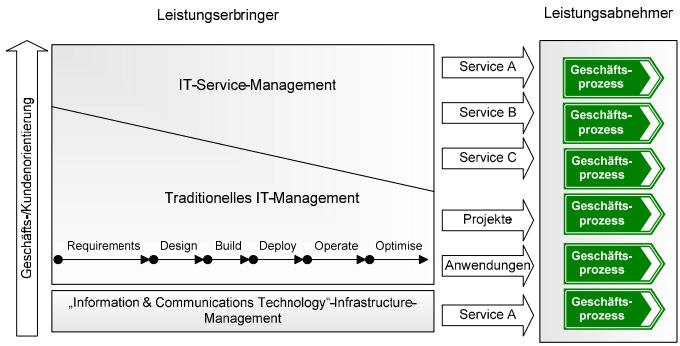

Abb. 1.1. Traditionelles und serviceorientiertes Management nach [09]

des Kunden. Dieser wird dabei gerne zum König gekürt, der zufrieden gestellt werden muss, um ein Unternehmen durch Service und Qualität auch dadurch gegenüber anderen Mitanbietern abzusetzen.

Serviceorientiertes IT-Management zeichnet sich durch Markt-, Service und Lebenszyklusorientierung aus. Anders ausgedrückt, werden Auftraggeber und -nehmer zu Kunden und Lieferanten und die Zusammenarbeit durch IT-Services definiert, deren Erhaltungskosten das Unternehmen interessieren. Aus einem Projektportfolio wird somit ein Leistungsportfolio [09] (vgl. Abb. 1.1).

All diese und weitere Probleme und Schwierigkeiten sind mit der „Information Technology Infrastructure Library" (ITIL) in den Griff zu bekommen, die bereits seit 1989 existiert. Sie ist aus dem Grund entstanden, weil Unternehmen und die öffentliche Verwaltung den gleichen Anforderungen ausgesetzt waren: Kosten reduzieren und Qualität der IT-Dienstleistungen verbessern [o11]. Dabei stellt ITIL keine verbindliche Norm dar, sondern einen „Best Practice"-Leitfaden [06], der für alle Unternehmen anwendbar ist. Es ist also auch

möglich, sein Unternehmen an ITIL lediglich anzulehnen, es muss keine hundertprozentige Realisierung sein. In der ITIL ist die Einführung des IT-Service-Managements (ITSM) beschrieben. Es wird aber nicht erläutert, wie, sondern was getan werden sollte, um die größtmögliche Effizienz der Geschäftsprozesse zu erreichen und ständig zu optimieren.

ITIL wurde in den letzten Jahren immer bekannter. Auch wenn nicht alle Unternehmen vollständig „ITIL sprechen", so sind ähnliche Rahmenwerke wie u. a. das „Microsoft Operations Framework" (MOF) stark an ITIL angelehnt. ITIL kann auch die Umstellung auf z. B. das Framework „enhanched Telecom Operation Map" (eTOM) erleichtern. Neben weiteren solchen Frameworks für das IT-Service-Management liegt ITIL bezüglich des Bekanntheitsgrades bei Unternehmen bei 98% [o13].

Folgerichtig ist es sinnvoll, sich mit dieser Thematik auseinanderzusetzen, um die Vorteile der Best-Practice für das eigene Unternehmen zu nutzen. Für den Fall, dass andere Marktbegleiter – im Gegensatz zum eigenen Unternehmen – ITIL nutzen, ist es sicherlich auch von Vorteil, deren Überlegenheit zu kennen und darauf zu reagieren.

1.2 Zielsetzung des Buches

Dieses Buch soll eine Einführung in das Thema der IT-Infrastructure-Library geben und zeigen, wo sie in der IT einzuordnen ist. Es sollen sowohl interessierte Studenten als auch Manager, Verantwortliche und Berater in der IT angesprochen werden.

Ein Student der IT oder des Managements kann sich zunächst theoretisches Basiswissen aneignen, das zum Schluss des Buches mittels Checklisten gefestigt und durch Aufgaben

übergeprüft werden kann. Ein IT-Manager, -Verantwortlicher oder -Berater, der sich für die praktischen, kritischen und finanziellen Aspekte interessiert, kann sich ebenfalls darüber informieren.

Dieses Buch ist auch als Nachschlagewerk zu nutzen. Es muss allerdings klargestellt werden, dass hier keine Garantie auf Vollständigkeit gegeben werden kann, da Unschärfen zum einen durch Übersetzungsfehler aus dem Englischen ins Deutsche, zum anderen durch Komprimierung der Originalbücher in nur ein Buch nicht vermieden werden können.

Im Wesentlichen wird hier noch auf die ITIL-Revision 2 eingegangen. Es werden die Bereiche Service-Support und Service-Delivery ausführlich beschrieben, da die Bücher der Revision 3 noch nicht veröffentlicht waren. Es kann also für ITIL v3 nur eine Einleitung gegeben werden. Allerdings stimmen die Revisionen zum Großteil überein, der ITIL-Philosophiekern bleibt bestehen. Es ist ferner davon auszugehen, dass ITIL v3 noch einige Zeit brauchen wird, sich neben ITIL v2 zu etablieren.

1.3 Vorgehensweise und Gliederung

Bevor in diesem Buch auf ITIL eingegangen wird, werden dessen Umgebung sowie die Begriffswelt des Managements und der Dienstleistung beschrieben, mit denen ITIL zu tun hat. Der Leser kann sich dadurch mehr theoretisches Hintergrundwissen aneignen, das für das ITIL-Verständnis notwendig ist.

Das zweite Kapitel gibt eine Einleitung in die IT-Infrastructure-Library: Wie ist ITIL entstanden? Welcher Gedanke bzw. welche Philosophie steckt dahinter? Welche Vorteile bringt für ein Unternehmen die Anwendung von ITIL? Da ITIL ein De-facto-Standard ist, der auf vielen internationalen

Standards und Normen aufbaut, werden diese ausführlich diskutiert. Schlussendlich werden die ITIL-Publikationen in der Revision 2 und 3 vorgestellt und die Gemeinsamkeiten aufgeführt.

Im dritten Kapitel sind nach einer kleinen Einleitung des Prozessgedankens die einzelnen Managementbereiche beschrieben. Unterteilt werden die ITIL-Prozesse in die operative Ebene des Service-Supports und der strategisch-taktischen Ebene des Service-Deliverys. Für jeden Prozess werden die spezifischen Begriffe definiert und Beziehungen zu anderen Prozessen aufgezeigt. Darüber hinaus wird jeder Prozess in seine Aktivitäten zerlegt. Jedes Unterkapitel enthält Praxishinweise und Vorteile, sowie die kritischen Erfolgsfaktoren und Leistungsindikatoren.

Der Anhang dieses Buches bietet dem Leser Checklisten zur Verfestigung seines Wissens. Dieses Wissen kann anschließend mit Hilfe von Aufgaben und den beigefügten Lösungsvorschlägen überprüft werden.

1.4 Begriffsklärung

Die IT-Infrastructure-Library, kurz ITIL, ist grundsätzlich in das IT-Service-Management einzuordnen. Um diese Thematik genauer zu verstehen, ist es wichtig, die Begriffswelt der Dienstleistung und des Managements zu kennen. In diesem Abschnitt werden die Wortbedeutungen kurz beleuchtet.

Ein **Prozess** kann definiert werden als „eine chronologische Abfolge aller Schritte, die zur Erstellung eines Produktes erforderlich sind“ [06]. Er ist zeitlich unbegrenzt und beliebig oft reproduzierbar. Ein Prozess im Sinne von ITIL ist ein iterativer Ablauf, der weder Anfang noch ein Ende hat und somit ständig verbessert werden kann. Ein Prozess benötigt einen Input, der zweckmäßig einen Output produziert (vgl. Abb. 1.2).

Abb. 1.2. Aufgabe eines Prozesses (vereinfacht)

Ein **Geschäftsprozess** besteht aus mehreren zusammenhängenden Aufgaben, die von einem oder mehreren Beteiligten durchgeführt werden, um ein Ziel bzw. einen Zweck zu erreichen [01] [02].

Als **Prozessmanagement** oder **Geschäftsprozessmanagement** (GPM) wird die „Aufgabe des Planens und Regulierens verstanden“ [02]. Im Grunde werden Geschäftsprozesse definiert und gestaltet, gesteuert, dokumentiert und verbessert, wobei zur Steuerung und Verbesserung Kennzahlen (quantitative, messbare Größen) benötigt werden [o22]. Das Management von Prozessen sorgt für Effektivität und Effizienz der Prozesse, d. h., das Delta vom erreichten und vorher definierten Prozess gilt es zu verringern, und das mit einem ökonomisch vertretbaren, im Idealfall minimalen Aufwand.

Ein **IT-Service** (IT-Dienstleistung) ist eine Dienstleistung der Informationstechnologie und kann u. a. die Beratung, Planung und Erbringung von Leistungen, wie die Bereitstellung von Hardware- und Software-Leistungen, beinhalten. Ein IT-Service ist immateriell, unteilbar, zeitlich begrenzt, individuell, standortbezogen und kann nicht zurückgerufen werden [06]. ITIL definiert den IT-Service als „ein oder mehrere IT-Systeme, die einen Geschäftsprozess ermöglichen oder unterstützen und vom Kunden als zusammenhängendes Ganzes wahrgenommen werden“ [02].

Dabei spielt die **Qualität** eines Service eine große Rolle. Durch einen iterativ-dynamischen Zyklus, den so genannten Demingkreis oder PDCA-Zyklus, kann eine **Qualitätssicherung** eines Prozesses erreicht werden, in dem die folgenden, iterativ zu wiederholenden Schritte befolgt werden:

- die Planung eines Prozesses (Plan),
- die Einführung bzw. Ausführung eines Prozesses (Do),
- die Überprüfung von eventuellen Abweichungen mittels eines Ist-Soll-Abgleiches (Check)
- das Eingreifen bzw. Handeln, um die festgestellten Abweichungen zu beseitigen (Act).

Abbildung 1.3 zeigt, wie der als Kreis abgebildete Prozess mit jeder Iteration auf der Qualitätsskala nach oben steigt und das Abrutschen mit einem Keil, der sich aus ITIL und anderen Normen zusammensetzt, verhindert wird.

Für die Qualitätsverbesserung existieren weitere vielfältige Ansätze, derer man sich bedienen kann. Hier seien das Six Sigma, Total Quality Management (TQM), Quality Triology und das europäische **EFQM**-Modell (European Foundation for Quality Management) erwähnt, die allerdings an dieser Stelle nicht weiter vertieft werden können. Der Reifegrad eines Unternehmens kann anhand des EFQM-Modells ermittelt und mit Hilfe des Prozessmodells „Capability Maturity Model Integration“ (**CMMI**) gesteigert werden. Der CMMI-Reifegrad bezieht sich auf die Prozesse der Produktentwicklung und

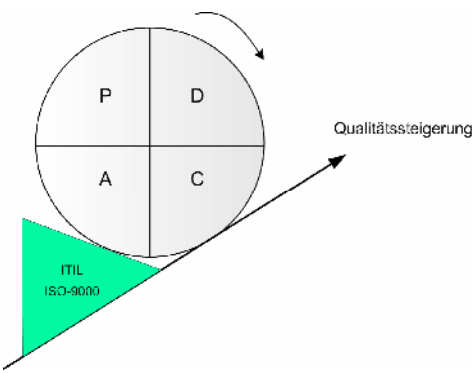

Abb. 1.3. Qualiltätsmanagement nach Deming nach [02]

besteht aus den Ebenen: *Initial, Repeatable, Defined, Managed* und *Optimizing*.

Ein **Serviceprozess** ist eine „Kombination aus Produktion und Verbrauch, an dem Anbieter und Abnehmer gleichzeitig teilnehmen“ [08]. Während der Erbringung ist es Kunden und Anbietern möglich, Einfluss auf den Service auszuüben. Ein Service kann, im Vergleich zu einem Produkt, erst nach der Erbringung bewertet werden.

Das **IT-Service-Management (ITSM)** ist als Konzept und prozessorientiertes Modell anzusehen [05]. Eine Eigenschaft von Konzepten ist ihre Skalierbarkeit. Damit können sie auf jedes Unternehmen unterschiedlicher Größe angepasst werden. Da sich die Geschäftsprozesse über viele Bereiche und Systeme ausdehnen, dürfen sie nicht technikorientiert betrachtet werden [05]. Die Aufgaben des ITSM sind umfangreich und umfassen die Lieferung und Unterstützung der IT-Services, das Management der IT-Infrastruktur und der Applikationen und die Einhaltung der Geschäftsziele [06]. Zu den wichtigsten Einflussfaktoren (vgl. Abb. 1.4) des ITSM zählen laut [06]:

- die Mitarbeiter (Motivation oder Engagement),
- die Unternehmensstrategie (strategische Vorgehensweise, dadurch Vorteile),
- das Know-how (Mitarbeiterschulung, abteilungsspezifisches Wissen etc.),
- die Prozesse (so wenig Unterbrechungen wie möglich, effizient),
- die Kunden (Zufriedenheit mit den in Anspruch genommenen Dienstleistungen),
- die Organisation und deren Kultur (Zweck der Organisation, Mentalität und Kultur einzelner Mitarbeiter oder einer Zweigstelle im Ausland),
- die Umgebung und Infrastruktur (vorteilhafter Firmenort, eingesetzte Technologie).

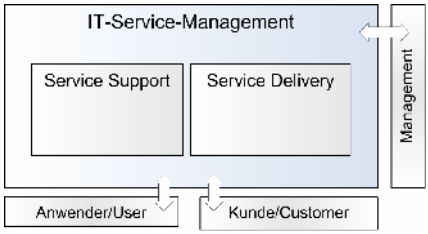

Abb. 1.4. Überblick der ITSM-Bereiche (vereinfacht)

Das Bindeglied zwischen dem Prozessmanagement und dem IT-Service-Management stellt das **Business-Service-Management** (BSM) dar, das eine bessere Zusammenführung des Business und der IT erlaubt. Ein BSM wird durch ein ITSM (z. B. auf Grundlage von ITIL) unterstützt [o18], dessen dienstorientierte Architektur der ICT (Information and Communications Technology) mit dem Managementkonzept SOA (**Serviceorientierte Architektur**) erfasst werden kann.

2 Was ist ITIL?

2.1 Historie und Philosophie

In den 80er Jahren hat die britische Regierung die „Central Computer and Telecommunications Agency“ (CCTA) damit beauftragt, herauszufinden, wie die eigenen IT-Ressourcen des öffentlichen Sektors effizienter und kosteneffektiver genutzt werden können [08]. Die Vereinheitlichung der Ergebnisse der Analysen wurde ITIL genannt und in verschiedenen Büchern definiert. Die damalige CCTA wurde im Laufe der Jahre in OGC (Office of Government Commerce) umbenannt, die seit 1989 als offizieller Herausgeber dieser Büchersammlung für den freien Markt tätig ist. Die Entwicklung der ITIL obliegt bis heute der OGC. Um ITIL anwendbar zu machen, wird sie dabei von namhaften Unternehmen in der ganzen Welt unterstützt. Dadurch wird es möglich, das ITIL-Werk weiterhin einen „Best Practice“-Leitfaden zu nennen. ITIL richtet sich an IT-Dienstleistungsfirmen, IT-Leiter und -Manager sowie an den Leiter für Informationstechnologie, den so genannten „Chief Information Officer“ (CIO) [o14].

Die erste Version bzw. Revision der Bibliothek oder Büchersammlung wurde 1995 abgeschlossen. Obwohl die Bezeichnung „erste Version“ nie in der Literatur zu finden ist, wurde diese verbessert und als offiziell zweite Version 1999 veröffentlicht. Seit Ende 2007 existiert ITIL in der dritten Revision. Diese Version ist zwar grundsätzlich bekannt, muss sich aber erst

noch neben ITIL v2 etablieren, da der Markt das entsprechende Know-how noch zu entwickeln hat.

ITIL beschreibt die wichtigsten Praktiken vieler IT-Organisationen. Das Augenmerk lag dabei nicht auf der verwendeten Software, so dass ITIL ein herstellerunabhängiges Rahmenwerk (Framework) darstellt, was die allgemeine Beliebtheit begünstigte. Das Interesse stieg vor allem in Großbritannien, schwappte danach wie eine Welle auf die Niederlande und infolgedessen u. a. auch auf Deutschland über, wo mittlerweile 98% der befragten Unternehmen ITIL als De-facto-Standard kennen [o13]. Die eigene Aussage des OGC über ITIL wird dadurch untermauert: „IT Infrastructure Library (ITIL) is the most widely accepted approach to IT service management in the world“ [o14].

ITIL kann zusammenfassend beschrieben werden als eine Bibliothek von Büchern, die das bestbewährte Erfahrungswissen aus der Praxis von IT-Organisationen vereinheitlichend zusammenfasst, in dem die Inhalte, Prozesse und Ziele innerhalb eines Unternehmens als „was zu tun ist“ verdeutlicht werden, ohne eine genaue Vorschrift über das „wie es zu tun ist“ festzulegen. Letzteres wird in entsprechenden Normen als Ergänzung definiert.

2.2 Vorteile und Nachteile

Die Anwendung von ITIL bringt viele Vorteile mit sich. Die OGC wirbt dafür mit dem Slogan „the key to managing IT services“ [o14]. Mit ITIL wird die Verständigung zwischen IT-Abteilungen innerhalb eines Unternehmens und unternehmensübergreifend mit Hilfe einer gemeinsamen Terminologie für das IT-Service-Management verbessert [o20]. ITIL gibt Hinweise darauf, was gemacht werden sollte, stellt

einem Unternehmen aber frei, wie es die Implementierung wählt [06].

Die Kundenorientierung wird innerhalb der IT als IT-Service-Management abgebildet, mit definierten Schnittstellen und Verantwortlichkeiten. Nur so kann ein Höchstmaß an Qualität und Kundenzufriedenheit gewährleistet werden [06]. Drei Hauptziele werden mit ITIL und dem daraus entstehenden ITSM verfolgt [o07]:

- Ausrichtung des IT-Services auf eigene Unternehmensanforderungen und die der Kunden,
- Qualitätsoptimierung der erbrachten IT-Services,
- Reduzierung der langfristigen Kosten von Dienstleistungen.

Welchen weiteren Nutzen bringt die Anwendung der Best-Practices für das eigene Unternehmen? Da es sich bei ITIL um einen Leitfaden praktischer Erfahrungen handelt, muss das Rad nicht neu erfunden werden. Bei gezieltem Einsatz kann eine hohe Produktivität erreicht werden. Für die eigene Organisation müssen lediglich die Prozesse angepasst werden, was weniger Aufwand bei der Entwicklung von Prozessen, Prozeduren und Arbeitsanweisungen bedeutet [o12]. Die Qualität der IT-Services und der unternehmensinternen Abteilungsbeziehungen, die u. a. eine verbesserte Kommunikation erhalten, wird messbar und bewertbar. Dies erlaubt einen Ist-Soll-Vergleich und somit eine Verbesserungsmöglichkeit (Optimierung) der Prozesse des eigenen IT-Service-Managements.

Dadurch, dass Anforderungen an IT-Services mit Hilfe so genannter Service-Level-Agreements (SLA) definiert werden, macht es die Sache leichter, den abgeschlossenen Verträgen und den damit festgelegten Pflichten gegenüber dem Kunden nachzukommen. Die erbrachten IT-Dienstleistungen entsprechen also den vereinbarten Anforderungen, die den Kunden zufrieden stimmen. Durch Struktur und festgelegte Zuständigkeiten kann eine höhere Mitarbeiterzufriedenheit erzielt werden, mit dem

Nebeneffekt, dass die Personalfluktuation niedrig bleibt bzw. sukzessiv abnimmt.

Für die Praxis und Anwendbarkeit ist ITIL auch deswegen interessant, weil es ein frei zugänglicher De-facto-Standard ist und dessen Anwendung keine Mitgliedschaft erfordert [05]. Es steht ein umfangreiches Wissen in einer Sammlung von Best-Practices zur Verfügung, das sich bei vielen IT-Organisationen bewährt hat. Durch die Befolgung des Leitfadens wird automatisch die vom Markt geforderte Kunden- und Anwenderorientierung im Unternehmen realisiert. Der Grad der Implementierung des ITSM im eigenen Unternehmen kann durch verschiedene Institutionen und Normen qualitätsgesichert werden, um sich auf dem freien Markt zu behaupten.

Wo es auch Fürsprecher gibt, sind die Gegner und Kritiker nicht weit. Was für manche als klarer Vorteil gilt, ist für andere ein Nachteil. So wird von den Kritikern beanstandet, dass die IT-Infrastructure-Library keine umfassende Standardisierung ist, sondern nur ein Best-Practice-Ansatz. Weiterhin wird bemängelt, dass mit ITIL nicht beschrieben wird, *wie* etwas getan werden soll. Hier muss man sich das Know-how selbst aneignen, was zeitaufwendig und unter Umständen teuer ist, oder es muss auf einen externen Dienstleister zurückgegriffen werden, der für seinen Service auch entlohnt werden möchte. Weil ITIL für alle Unternehmen adaptiert werden kann, fallen die Beschreibungen ungenau aus [o20]. Das lässt viel Spielraum für mehrdeutige Lösungsansätze und Fehlinterpretationen. Als Neuling auf diesem Themengebiet ist man schnell verunsichert und greift auf die konkretisierende Sekundärliteratur zurück.

Der ITIL-Skeptiker allgemein beschwert sich über die vielen Abkürzungen („too many three letter acronyms (TMTLA)“ [o05]), die in ITIL verwendet werden und stellt die ITIL-Philosophie mit der Gleichung „ITIL = TMTLA?“ in Frage. Weitere neue Thesen des ITIL-Skeptikers zeigen auf, dass solche ITIL-

Projekte „überteuerte Renovierungen“ [o06] seien und die CMDB (Configuration Database) „nicht umsetzbar“ sei, wie ITIL sie definiert [o06]. In einigen Fällen werden andere ITSM-Frameworks – wie das MOF – empfohlen, die frei zugänglich sind und konkrete Anweisung zur Umsetzung beinhalten.

In der Ausarbeitung [o16] der Universität St. Gallen wird u. a. als Fazit gezogen, dass, obwohl das ITIL-Framework auf jedes Unternehmen adaptiert werden kann, es dennoch in der Praxis nicht zutrifft. Einige Methoden und Konzepte sind nur dann sinnvoll, wenn die IT-Organisation eine bestimmte Größe aufweist (vgl. auch [03]). Es existieren keine verfügbaren Leitlinien, die die Auswahl eines für das Unternehmen relevanten serviceorientierten IT-Managements erleichtern. Ein Auszug aus dem Fazit macht die Notwendigkeit einer Verbesserung des ITIL-Frameworks unter den beschriebenen Nachteilen deutlich: „A mere orientation to ITIL is not enough“ [o16].

Alle genannten Nachteile, ob begründet oder nicht, werden überwiegend mit der neuen ITIL-Revision 3 behoben (siehe nachfolgende Abschnitte). Einen Vorwurf muss sich ITIL jedoch gefallen lassen: Es ist nicht branchen-spezifisch.

2.3 Standards und Normen

ITIL bildet eine mögliche Grundlage für ein IT-Service-Management. Es gibt weitere ITIL-„Abkömmlinge“, wie in diesem Abschnitt noch beschrieben wird. Im Abschnitt zuvor wurde erwähnt, dass ITIL nicht vorschreibt, wie das ITSM realisiert werden soll. Es übernimmt also keine Aufgaben des Projektmanagements, weil es die „Einführung einer IT-Infrastruktur nicht organisiert“ [o20]. ITIL hilft vielmehr aufgrund seiner Prozessorientierung bei der Organisation des Betriebs einer IT-Infrastruktur durch definierte Aufgabenstellungen. Aus

diesem Grund kann die IT-Infrastructure-Library auch beim IT-Outsourcing von Vorteil sein.

Das OGC hat für das Projektmanagement ebenfalls eine Lösung parat. Weil es 1989 von der gleichen Organisation entwickelt wurde, empfiehlt OGC neben der Anwendung von ITIL auch die Anwendung von **PRINCE**. „Projects in controlled Environments“ (PRINCE) ist eine Methode des Projektmanagements. Seit 1996 liegt die überarbeite Version **PRINCE2** vor, die einen prozessorientierten Ansatz des Projektmanagements bietet und heute, ebenfalls wie ITIL, als De-facto-Standard gilt. Ohne auf weitere Details einzugehen, bietet die Abb. 2.1 einen Gesamtüberblick über die acht Prozesse.

Nachdem das ITSM im eigenen Unternehmen realisiert worden ist, besteht die Möglichkeit, es zertifizieren zu lassen. Dadurch kann der Nachweis der Qualität erbracht werden, der das Image der Organisation aufwertet und ermöglicht, unter Umständen mehr Verträge abzuschließen, wenn vom Kunden solch eine Zertifizierung für die Zusammenarbeit verlangt wird.

Damit eine bestimmte Qualität nachgewiesen werden kann, muss diese gemessen und bewertet werden können. Aus diesem

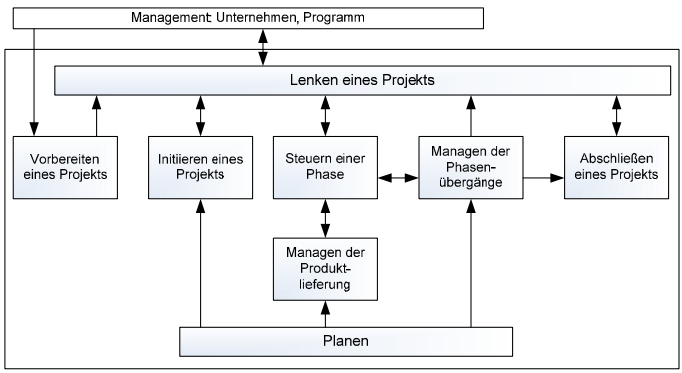

Abb. 2.1. Übersicht über die acht PRINCE2-Prozesse nach [o20]

Grund erlaubt ITIL mit Hilfe so genannter (quantitativer) Leistungsindikatoren (Key Performance Indicators, kurz **KPI**s), die Messung und Bewertung der erbrachten IT-Dienstleistungen und somit der Geschäftsprozesse und der IT-Infrastruktur. In [06] werden unterschiedliche Normen des „Deutschen Instituts für Normung e. V." (DIN) genannt, die eine Messung und Auswertung ermöglichen: DIN 40080, DIN ISO 5725, DIN 53803, DIN 53804, DIN 55302, DIN 55350 und die DIN 55303 für die statistische Auswertung von Daten. Eine Norm ist nicht verbindlich, d. h., sie ist nicht gesetzlich vorgeschrieben und muss nicht eingehalten werden. Normen werden nur dann verbindlich, wenn dies vertraglich festgesetzt wird. Die DIN ist für die deutschen Interessen in den internationalen und europäischen Gremien für Normung (ISO, CEN) verantwortlich, kann aber auch internationale Normen in nationale übernehmen.

Im Jahr 2000 wurde von der „British Standards Institution" (BSI) der British-Standard „**BS 15000**" festgelegt. Dieser Standard macht es möglich, die Konformität des implementierten ITSM gegenüber dem ITIL-Grundgerüst zu belegen. BS 15000 wurde in 2005 zu einem neuen internationalen ISO-Standard „**ISO/IEC 20000**" (kurz: ISO 20000). Er beschreibt einen Satz an Managementprozessen, die auch in ITIL definiert sind, und ergänzt diese. Betrachtet man das ITSM in erster Linie aus der Sicht des Standards ISO/IEC 20000, so bieten die ITIL-Bücher erweiterte Informationen und Leitlinien dazu [08]. Der Standard ISO 20000 ist in zwei Teile unterteilt. Der erste Teil ISO 20000-1, ausgesprochen „ISO 20000 Part 1", enthält die formale Spezifikation des Standards und ist betitelt als „Spezifikation". Der zweite Teil ISO 20000-2 („ISO 20000 Part 2") trägt die Überschrift „Code of Practice" und beinhaltet detailliertere Erläuterungen der Best-Practices. Er enthält Leitlinien und Empfehlungen [08] (vgl. Abb. 2.2).

Die erfolgreiche Umsetzung der ISO 20000 in einer Organisation kann ebenfalls zertifiziert werden. Welche Prozesse das

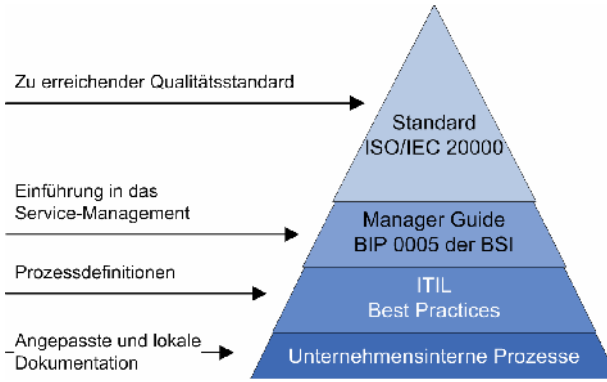

Abb. 2.2. Einordnung von ISO/IEC 20000 und ITIL nach [08]

ISO 20000 definiert, kann der Tabelle 2.1 entnommen werden. Hier ist auch die starke Anlehnung der ITIL-Prozesse an diesen Standard erkennbar.

Als Ergänzung zu ITIL beinhaltet der Standard ISO 20000 den zuvor beschriebenen PDCA-Zyklus (nach Deming) zur Qualitätsverbesserung. Dieses Prinzip wird als „Aufwärtszyklus nie abgeschlossener Verbesserungen" bezeichnet [08] (vgl. Abb. 2.3).

Der Standard ISO/IEC 20000 enthält Anforderungen an ein professionelles ITSM und dient als messbarer Qualitätsstandard. Die Maßnahmen zu einem Qualitätsmanagement für das ITSM stehen jedoch in der international anerkannten **DIN EN ISO 9000 ff** (oft auch ISO 9000). Früher bekannt als ISO 9000:2000, existiert diese Norm derzeit in der aktuellen Fassung **ISO 9000:2005** vom Jahr 2005. Sie bildet ein „umfangreiches Werk bestehend aus Leitfäden, Normen, Begriffen und QM-Modellen" [o17], das prozessorientiert aufgebaut ist. Die (unvollständige) Tabelle 2.2 beschreibt die wichtigsten Normen für das Qualitätsmanagement.

Tabelle 2.1. Prozesse des Standards ISO/IEC 20000 und ITIL [08]

Prozesse ISO/IEC 20000	Prozesse in ITIL
Configuration-Management	Configuration-Management
Change-Management	Change-Management
Release-Management	Release-Management
Incident-Management	Incident-Management
Problem-Management	Problem-Management
Capacity-Management	Capacity-Management
Service-Continuity- und Availability-Management	Service-Continuity- und Availability-Management
Service-Level-Management	Service-Level-Management
Service-Reporting (Berichte)	–
Information-Security-Management	Security-Management
Finanzplanung und Kostensenkung für IT-Services	Financial-Management
Business-Relationship-Management	Die Reihe „Business Perspective“ und die Version der Ausgabe der „Customer Liaison“
Lieferanten-Management	ITIL v1: „Managing Facilities and Third Party Relationships“; Teilinhalte des Buchs „Business Perspective“
–	ICT-Infrastructure-Management
–	Application-Management
–	Planning to Implement Service-Management

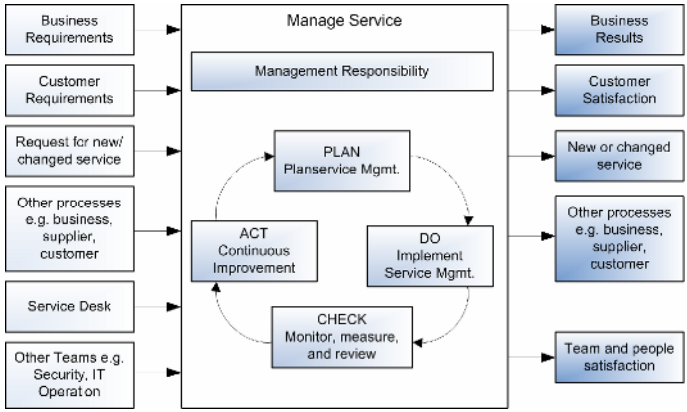

Abb. 2.3. Service-Management-Sicht nach [07]

Die Norm ISO 9001 beschreibt das Modell eines prozessorientierten Qualitätsmanagementsystems. Die Abb. 2.4 zeigt sehr deutlich, dass die Qualität eines Produktes, einer Dienstleistung

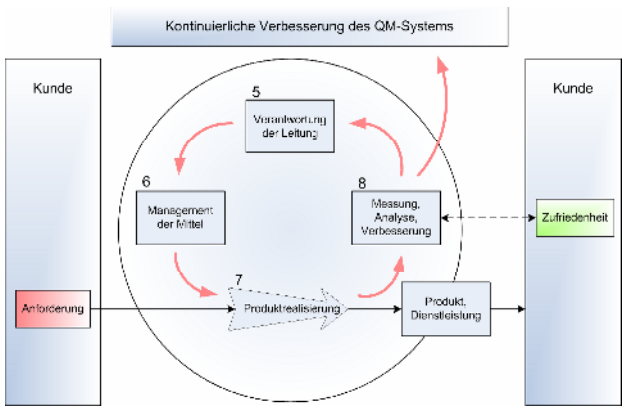

Abb. 2.4. Modell eines prozessorientierten QM-Systems nach [o04]

Tabelle 2.2. Übersicht der Qualitätsnormen

Norm	Bezeichnung
ISO 9000	Begriffe, Definitionen
ISO 9001	Nachweisforderung (bisher 9001, 9002, 9003)
ISO 9004	Anleitung zur Verbesserung der Leistungen
ISO 19011	Auditwesen, Leitfaden für das Auditieren

oder eines Prozesses iterativ geprüft und gesteuert werden muss. Es wird deutlich, dass es bei einem Prozess im Prinzip egal ist, zu welchem Zeitpunkt er begonnen wird, da es – im Gegensatz zu einem Projekt – weder Anfang noch Ende gibt.

Zum Schluss dieses Abschnitts soll für den besseren Überblick die Abb. 2.5 ausreichen. Es werden die unterschiedlichen Initiatoren des ITSM und die sich daraus ergebenden Initiativen in Bezug gebracht.

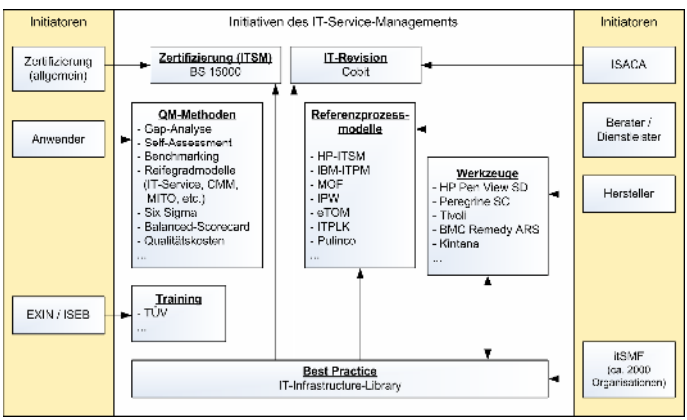

Abb. 2.5. Initiativen des IT-Service-Managements nach [o15]

2.4 Publikationen, ITIL v2 und v3

ITIL in der zweiten Revision besteht aus sieben Kernpublikationen und einem ergänzenden Teil. In der Revision 3 ist ITIL auf insgesamt fünf Kernelemente und einer umfangreichen Einführung beschränkt. In Abb. 2.6 sind die beiden Revisionen übersichtlich gegenüber gestellt.

In der zweiten Revision beschäftigt sich der **Service-Support** mit der Unterstützung der IT-Dienstleistungen, also mit der operativen Ebene, ohne die jeder IT-Service, und somit auch jeder Geschäftsprozess, zusammenbrechen würde. Störungen werden registriert, Probleme daraufhin erkannt und behoben und Änderungen an der IT-Infrastruktur vorgenommen und dokumentiert. Hier spricht man von dem Incident-, Problem-, Change-, Configuration- und Release-Management, welche stark verzahnt werden können. Das **Service-Delivery** beschreibt die taktische Ebene und fasst die Prozesse zusammen, die eine Dienstleistung durch Planung und Steuerung erst ermöglichen. Es werden Dienstleistungen zunächst definiert, die Kosten und Kapazitäten und die Verfügbarkeit zur Serviceerbringung überprüft, und schließlich diese dem Kunden angeboten. Konkret spricht man hier von dem Service-Level-, Financial-, Capacity-, Continuity- und dem Availability-Management. Die weiteren Disziplinen erfüllen u. a. die IT-Infrastruktur-Anforderungen der Planung und Umsetzung und der Sicherheit.

Das **Security-Management** formuliert ein definiertes Sicherheitsniveau für die IT-Umgebung [o21]. Wichtige Sicherheitsfaktoren wie Vertraulichkeit, Integrität und Verfügbarkeit der IT werden detailliert beleuchtet. Mit Hilfe der Risikoanalyse werden die unternehmensinternen und die kundenspezifischen Sicherheits-Level ermittelt. Der IT-Grundschutz beinhaltet den internen, minimalen Sicherheitsanspruch. Für ein IT-Service-Management kann die Norm ISO 17799 befolgt werden. Im **ICT-**Infrastructure-Management werden die für

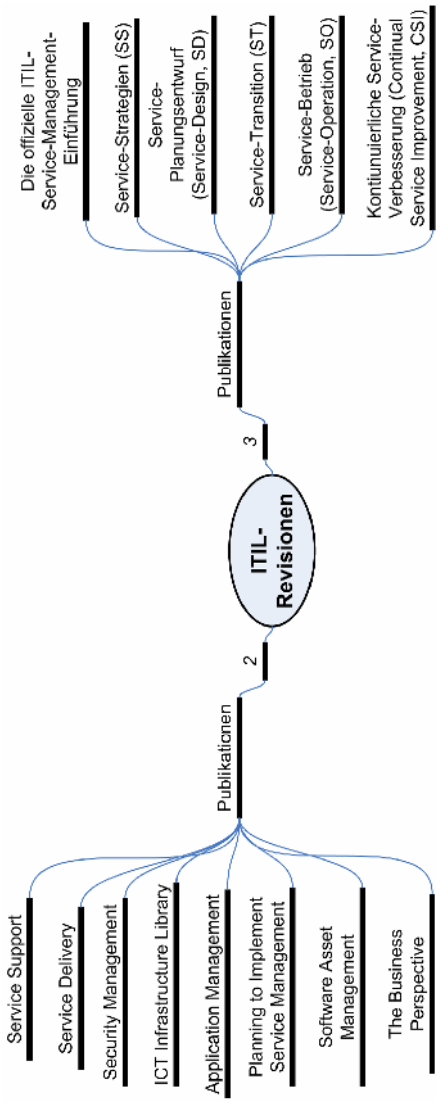

Abb. 2.6. Übersicht der ITIL-Revisionen 2 und 3

den Aufbau und Einführung einer IT-Infrastruktur wichtigen IT-Strategien und IT-Prozesse entwickelt und gepflegt („Design and Planning“). Im „Deployment“ spielt das Rollout, also die Einführung von neuen oder erweiterten Hardware- und Software-Releases in die Produktion, eine Rolle. Der Bereich „Operations“ stellt die Basis für alle IT-Services und die damit verbundenen Infrastrukturaktivitäten dar, wo hingegen sich der „Technical Support“ um die aktuellen und zukünftigen IT-Infrastrukturlösungen kümmert. Das **Application-Management** beschreibt den IT-Service-Lifecycle durch die nötigen Erfordernisse, das Design, die Herstellung, Auslieferung und das Optimieren der IT-Dienstleistungen. Die Beziehung der IT zum Kunden wird in der **Business-Perspective** beschrieben. Das **Software-Asset-Management** kümmert sich um die Steuerung der Lebenszyklen von Software und Assets (Aktivposten). Das letzte Buch der ITIL „**Planning to Implement**

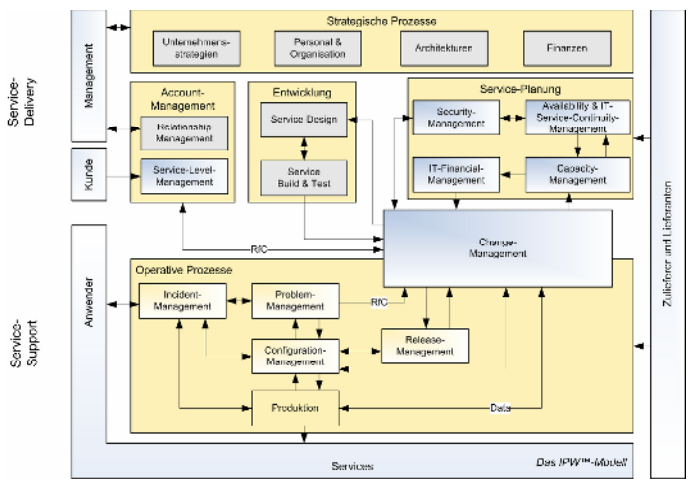

Abb. 2.7. Das Management-Modell nach ITIL (IPW™)

Service Management“ dient als Anleitung zur Einführung und Nutzung von ITIL in eine reale IT.

In der Abb. 2.7 werden die einzelnen ITIL-Prozesse des Service-Supports und des -Delivery in die drei Ebenen – operativ, strategisch und taktisch – für den Überblick dargestellt.

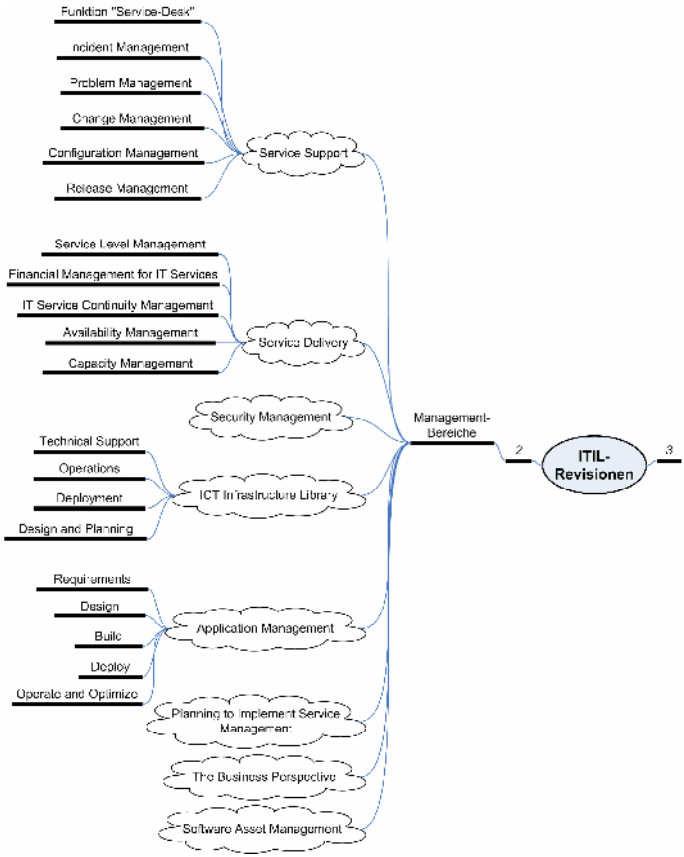

Abb. 2.8. Managementbereiche der zweiten ITIL-Revision

Die einzelnen Publikationen werden in Managementprozesse bzw. -bereiche unterteilt, die nachfolgend für die ITIL-Revision 2 in der Abb. 2.8 übersichtlich präsentiert werden.

Während die ITIL-Revision 2 überprüft wurde (Review), war der Begriff „ITIL Refresh“ in aller Munde. Der dazugehörige „Scope and Development Plan“ stellt die Anforderungen an die neue ITIL-Version zusammen und kann in [o10] genauer nachgelesen werden. Die IT-Infrastructure-Library wurde vom OGC und seinen Partnern neu strukturiert und im Hinblick auf die Nützlichkeit und konkrete Anwendbarkeit in den IT-Organisationen hin verbessert. Alle Anstrengungen mündeten in der ITIL-Revision 3.

Einige der wichtigsten Punkte sind hier kurz zusammengefasst (vgl. [o08] und Abb. 2.9):

- ITIL richtet sich noch ausdrücklicher nach dem Business-Nutzen.
- Der Fokus liegt auf dem Service Life Cycle – und erst in zweiter Linie auf den Prozessen.

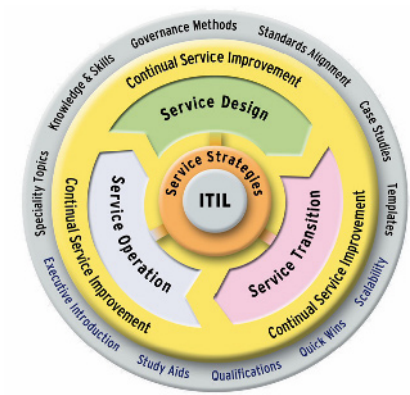

Abb. 2.9. Das Core-Framework [o08]

- Mit ITIL V3 wird die Grundlage zu einer Balanced-Score-Card (BSC) geschaffen.
- Qualitätsmanagement auf Basis des Deming Quality Cycle stellt die lernende Organisation in den Mittelpunkt.
- ITIL V3 ist mit dem Standard ISO/IEC 20000 abgestimmt.
- Verbesserung in der Messbarkeit und Erbringung des Nachweises der echten Wertschöpfung.
- Alle V2-Prozesse sind wieder in V3.

Das Kernbuch **Service-Strategy** befasst sich mit der Konzeption und Strategie von Service-Prozessen aus der Geschäftsperspektive. Es geht hier um die Definition, Spezifikation, aber auch um die Logistik und die Buchhaltung (Finanzen) der zu erbringenden Dienstleistungen. Dies wird mit den Disziplinen Service-Management-Life-Cycle, Service-Strategy-Processes (Strategieentwicklung und Finanzmanagement), Organizational-Development-and-Design und Implementing-Service-Strategy abgedeckt.

Das **Service-Design** befasst sich mit der Architektur von Service-Prozessen. Neben ihrer Definition, Spezifikation und Logistik werden die Sicherheitsaspekte aus der operativen Sicht beachtet. Die Geschäftsperspektive wird in Service-Leistungen übertragen, unter der Beachtung der unternehmerischen Ziele. Das Service-Design umfasst somit die Service-Design-Principles, Service-Design-Technology und die Service-Design-Implementation. Ersteres wird noch unterteilt in den Service-Design-Process, das Service-Portfolio-Design, das Service-Catalogue-Management, das Capacity-, Availability-, Service-Level-, Service-Continuity- Information-Security- und das Supplier-Management.

In der Service-Transition wird die „praktische und faktische Umsetzung und Übertragung der geschäftlichen Anforderungen in konkrete IT-Dienstleistungen“ [o21] behandelt. Die Aufgaben des Change-Managements werden erweitert und die Über-

mittlung der Service-Leistungen ist nun standardisiert. Enthalten sind die für eine Service-Bereitstellung erforderlichen Aspekte, wie die Risikoanalyse, die Nutzenrechnung, sichere Auslieferung und die Gewährleistung für eine stabile Erfüllung der Dienstleistungen. Gegenständlich sind die Managementbereiche unterteilt in die Service-Transition-Principles, Service-Transition-Processes, Common-Operation-Activities, sowie Technology- und Implementation-Considerations. Der Bereich Service-Transition-Processes ist nochmals unterteilt in das Change-, Service-Assets-and-Configuration- und Knowledge-Management sowie das Service-Release-Planing, Performance-and-Risk-Evaluation, „Acquire-Assets, Build and Test Release", „Service Release Acceptance, Test and Pilot" und zuletzt das „Deployment, Decommission and Transfer".

Das Buch **Service-Operation** beschreibt die operativen Aufgaben, um den Betrieb der vereinbarten Dienstleistungen reibungslos zu gewährleisten. Die Bereiche Service-Delivery und Service-Support aus der ITIL-Revision 2 bilden hier den Hauptteil. Zunächst wird auf den operativen Grundsatz eingegangen (Service-Operation-Principles). Hiernach werden die Prozesse wie das Event-, Incident-, Request-, Problem- und Access-Management unter dem Titel Service-Operation-Processes zusammengefasst. Die bei einem Service allgemein anfallenden Tätigkeiten werden in der Disziplin Common-Service-Operation-Activities angesprochen. Zum Schluss finden sich noch die Abschnitte der IT-Sicherheit und der Organisation der Dienstleistungen (Service-Desk etc.).

Die letzte noch zu beschreibende Publikation beschäftigt sich mit der Verbesserung von Dienstleistungen. Dabei geht es bei **Service-Improvement** um die Optimierung der Servicequalität durch Nutzung von Leistungsparametern und Messgrößen, Überwachung der vereinbarten Ziele und das Auffindung von Schwachstellen. Dies kann, wie bereits im vorangegangenen Abschnitt erwähnt, den geschäftlichen Erfolg sichern. Das

Prinzip der Service-Verbesserung ist in Continual-Service-Improvement-Principles niedergeschrieben. Die Prozesse zur Verbesserung der Leistungen werden als Measurement-and-Control, Service-Assessment-and-Analysis und Service-Level-Management definiert. Wie bei den anderen Kernbüchern auch, bildet das „Organizing for Service Continual Improvement“, in dem es um die Einrichtung einer Service-Steigerung geht, das Schlusslicht.

Einen grafischen Überblick über die Einordnung der einzelnen Prozesse liefert die Mind-Map der Abb. 2.10.

Nach dieser etwas genaueren Betrachtung der Revisionen des ITIL-Frameworks wird deren Ähnlichkeit deutlich. Doch wie viel ITIL v2 steckt in ITIL v3 wirklich? Wie sind die

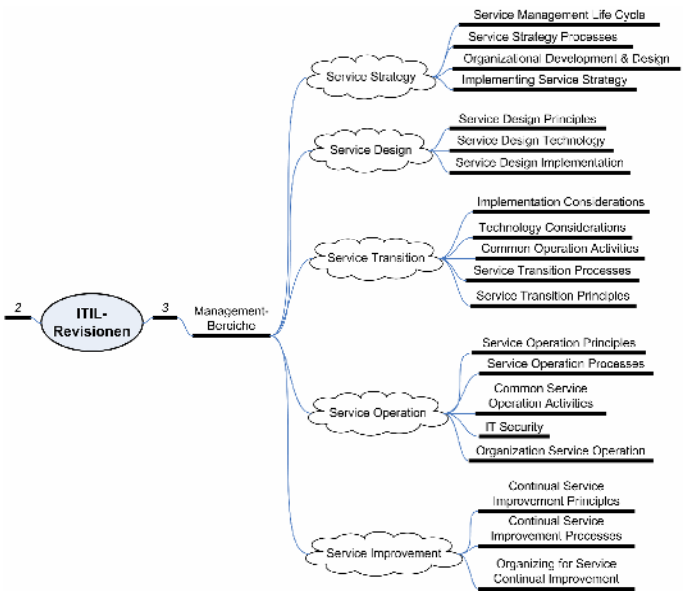

Abb. 2.10. Managementbereiche der dritten ITIL-Revision

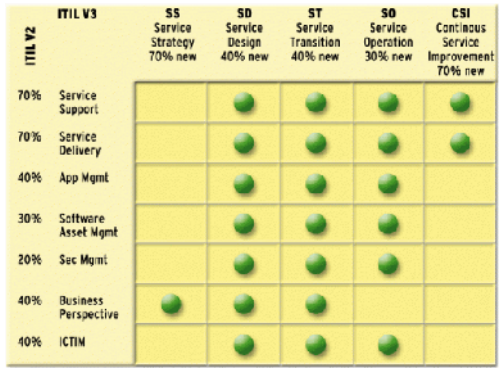

Abb. 2.11. Mapping ITIL v3 und v2 [o09]

Managementprozesse aufgeteilt worden? Diese Fragen werden in [o09] anschaulich in einem Mapping in Abb. 2.11 aufgezeigt.

Das Mapping in Abb. 2.11 zeigt deutlich, dass der Grundgedanke der zweiten Revision in der dritten Version neu aufgeteilt worden ist. Die sieben Kernbücher werden auf die neuen fünf verteilt. Dabei wird von den „alten" Büchern minimal 20 Prozent, maximal aber 70 Prozent von Service-Support und Service-Delivery übernommen. Es kann beobachtet werden, dass das Wissen überwiegend auf die drei Bereiche Service-Design, Service-Transition und Service-Operation verteilt ist. Der Best-Practice-Ansatz ist in der dritten Revision, wie versprochen, erweitert worden. Das neu eingeflossene Wissen ist bei Service-Strategy und Continous-Service-Improvement mit jeweils 70 Prozent eingeflossen. Dabei ist in Service-Design und Service-Transition 60 Prozent und bei Service-Operation 70 Prozent der alten Revision vorhanden. Anders ausgedrückt bedeutet dies, dass die neue ITIL-Revision 3 zur Hälfte aus altem, zur Hälfte aus neuem Wissen besteht.

In diesem Buch wird noch die ITIL-Revision 2 beschrieben, und zwar u. a. aus zwei Gründen. Zum einen erfolgte die Liefe-

rung der Bücher der neuen Revision 3 erst ab Juni 2007, die deutsche Ausgabe erst ab dem Frühjahr 2008 [o03]. Der TÜV Süd bietet deswegen die ITIL v3-Zertifizierungen überhaupt erst ab dem Herbst 2007 an. Zum anderen ist die Ähnlichkeit der beiden Revisionen zum Großteil gegeben. Weiterhin wird von einem schnellen Umstieg von der Revision 2 auf 3 abgeraten und dafür plädiert, erst die „ITIL-V-2-Projekte in Ruhe zu Ende zu bringen“ [o02]. Mit dem Werkzeug „ITSM Self-Check“ besteht die Möglichkeit, die „Rosinen aus ITIL 3 zu picken“ [o02] und somit risikofreie und zielorientierte Migration von ITIL v2 auf v3 zu ermöglichen.

3 Die ITIL-Managementbereiche

3.1 Einleitung

Ein Unternehmen, das Produkte entwickelt oder IT-Services anbietet, muss überlebensfähig sein. Bei der Gründung wird ein Business-Plan erstellt, der sich mit dem zu betretenden Markt und den Unternehmenschancen, der Organisation, den Zielen und Finanzen beschäftigt. Kurz gefasst geht es dabei um die Visionen, Ziele und Politik eines Unternehmens. Für eine Dienstleistungsfirma sind diese Aspekte von großer Wichtigkeit, um die Qualität der IT-Dienstleistungen für die Erbringung zu definieren. Durch definierte Visionen, Ziele und Politik kann die Qualität der Prozesse innerhalb des Unternehmens und die der angebotenen IT-Services steigen. Mit Hilfe einer Reifegradermittlung kann eine Organisation Verbesserungsstrategien und konkrete Pläne zur Umsetzung der Visionen entwickeln. Es muss dabei beachtet werden, dass der Reifegrad der Prozesse innerhalb der IT anhand der Firmenziele stetig gesteigert wird. Dieses Kapitel beschäftigt sich mit diesen Aspekten und gibt hierzu eine Einleitung in die ITIL-Philosophie.

Eine Vision einer Organisation hat etwas mit dem Image-Aufbau zu tun. Das öffentliche Ansehen sollte gut oder hoch sein, um die Attraktivität eines Arbeitsplatzes zu steigern, was dem Unternehmen zu Gute kommt, indem es z. B. expandiert. Zur Vision gehört auch ein kurzer Abriss der Ziele und die

dabei zu berücksichtigenden Werte [02]: das so genannte **Mission**-Statement. Im nächsten Schritt werden in der Zielsetzung die angestrebten Ziele im Einzelnen beschrieben. Hier ist darauf zu achten, dass ein Ziel spezifisch, messbar, erreichbar, relevant/realistisch und zeitbezogen ist. Dieser Maßstab ist auch bekannt unter dem Akronym „SMART“: **S**pecific, **M**easurable, **A**chievable, **R**ealistic/Relevant, **T**imely/time-bound. Um die Zielsetzungen zu konkretisieren und zu realisieren, ist die Politik eines Unternehmens entscheidend. Die Politik ist die Gesamtheit der Entscheidungen und Maßnahmen zur Erreichung der Ziele (vgl. Abb. 3.1).

Der Ist-Zustand des Unternehmens muss ständig beobachtet und überprüft werden. Für die Umsetzung der Politik können Jahres-, Quartals- und/oder Projektplanungen durchgeführt werden. Der Fortschritt kann anhand von Mess- und Prüfpunkten während der Ausführung ermittelt werden. In diesem Zusammenhang ist die gängigste Mess- und Prüfmethode die **Balanced-Score-Card** (BSC) [02]. Die BSC-Methode erlaubt es, aus den Zielen der Organisation oder der Prozesse die so genann-

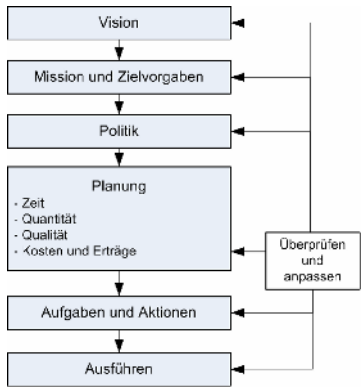

Abb. 3.1. Vision, Ziele und Politik nach [02]

ten kritischen Erfolgsfaktoren (Critical-Success-Factors, **CSF**) abzuleiten. Im Anschluss daran werden die quantitativen Leistungsindikatoren (Key-Performance-Indicators, **KPI**) ermittelt [02]. Mit den CSFs und KPIs stehen für die Messung qualitative und quantitative Leistungsindikatoren zur Verfügung. Mit einem CSF können der Kunde bzw. Markt, die Unternehmensprozesse, das Personal, die Innovation oder die Finanzen gemeint sein. Anhand der KPIs können die kritischen Faktoren überprüft werden, ob sie wie vereinbart erreicht werden.

Nachdem das Unternehmen weiß, wo und wie es dorthin gelangen möchte, kann der Reifegrad bestimmt werden. Dies ist z. B. mit dem Modell „European Foundation for Quality Management“ (EFQM) möglich.

In diesem Zusammenhang ist auch der Reifegrad des Kunden wichtig, damit die Kommunikation problemlos funktioniert. Die Kommunikation sollte auf gleicher Ebene geführt werden, um Fehlkommunikation zu vermeiden. Hier spricht man von einer horizontalen Kommunikation. Tabelle 3.1 zeigt die Abstufungen einer Organisation auf (nach EFQM-Modell).

Tabelle 3.1. Abstufungen des EFQM-Modells [02]

Stufe	Erläuterung
Produktorientiert	Jeder Mitarbeiter gibt sein Bestes, output-orientiert.
Prozessorientiert	Alle Leistungen sind geplant und wiederholbar.
Systemorientiert	Es findet eine abteilungsübergreifende Zusammenarbeit statt.
Kettenorientiert	Organisation konzentriert sich auf den erbrachten Wert zwischen der Kette von Anbietern zu den Kunden.
Absolute Qualitätssorgfalt	Das permanente und ausgewogene Streben nach Verbesserungen ist zum festen Bestandteil der Unternehmenskultur geworden.

Tabelle 3.2. Fünf Ebenen des Modells CMMI [o19, 09]

Ebene	Erläuterung
1 – Initial	Ad-hoc-Arbeitsweise der Prozesse, keine Anforderungen, automatischer Reifegrad für jede Organisation.
2 – Managed	Projekte unterstehen einer Leitung, ein ähnliches Projekt kann erfolgreich wiederholt werden.
3 – Defined	Prozesse sind dokumentiert, standardisiert und integriert.
4 – Quantitatively Managed	Ergebnisse werden kontrolliert und die Servicequalität wird bewusst gesteuert.
5 – Optimizing	Optimierung der Prozesse zur Steigerung der Servicequalität, Anwendung neuer Technologien oder Entwicklung neuer Services.

Ist nun bekannt, zu welcher Stufe sich ein Unternehmen zählen kann, sollte nach Möglichkeit eine Verbesserung dieses Zustandes angestrebt werden. Die Prozesse sollten weiter in ihrer Reifung gesteigert werden. Wie zu Anfang erwähnt, ist dies mit dem CMMI-Prozessmodell möglich. Bezogen auf die Prozesse ist das integrierte Capability-Maturity-Model in fünf Ebenen unterteilt (vgl. Tabelle 3.2).

Bei den fünf Ebenen sollte die höchste („Optimizing“) erzielt werden. Von Ebene zu Ebene können Prozesse nur durch ständige Verbesserung gelangen, indem sie bewusst gesteuert werden. Auch in diesem Fall existiert als Hilfestellung ein Modell zur Prozessverbesserung, das immer wiederkehrende Fragen innerhalb eines IT-Service-Managements zu lösen weiß, wie die Abb. 3.2 zeigt.

In der IT-Infrastructure-Library werden Prozesse definiert, da ein ITSM prozessorientiert ist. Um zu prüfen, ob ein Ziel bezüglich eines Prozesses erreicht ist, werden Messdaten benötigt. Der Key-Performance-Indicator stellt solche Messgrößen be-

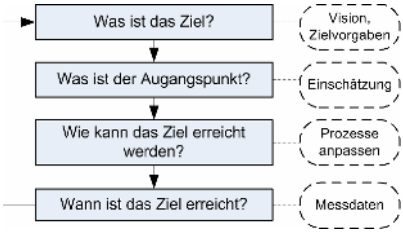

Abb. 3.2. Prozessverbesserungsmodell nach [02]

reit, die auch für den ITIL-Einsatz notwendig sind. KPIs können in vielen Fällen direkte Überwachungsaufgaben übernehmen, wenn Abweichungen registriert werden, auf die reagiert werden muss. Der Erfolg und Nutzen einer ITIL-Implementierung lassen sich dadurch ermitteln.

Ein KPI liefert betriebswirtschaftliche oder andere Kennzahlen, deren Erreichung die Grundlage eines Vertrages darstellen kann. In diesem Fall müssen sie in einem Service-Level-Agreement (SLA) formuliert werden, den es einzuhalten gilt. KPIs sind also Messgrößen für Prozesse im Zusammenhang mit den SLAs [05]. Im Idealfall sind die KPIs vor ITIL vorhanden, werden aber des Öfteren auch während eines Prozesses bestimmt. Es gibt unterschiedliche KPIs und Ermittlungsmethoden. Einerseits gibt es typische Durchlaufzeiten (pro Fraktion): Wie lange dauert die Bearbeitung im First-Level-Support? Wie sind die Reaktionszeiten im Problem-Management? Wie viele Störungen werden im Incident-Management pro Zeiteinheit bearbeitet? Andererseits gibt es die Angaben ohne direkten Prozessbezug: Anruferanzahl im Service-Desk pro Tag, Lizenzkosten pro Mitarbeiter oder Team, Anzahl betreuter Kunden pro Service-Desk-Mitarbeiter usw.

In ITIL ist es vorgesehen, dass jeder Prozess einen Verantwortlichen/Manager hat, den so genannten Prozessinhaber. Dieser prüft anhand der Qualitäts- und Leistungsindikatoren,

ob das Ziel des Prozesses erreicht ist. Diese Prozessüberwachung hat Einfluss auf die Prozessausführung, die wiederum von den Prozessbedingungen abhängig ist. Als Bedingung zählen die zur Verfügung stehenden Ressourcen und die zugesprochenen Rollen. So beschreibt ITIL sein generisches Prozessmodell, welches das einfache, in der Begriffsklärung zuvor erwähnte Prozessmodell erweitert (vgl. Abb. 3.3).

Das ITSM-Gebilde sollte von jeder Abteilung und IT-Person verstanden werden, damit jeder seine Rolle, seine Verantwortlichkeit und Wichtigkeit innerhalb der Prozesse kennt. Aus diesem Grund ist in erster Linie das IT-Management gefragt, sämtliche an den Prozessen Beteiligte für ITIL zu sensibilisieren. Diese Aufgabe kann sich auf das gesamte Unternehmen beziehen, da mit ITIL interne und externe Unternehmensbeziehungen abgebildet werden können und weil ITIL-Prozesse horizontal durch die Organisationshierarchie

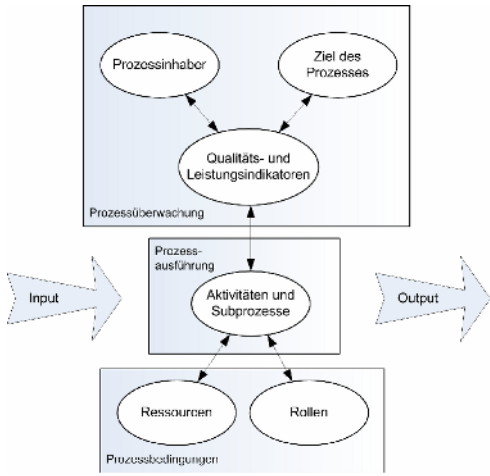

Abb. 3.3. Generisches ITIL-Prozessmodell nach [02]

verlaufen [02]. Administratoren erhalten leistungsfähige Werkzeuge zur Verwaltungs der Netzwerke, und somit „optimale Kontrolle von Services und Geschäftsprozessen“ [05]. Anwender sollten bereits während des ITIL-Projekts einbezogen werden, damit diese ihren Beitrag durch Vorstellungen und Anliegen leisten können. Der Help-Desk bzw. Service-Desk muss seine Bedeutung verstehen und die Aufgabe wahrnehmen, zu jeder Zeit schnelle Unterstützung und Betreuung bieten, wodurch Kunden- bzw. Anwenderzufriedenheit erreicht wird. Im IT-Management ist der CIO der Hauptverantwortliche, der an das Top-Management berichtet und die Verantwortung hat, die notwendige Infrastrukturen und IT-Komponenten zur Verfügung zu stellen. Die Partnerfirmen und Lieferanten müssen ebenfalls einbezogen werden, um die Kommunikation der Daten auf bestmöglichem Wege abzuwickeln (Excel-Listen, Web-Service-Anfragen, usw.). Ein Projektleiter und sein Team sollten die Prozesszusammenhänge und ITIL am besten kennen. Der Programmierer mit ITIL-Grundkenntnissen, der bei einer gekauften Software die Lieferfirma kontaktiert, handelt richtig. Das Top-Management mit seiner Geschäftsführungsfunktion fällt die notwendigen Entscheidungen und beteiligt sich an den ITIL-Diskussionen, wenn das Wissen präsent ist [05].

Die einzelnen Prozesse des IT-Service-Managements können im Unternehmen sequenziell oder parallel implementiert werden (siehe Abb. 3.4). Als Hintergedanke sollte festgehalten werden, dass die ITSM-Implementierung iterativ dynamisch ist [06] und ständig verbessert werden kann, ja sogar verbessert werden muss. Im Grunde sind die Prozesse ständig optimierbar und erreichen nie ein Verbesserungsende. Dies ist u. a. dadurch begründet, dass ein Unternehmen und seine Kunden selbst ein dynamisches Gebilde darstellen, das lebt und sich ständig an die ändernde Umgebung, wie z. B. neue Technologien, anpassen muss.

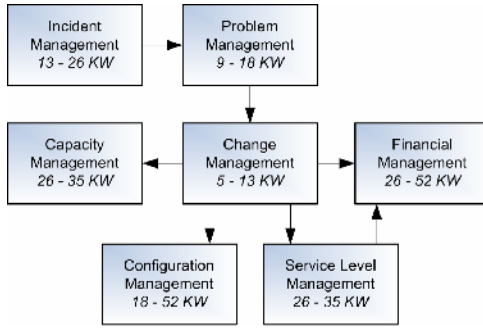

Abb. 3.4. Zeitliche Schätzung der Implementierung der ITIL-Prozesse nach [06]

In den meisten Fällen wird mit den Prozessen des Service-Supports begonnen. Insbesondere das Incident-Management, mit seiner Funktion des Service-Desks, wird zuerst implementiert. Diese Tatsache ist darauf zurückzuführen, dass die Optimierung der Prozesse in der Regel durch den äußeren Druck (Kunden, Anwender) angestoßen wird [03]. Nach dem Incident-Management folgen Prozesse wie das Problem- und Change-Management. An vierter Stelle folgen erst einige Planungsprozesse wie z. B. das Release-, Capacity- und Availability mit gleicher Priorität [03]. Es ist auch nicht ungewöhnlich, dass an zweiter Stelle das Configuration-Management implementiert wird, da es die anderen ITIL-Prozesse mit den Config-Items (Konfigurationselemente) wie Workstation, Server, Dokumentation, Verträge usw. unterstützt. Der in der Abb. 3.4 gezeigte Implementierungszeitraum von einem Jahr entspricht nur 26% der befragten Firmen (vgl. [03]). Bei einigen Unternehmen (ca. 85%) dauert die ITSM-Implementierung nach ITIL „zwischen sechs Monaten und über zwei Jahre“ [03]. Die Dimensionen sind auch stark davon abhängig, ob externe Berater herangezogen werden und ob die Implementierung neben dem

Tagesgeschäft abgewickelt wird. Weitere interessante Studien und Befragungen befinden sich in [03].

In den nachfolgenden Abschnitten werden die eng aufeinander bezogenen und hochgradig verzahnten ITIL-Prozesse beschrieben, die für die Bereitstellung und Durchführung eines IT-Services wichtig sind. Für die Prozessmodellierung wird Microsofts Visio™ als Werkzeug verwendet, das auch zum Großteil (über 60%) in Unternehmen eingesetzt wird [03].

3.2 Service-Support

In diesem Abschnitt wird der ITIL-Service-Support behandelt, welcher für die Durchführung der IT-Dienstleistungen essenziell ist. Die beschriebene operative Ebene beschäftigt sich einerseits mit den Prozessen zur Unterstützung von IT-Services, andererseits auch mit den Kunden- und Anwenderschnittstellen. Es werden folgende Prozesse behandelt:

- Service-Desk (Funktion),
- Incident-Management,
- Problem-Management,
- Configuration-Management,
- Change-Management,
- Release-Management.

3.2.1 Service-Desk

Der Service-Desk ist die zentrale Anlaufstelle für Kundenwünsche und Störmeldungen (engl. „Trouble Tickets“) der Anwender des Kunden. Er ist somit ein „Single Point Of Contact“ (SPOC), der die IT-Organisation dem Kunden als Front-Office mit fachlicher Kompetenz, rhetorischen Methoden und

Gesprächsführung [06] präsentiert. Er stellt keinen Prozess, sondern eine Funktion dar, die alle Prozesse des Service-Supports koordiniert, indem er als eine Art Kommunikationsplattform zwischen diesen fungiert und die Abarbeitung der Tickets überwacht. Ein Service-Desk bildet Teile des Incident-Managements operativ ab [06]. Entgegengenommen werden z. B. Störungen, Verbesserungsvorschläge, Änderungswünsche, Bestell- und Supportanfragen und natürlich Beschwerden.

Das Gebiet des Service-Desks hat etwas mit den bekannten Begriffen „Hotline“ oder „Helpdesk“ bzw. „User Helpdesk“ (UHD) zu tun. Ein Service-Desk kann aber nicht nur auf die Aufgaben eines Helpdesks oder Call-Centers beschränkt werden. Andererseits kann er auch nicht nur auf das Incident-Management begrenzt werden, da es operative Aufgaben übernimmt und mehrere Prozesse unterstützt. Ein Service-Desk nimmt Störungen (engl. „Incidents“) entgegen und macht somit Services erst abrufbar (vgl. Abb. 3.5).

Ein **Call-Center** erfasst Störungen ohne Kategorisierung und leitet diese ohne Bearbeitung oder Lösung an das Competence-Center weiter. Ein erfassender Service-Desk (**Unskilled Service-Desk**) registriert Störungen (Aufnahmen und Dokumentation), klassifiziert sie und ist um eine schnelle Weiterleitung

Abb. 3.5. Service-Desk als zentrale Funktion nach [02]

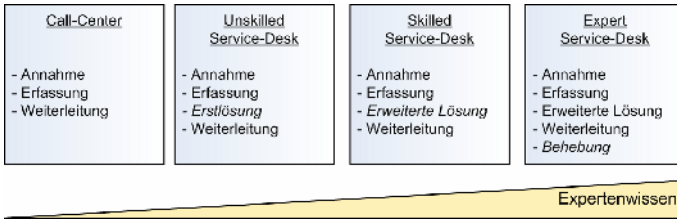

Abb. 3.6. Ausprägungen Service-Desk nach [06]

bemüht. Ein lösender Service-Desk (**Skilled Service-Desk**) besitzt größere Sachkenntnis, greift auf dokumentierte Lösungen zu und leitet erst dann schwerfälligere Fälle an die Spezialisten weiter. Als letzte Steigerung der Service-Desk-Kompetenz existiert das **Expert-Service-Desk**, das die meisten Störungen behebt. Bei dieser Realisierung muss die Erreichbarkeit aber gewährleistet bleiben (vgl. Abb. 3.6).

Als einzige Anlaufstelle für Probleme und Anfragen unterbindet der Service-Desk den „Hey Joe"-Support, wo die Hilfe der Experten direkt abgerufen und somit Zeit ineffizient verbraucht wird. Der Service-Desk ist verantwortlich für die Lösungen der eingestellten Incidents und bildet die wichtigste Funktion aus Sicht des Kunden [02]. Als weitere Aufgaben übernimmt er den First-Level-Support (1st-Level) mit Entgegennahme und Dokumentation der Anwendersituation, bietet die erste Bearbeitung (keine Analyse!), verwaltet die Eskalation und Verfolgung des Incidents und kann Management-Berichte erstellen.

Der Prozess eines Service-Desks entspricht dem des Incident-Managements und fängt bei der Entgegennahme einer Störung an. Diese wird registriert (d. h. aufgenommen und dokumentiert), klassifiziert und nach Möglichkeit zum sofortigen Abschluss gebracht. Der Lösungsweg wird ggf. gespeichert. Mit „registrieren" ist hier die Aufnahme und Dokumentation gemeint, unter „klassifizieren" versteht man die Kategorisierung

und Priorisierung von Incidents. Mit Hilfe der Klassifizierung wird der nachgelagerte Support (2^{nd}-, 3^{rd}-, 4^{th}-Level) entlastet, da das Fachpersonal nur die gefilterten und fachspezifischen Informationen erhält.

Ein Service-Desk verfolgt verschiedene Ziele. Sein Einsatz soll

- qualitativ hochwertige Unterstützung der Kunden/Anwender bieten,
- die Kunden durch Steigerung der Zufriedenheit mit Hilfe von hoher Erreichbarkeit und schnellen Reaktionszeiten binden,
- ein gutes Image aufbauen und die Mitarbeiterzufriedenheit steigern,
- die nachgelagerten Abteilungen entlasten,
- die „First Fix"-Rate (erste Lösung) steigern,
- das Störungsaufkommen und unnötige Eskalationen minimieren,
- die Servicekosten senken und
- die Ressourcen effizient auslasten.

Die Entscheidungsträger müssen sich der Wichtigkeit eines Service-Desks bewusst werden. Auch wenn bei der Einführung die Kosten wegen neuer Hard-/Software, Aus-/Weiterbildung und der Betriebskosten steigen, so werden diese aber nachhaltig deutlich gesenkt [06]. Es müssen sich die Risiken ohne ein Service-Desk vor Augen geführt werden [06]:

- Unwissenheit über Zuständigkeiten (Zeitverlust bei Suche).
- Fachpersonal steht ungefiltert direkt mit Kunden im Kontakt.
- Vorfälle werden gar nicht oder lückenhaft erfasst (Nachweisführung wichtig!).
- Wiedelholende Störungen werden immer wieder von Neuem gelöst (da Knowledge-Management fehlt).

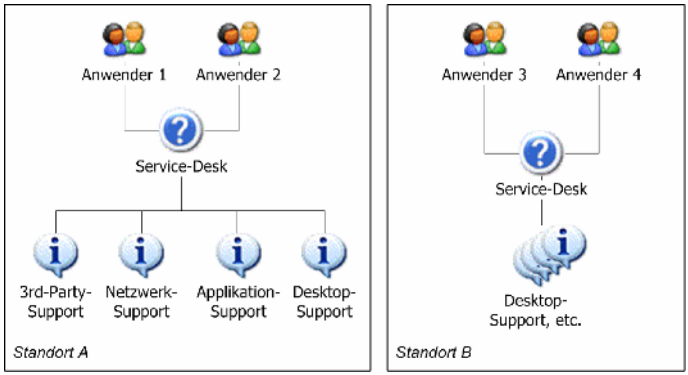

Abb. 3.7. Lokaler Service-Desk nach [06]

Für die Realisierung eines Service-Desks gibt es drei Formen: lokal, zentral und virtuell. Die nachfolgenden Abb. 3.7, 3.8 und 3.9 verdeutlichen deren Aufbau. Die Vorteile und Nachteile der jeweiligen Form werden ebenfalls diskutiert.

Ein lokaler Service-Desk ist nur für jeweils einen Standort verfügbar. Bei unterschiedlichen Sprachen und Gesetzesgebun-

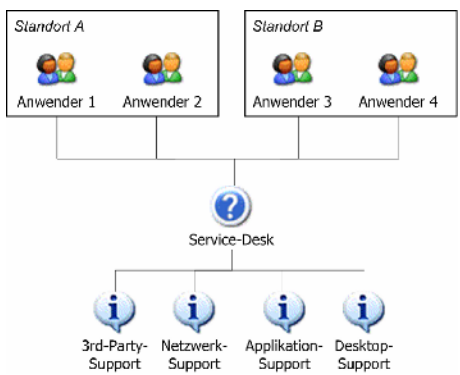

Abb. 3.8. Zentraler Service-Desk nach [06]

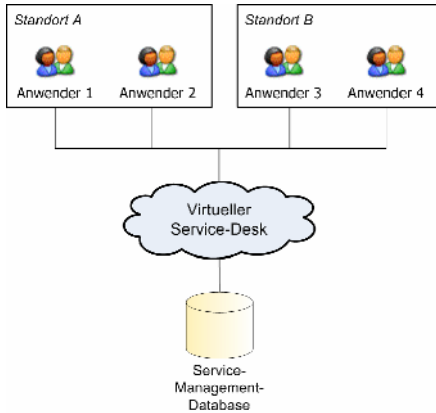

Abb. 3.9. Virtueller Service-Desk nach [06]

gen kann dies einen Vorteil bedeuten. Die Service-Desks verschiedener Standorte sind in keinster Weise miteinander verknüpft, so dass eine Kommunikation untereinander nicht stattfinden kann. Dadurch werden unter Umständen Incidents mit gleichen Symptomen und Lösungen mehrfach erfasst – das Wissen ist redundant abgelegt. Bei einer Zusammenführung oder für eine übergreifende Zusammenarbeit muss hier auf Kompatibilität und die eingesetzten Standards geachtet werden [06], was einen enormen Zeitaufwand bedeutet. Vorteilhaft ist jedoch für lokale Service-Desks, dass die Reaktionszeiten kurz sind und eine kundennahe Betreuung gegeben ist (vgl. Abb. 3.7).

Ein zentraler Service-Desk für mehrere Standorte weist eine umfangreiche Datenmenge auf, die aber sehr informativ ist und als Wissensdatenbank genutzt werden kann (vgl. Abb. 3.8). Die Auslastung der Ressourcen ist im Vergleich zur lokalen Lösung optimierter. Weiterhin können Kosten im Bereich Personal und Administration gesenkt werden. Mit zunehmender Größe der zentralen Lösung ist die kundennahe Betreuung immer weniger gegeben. Bei jedem Anruf wird die Wahrschein-

lichkeit höher, dass ein Anwender von einer neuen Person bedient wird. Zusätzlich steigt der Verwaltungs- und Organisationsaufwand [06], der nicht unterschätzt werden darf.

Ein virtueller Service-Desk ist durch dezentrale Standorte und eine zentrale Datenhaltung gekennzeichnet (vgl. Abb. 3.9). Diese Lösung vereint die Vorteile der zentralen und dezentralen Lösungen, bedeutet aber gleichzeitig einen erheblichen Mehraufwand an Ressourcen und Organisation [06]. Viele namhafte Unternehmen der Telekommunikationsbranche entscheiden sich für diese Architektur.

Eine Umfrage der Computerwoche (siehe [04]) stellt die heutige Situation eines Call-Centers deutlich dar. Eine schlechte Menüführung, für den Kunden unklare Zuständigkeiten und das Preis-Leistungs-Verhältnis stellen nur einen geringen Prozentsatz an Unzufriedenheit dar. Das, was den Kunden am meisten nervt, sind die langen Wartezeiten (28%) und die Inkompetenz des Personals (47%). Vielleicht kann man diese Zahlen für seinen Service-Desk nutzen und sich für die richtige Strategie entscheiden. Dazu können die in Tabelle 3.3 angege-

Tabelle 3.3. CSFs und KPIs des Service-Desks

CSF	KPI
Erreichbarkeit des Service-Desks	Anzahl angenommener Anrufe pro Zeiteinheit
Effektivität und Effizient (das Richtige schnell tun)	Anzahl entgangener Anrufe pro Zeiteinheit
Hey-Joe-Support	Erstlösungsquote
Unklare Zuständigkeiten	Kundenzufriedenheitsindex (Befragung)
Keine eindeutigen Service-Level-Agreements (SLAs) und kein Service-Katalog	Durchschnittliche Lösungszeit für Störungen
	Durchschnittliche Telefonatdauer

benen kritischen Erfolgsfaktoren (CSFs) und Leistungsindikatoren (KPIs) als Bewertungsmaßstab verwendet werden.

3.2.2 Incident-Management

Das Incident-Management ist für eine schnellstmögliche Wiederherstellung des normalen Service-Betriebs bei minimaler Behinderung der Geschäftsprozesse zuständig. Neben Störungen werden auch Anfragen (Service-Requests) der Anwender über den Service-Desk erfasst. Ein Service-Desk übernimmt die operative Steuerung und Dokumentation der Aktivitäten im Rahmen der Incident-Bearbeitung [06]. Als weitere Leistung ist der in vereinbarten Zeitintervallen dem Anwender mizuteilende Status der Fehlerbeseitigung vorgesehen [o20]. Jeder aufgegebene Incident bleibt für seinen gesamten Lebenszyklus im Besitz des Incident-Managements. Hier gilt das Incident-Management als „Owner“ seiner Störungen. Der Prozess Incident-Management besitzt einen Incident-Manager, der für eine reibungslose und effektive Funktionsfähigkeit zuständig ist [06]. Er leitet hierarchische Eskalationen weiter und arbeitet eng mit dem Service-Level-Management zusammen, wenn die Leistungsvereinbarungen im Rahmen des Incident-Managements nicht eingehalten werden.

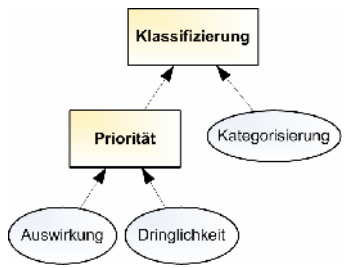

Abb. 3.10. Definition Priorität und Klassifizierung

Ein **Incident** wird laut ITIL dargestellt als „ein Ereignis, das nicht zum standardmäßigen Betrieb eines Services gehört und das tatsächlich oder potenziell eine Unterbrechung oder Minderung der Service-Qualität verursacht“ [09]. Er stellt eine Störung oder einen Service-Request (SRQ) dar. Eine Störung liegt vor, wenn z. B. ein PC komplett ausfällt oder der Zugriff auf eine Datenbank nicht möglich ist. Für die schnellstmögliche Bearbeitung eines Incidents wird er mit einer **Priorität** versehen. Diese setzt sich aus den beiden Faktoren Auswirkung und Dringlichkeit (engl. „impact and urgency“) zusammen. Die Priorität fließt neben der Kategorisierung als ein weiterer Faktor in die **Klassifizierung** eines Incidents, wie die Abb. 3.10 zeigt.

Unter einem **Service-Request** versteht ITIL „die Anfrage eines Anwenders zur Unterstützung, Service-Erweiterung, Lieferung, Information, zum Rat oder Dokumentation“ [09]. Ein SRQ ist u. a. die Anforderung einer Dokumentation oder für einen neuen Mitarbeiter die Bereitstellung eines PCs, samt der Zugangs- und Zugriffsberechtigungen. Kann ein Service-Desk-Mitarbeiter nicht auf eine existierende Lösung eines Problems zurückgreifen, so kann er eine Umgangslösung bzw. ein **Workaround** selbst finden, die zwar das Problem nicht komplett löst, aber ein Weiterarbeiten möglich ist. Ein Beispiel wäre hier ein nicht funktionierender lokaler Drucker. Der Anwender kann als Umgangslösung den Drucker seines Kollegen mitnutzen.

Ein Incident mag für einen Anwender immer ein Problem darstellen, doch in ITIL werden die Begriffe „Störung“ und „Problem“ stark differenziert. Ein Incident *kann* zu einem Problem werden, ist es aber nicht automatisch. Ein Incident kann geschlossen werden, obwohl das daraus resultierende Problem im System offen bleibt. Eine Störung könnte es sein, wenn ein lokaler Drucker nicht funktioniert. Ein **Problem** wird es erst dann, wenn die Ursache unbekannt ist und eine Analyse der Störung durchgeführt wird und als Lösung der Druckeraus-

tausch angeordnet wird (**Unknown-Error**). Ein Problem wird auf Grund von Incident-Analysen oder Beurteilungen von so genannten Trends erkannt. Hier spricht man vom reaktiven oder proaktiven Problem-Management. Es kann vorkommen, dass ein oft auftretendes Problem als ein bekannter Fehler oder **Known-Error** dokumentiert ist. Ein Beispiel sei ein bereits bekannter Softwarefehler genannt, der nur mit einem Patch behoben werden kann. Mehr zum Thema Problem-Management ist im nachfolgenden Abschnitt nachzulesen.

Bei der Implementierung eines Incident-Managements (vgl. Abb. 3.11) muss geklärt werden, welche Informationen zu Anfang vom Service-Desk erfasst werden sollen. Welche Attribute sind wichtig für die möglichen nachfolgenden Prozesse? Da ein Incident zu einem Problem werden kann, sollten zu Anfang die für das Problem-Management wichtigen Informationen erfasst werden. Für die Attributfindung sind also das Gesamtbild des Service-Supports wichtig und das Wissen der Schnittstellen der einzelnen Prozesse.

Da aus einem Incident weiterhin ein Change mit einer möglichen Auswirkung auf das Configuration- und Release-Ma-

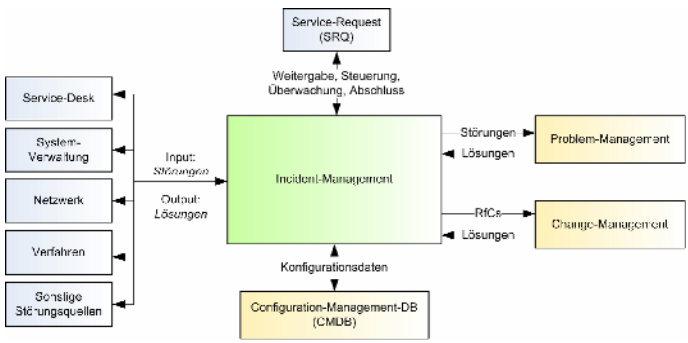

Abb. 3.11. Positionierung Incident-Management nach [02]

nagement entstehen kann, finden sich die folgenden Schnittstellen des Incident-Managements, die hiernach grafisch abgebildet werden:

- Problem-Management,
- Change-Management (bei Service-Requests),
- Configuration-Management (auch nur „Config“ genannt),
- Service-Level-Management.

Aus diesen Schnittstellen des Incident-Managements können die von ITIL vorgeschlagenen zu erfassenden Informationen ergänzt werden [06]:

- eindeutige Referenznummer (Ticket-ID, z. B. „INC00001“),
- Erfassungszeitpunkt (Timestamp),
- Person, die den Incident erfasst,
- Person, die den Incident meldet,
- Kontaktdaten (Adresse, Tel., E-Mail etc.),
- Incident-Beschreibung,
- Incident-Klassifizierung:
  - Kategorie (Haupt-/Unterkategorie: Netzwerk → Router, Hub, IP-Adresse etc.),
  - Priorität (Auswirkung/Dringlichkeit),
- Statusinformation (in Bearbeitung, geschlossen etc.),
- mit dem Incident verknüpfte CIs (Configuration-Items),
- Stelle, der der Incident zugewiesen wird (zuständige Gruppe),
- Beziehungen zu Problems oder Known-Errors (vgl. Problem-Mgmt),
- Zeitpunkt der Lösung,
- Lösungskategorie,
- Zeitpunkt des Abschlusses (Incident-Closure).

Mit Hilfe dieser Attribute kann der ganze Lebenszyklus eines Incidents, wenn auch nur rudimentär, abgebildet werden. In der Abb. 3.12 wird der Incident-Life-Cycle verdeutlicht.

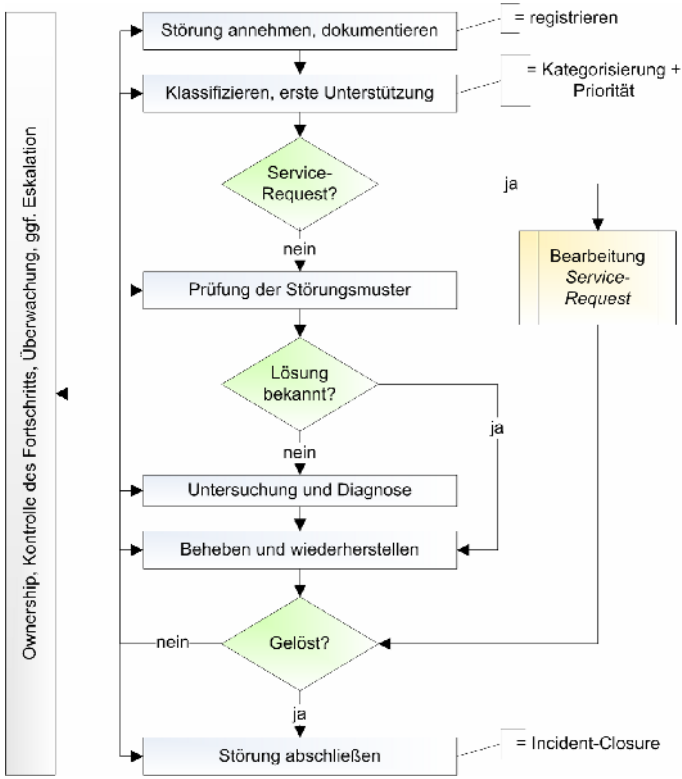

Abb. 3.12. Incident-Lebenszyklus nach [02]

Gezeigt wird die logische Reihenfolge der Abarbeitung eines Incidents. Er wird zunächst erfasst und registriert. Hiernach wird die Störung klassifiziert und die erste Unterstützung, in Form einer Erstlösung, geleistet. Handelt es sich dabei nicht um einen Service-Request, erfolgt im weiteren Verlauf die Prüfung des Störungsmusters z. B. in einer FAQ-Liste. Ist bis zu diesem Zeitpunkt keine Lösung gefunden,

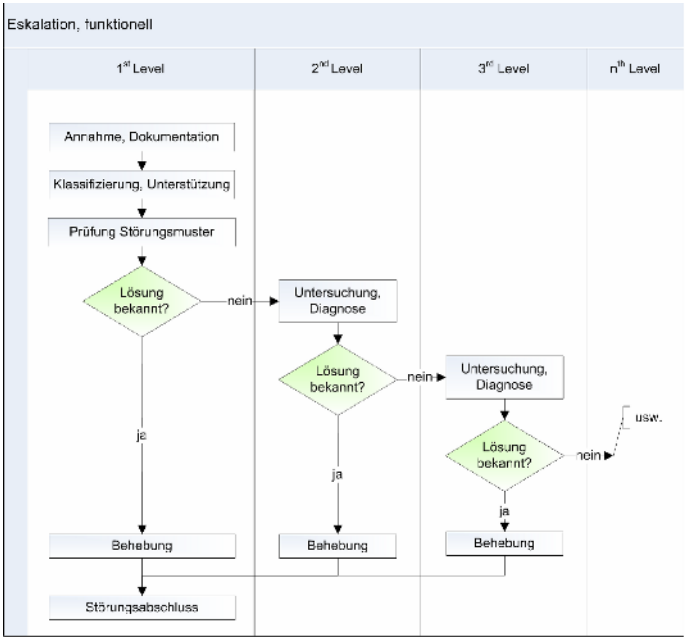

Abb. 3.13. Funktionale Eskalation nach [02]

wird in der Analyse und Diagnose nach Lösungen in der so genannten Wissensdatenbank (WDB) bzw. Knowledge-Base gesucht und bei Bedarf die funktionale Eskalation, d. h. Weiterleitung an den 2nd-Level-Support, angestoßen. Die funktionale Eskalation folgt auch dann, wenn die Störung nicht behoben werden kann, also nicht gelöst ist. Erst nach erfolgreicher Lösung des Incidents kann dieser den Status „abgeschlossen“ erhalten und die Lösung darf ggf. in einer Lösungsdatenbank dokumentiert werden.

Eine **Eskalation** ist ein Mechanismus, der für eine schnelle Behebung eines Incidents sorgt. Sie wird angestoßen, wenn eine

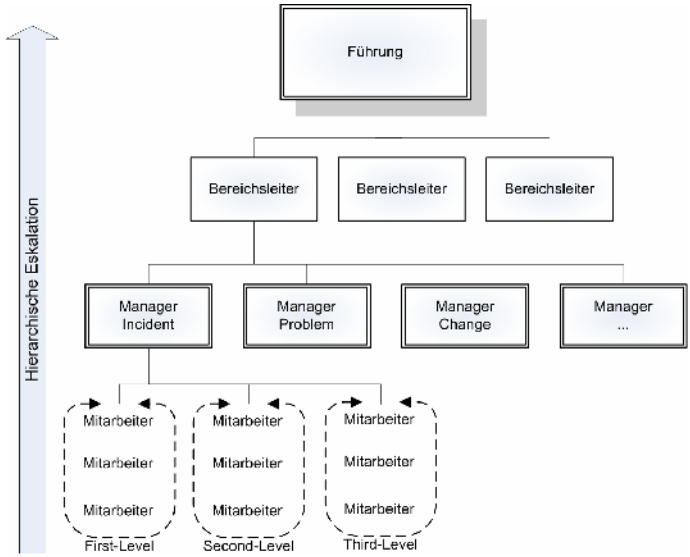

Abb. 3.14. Hierarchische Eskalation

Störung nicht in erster Instanz oder innerhalb der vereinbarten Zeit behoben werden kann [02]. In ITIL ist dies die funktionale (fachliche oder horizontale) und hierarchische (vertikale) Eskalation (vgl. Abb. 3.13 und 3.14).

Unter der **funktionalen Eskalation** verbirgt sich die Weiterleitung einer Störung an Spezialisten zur weiteren Bearbeitung (und zurück zum Service-Desk). Support-Teams werden anhand ihrer Kenntnisse und Erfahrungen gebildet und in verschiedene Support-Stufen wie First-Level-, Second-Level-, Third-Level- bis n-Level-Support eingeteilt. Obwohl n Level möglich sind, findet man in der Praxis nie mehr als drei oder vier Ebenen. Meistens stellt der 3rd-Level-Support den unter Vertrag (engl. „underpinning contract“, UC) stehenden Produkthersteller dar (s. Abb. 3.13).

Tabelle 3.4. CSFs und KPIs des Incident-Managements

CSF	KPI
Keine aktuelle und gewissenhaft gepflegte CMDB	Anzahl bearbeiteter Incidents pro Zeiteinheit
Gepflegte Datenbank für Probleme und bekannte Fehler (unknown-, known-errors)	Anzahl resultierender Changes pro Zeiteinheit
Ein nicht ausreichend unterstützendes System für Erfassung, Verfolgung, Überwachung von Störungen	Durchschnittliche Lösungszeit mit Bezug auf die SLAs
Keine Beziehung zum SLM	Durchschnittliche Support-Kosten pro Störung
	Anzahl der zu Anfang falsch klassifizierten Störungen
	Anzahl der falsch weitergeleiteten Störungen

Eine **hierarchische Eskalation** kommt zum Einsatz, wenn die funktionale Eskalation erfolglos war und weitere Mitarbeiter mit mehr Befugnissen hinzugezogen oder mehr Ressourcen zur Verfügung gestellt werden müssen (s. Abb. 3.14).

In der Praxis wird oft gewünscht, dass Eskalationen nach abgelaufener Bearbeitungsfrist automatisiert angestoßen werden. Automatisch sollen auch die gelösten Incidents zum Abschluss gebracht werden können. Für eine schnellere Klassifizierung wird oft eine vordefinierte Auswahlliste verwendet. Zusätzlich werden Reportings, eine Historienführung und Archivierung einem unterstützenden Werkzeug abverlangt. Für die Praxis sollten für ein erfolgreiches Incident-Management die in Tabelle 3.4 dargestellten kritischen Erfolgs- und Leistungsfaktoren beachtet werden.

Zum Schluss dieses Abschnitts sollen die Vorteile bzw. Ziele eines eingesetzten Incident-Managements aufgelistet werden:

- Erhöhung der Produktivität der Anwender (kundenseitig).
- Verbesserte Verfügbarkeit der IT-Services.
- Verbessertes Monitoring der Leistungsfähigkeit bezogen auf die SLAs.
- Sinnvolles Berichtwesen (für IT-Management, weitere ITIL-Prozesse).
- Verbesserter und effizienter Ressourceneinsatz.
- Störungen und Service-Requests gehen nicht verloren und werden richtig registriert.
- Kontinuierliche Aktualisierung der CMDB.
- Kontinuierliche Verbesserung der Kundenzufriedenheit.

3.2.3 Problem-Management

Das Problem-Management wird für die Minimierung von Auswirkungen der Incidents und Probleme, bedingt durch Fehler in der IT-Infrastruktur, eingesetzt. Es könnte als 2. Ebene des Incident-Managements betrachtet werden [05], da im Problem-Management die Incidents gesichtet und ggf. Problem-Tickets aufgegeben werden. Dennoch arbeitet es eigenständig und parallel zum Incident-Management [06]. Während beim Incident-Management eine möglichst schnelle Behebung der Störung angestrebt wird (Zeitmangel), besitzt das Problem-Management genügend Zeit, um die Ursachen von Störungen zu ergründen und diese optimal zu eliminieren. Das Problem-Management dient also der Ursachenforschung von Störungen, wenn ein Incident, ohne eine bekannte Ursache, zum Problem wird. Neben der Beseitigung von Störungen bzw. Fehlern steht die Entdeckung der Ursachen im Vordergrund [05]. Deswegen stellt das Problem-Management hohe Anforderungen an seine Mitarbeiter, zumal das Know-how für die eingesetzten Hilfsmittel, wie z. B. spezielle Programme und Datensammlungen, zur Fehlersuche vorhanden sein muss. Notwendige Informationen

müssen von und zu anderen ITIL-Prozessen kommuniziert werden. Dabei stellen die im Unternehmen vorhandenen Anwendungssysteme und Datenbanken sowie die Dokumentationen der Hersteller wichtige Quellen dar [05]. Die erworbenen Erkenntnisse des Problem-Managements fließen in das Change-Management ein, wenn z. B. eine Fehlerursache in der IT-Infrastruktur oder in der selbst entwickelten Software liegt und diese angepasst werden muss. Mit einem Problem-Management können nachhaltig Störungen beseitigt und die Produktivität gesteigert werden [06]. Neben der frühzeitigen Erkennung von Fehlerhäufigkeiten und Fehlermuster und der Erarbeitung von Workarounds, kommt die Nachbereitung dokumentierter Lösungen der Qualitätssicherung zugute.

Ein **Problem** ist laut ITIL „eine unerwünschte Situation, hinweisend auf die noch unbekannte Ursache einer oder mehrerer (potenzieller) Störungen“ [02]. Ein Problem kann nicht aus einem Incident eskalieren, es kann aber neben der Störung ein neues Problem definiert werden (neues Problem-Ticket). Für ein Problem kann eine temporäre Lösung (**Workaround**) erarbeitet werden. Das eigentliche Ziel ist es aber, aus einem Problem (hier: unbekannter Fehler, Unknown-Error) einen bekannten Fehler zu erarbeiten. Ein **Known-Error** ist ein „bekanntes Problem, dessen Ursache erfolgreich festgestellt wurde“ [02]. Ein bekannter Fehler und dessen Beseitigung kann dem Change-Management mit dem so genannten **Request for Change** (**RfC**) mitgeteilt werden. Das Problem-Management existiert aus zwei Teilen: ein reaktiver und ein proaktiver Teil. Zum einen reagiert ein **reaktives** Problem-Management erst dann, wenn Störungen auftauchen (Support, Problemlösung). Zum anderen kann ein **proaktives** Management betrieben werden, das sich mit der Störungsvermeidung und Trendanalysen prophylaktisch befasst [o20], bevor diese Störungen gemeldet werden. Optimalerweise sollte angestrebt werden, das proaktive Problem-Management bis zu 100 Prozent zu betreiben. Das

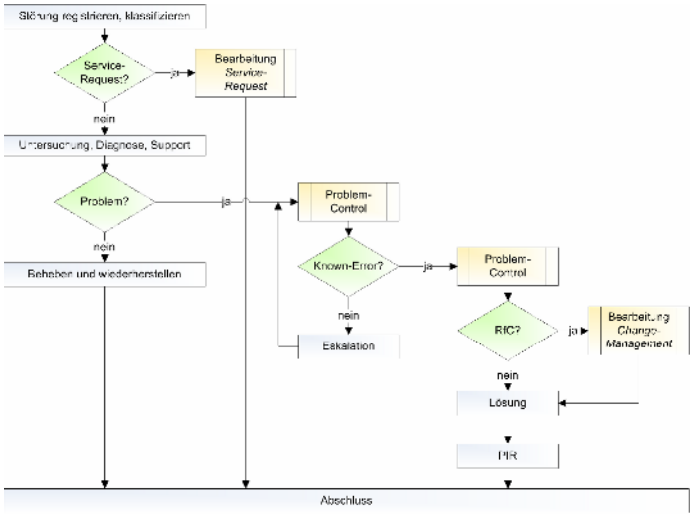

Abb. 3.15. Incident-Bearbeitung und reaktives Problem-Management nach [06]

Zusammenwirken des Problem-Managements mit anderen Prozessen wird in Abb. 3.15 verdeutlicht.

Das Problem-Management besitzt zusammengefasst folgende Schnittstellen zu anderen Prozessen. Sie werden in Abb. 3.16 grafisch dargestellt:

- Incident-Management (qualitativ gute Störungserfassung).
- Change-Management (kontrollierte Durchführung der RfCs).
- Configuration-Management (liefert Informationen über Infrastruktur).
- Availability (vereinbart Verfügbarkeitsstufen, verlangt Reports über Nichtverfügbarkeit).
- Capacity-Management (kann Probleme definieren, verlangt Reports von Ursachen bezüglich der Kapazität).

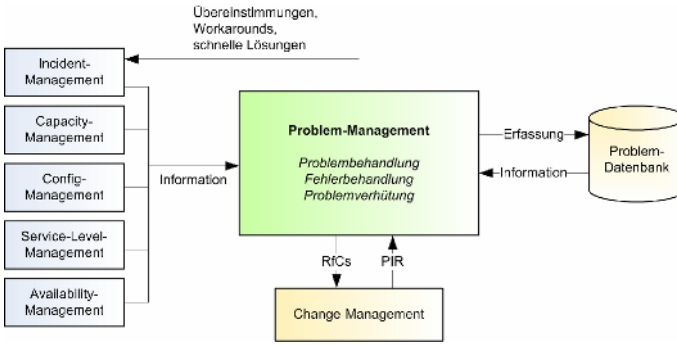

Abb. 3.16. Positionierung Problem-Management nach [02]

Service-Level-Management (Qualitätsanforderung, Priorisierung von Problemen).

Wie bei anderen ITIL-Prozessen auch, besitzt das Problem-Management einen Manager. Dieser hat die Aufgabe, bei der Entwicklung und Pflege von Problem- und Fehlerbehandlungen mitzuwirken, in dem er u. a. die Effektivität und Effizienz beurteilt. Er ist für die Beschaffung von Managementinformationen und der nötigen Ressourcen zuständig.

Die im Problem-Management definierten Aktivitäten setzen sich zusammen aus der Problem- und Fehlerbehandlung, dem proaktiven Management und der Informationsbereitstellung für andere ITIL-Prozesse. Die ersten beiden Aktivitäten werden **Problem-Control** und **Error-Control** genannt und in Abb. 3.17 genauer betrachtet.

Die Abb. 3.17 kann grob in zwei Bereiche unterteilt werden: In der Problembehandlung bzw. -bearbeitung geht es um die Identifikation, Dokumentation, Klassifizierung und Diagnose eines Problems. In der unteren Hälfte ist die Fehlerbehandlung aufgeführt, die sich aus der Dokumentation, Bewertung und Behebung eines Fehlers zusammensetzt.

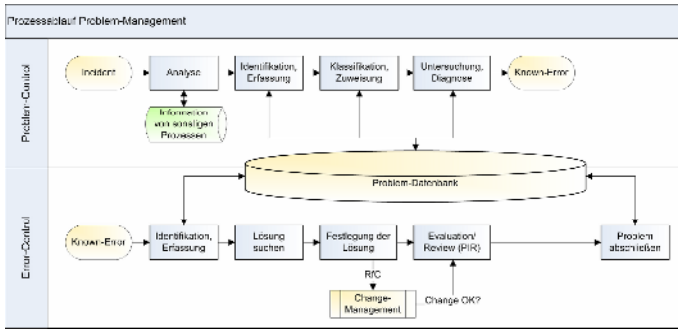

Abb. 3.17. Prozessablauf im Problem-Management nach [02]

In der Analyse des **Problem-Control** müssen bei häufigen oder schwerwiegenden Störungen Inputs aus anderen Prozessen erforscht werden. Die Identifikation und Erfassung eines Problems befasst sich u. a. mit der Ermittlung der CI-Ebene (Server, Client etc.). Während der Klassifizierung und Zuweisung werden die Schwere kategorisiert, die Auswirkung und der Status des Problems festgehalten. Hiernach erfolgt die genauere Untersuchung und Diagnose des Problems, in dem der Fehler z. B. in einer Testumgebung reproduziert wird. Ein unbekannter Fehler kann erst dann zu einem bekannten Fehler deklariert werden, wenn die Ursache des Fehlers lokalisiert ist und der logische Zusammenhang zwischen einem CI und einer oder mehreren Störungen besteht.

Der Input für das **Error-Control** ist der Known-Error der Problembehandlung. Kann der Fehler identifiziert werden, wird ggf. ein Workaround an das Incident-Management weitergeleitet. Ist dies nicht der Fall, wird unter Beachtung der SLAs und des Aufwandes die Lösungssuche unter Angabe der Auswirkung und Dringlichkeit für einen RfC angestoßen. Konnte eine optimale Lösung gefunden werden, wird der RfC formuliert, die Vorgehensweise für das Incident-Management dokumen-

tiert und der Behebungsauftrag dem Change-Management überreicht. Das Problem-Ticket kann erst dann geschlossen werden, wenn die Evaluierung bzw. der Post-Implementation-Review (PIR) durchgeführt worden ist. Nach Rücksprache mit dem Incident-Management können ggf. noch offene Störungen geschlossen werden.

Für die Praxis ist es von großer Wichtigkeit, dass sich ein multidisziplinäres Team mit dem Problem-Management auseinandersetzt [06], um die beste Effizienz und Effektivität auf allen Gebieten zu erreichen. Mit dem für die Unterstützung eingesetzten Werkzeug sollte eine lückenlose Dokumentation möglich sein. Eine gut funktionierende Kommunikation zwischen den Beteiligten ist auch hier von Vorteil [05]. Bei der Implementierung eines Problem-Managements können die in Tabelle 3.5 dargestellten kritischen Erfolgs- und Leistungsindikatoren behilflich sein.

Tabelle 3.5. CSFs und KPIs des Problem-Managements

CSF	KPI
Effektives automatisierte Erfassung von Störungen	Anzahl sich wiederholender Incidents und Problems
Effektives Infrastruktur-Monitoring	Reduktion von Incidents und Problem in Prozent
Realistische Zielvorgaben (Mitarbeiter, zeitliche Komponente)	Zeitaufwand für die Behebung eines Problems
Zusammenarbeit zwischen Incident- und Problem-Management	Reduktion von Eskalationen
Ausgewogenheit zwischen schneller Störungsbehebung und Ermittlung der Ursachen	Stundennachweis Problem-, Error-Control, proaktives Management
Schlecht definierte Aufgabenbereiche und Zuständigkeiten	Qualität der Produkte (Anzahl betroffener Incidents)
	Anzahl eingereichter RfCs

Zum Schluss dieses Abschnitts sollen die Vorteile bzw. Ziele eines eingesetzten Problem-Managements aufgezeigt werden:

- Fehler werden lokalisiert, dokumentiert und sind verfolgbar.
- Symptome und Lösungen von Störungen werden dokumentiert.
- Neue Störungen werden verhindert.
- Bessere Qualität und Beherrschung der IT-Services.
- Reflektives Lernen aus der Vergangenheit.
- Verbesserte Störungserfassung und Berichtswesen.
- Höhere Erfolgsquote im 1st-Level-Support.

3.2.4 Configuration-Management

Das Configuration-Management stellt allen anderen Prozessen ein logisches Modell der IT-Infrastruktur zur Verfügung, mit dem die Verbesserung der Servicequalität angestrebt wird. Dazu werden die einzelnen Elemente und deren Beziehungen untereinander in einer Datenbank, der Configuration-Database (CMDB), verwaltet. Ein Element wird Configuration-Item (CI) genannt und durch weitere Attribute und Verknüpfungen beschrieben. Soll ein Bestandteil der IT-Infrastruktur einen Prozess durchlaufen können oder einfach nur kontrolliert werden, so wird dieser als ein CI in die CMDB aufgenommen. Für die Aktualität dieser Informationen und Dokumentationen kann das Configuration-Management mit Hilfe anderer ITIL-Prozesse Sorge tragen. Somit wird gewährleistet, dass aktuelle, historische und konsistente Informationen über die Configuration-Items abrufbereit sind [o20]. In einer CMDB können IT-Konfigurationen und die damit verknüpften IT-Services hinterlegt werden. Sie stellt die wichtigste Informationsquelle für das ITSM dar, weil sie mit dem Service-Support und Service-Delivery interagiert [06]. Ist eine CMDB nicht vorhanden, so ergeben sich Einschränkungen u. a. für das Incident-, Problem-

und Change-Management. Das Configuration-Management ermöglicht zusätzlich anhand dieser wertvollen Informationen eine Folge- und Schwachstellenanalyse. Eine Schwachstelle ist auch bekannt als „Single Point Of Failure“ (SPOF). Auch wenn das Configuration-Management mit IT-Vermögenswerten (engl. „Assets“) zu tun hat, darf es dennoch nicht mit dem **Asset-Management** gleichgesetzt werden. Ein Asset-Management ist der Buchhaltung zuzuordnen und überwacht die Abschreibungen der Artikel [02]. Wichtige Attribute spielen hierbei u. a. der Beschaffungswert, die Abschreibung, der Geschäftsbereich und der Standort. Im Configuration-Management hingegen sind Informationen über interne Zusammenhänge zwischen CIs hinterlegt. Zusätzlich geht es um den Status und Verbleib von Betriebsmitteln sowie der vorgenommenen Änderungen. Der einzige Zusammenhang zwischen den Disziplinen ist der, dass auf Basis eines Asset-Managements das Configuration-Management eingerichtet werden kann.

Die **Configuration-Database** (**CMDB**) stellt eine große Karteikarte dar. Die CMDB-Architektur ist in ITIL nicht definiert. Sie kann als eine einzige Datenbank oder aus verschiedenen Datenbanken bzw. Quellen realisiert werden. Ein heterogenes System ist demzufolge möglich, sofern der Zugriff auf sämtliche IT-Betriebsmittel bzw. CIs möglich ist. Eine CMDB enthält so genannte **Configuration-Items** (**CI**s). Ein CI entspricht einem Datensatz mit individuellen Attributen und Verknüpfungen zu weiteren CIs [06]. Damit ein Configuration-Item systemweit eindeutig identifizierbar ist, besitzt dieser eine eindeutige Referenznummer bzw. einen Item-Key (Schlüssel).

Wegen der umfangreichen Informationen und unterschiedlichen Objekttypen werden CIs kategorisiert. Konkrete Beispiele zeigt die Tabelle 3.6 auf.

Bei der Konzeption einer Configuration-DB ist es wichtig den Umfang (engl. „Scope“) und den Detaillierungsgrad (engl. „CI Level“) am Anfang festzulegen. Dies ist von Fall zu Fall

Tabelle 3.6. Kategorisierung von CIs [05]

Kategorie	Configuration-Item
Software	Betriebssystem, Anwendungsprogramm, TK-Software, Treiber, Firmware, E-Mail
Hardware	Mainframe, Workstation, Server, Router
Dokumentation	Systeme, Anwendungen, Applikationen, Bedienungsanleitungen, Verträge, Notfallpläne, Unternehmensrichtlinien
Datensammlungen	Datenbanken, Einzeldateien, Stammdaten, Texte, Grafiken
Nicht direkt der IT zugeordnet	Mobiliar, Materialien, Ersatzteile, Fachliteratur

unterschiedlich und muss für jedes Unternehmen individuell entschieden werden. In einer Organigrammnotation ist der Umfang der horizontalen und der Detaillierungsgrad der vertikalen Ausprägung zu entnehmen, wie die Abb. 3.18 zeigt. Die objekthierarchische Struktur der CMDB wird hierdurch deutlich.

Die Attributausprägungen eines Configuration-Items sollen laut ITIL erlauben, ein CI genauer zu bezeichnen, die Dokumentation von technischen Informationen zu ermöglichen und die Beziehungen zu anderen CIs anzugeben. Typische Attribute eines CI sind:

- CI-Name,
- Copy or Serial Number,
- Category,
- Type,
- Model Number (hardware),
- Warranty Expiry Date,
- Version Number,
- Owner Responsible,

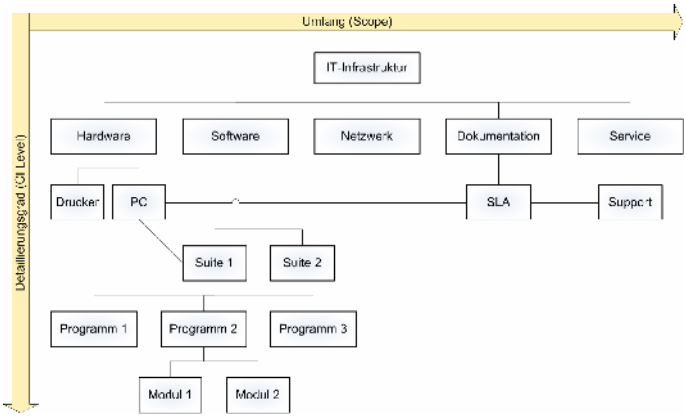

Abb. 3.18. Detaillierungsgrad und Umfang einer CMDB nach [06]

- Responsibility Date,
- Licence,
- Parent CIs Relationship,
- Child CIs Relationship,
- RfC Numbers,
- Change Numbers,
- Problem Numbers,
- Incident Numbers,
- Comment,
- Current Status.

Das CMDB-Modell beinhaltet auch eine Abbildung der Beziehungen der Konfigurationselemente der realen Welt. Diese können unterteilt werden in physische und logische Beziehungen. Ersteres deckt die in der Objektmodellierung gängigen Beziehungsformen „Is-A“ und „Is-Part-Of“ ab. Eine logische Beziehung wäre „Is-Copy-Of“ oder „Is-Used-By“. Weitere Formen können der Tabelle 3.7 entnommen werden.

Tabelle 3.7. Beziehungsformen- und arten von CIs

Beziehungsform	Beziehungsart
Physisch	X ist Teil von Y X ist verbunden mit Y X ist ein Y
Logisch	X ist Kopie von Y X bezieht sich auf Y X wird verwendet von Y X ist erforderlich für Y

Wie zu Anfang dieses Kapitels erwähnt, greifen viele Prozesse auf die Configuration-Datenbank zurück, um einen betroffenen CI u. a. mit Incidents oder Problems zu assoziieren. Im Folgenden werden weitere Schnittstellen aufgelistet [05] und anschließend grafisch beschrieben (vgl. Abb. 3.19):

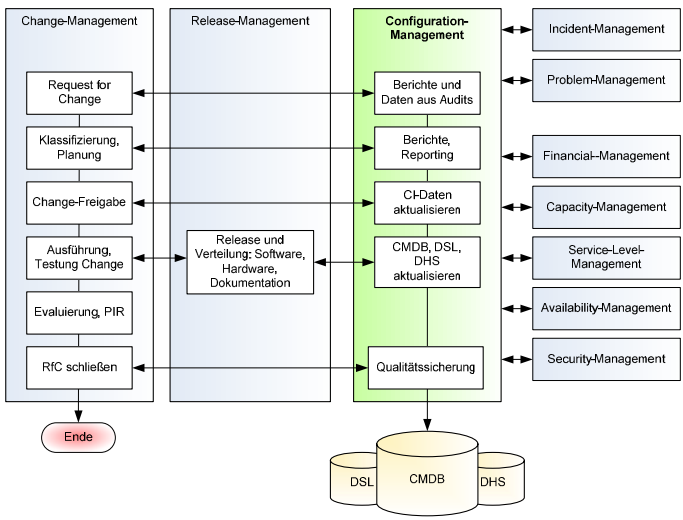

Abb. 3.19. Positionierung Configuration-Management nach [02]

- Service-Desk,
- Asset- und Inventarisierungssysteme,
- IT-Anwendungen verschiedener Ausprägung,
- IT-Entwicklungsabteilung,
- Anwendergruppen bzw. Fachbereiche,
- Change-Management,
- Incident-Management,
- Release-Management,
- Problem-Management,
- Capacity-Management,
- Availability-Management,
- Continuity-Management,
- Operations-Management.

Das Incident-Management greift bei der Störungserfassung auf die CMDB zu, um einen Zusammenhang zwischen Incident und CI herzustellen. Weiterhin sind daraus der Standort, der verantwortliche Administrator, bekannte und unbekannte Fehler, die Service-Level-Agreements usw. ersichtlich. Im Problem-Management werden die für das Incident-Management und den Service-Desk wichtigen Zusammenhänge von Problems und Known-Errors zu einem Konfigurationselement hergestellt.

Das Release-Management liest und schreibt Informationen wie der Status, Standort, Quellcode und die Rückmeldung nach einem Rollout aus bzw. in die CMDB. Das Change-Management behilft sich der CMDB für eine Impact-Analyse oder um die Anpassung z. B. bei neuen CIs. Das Capacity-Management verwendet die CMDB für das Tuning der IT-Infrastruktur und die Erstellung eines Kapazitätsplans. Im Financial-Management werden Informationen zur Verrechung von IT-Services benötigt. Die Überwachung der Assets und Investitionen sollten mit einer CMDB ebenfalls möglich sein. Um einen neuen Alternativstandort für den Katastrophenfall aufbauen zu können, muss das Continuity-Management die Ausgangskonfiguration (engl.

„Configuration-Baseline“) der CMDB entnehmen. Für Verbesserungen und Schwachstellenanalysen benötigt das Availability-Management eine Schnittstelle zum Configuration-Management. Schlussendlich benötigt das Service-Level-Management die CMDB für die Überwachung von Services und das Service-Improvement-Programm (SIP). Wie die Abb. 3.19 zeigt, besteht die CMDB noch aus weiteren Komponenten: Definitive-Software-Library (DSL) und Definitive-Hardware-Store (DHS). Diese werden im Abschnitt 3.2.6 ausführlicher behandelt.

Das Configuration-Management umfasst fünf Aktivitäten bzw. Aufgaben, die eine gepflegte Configuration-Database garantieren und eine reibungslose Zusammenarbeit mit anderen Prozessen erlauben. In den meisten Fällen werden diese Aktivitäten durch das Change-Management initiiert, welches genauere Angaben in den RfCs bereits liefert. Zusammengefasst ergeben sich fünf Tätigkeiten des Config-Managements:

- Planung,
- Identifizierung,
- Kontrolle,
- Statusüberwachung,
- Verifizierung und Audits.

Zu Beginn der Implementierung eines Config-Managements werden während der **Planung** Strategien, Grundsätze (Policies) und Zielsetzungen festgelegt. Die Beziehungen zu anderen Prozessen und die dafür wichtigen Informationen werden aufzeigt. Darüber hinaus werden der Zweck, Umfang und der technische sowie organisatorische Kontext von Configuration-Items definiert [06]. Direkt im Anschluss wird während der **Identifizierung** das initiale Datenmodell erstellt. Es werden alle Komponenten und deren Beziehungen und Verantwortlichkeiten (engl. „Ownership“) ausgewählt. Festzulegen sind die Versionierung und Kennzeichnung von CIs [06] sowie das Verfahren für die Integration neuer CIs und ihre nachfolgende

Änderung. Wichtig während dieser Tätigkeit ist die Ausgewogenheit zwischen Umfang, Detaillierungsgrad und der Performanz, frei nach der Devise „Maximum control with minimum records“. Nachdem eine CMDB im Einsatz ist, beginnt die Aktivität der **Kontrolle**. Hier ist dafür zu sorgen, dass in der Produktivumgebung nur autorisierte und registrierte Komponenten vorhanden sind [06]. Eine wichtige Regel dabei ist, Ergänzungen und Entfernungen, d. h. Modifikationen jeder Art, nur bei vorliegendem RfC durchzuführen und zu dokumentieren. Die Tätigkeit der **Statusüberwachung** beschäftigt sich mit den Life-Cycle-bezogenen, d. h. aktuellen und historischen Informationen. Sämtliche CI-Änderungen werden aufgezeichnet und somit wird eine Historie geführt [06]. Die letzte Aufgabe eines Config-Managements ist überschrieben mit dem Titel **Verifizierung und Audits**. Regelmäßige Reviews und Verifizierung der Soll-Situation der physikalischen CMDB-Daten garantieren die Integrität bzw. Korrektheit der gespeicherten Daten. Die Befolgung dieser Aktivitäten führt zu den drei Ergebnissen [05]:

- Stets aktuelle CMDB.
- Management-Reporting an verschiedene Personenkreise.
- Informationsweiterleitung an weitere ITIL-Prozesse.

In der Praxis sind oft historisch gewachsene Systeme zu finden. Wegen der offenen CMDB-Architektur in ITIL ist es möglich, heterogene Systeme mit einem virtuellen CMDB-Modell zu realisieren. Es muss aber beachtet werden, dass der interne Datenaustausch zwischen solchen Systemen nur selten standardisiert ist [06] und dass vielleicht ein neu konzipiertes Datenbankmodell mehr Vorteile mit sich bringt. Wahlweise können mehrere CM-Datenbanken verwendet werden. Viele Informationen für die Attributbestimmung können aus den Anforderungen eines Change-Managements gewonnen werden. Bereits am Anfang der Einführung müssen die Bedeutung und

Tabelle 3.8. CSFs und KPIs des Config-Managements

CSF	KPI
Aktualität der Datenbank	Anzahl erfolgreich autorisierter CIs
Örtliche und zeitliche Verfügbarkeit der richtigen Informationen für z. B. CMDB-Änderung	Anzahl fehlender oder mehrfacher CIs
Ausgeglichenheit zwischen Umfang und Detaillierungsgrad des DB-Modells	Anzahl nicht genutzter Lizenzen
Unterschätzung der zeitlichen Komponente für die Einführung des Config-Prozesses	Häufigkeit nicht zugelassener oder nicht erfasster Konfigurationen
Warnung vor Forderung eines kurzfristigen Nutzennachweises des Prozesses	Geschwindigkeit der Abarbeitung eines Antrags um Aufnahme eines CIs
Entsprechende Ausbildung der Mitarbeiter für Dokumentationsaufgaben	Statistische Daten zu Aufbau und Zusammensetzung der IT-Infrastruktur
Erfassung von CIs vor der Einführung der erforderlichen Subprozesse → „Schatten CMDBs“	Überblick über Aufwand verschiedener Aktivitäten

der Nutzwert gegenüber den Mitarbeitern und Anwendern betont werden [05], um Akzeptanz zu erreichen. Diese erreicht man auch dadurch, dass die anderen Management-Disziplinen ein Mitspracherecht bei der CMDB-Modellierung haben. Bestehende Daten sollten nach Möglichkeit mit einem Werkzeug in die CMDB importiert werden, um den zeitlichen Aufwand und die Fehler einer manuellen Eingabe zu vermeiden. Der Configuration-Manager sollte ausdrücklich darauf bestehen,

dass Aktionen im Config-Management nur durch Anweisung des Change-Managements durchgeführt werden dürfen. Dieser Punkt wird oft umgangen, weil es zum einen ohne Umwege schneller geht, zum anderen deswegen, weil auf eine Genehmigung nicht gewartet werden möchte. Bei der Implementierung eines Configuration-Managements können die folgenden kritischen Erfolgs- und Leistungsindikatoren behilflich sein (vgl. Tabelle 3.8).

Zum Schluss dieses Abschnitts sollen die Vorteile eines eingesetzten Configuration-Managements aufgezeigt werden:

- Strukturiertes Abbild der realen IT-Infrastruktur.
- Qualitätsgesicherte Basis für alle Prozesse.
- Verbessertes Asset-Management.
- Kontroll- und Nachweismöglichkeit.
- Einfachere Umsetzung von Changes.
- Einhaltung gesetzlicher Bestimmungen, Produktrichtlinien (Policies).

Simulation erlaubt schnellere Umsetzung von Änderungen und effektive Problemlösungen.

3.2.5 Change-Management

Die IT-Infrastruktur eines Unternehmens ist sein höchstes Gut, das es zu schützen gilt. Es dürfen keine unautorisierten Änderungen daran vorgenommen werden, da jede Änderung im System ein potenzielles Störungsrisiko darstellt [06]. Jede Änderung an einem Configuration-Item muss genauestens auf ihre Notwendigkeit und Auswirkung auf das Gesamtsystem (engl. „Change-Impact“) geprüft, später geplant, organisiert und überwacht werden. Ein Change oder RfC wird genehmigt, dokumentiert und die Ausführung überprüft (engl. „Review“). Das Change-Management soll die Auswirkungen von änderungs-

bedingten Störungen für den IT-Service minimieren. Dies gelingt durch die Bereitstellung standardisierter Prozeduren und Methoden für eine effiziente und wirtschaftliche Implementierung autorisierter Changes mit kleinstmöglichem Risiko für die bestehende und neue IT-Infrastruktur [02]. Standard-Changes kann der Change-Manager genehmigen. Sie sind entweder Routineänderungen oder sie betreffen die IT-Infrastruktur nur in geringem Maße. Bei weitreichenden Veränderungen spielen weitere Gremien, wie z. B. das CAB (Change-Advisory-Board), eine Rolle [o20], die je nach Priorität von einem EC (Emergeny-Committee) ersetzt werden können. Einige das Change-Management betreffende Änderungen sind z. B. Software- und Hardware-Änderungen, eine SAN-Einrichtung oder die Realisierung eines ITSM nach ITIL.

Im Change-Management wird der allgemeine Begriff **Change** als Synonym für Neuerungen und Verbesserungen, Änderungen oder Korrekturen der IT-Infrastruktur verwendet. Dieser Begriff wird weiter unterteilt. Es gibt Änderungen, die ständig wiederkehren und somit vollständig beschrieben sind und keine Freigabe und Kontrolle des Change-Managements bedürfen und lediglich erfasst und dokumentiert werden müssen. Solche Änderungen werden **Standard-/Routine-Changes** und **Service-Requests** genannt. Alle übrigen Änderungen erfolgen auf Grund eines **RfC**s. Dieser **Reguläre Change** verlangt nach einer Abschätzung, Freigabe, Planung und Kontrolle. Solch ein Request-for-Change betrifft nur ein tatsächlich vorhandenes CI. Es muss mindestens festgehalten werden, wer was wann aus welchem Grund beantragt hat. Im optimalen Fall aber sind folgende Attribute eines RfCs vorhanden [06]:

- Eindeutige RfC-Nr.,
- CIs, die von der Änderung betroffen sind,
- Begründung der Änderung,
- Konsequenzen bei Nichtdurchführung der Änderung,

- Priorität,
- Ansprechpartner,
- Zeitpunkt der Antragstellung, Genehmigung,
- Geplanter Änderungstermin,
- Back-Out-Plan (Wiederherstellung eines Service),
- Statusinfos,
- Unterschrift, ggf. elektronisch.

Eine niedrige oder mittlere Priorität fordert eine Behebung bei Gelegenheit oder demnächst. Ist sie hoch oder dringend, so ist eine möglichst baldige und sofortige Behebung gewünscht. Für eine korrekte Durchführung eines Change wird ein Änderungskalender oder **Forward-Schedule-of-Change** (**FSC**) geführt, der einen übersichtlichen Zeitplan der bevorstehenden Veränderungen darstellt. Die Verfügbarkeit eines IT-Service während eines Change wird in einem Dokument beschrieben, das **Projected-Service-Availability** (**PSA**) genannt wird.

Wie bei anderen ITIL-Prozessen auch, so gibt es für dieses Management einige Entscheidungsträger, die für oder gegen eine Änderung stimmen. Der **Change-Manager** nimmt sich der Standardänderungen und einfachen RfCs an. Ein **Change-Koordinator** kann die Planung und Koordinierung der Änderungen einzelner Bereiche übernehmen. Das **Change-Advisory-Board** (**CAB**) kommt zum Einsatz, wenn umfangreiche oder kritische Änderungsanträge vorliegen [06]. Es ist ein Beirat aus technisch operativ und wirtschaftlich orientierten Mitgliedern.

Konkret setzt sich das CAB optimal aus den folgenden Mitgliedern zusammen:

- Change-Manager (Vorsitzender),
- Service-Level-Manager,
- Chief Financial Officer (CFO, Finanzchef),
- Vertreter aus dem Incident-Management,
- Vertreter aus dem Problem-Management,

- Vertreter aus dem Release-Management,
- Vertreter aus der Anwendungsentwicklung,
- Vertreter des Kunden,
- IT-Spezialisten,
- Bereichsmanager,
- Externe Dienstleister.

Weiterhin wird für einen Notfall ein **Emergency-Committee** (**EC**) aus dem CAB gebildet. Seine Mitglieder sind „befugt, stellvertretend für das CAB Notfallentscheidungen für dringliche Änderungsmaßnahmen (**Urgent-Change**) zu treffen“ [06].

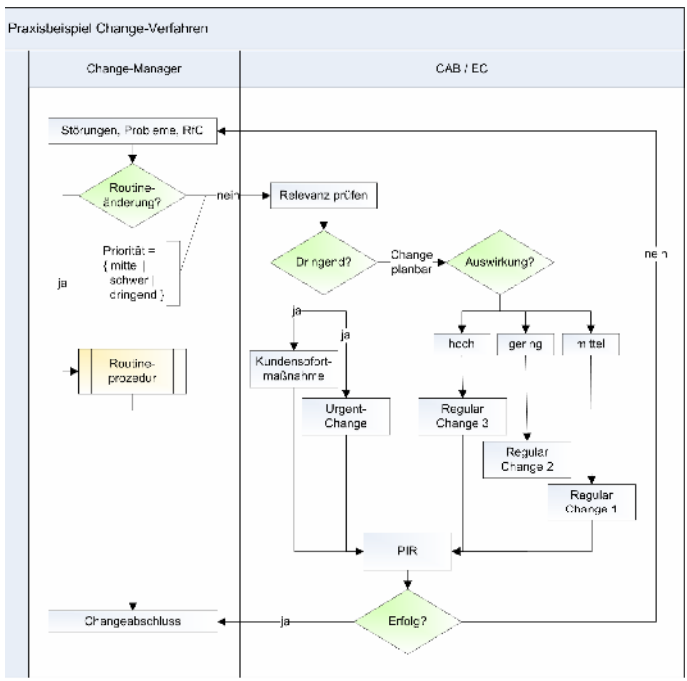

Abb. 3.20. Praxisbeispiel Change-Verfahren nach [02]

Die Geschäftsleitung wird nur dann hinzugezogen, wenn der Fall kritisch oder mit hohen Kosten verbunden ist. Das EC kann in der Minimalbesetzung aus dem Change-Manager und dem Change-Koordinator (und ggf. weitere) bestehen. In Abb. 3.20 folgt die Veranschaulichung eines Beispieles.

Das Change-Management hat, wie zu Anfang in Abb. 2.7 gezeigt, sehr viele Schnittstellen zu fast allen der ITIL-Prozesse. In der nachfolgenden Abb. 3.21 wird dies nochmals verdeutlicht.

Durch das Incident-Management gelangen Request-for-Change-Anträge aufgrund auftretender Störungen oder vom Kunden gemeldeter Service-Requests. Zu einigen Störungen können auch Probleme erstellt werden, wodurch das Problem-Management ausgelöst wird. Oft betreffen Änderungen die

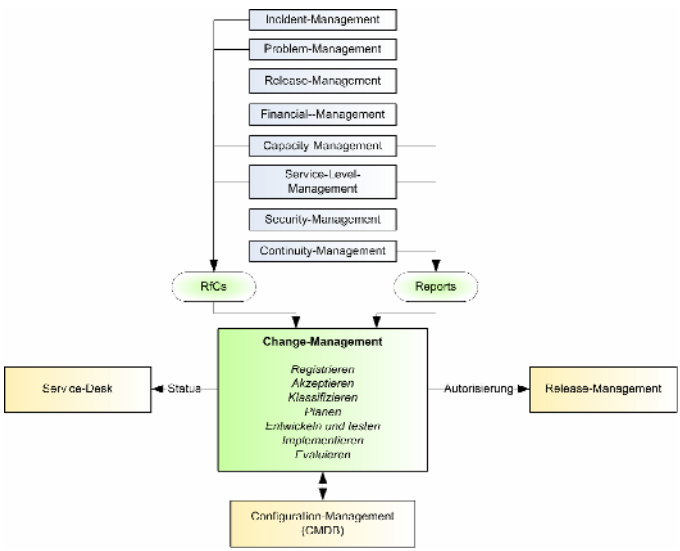

Abb. 3.21. Positionierung Change-Management nach [02]

Installation (Roll-out) von neuen Programmversionen, wofür das Release-Management, unter der Kontrolle des Change-Managements, zuständig ist [02]. Vom Capacity-Management werden ständig Erweiterungen in Form von Changes beantragt. Einige Änderungen bedeuten einen großen Aufwand, wovon einige Vertragskunden betroffen sein können. Hierzu stellt das Change-Management dem Service-Level-Management den PSA-Bericht zur Verfügung, der auch den Zeitplan (FSC) beinhaltet. Das Continuity-Management ist dafür zuständig, dass Continuity-Pläne stets aktuell und durchführbar sind. Mit Hilfe von Berichten wird dies überprüft und der Plan ggf. angepasst. Das Configuration-Management ergänzt in diesem Fall das Change-Management, indem es den Status der Configuration-Items an das Change-Management wiedergibt. Das Zusammenspiel zeigt die Abb. 3.32.

Der Change-Management-Prozess wird vor der Implementierung gemeinsam mit dem Configuration-Management erarbeitet. Bei der Erfassung eines RfCs dokumentiert der Manager die Referenz zu einem Known-Error, wenn es sich um eine Problemlösung handelt. In diesem Fall werden die Änderungen in Standard-Changes oder Service-Requests eingeteilt, um die eigentlichen RfCs zu bekommen. Hiernach werden sie nach durchführbaren, unnötigen oder doppelten RfCs gefiltert und mit den aktuellen CI-Informationen aus der CMDB ergänzt. In der Klassifizierung ist ein RfC zu kategorisieren und priorisieren. Die Kategorie definiert den Umfang und die Folgen eines Change, die Priorität sagt etwas über die Wichtigkeit der Änderung aus. Ist ein Change nicht dringend, so geht der Change-Manager davon aus, dass genügend Zeit zur Verfügung steht, um über den Change abzustimmen. Dies erfolgt in der Planung, an der auch das CAB beteiligt ist. Es findet eine Bewertung der RfCs bezüglich ihrer Auswirkung, Kosten, Vorteile und Risiken statt. Änderungsstrategien werden entwickelt und die Genehmigung (Change-Approval) abgewartet. Nach den finanziellen,

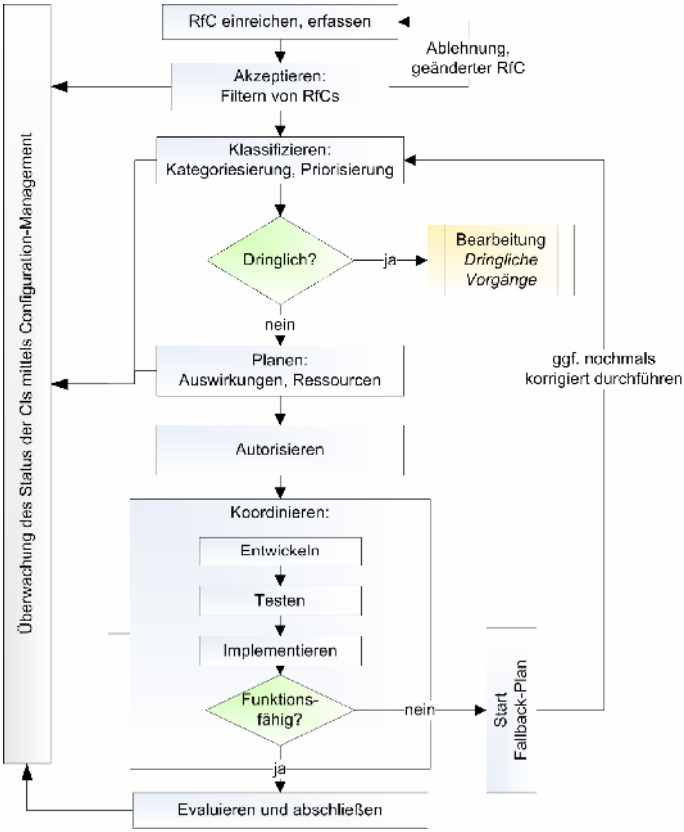

Abb. 3.22. Prozessablauf des Change-Managements nach [02]

technischen und geschäftlichen Genehmigungen autorisiert und koordiniert das Change-Management das Release-Management bei der RfC-Umsetzung. Für jede Umsetzung wird ein Backout-/Fallback-Plan entwickelt, die Änderung zunächst in einer Testumgebung getestet und bei Erfolg auch in das Produktivsystem

implementiert. Falls das produktive System funktionsfähig bleibt, wird die Änderung mit Hilfe des Problem-Managements und PIR (Post-Implementation-Review) evaluiert. Für den Fall, dass dringliche RfCs bearbeitet werden müssen, existiert ein separater und vereinfachter Änderungsprozess. Je nach Kategorie wird das CAB oder das EC einberufen und die Ressourcen werden unmittelbar bereitgestellt.

In der Praxis hilft das Change-Management durch seinen Prozess auch bei der Durchsetzung von großen Änderungen, die sonst ohne ein Management wegen der Größe unterbunden wären. Es wird empfohlen, ein den Prozess unterstützendes Werkzeug zu verwenden. In einigen Unternehmen ist auch die folgende Besetzung des CAB zu finden [05]:

- Anwendungsabteilungen (Leiter),
- CIO (Chief Information Officer),
- Incident-Management,
- IT-Experten (Analysten, Organisatoren),
- Kundenmitarbeiter bei Bedarf,
- Problem-Management,
- Release-Management,
- Service-Desk,
- Service-Level-Management.

Bei der Implementierung eines Change-Managements können die kritischen Erfolgs- und Leistungsindikatoren aus Tabelle 3.9 behilflich sein.

Zum Schluss dieses Abschnitts sollen die Vorteile eines eingesetzten Change-Managements aufgezeigt werden:

- Risikominimierung bei durchzuführenden Änderungen.
- Reduzierung negativer Einflüsse auf Qualität der IT-Services.
- Bessere Abschätzung der Kosten für Änderungen.
- Für den Fehlerfall existiert ein Fallback-/Backout-Plan.
- Stabile IT-Umgebung trotz hoher Anzahl an Änderungen, wegen Koordination.

Tabelle 3.9. CSFs und KPIs des Change-Managements

CSF	KPI
Vermeidung der Bürokratie bei einfachen Änderungen (→ Standard-Changes)	Anzahl abgelehnter RfCs
Widerstand gegen Forderung, jede Änderung zu erfassen	Rückgang unautorisierter Changes
Enge Zusammenarbeit mit Config-Management (wünschenswert)	Anzahl fehlgeschlagener Changes
Sorge um die Qualität der CMDB	Reduktion von Urgent-Changes
	Störungen im Verhältnis zu den durchgeführten Änderungen
	Anzahl implementierter Änderungen pro Zeitraum (insgesamt pro CI)
	Kosten durchgeführter Änderungen

3.2.6 Release-Management

Änderungen an der IT-Infrastruktur werden vom Change-Management geplant und koordiniert. Das autorisierte Release-Management führt diese Änderungen aus. Dazu gehört ein erfolgreiches Rollout von Releases, inkl. Integration, Test und Lagerung. Das Release-Management stellt sozusagen „die rechte Hand“ des Change-Managements dar [02]. Mit einem ganzheitlichen Blick auf Änderungen an IT-Services und die Beachtung von technischen und nicht-technischen Aspekten eines Release, ist die Aufgabe eines Release-Managements definiert. Technisch ist hierbei z. B. die Freigabe neuer Hard- und Software anhand von gültigen Richtlinien [o20]. Ein Beispiel für

eine nicht-technische Seite ist die gleichzeitige Schulung von Anwendern, die nach einem PC-Rollout mit dem neuen Betriebssystem bekannt gemacht werden müssen. Das Release-Management stellt somit technische und organisatorische Mittel und Methoden bereit, die effektive, sichere und nachvollziehbare Durchführung von Änderungen an Konfigurationselementen erlauben [06]. Für eine weitgehende homogene IT-Infrastruktur und die Vereinfachung der Administration werden im Release-Management qualitätsgesicherte Standards und Grundkonfigurationen (engl. „Baselines“) erarbeitet. Hier hat der Einsatz von gleichartigen Computern einen klaren administrativen Vorteil. Dem Release-Management stehen Testumgebungen zur Verfügung, in denen Programme und Prozesse reichlich geprüft werden, um sie dann qualitätsgesichert auf die Produktionsumgebung zu spielen. Die produktive Umgebung stellt dabei immer einen isolierten Bereich dar, der nicht einfach so verändert werden darf [05]. Unregistrierte Änderungen von Anwendern werden dadurch vermieden.

Das Release-Management beschäftigt sich mit Releases. Ein **Release** ist „eine Reihe neuer oder geänderter Konfigurations-Elemente (Configuration Items – CIs), die zusammenhängend getestet und in die Produktivumgebung überführt werden.“ [02]. Es wird durch ein RfC definiert, das implementiert werden muss. Werden neue Komponenten eingeführt bzw. installiert, spricht man von einem **Rollout**. Ein **Rollin** oder auch Roll-in ist das Wiedereinfahren, die Zurücknahme oder der Abbau von Komponenten aus der Produktivumgebung. Je nach Grad der Veränderung handelt es sich um eine besondere Release-Form. Das **Major-Release** ist ein wichtiges Rollout neuer Hardware oder Software, das Funktionserweiterungen und zusammengefasste Workarounds und Hot-/Quick-Fixes zusammenfasst. Ein **Minor-Release** enthält zumeist geringfügige Verbesserungen und Hot-Fixes, die als Notreparaturmaßnahmen anzusehen sind [02]. Solch ein Release setzt auf

die letzte funktionierende Basisikonfiguration auf. Die letzte Unterteilung von Releases ist das **Emergency-Fix**, das eine schnelle vorübergehende Problembehebung (auch Workaround) beschreibt. Ein Unternehmen, das auf Programmierfehler, einen Festplattenaustausch oder auf die Einführung eines neuen Applikationssystems entsprechend reagieren möchte, wendet das Change- und Release-Management an.

Da Releases in unterschiedlichen Umgebungen gleichzeitig existieren können, werden diese mit Versionsnummern (engl. „Release Number“) beziffert. Releases werden folgendermaßen identifiziert (Release-Identifikation):

- Major-Release: v1, v2, v3 usw.
- Minor-Release: v1.1, v1.2, v1.3 usw.
- Emergeny-Fix: v1.1.1, v1.1.2, v1.1.3 usw.

Eine **Release-Unit** (Release-Einheit) beschreibt einen Teil der IT-Infrastruktur, der im Zusammenhang mit mehreren Changes steht, also zusammenhängend getestet, freigegeben und eingeführt wird. Wie viele Changes in ein Release übernommen werden sollen, kann mit Hilfe von drei Release-Arten definiert werden. Ein **Delta-Release** enthält meistens nur die geänderte Hard- oder Software und ist in den meisten Fällen als Notlösung gedacht [02]. Sind die Änderungen nicht zu überschauen, so kann ein **Full-Release** ausgerollt werden, das sogar die nicht geänderten Teile beinhaltet. Für ein **Package-Release** kann man sich entscheiden, wenn z. B. kleine Fehlerbehebungen und neue Funktionalitäten verbunden werden sollen.

Jegliche Änderung, die durch das Release-Management ausgeführt wird, hat Auswirkung auf die CMDB des Configuration-Managements. In dieser Datenbank wird die gesamte IT-Infrastruktur abgebildet oder zumindest das, was kontrolliert mit einem Prozess verändert werden soll. Zum Bestand eines IT-Unternehmens gehören folglich Hardware und Software. Ersteres wird in der **Definitive-Software-Library** (**DSL**) ver-

waltet, die Hardware aber in dem so genannten **Definitive-Hardware-Store** (**DHS**). Die DSL stellt einen sicheren Aufbewahrungsort aller autorisierter Versionen dar. Die im Unternehmen produktiv eingesetzte Software (Eigenentwicklung, Fremdsoftware) existiert als eine archivierte Masterkopie. Softwarelizenzen und ältere Stände sind zu Test- und Recovery-Zwecken somit jederzeit reproduzierbar [06]. Das DHS kann als Vorrats- und Ersatzteillager geprüfter wichtiger Hardwarekomponenten (Basiskonfiguration) gesehen werden, die fehlerhafte Komponenten ersetzen oder für einen kurzfristigen Ausbau bei Kapazitätsengpässen verwendet werden können [06]. Die CMDB sollte Beschreibungen zu Releases, DSL und DHL enthalten und die Verweise auf die ursprünglichen RfCs abbilden.

Die vorangegangene Beschreibung des Problem-Managements zeigt enge Beziehungen zu den Prozessen des Change- und Configuration-Managements auf. Die genauere Positionierung des Problem-Managements kann der Abb. 3.23 entnommen werden.

Der für das Release-Management verantwortliche Release-Manager trägt die Verantwortung für die Einführung, Einhaltung und Weiterentwicklung des Prozesses. Er hält engen

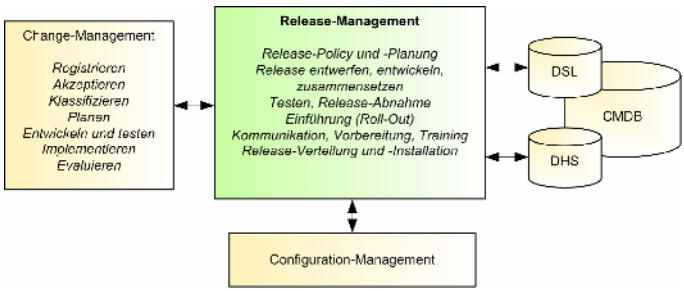

Abb. 3.23. Positionierung Release-Management nach [02]

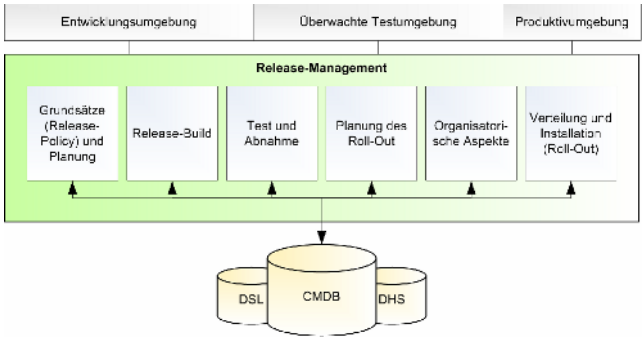

Abb. 3.24. Prozess des Release-Managements nach [02]

Kontakt zu den Managern der Bereiche Configuration- und Change-Management. Da das Release-Management auch mit unterschiedlichen Umgebungsvarianten des Testens und des Rollout zu tun hat, ist die Beziehung zu solchen Entwicklungs- und Testorganisationen von Vorteil. Ein Release-Manager kann die gleiche Person wie der Change- und Configuration-Manager sein. Die in Abb. 3.24 dargestellten Aktivitäten fallen einem Release-Manager zu.

Am Anfang eines jeden Release steht die Vorbereitung im Vordergrund. Vor der eigentlichen Planung wird die Release-Policy festgesetzt. Diese beinhaltet Informationen über die Zusammensetzung und die Release-Units eines Release. Besprochen werden ebenfalls die Auswirkung auf andere Komponenten und der Aufwand an Personal und Zeit. In der Planung werden der Inhalt, die zeitliche Abfolge, die involvierten Standorte, die Verantwortlichkeiten und die Abnahme durch Betrieb und Anwender abgestimmt. Zu diesem Zeitpunkt wird auch der vom Change-Management beschlossene Backout-Plan auf die Durchführbarkeit geprüft. Für das danach folgende Release-Build wird ein Standardverfahren entwickelt, nach dem z. B. die Zusammenstellung der Komponenten erfolgt. Der

Backout-Plan sollte zu diesem Zeitpunkt insbesondere bei Package-Releases abgestimmt werden. Jedes fertige Release muss in der CMDB dokumentiert werden. Zur Qualitätssicherung eines Release stehen der Test und die Abnahme in einer kontrollierten Testumgebung bereit. Durch Anwender und Entwickler ist die formale Abnahme zu bestätigen. Nach einer erfolgreichen Abnahme beschäftigt sich das Release-Management mit der Planung für die Implementierung (Rollout) eines Release. Wichtig dabei sind u. a. der genaue Zeit- und Aktionsplan, die Liste der Ressourcen, die erforderlichen Besprechungen, die Erfassung neuer CIs und die Art und Weise der Release-Installation (inkrementell oder „Big Bang"-Verfahren). Im nächsten Prozessschritt werden die nicht-technischen Aspekte ausfindig gemacht. Es wird abgestimmt, ob z. B. Schulungen gehalten werden müssen oder ob von der Infrastrukturänderung die Service-Level- oder Operational-Level-Agreements betroffen sind. Im letzten Schritt wird das Release in die Produktivumgebung ausgerollt. Dies kann aus Qualitätsgründen mit Hilfe von automatisierten Werkzeugen passieren. Informationen in der CMDB sollten hier auf den neuesten Stand gebracht werden.

Für die Praxis ist es wichtig, dass die Komponenten gründlich getestet und alle wichtigen Daten gesichert sind, bevor Änderungen an der Produktivumgebung vollzogen werden [06]. Ein qualitätsbewusstes Release-Management setzt Last- und Stresstests sowie spezielle Tools ein. Im Idealfall stehen unterschiedliche Umgebungen für die Entwicklung und die Tests bereit [06]. Während und nach einem Release muss der Anwender durch das Service-Desk unterstützt werden, für den Fall, dass fehlerhafte Komponenten eingesetzt wurden. Im Prinzip gilt es, ein Release-Wechsel nicht zu unterschätzen [05].

Bei der Implementierung eines Release-Managements können die in Tabelle 3.10 dargestellten kritischen Erfolgs- und Leistungsindikatoren herangezogen werden.

Tabelle 3.10. CSFs und KPIs des Release-Managements

CSF	KPI
Genügend Zeit für Planung und Rollout	Anzahl Softwareinstallationen, die nicht aus der DSL stammen
Motivation der Kunden für planmäßige Vorgehensweise schaffen	Anzahl nicht lizenzierter Software- und Hardwareprodukte
	Anzahl ungetesteter ausgerollter Releases
	Anzahl fehlgeschlagener Installationen und Backouts
	Kosten von Releases
	Größe und Kapazität der DSL, des DHL

Zum Schluss werden noch einmal die Vorteile eines Release-Managements zusammengefasst aufgelistet:

- Zentrales Management getesteter und autorisierter Komponenten.
- Reproduzierbare Versionen für Tests und Fallback.
- Bessere Ausführung koordinierter Changes.
- Gutes Qualitätsniveau von Software und Hardware.
- Minimierung der Gefahr von Incidents und Known-Errors.
- Einbeziehung der Anwender in Testphase.
- Weniger illegaler Kopien im Unternehmen.
- Veröffentlichung eines Release-Kalenders.

3.3 Service-Delivery

Dieses Kapitel beschreibt das ITIL-Buch Service-Delivery. Es formuliert die Prozesse zur Planung und Service-Bereitstel-

lung, definiert aber auch die Voraussetzungen und Maßnahmen, die dafür nötig sind. Arbeitsergebnisse werden in einem Plan zusammengefasst, wobei jeder Prozess periodisch verläuft. Es werden folgende Prozesse behandelt:

- Service-Level-Management,
- Financial-Management für IT-Services,
- Capacity-Management,
- Availability-Management,
- Continuity-Management für IT-Services,
- Security-Management.

3.3.1 Service-Level-Management

Im Service-Level-Management stehen die strategisch-taktischen Aspekte eines IT-Dienstleisters im Fokus. In vielen Unternehmen ist diese Schnittstelle zum Kunden bereits realisiert. Der Gegenstand solcher Beziehungen sind die Service-Level-Agreements (SLAs), also Vereinbarungen zwischen Dienstanbietern und Dienstabnehmern bezüglich der Qualität und Quantität des Service-Managements [05]. Hiermit werden die abstrakten Erwartungen der Geschäftsperspektive mit den notwendigen Dienstleistungen abgeglichen. Grundlage für die SLAs bilden abgeschlossene Verträge, die oft die SLAs als Hauptbestandteil aufnehmen. Die SL-Agreements erlauben eine Beurteilung der IT, wenn notwendige Angaben und Zielsetzungen enthalten sind. Beide Partner kennen somit den Aufwand und die Kosten einer IT-Dienstleistung genau. Konsequenzen der Nichteinhaltung von festgelegten Rahmenbedingungen eines Service sind ebenfalls enthalten. Das Service-Level-Management überprüft und überwacht die Qualität und Aktualität der Services mit Hilfe von Optimierungszyklen [06]. Seine Aufgabe ist es auch, Verhandlungen mit internen und externen Dienstleistern zu führen, um SLAs zu ermöglichen. Für die

Realisierung der IT-Dienstleistungen ist aber der Service-Desk verantwortlich, der ja Services erst abrufbar macht. Deswegen ist zwar bei der Erarbeitung von SLAs der Service-Level-Manager federführend, der Service-Desk, der Kunde und einige IT-Experten sind aber daran beteiligt [05].

Die von einem Dienstleister angebotenen Leistungen und ihre Merkmale, Komponenten und Kosten werden in einem Dienstleistungskatalog, dem so genannten **Service-Katalog**, definiert – am besten in der Configuration-Database. In solch einem Katalog sind die Leistungen aller SLAs in einem Unternehmen wiederzufinden. Leistungserbringungen außerhalb des Service-Katalogs sind nicht zulässig [06]. Der Katalog kann aber, wenn es die Umstände verlangen, aktualisiert werden. Auf Grundlage dieses Service-Kataloges werden der vom Kunden geforderte Leistungsumfang (engl. „**Service-Level-Requirement**"), die notwendigen Ressourcen und die Kosten definiert. Ein SLR kann mit einem Lastenheft verglichen werden. Die nicht technisch verfassten SLRs werden in die Service-Spezifikationen (engl. „**Service-Specification-Sheet**" (SSS) oder „**Service-Specsheet**") übersetzt. Sie enthalten die technische Beschreibung von IT-Services, beschreiben die Kundenwünsche detaillierter und beschäftigen sich mit den daraus entstehenden Konsequenzen für den Dienstleister (Ressourcen usw.). Ein Service-Specsheet entspricht einem Pflichtenheft und ist Bestandteil einer SL-Anforderung, kann aber, um den Rahmenvertrag zu entlasten, auch als gesondertes Dokument ausgegliedert werden.

Laut ITIL sollen in einer Service-Spezifikation enthalten sein [05]:

- Backup-Prozesse,
- genaue Beschreibung des Dienstes,
- notwendige Change-Requests,
- spezielle Genehmigungsprozeduren,

- erforderliche Dokumente und Dokumentationen,
- Leistungsdetails,
  - Ergebnisse
  - Produkte (Dateien)
  - zusätzliche Dienste
- Notfallpläne bei Problemen,
- Festlegung der Partner (Kontakte und Verantwortungen),
- der Service-Level,
  - Kapazität
  - Durchsatz (Performance)
  - Unterstützungsleistungen
  - Verfügbarkeit
  - Zeitrahmen
- vertragliche Details,
  - Termine
  - Lieferort
  - Zahlungsmodalitäten
  - Zeitaufwand für bestimmten Dienst.

Kommt es zu einer Übereinstimmung zwischen Dienstanbieter und Kunden, so werden diese verbindlichen Vereinbarungen auf Basis einzelner Leistungsvereinbarungen (engl. „Service-Level“) in den **Service-Level-Agreements** (**SLAs**) definiert. Ein typischer SLA würde z. B. für den Service „Tagesumsätze der Filialen“ den Start und das Ende der Datenübertragung vereinbaren. Für eine Helpdesk-Anfrage könnte die Anzahl der maximalen Warteschleifen festgelegt werden. SLAs werden ebenfalls in der CMDB dokumentiert, da ein SLA laut ITIL auch ein Configuration-Item darstellt, das folgende Informationen beinhalten sollte [05]:

- Bezeichnung des Service (Diensttitel),
- Kurzbeschreibung,
- die SLA-Version,
- Definition der beteiligten Parteien,

- Verantwortung und Funktionen,
- die auslösenden SLRs,
- das dazugehörige SSS mit Details,
- Eskalationsprozesse,
- Begriffsdefinitionen,
- Berichtsmethoden für das SLM,
- Konventionalstrafen bei Nichteinhaltung,
- Einbezug zu Change- und Release-Management,
- Relationen zu weiteren SLAs.

Ein SLA kann sich auf externe Kunden oder unternehmensinterne IT-Organisationen beziehen. Im ersten Fall handelt es sich um eine Vereinbarung mit kaufmännischem und juristischem Teil, im zweiten Fall ist ein kaufmännischer Teil optional und die juristischen Schritte bei Nichteinhaltung fallen weg, da diese meist firmenintern (z. B. ohne Sanktionen) geklärt werden können. Weitere Komponenten eines Vertrages stellen die Mitarbeiter (Umsetzung, Schulung), Kunden (Erwartung, Kosten, Service-Katalog) und die technische Seite (Messverfahren, Tests) dar. Zusätzlich zu den SLAs existieren in ITIL die so genannten **Underpinning-Contracts** (**UCs**) und die Operational-Level-Agreements (OLAs). Ein UC ist ein Absicherungsvertrag gegenüber einem externen Lieferanten und beinhaltet einen kaufmännischen und juristischen Teil. Es handelt sich dabei um einen Vertrag über die Abwicklung bestimmter Bereiche eines Service (Herstellersupport, vgl. 3rd-Level-Support). Im Grunde ist ein UC aus der Sicht des Lieferanten nichts anderes als ein Service-Level-Agreement. Die unterschiedlichen Begriffe sollen aber den Einsatzzweck von Verträgen besser verstehen helfen. Somit kommen wir zu den OLAs, die eine weitere Beschreibung von UCs sind. Der Unterschied liegt aber darin, dass Operational-Level-Agreements mit internen Organisationseinheiten abgeschlossen werden, um die dem Kunden vertraglich zugesicherten Services vollständig

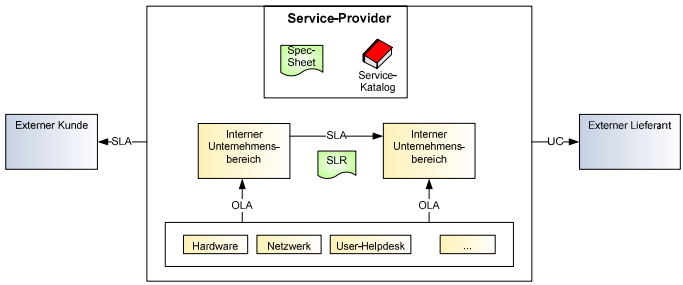

Abb. 3.25. Vertragsarten des Service-Level-Managements nach [02] und [06]

erbringen zu können. In einem OLA darf, wie bei unternehmensintern abgeschlossenen SLAs, auf den juristischen Teil verzichtet werden. Der kaufmännische Teil ist auch hier optional zu integrieren. Die Abb. 3.25 stellt die unterschiedlichen Vertragsarten eines IT-Service-Managements übersichtlich dar.

Neben den Vertragsarten werden auch die Vertragsformen unterschieden (vgl. Abb. 3.26). Eine Service-basierte Vereinbarung ist unternehmensweit einheitlich für viele Kunden gleich [06]. Ein kundenbasierter Vertrag enthält kundenspezifische Anforderungen oder ist pro Kundengruppe definiert. Ein Multilevel-SLA enthält das Corporate-Level (AGBs, Klauseln, Rollen usw.), das Customer-Level (übergeordnete individuelle Kundenvereinbarungen) und das Service-Level (kundenspezifisch) [06].

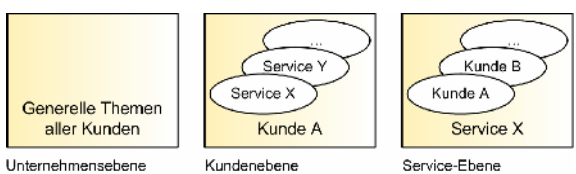

Abb. 3.26. Vertragsformen im Service-Level-Management nach [02]

Das Service-Level-Management ist für die Verbesserung eines IT-Service verantwortlich, wofür er auch das Budget dafür einplanen muss. Für die Verbesserung steht dem SLM ein Service-Verbesserungsprogramm zur Verfügung. Mit diesem **Service-Improvement-Program** (**SIP**) initiiert das SLM ein Projekt, das die Aktionen, Phasen und Meilensteine zur Verbesserung eines IT-Service in einem definierten Arbeitsbereich oder Prozess festlegt [02]. Dem Service-Level-Management steht weiterhin ein Werkzeug zur Verfügung, das alle notwendigen Management-Informationen zur Steuerung der IT-Organisation und externer Lieferanten (Provider) enthält: der Service-Qualitätsplan. Mit eingeschlossen sind in solch einem **Service-Quality-Plan** (**SQP**) u. a. die Zielsetzungen eines IT-Service und Leistungsindikatoren (KPIs) sowie Parameter für die Service-Management-Prozesse und das operative Management. Verrechenbare Kosten entstehen als Ergebnis des **Service-Achievements** (**SA**), womit tatsächlich erbrachte Leistungen und der erforderliche Aufwand nachgewiesen werden können.

Der Manager eines Service-Level-Managements hat vielfältige Aufgaben zu erledigen. Er erstellt und pflegt den Service-Katalog und formuliert anhand der Verträge (SLAs, OLAs und UCs) und Optimierungsprogramme ein effektives Service-Level-Management. Neben den verschiedenen Berichten wird im SLM die Verbesserung der IT-Organisation mittels Leistungsanalysen angestrebt. Aus diesem breiten Aufgabenfeld ergeben sich folgende Beziehungen zu anderen Prozessen:

- Service-Desk,
- Incident-Management,
- Configuration-Management,
- Availability-Management,
- Capacity-Management,
- Change-Management,

- IT-Service-Continuity-Management,
- Security-Management,
- Financial-Management.

Der Service-Desk filtert alle Anwenderanfragen und Beschwerden, wobei das Incident-Management für die schnelle Wiederherstellung der Services bemüht ist und über etwaige Ausfälle berichtet. Im Availability-Management wird die Verfügbarkeit eines in den SLAs definierten Service optimiert. Das Capacity-Management kümmert sich um die notwendigen Kapazitäten des zu erbringenden Dienstes. Jede Änderung an einem SLA fordert das Eingreifen des Change-Managements, ohne das keine Änderung an einem CI getätigt werden darf. Das Security-Management ist für die Erbringung der in einem SLA festgelegten Sicherheitsvereinbarung verantwortlich. Welche Kosten ein IT-Service verursacht, teilt das Financial-Management mit. Das IT-Service-Continuity-Management wird bei abgeschlossenen Verträgen ebenfalls in Mitleidenschaft gezogen. Die in einem SLA definierten Maßnahmen und die damit vereinbarten Kosten müssen umsetzbar sein.

Der SLM-Prozess (vgl. Abb. 3.27) beginnt mit der Identifizierung des Bedarfs und beachtet auch die indirekte Erwartungshaltung des Kunden. In diesem Schritt werden die SL-Requirements festgehalten. Hiernach werden sie in interne und externe Standards überführt. Nun müssen die sich daraus ergebenden Verträge erstellt, angepasst, ggf. neu verhandelt und der Service-Katalog bei Bedarf erweitert werden. Darüber hinaus bietet der Prozess immer wiederkehrende Aktivitäten wie das Monitoring der Service-Level, die regelmäßige Abgabe von Leistungsberichten und die Evaluierung mit der daraus resultierenden Optimierung der Service-Level (engl. „Service-Level-Optimizing“, SLO).

In der Praxis ist es für ein SLM wichtig, dass Textverarbeitungsprogramme wegen der Dokumentenvorlagen integriert

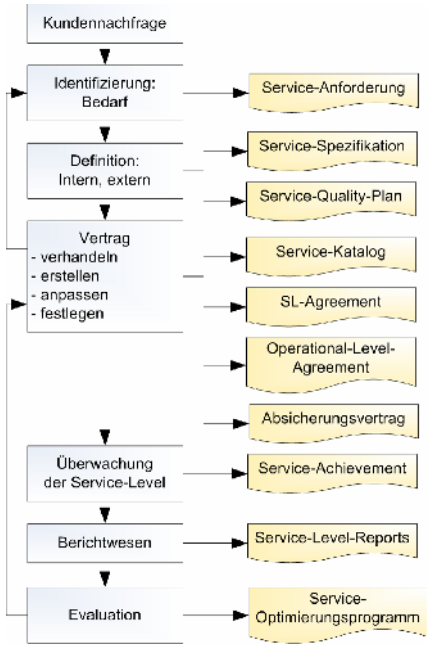

Abb. 3.27. Prozess des Service-Level-Managements nach [02]

werden können. Es ist auch von Vorteil, wenn die Überwachung der Service-Level anhand von Kennzahlen automatisiert abläuft. Die Auswirkung einer Änderung am Service-Katalog auf ein Service-Level-Agreement sollte genauso beachtet werden wie die Mehrsprachenfähigkeit von Verträgen [06]. Bei vielen erbrachten Services ist eine eindeutige Identifikation dieser für die Preiszuordnung und Preisfindung wichtig. Die Aufwände für IT-Services werden somit verrechenbar. Eine beispielhafte Gliederung eines Service-Kataloges könnte wie folgt aussehen [06]:

Änderungshistorie

Vorwort

1. *Zur Organisation*
2. *Ansprechpartner*
3. *Services*
   - *3.1. Allgemeiner Teil*
   - *3.2. Detailbeschreibung*
     - *3.2.1. Service A*
       - *3.2.1.1. Service-Beschreibung*
       - *3.2.1.2. Ansprechpartner*
       - *3.2.1.3. Service-Requirements*
       - *3.2.1.4. Leistungs- und Lieferumfang*
       - *3.2.1.5. Service-Level*
       - *3.2.1.6. Dokumentation und Berichte*
       - *3.2.1.7. Qualitätsnachweis*
       - *3.2.1.8. Preise und Konditionen*
     - *3.2.2. Service B*
       - *3.2.2.1. Service-Beschreibung*
       - *3.2.2.2. Ansprechpartner*
       - *3.2.2.3. …*
     - *3.2.3. …*
4. *Change-Prozess*
5. *Service-Verzeichnis*
6. *Glossar*
7. *Anhang*

Für den SL-Manager ergeben sich für die Praxis wichtige Erwartungen und Fähigkeiten [05] (vgl. Tabelle 3.11).

Bei der Implementierung eines Service-Level-Managements können die in Tabelle 3.12 dargestellten kritischen Erfolgs- und Leistungsindikatoren herangezogen werden.

Tabelle 3.11. Anforderungen an einen Service-Level-Manager

Erwartungen	Fähigkeiten
Beziehungen zu Kunden/Anwendern pflegen	IT-Kenntnisse
als Person Wünsche und Probleme der Benutzer kennen, berücksichtigen	betriebswirtschaftliches Wissen
verfügt über technologisches IT-Grundwissen	Buchhaltungs-, Finanzwesen
benötigt Verhandlungsgeschick	Fachwissen aus den Bereichen der Anwender
Grundkenntnisse für juristische Aspekte (für Ausarbeitung von Verträgen) von Vorteil	Kommunikationstechniken
psychologische Fähigkeiten (für Kommunikationsfreudigkeit und Konfliktbewältigung)	Verhandlungsgeschick

Tabelle 3.12. CSFs und KPIs eines Service-Level-Managements

CSF	KPI
Kompetenter Service-Level-Manager mit Wissen über IT und Geschäftsprozesse	Anzahl und Schwere von Vertragsverletzungen
Prozessziel sollte klar definiert sein	Anzahl Vertragsverletzungen wegen nicht eingehaltener UCs/OLAs
Klare Verteilung von Aufgaben, Befugnissen und Zuständigkeiten	Durchlaufzeit bis zum Vertragsabschluss
	Anzahl der durch SLAs abgedeckten Services
	Aktualität der Verträge
	Prozentsatz von OLAs und UCs für alle SLAs

Zum Schluss dieses Kapitels sollen die Vorteile eines implementierten Service-Level-Managements aufgelistet werden:

- Entwurf der IT-Services gemäß den Erwartungen des Kunden.
- Transparente IT-Services für Kunden und Anwender.
- Aufwand für IT-Services verrechenbar.
- Dienste werden messbar, vergleichbar.
- Anwender-/Kundenzufriedenheit durch garantierte Ergebnisse.
- Bessere Übersicht und Planung der zu leistenden Aufgaben für andere Prozesse und Mitarbeiter.
- Entwicklung der Beziehungen beider Parteien.

3.3.2 Financial-Management

Qualität im Allgemeinen ist immer mit Kosten verbunden. Hohe Qualität erfordert einen hohen Aufwand, der die Kosten in die Höhe treibt. Zwischen diesen beiden Gesichtspunkten muss ein Gleichgewicht geschaffen werden, unter gleichzeitiger Berücksichtigung der Kundenwünsche. Es ist also für ein Unternehmen das eigene wirtschaftliche Verhalten wichtig, um die gewünschte Qualität seiner Produkte bzw. Dienstleistungen bereitzustellen und dabei selbst nicht im Nachteil zu sein. In den letzten Jahren sind die Kosten von IT-Organisationen soweit gestiegen, so dass über eine Auslagerung der eigenen IT nachgedacht wurde. Das Financial-Management beschäftigt sich nicht mit Unternehmens-Controlling oder Finanzbuchhaltung. Es betrifft ausschließlich die IT-Umgebung [05]. Kosten werden überwacht, den verursachenden Organisationseinheiten zugeordnet und verrechnet. Im besten Fall kann die zeitlich beschränkte Nutzung eines IT-Service exakt einem Benutzer zugeordnet werden. Das Financial-Management greift auf die Finanzbuchhaltung zurück, um eine Budgetplanung, Kostenkontrolle und die Leistungsverrechnung zu ermöglichen. Das

Financial-Management stellt betriebswirtschaftliche Informationen zur Steuerung der IT-Organisation bereit, verwaltet die Erbringungskosten der zugesicherten Services, fördert wirtschaftliches Handeln, schafft Transparenz über Kosten und Leistungen und kann bei gleichzeitiger Leistungssteigerung die Kosten senken helfen, indem z. B. die Kosten von Services, Changes und Ressourcen ermittelt und optimiert werden [06].

Das Financial-Management trifft Schätzungen über die erforderlichen Finanzmittel mittels der Finanzplanung bzw. des **Budgeting**. Hierbei werden die tatsächlichen und die geschätzten Ausgaben miteinander verglichen und die ausgegebenen Mittel gerechtfertigt. Es müssen ebenso laufende Projekte, der vergangene Geschäftsverlauf und die mittel- und langfristige Geschäftsplanung berücksichtigt werden [06]. Aus diesem Grund beeinflusst das Budgeting die strategische und taktische Unternehmensplanung. Die Kostenrechnung bzw. das **Accounting** dient der Ermittlung und Zuordnung von Kosten für einen bestimmten Service pro Anwender. Das Ziel sollte sein, nur direkte Kosten zu haben, die unmittelbar mit spezifizierten Diensten verbunden sind [05]. Ein Problem stellen die indirekten Kosten dar, die auf Kostenstellen umgelegt werden müssen.

Die Grundlage für das Accounting sind die Kosten-Nutzen-Analyse und die ROI-Analysen (engl. „Return On Invest“) bzw. der Investitionsrückfluss. Unterstützt wird vom Accounting die Entwicklung von Investitionsstrategien und der Leistungsverrechnung. Letztere wird auch **Charging** genannt. Hier geht es um die Weiterverrechnung der Kosten auf Grund der tatsächlich bezogenen Leistungen [02]. Das Charging sollte einfach, verständlich, realistisch und fair sein [06]. Mittels der Preisgestaltung kann das Kundenverhalten für ein Unternehmen positiv beeinflusst werden. Der Manager dieser Management-Disziplin ist verantwortlich für die Entwicklung und Pflege des Finanzsystems. Er legt die Richtlinien für die Finanzplanungs-, Kostenrechnungs- und Verrechnungssysteme fest (vgl. Abb. 3.28).

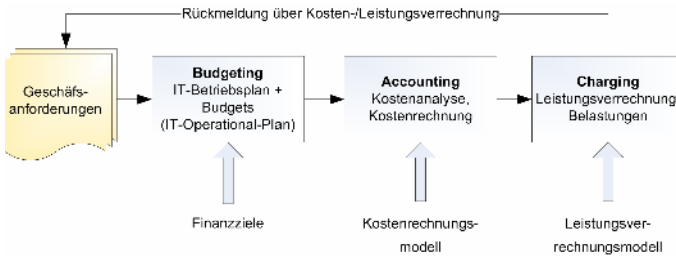

Abb. 3.28. Prozess des Financial-Managements nach [02]

Der Prozess des Financial-Managements beginnt mit dem Budgeting. Als Methoden der Finanzplanung nennt ITIL das Incremental-Budgeting und das Zero-Based-Budgeting. Ersteres basiert auf den Vorjahreszahlen und greift auf Daten aus dem Service-Level-Management zu, da den angebotenen Dienstleistungen Kosten zugeordnet sind. Darüber hinaus lassen sich Vergleichswerte von Lieferantenangeboten und externen Dienstleistern ermitteln. Das Zero-Based-Budgeting besitzt keine Referenzzahlen, sondern Kennzahlen (KPIs) aus dem SLM. Dies ist z. B. für neu angebotene Services vorteilhaft. Das Budgeting beinhaltet als Aufgabe zusätzlich die Überwachung des Budgets (Kosten und Erlöse) und die Einplanung von Spielräumen für Changes. Ein Budgeting hat oft Auswirkungen auf das Service-Level-Management. Das Accounting bzw. die Kostenrechnung folgt als zweiter Schritt nach dem Budgeting. Hier werden sämtliche Kosten berechnet, die die IT verursacht. Es wird die Zusammensetzung der Kosten ermittelt und klassifiziert. ITIL definiert dabei folgende Kostengruppen:

- Energiekosten,
- Gebäudekosten,
- Hardwarekosten,
- IT-Betriebskosten,
- Materialkosten,

Tabelle 3.13. Kostenarten nach ITIL

Kostenart	Zusammensetzung
Hardware	Großrechner, Speicher, Netzwerke, PCs
Software	Betriebssysteme, Datenbanken, Anwendungen, Monitor- und System-Management-Werkzeuge
Personal	Lohnkosten, Spesen, Umzug, Extras
Liegenschaften	Büros, Lager, Produktions- und Energieanlagen
Externe Dienstleistungen	Beratung, Outsourcing
Transferkosten	Interne Leistungsverrechnung im Unternehmen

- Netzwerkkosten,
- Personalkosten,
- Softwarekosten,
- Support-Kosten.

Als Kostenarten werden Kategorien für eine dedizierte Kostenzuordnung betrachtet [06] (vgl. Tabelle 3.13).

Diese Kosten können in unterschiedliche Kategorien eingeteilt werden:

- Kapital (Vermögenswerte),
- Betrieb (laufende Kosten),
- Direkt (eindeutig Kunden zuzuordnen),
- Indirekt (zu verteilen auf mehrere Kunden),
- Fest (bei Produktionsänderung konstant),
- Variabel (schwankend bei Produktionsänderung).

Nach der Kostenrechnung folgt der dritte und letzte Schritt der Leistungsverrechnung: das Charging. Hinter dem Begriff Chargable-Unit steht die Orientierung am Bedarf, d. h. „für was muss ich mich bezahlen lassen“ steht im Vordergrund. Es werden unterschiedliche Preisstrategien zur Verfügung gestellt, die verfolgt werden können:

- Cost-Plus (Preis = Kosten + Gewinnzuschlag),
- Going-Rate (Preis wie bei internen IT-Abteilungen),
- Marktpreis, branchenüblicher Preis,
- Negotiated-Contract-Price (Preisverhandlung mit Kunden).

Für die Praxis ist es von Vorteil, dass das Financial-Management Schnittstellen zu z. B. der CMDB und Finanzbuchhaltungssystemen aufweist. Die Budgetschätzungen sollten mit den realen Kosten verglichen werden, um die Erfahrung im Schätzungsprozess zu fördern, was im Laufe der Zeit genauere Schätzungen erlaubt. Für die Kostenrechnung, Leistungsverrechnung und zu kundenbezogenen Abrechnungen

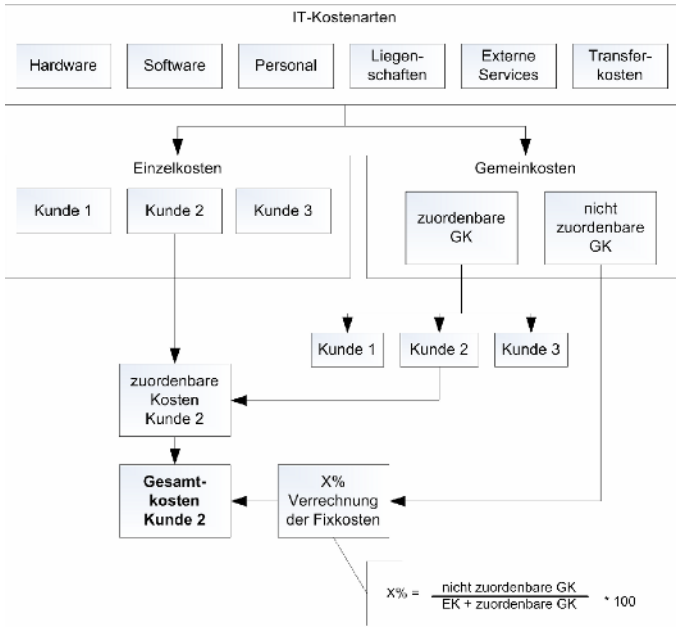

Abb. 3.29. Kostenermittlung nach [09]

sollten die Daten effektiv ermittelt werden [06]. Wenn ein Unternehmen mit ausländischen Firmen zu tun hat, sollten die Schwierigkeiten der unterschiedlichen Währungen und Sprachen beachtet und durch Mehrwährungsfähigkeit und Mehrsprachigkeit gelöst werden. Die Praxis hat gezeigt, dass in einem Cost-Center die Kosten geschätzt werden, die Verrechnungssätze aber sind oft nicht realistisch [05]. Für ein Profit-Center gilt, dass die IT als Unternehmen im Unternehmen auf Gewinn ausgerichtet ist, d. h., auf die Selbstkosten kommt ein Aufschlag hinzu. Dazu im Gegensatz steht der Service-Center, der lediglich die reinen Selbstkosten ermittelt und verrechnet. Für die kundenspezifische Kostenermittlung wird oftmals, wie in Abb. 3.29 dargestellt, vorgegangen.

Schlussendlich können die in Tabelle 3.14 aufgestellten kritischen Erfolgs- und Leistungsindikatoren bei der Implementierung eines Financial-Managements helfen.

Tabelle 3.14. CSFs und KPIs eines Financial-Managements

CSF	KPI
Aufklärung der Anwender über Services, die bezahlt werden müssen	Höhe der gesamten IT-Kosten
Kostenüberwachung	Anzahl und Höhe von Budgetüberschreitungen
Aufklärung über Kosten und Folgen der Einführung eines Finanz-Managements	Gesamtkosten (TCO)
Configuration-Management muss richtige Informationen liefern	Zeitaufwand Finanzplanung
	Anzahl Änderungen am Verrechnungsmodell
	Abweichungen in der Finanzplanung

3.3.3 Capacity-Management

Ein Unternehmen hat viele Faktoren zu beachten, damit es auf dem globalen Markt bestehen kann. Diese Faktoren stehen meistens im Gegensatz zueinander, weswegen eine Balance gefunden werden muss. So verhält es sich z. B. mit den Kosten und der Kapazität (engl. „Cost versus Capacity"). Wie viel kostet die Anschaffung von Kapazitäten, um die geschäftlichen Anforderungen zu erfüllen? Wird die Kapazität effizient genutzt? Ist die Kapazität ausreichend für die künftige Nachfrage des Kunden (engl. „Supply versus Demand")? Wann ist die Performanz ausgereizt und wann sollte zusätzliche Kapazität geschaffen werden (engl. „Performance Tuning")? Mit diesen und weiterführenden Fragen beschäftigt sich das Capacity-Management. Es erstellt aus den Geschäftsanforderungen den Kapazitätsplan und überwacht dessen Einhaltung (engl. „Monitoring") [o20]. Nach dem Motto "Planned buying is cheaper than panic buying" [06] sollen für die zu erbringenden Service-Level der Umfang und die Kosten ermittelt werden, um Kapazitätsengpässe zu vermeiden. Das Hauptaugenmerk liegt hierbei auf der Hard- und Software und dem Personal. Die IT-Infrastruktur wird mittels Belastungs- und Auslastungsszenarien geprüft, um somit Leistungsreserven besser einzuplanen [05]. Das Capacity-Management ist um einen effizienten Einsatz der Ressourcen bemüht. Die technologischen und unternehmerischen Aspekte sind genauso von Bedeutung wie die finanziellen. Das Capacity-Management ist wichtig für die Business-Strategie, den Business-Plan, die IT-Strategie und den IT-Business-Plan. Der Capacity-Manager ist für diesen Prozess verantwortlich, indem er für die Erstellung und Aktualität des Kapazitätsplans und der Kapazitätsdatenbank Sorge trägt.

Das Capacity-Management besitzt die **Capacity-Management-Database** (**CDB**), in der Informationen aus dem laufen-

den Betrieb enthalten sind. Dies erlaubt ein rechtzeitiges Erkennen von Leistungsgrenzen der IT-Komponenten. Aus diesem Grund ist das Capacity-Management immer proaktiv. Neben der CMDB erhält die CDB zusätzliche Informationen über Leistung und Auslastung (engl. „**Workload**“) u. a. von Business-, Service- und Finance-Daten. Anhand dieser Daten werden unterschiedliche Berichte über IT-Services, IT-Komponenten, Kapazitätsprognose usw. und **Kapazitätspläne** erstellt. Im Kapazitätsplan werden die Anforderungen und die Kosten benannt. Er sollte folgende Inhalte aufweisen [06]:

- Einleitung (Rahmenbedingungen der Planung),
- Annahmen und Voraussetzungen,
- Bewertungsgegenstand, Geschäftsszenarien,
- Mengengerüst, Ressourcenübersicht,
- Kostenplan,
- Empfehlungen, Nutzen-Risiko-Analyse,
- Management-Zusammenfassung.

In der Prozessdarstellung der Abb. 3.30 werden die Schnittstellen zu anderen Prozessen erkennbar und danach beschrieben.

Im Incident-Management können Störungen auftreten, deren Ursache ein Kapazitätsproblem ist. Hier und für das Problem-Management könnte das Capacity-Management Werkzeuge zur Verfügung stellen, um solche Diagnosen durchzuführen und

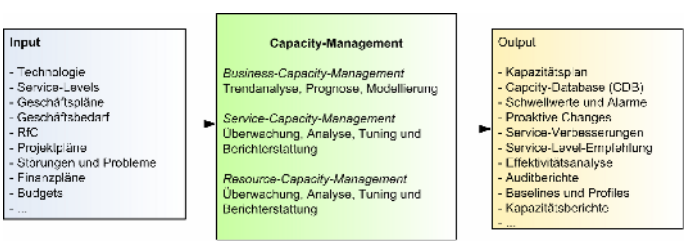

Abb. 3.30. Prozess des Capacity-Managements nach [02]

unter Umständen das Problem lösen zu können. Das Change- und Release-Management können sich einen Überblick über den Kapazitätsbedarf verschaffen oder selbst Informationen über Änderungen und Releases bereitstellen. Das Configuration-Management hat eine enge Beziehung zum Capacity-Management, da wichtige Informationen aus der CMDB in die CDB fließen. Das Service-Level-Management profitiert vom Capacity-Management, indem Informationen für die Kontrolle und Abgleich der Service-Level bezogen werden können. Umgekehrt berät das Capacity-Management über die Realisierung von Service-Levels. Das Finance-Management ist anhand des Capacity-Managements imstande, die Investitionsfinanzpläne und Kosten-Nutzen-Analysen zu erstellen und Investitionsentscheidungen zu treffen. Für die Kontinuität von Services kann die erforderliche Mindestkapazität ermittelt und aufrechterhalten werden. Das Availability-Management verwendet dieselben Werkzeuge und Techniken, um eine Nichtverfügbarkeit von Services, auf Grund von Leistungs- und Kapazitätsproblemen, ausfindig zu machen.

Der Capacity-Management-Prozess besteht aus drei Subprozessen. Das proaktive **Business-Capacity-Management** (**BCM**) trifft Vorhersagen über zukünftige Bedürfnisse und Anforderungen der Kunden [02], indem Strategiepläne und Trendanalysen formuliert werden. Hier werden ebenfalls die Service-Vereinbarungen definiert. Die Aktivitäten dieses untergeordneten Prozesses umfassen die Erstellung eines Kapazitätsplans, die Modellierung u. a. von Schätzungen, Analysen und Simulationen und schließlich das Application-Sizing. Letzteres formuliert die Vorhersagen über die benötigte Hardware und die Angaben über voraussichtliche Performanz und die Kosten [02]. Der zweite Subprozess ist das **Service-Capacity-Management** (**SCM**), das im Wesentlichen die Nutzung von IT-Dienstleistungen bestimmt. Der dritte Subprozess **Resource-Capacity-Management** (**RCM**) hat die Aufgabe, die Nutzung

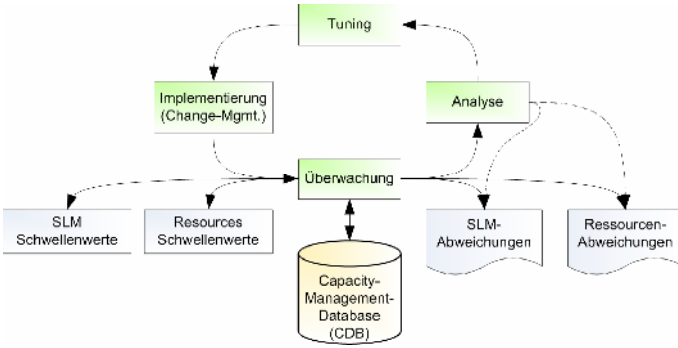

Abb. 3.31. Interaktive Tätigkeiten des Capacity-Managements nach [02]

der IT-Infrastruktur zu bestimmen und potenzielle Probleme zu erkennen. SCM und RCM besitzen identische Aktivitäten, die sich aber in unterschiedlichen Schwerpunkten und dem Umfang unterscheiden: Implementierung, Überwachung, Analyse und die Feinabstimmung (engl. „Tuning“). Abbildung 3.31 verdeutlicht diese Kernaktivitäten.

Neben diesen Aktivitäten gehört zum Capacity-Management der Aufbau einer Kapazitätsdatenbank (CDB), um den besagten Kapazitätsplan, die technischen Berichte und die Berichte für das Management zu erstellen. Weiterhin ist das Capacity-Management durch ein Bedarfsmanagement (engl. „Demand-Management“) gekennzeichnet, mit dem sich die Kapazitätsnachfrage beeinflussen bzw. verschieben lässt. Hierbei unterscheidet ITIL in ein kurzfristiges und langfristiges Bedarfsmanagement. Das Short-term-Demand-Management kommt zur Anwendung, wenn ein kurzfristiger Kapazitätsmangel entsteht. Für Fälle, in denen es aus Kostengründen schwer vertretbar ist, zusätzlich in die IT-Infrastruktur zu investieren, und es genügend Zeit zur Verfügung steht, gibt es das Long-term-Demand-Management.

In der Praxis wird das Capacity-Management angewendet, wenn z. B. ein neuer Mitarbeiter eingestellt wird und der Drucker, sein Arbeitsplatzcomputer, die Berechtigungen zu Anwendungen, Systemen und Datenbanken bereitgestellt werden müssen. Als weitere Beispiele sind die Einführung eines SAN oder die Implementierung eines modernen E-Mail-Systems zu benennen [05]. Für das Capacity-Management sollten mindestens Schnittstellen zu der Configuration-Management-Datenbank (CMDB) und ggf. den Inventarisierungsdaten bestehen [06]. Mit Hilfe einer Simulation von IT-Komponenten und deren Lifecycle-Eigenschaften ist eine bessere Modellierung von Planungsdaten möglich. Weiterhin ist eine automatisierte Anfertigung von Kapazitätsplänen von Vorteil.

Für die Implementierung eines Capacity-Managements können die in Tabelle 3.15 dargestellten kritischen Erfolgs- und Leistungsindikatoren helfen.

Tabelle 3.15. CSFs und KPIs des Capacity-Managements

CSF	KPI
Genaue Vorhersagen und Prognosen für das Unternehmen	Abweichung zwischen Business-Plan und Kapazitätsplan
Kenntnis der IT-Strategie und IT-Planung	Anzahl überwachter IT-Services und IT-Komponenten bezogen auf die Performanz und den Durchsatz
Kenntnis der Entwicklung im Bereich der Technologie	Anzahl von Überkapazitäten
Zusammenarbeit mit anderen Prozessen	Anzahl der Vertragsverletzungen wegen Kapazitätsengpässen
	Verringerung der Anzahl der Panikkäufe
	Reduzierung der Störungen auf Grund von Perfomanzproblemen

Zum Schluss dieses Abschnitts werden die Vorteile der Implementierung eines Capacity-Managements zusammenfassend aufgelistet:

- Risikominimierung für IT-Services durch ständige Überwachung und die durch das Application-Sizing bekannten Auswirkungen von Änderungen.
- Gesteigerte Effizienz auf Grund von frühzeitigen Abstimmungen von Angebot und Nachfrage.
- Kostensenkung wegen effizienter Ressourcennutzung und zeitlicher Investitionen.

3.3.4 Availability-Management

Wenn ein IT-Unternehmen Dienstleistungen offeriert, so müssen die unterschiedlichen Services jederzeit abrufbereit, funktionstüchtig und wirtschaftlich sein. ITIL bietet für diese Thematik einen weiteren Prozess: das Availability-Management. Es dient zur „Optimierung der Nutzung und der Leistungsfähigkeit (Performance Management) der IT-Infrastruktur“ [06]. Aus den Geschäftsanforderungen werden ein allgemeines und ein servicespezifisches Verfügbarkeitsniveau definiert und die Umsetzung geplant. Darüber hinaus werden für die Qualitätskontrolle die KPIs überwacht und ein Verfügbarkeitsplan erstellt und gepflegt. Das Verfügbarkeitsmanagement soll die Service-Verfügbarkeit kontrollieren und bei Ausfall die Wiederverfügbarkeit sicherstellen. Im Fokus steht also auch die Kundenzufriedenheit, von der der Unternehmenserfolg abhängt. Diese wird erreicht, indem durch Optimierung der Verfügbarkeit die Erbringung der vereinbarten Service-Level garantiert werden kann. Die Verfügbarkeit wird oft im Format *HH*TT*WW* – d. h. eine Multiplikation von Stunden, Tagen und Wochen – angegeben. Das Availability-Management hat zu fast allen ITIL-Prozessen eine Schnittstelle, die sich mit Betriebsunterbrechungen

beschäftigen. In besonderen Fällen kann der Prozess Einfluss auf die Service-Level-Agreements haben. Ein Availability-Manager definiert und entwickelt diesen Prozess im Unternehmen. Bei IT-Services mit unrealistischen Service-Levels greift dieser korrigierend ein. Der Manager ist für die Optimierung der Verfügbarkeit der IT-Infrastruktur und die Berichterstattung zum Top-Management oder anderen ITIL-Prozessen verantwortlich.

In einem Verfügbarkeitsmanagement muss zunächst der Begriff „Verfügbarkeit", um den sich alles dreht, definiert werden. Unter **Verfügbarkeit** wird die mögliche Nutzung in einem Zeitfenster verstanden. Ein hohes Maß an Verfügbarkeit bedeutet, dass „der Anwender jederzeit bzw. im vereinbarten Rahmen über den IT-Service verfügen kann" [02]. Die Verfügbarkeit setzt sich zusammen aus der Zuverlässigkeit (engl. „Reliablility"), Wartbarkeit (engl. „Maintainability"), Servicefähigkeit (engl. „Serviceability") und der IT-Sicherheit (engl. „Security"). Mathematisch betrachtet handelt es sich um das Verhältnis zwischen der erreichten Verfügbarkeit und den vereinbarten Service-Zeiten (vgl. Abb. 3.32). Wenn beispielsweise ein Service sieben Tage lang von 7 Uhr bis 17 Uhr verfügbar sein soll, wovon drei Stunden dies nicht der Fall war, so ergibt sich nach der nachfolgenden Formel folgendes Ergebnis:

$$((7 * 10) - 3) / (7 * 10) * 100 = 95{,}71\%.$$

$$\text{Verfügbarkeit (in \%)} = \frac{\text{AST - DT}}{\text{AST}} * 100$$

Abb. 3.32. Verfügbarkeitsformel

Der Zähler der obigen Formel aus Abb. 3.32 ergibt sich aus der erreichten Verfügbarkeit, d. h. aus der Differenz zwischen der vereinbarten Service-Zeit (engl. „**Agreed Service Time**", AST), und der zeitlichen Nichtverfügbarkeit (engl. „**Downtime**", DT).

Weitere Begriffe, die die Verlässlichkeit (engl. „**Reliability**“) definieren, sind die folgenden:

- MTTR (Mean time to repair): durchschnittlicher Aufwand der Reparatur,
- MTBF (Mean time between Failures): durchschnittliche Zeit zwischen Fehlern = Uptime,
- MTBSI (Mean time between System Incidents): durchschnittliche Zeit zwischen Störungen,
- ADT (Average Downtime): durchschnittliche Ausfallzeit,
- AFR (Annual Failure Rate): jährliche Fehlerrate.

Die Verfügbarkeit wird in serielle und parallele Verfügbarkeit unterteilt. Im seriellen Fall stehen zwei oder mehrere Komponenten bzw. Managed-Objects (MO) hintereinander. Die Gesamtverfügbarkeit ergibt sich aus der Multiplikation der einzelnen Verfügbarkeiten. In solchem Fall verringert sich die Gesamtverfügbarkeit. In einem parallelen Fall stehen zwei oder mehrere Managed-Objects parallel zueinander, von denen nur eines eine Aufgabe übernehmen kann. Hierbei wird die Wahrscheinlichkeit ermittelt, mit der die parallelen Objekte gleichzeitig ausfallen. Bei einer parallelen Konstellation erhöht sich die Gesamtverfügbarkeit. Zur Verdeutlichung dient Abb. 3.33.

Wie bereits einleitend erwähnt, besitzt das Availability-Management Beziehungen zu sehr vielen ITIL-Prozessen. Das **Security-Management** befasst sich mit der Vertraulichkeit,

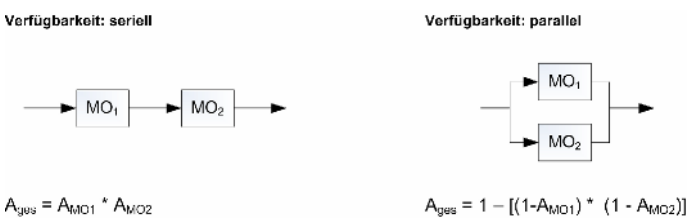

Abb. 3.33. Verfügbarkeit: parallel, seriell nach [02]

Integrität und Verfügbarkeit von Systemen. Das Verfügbarkeitsmanagement stellt hierbei die Anforderungen von Sicherheitsrichtlinien, wobei die Einhaltung von dem Security-Management überprüft werden muss [06]. Das **Configuration-** und das **Capacity-Management** liefern dem Verfügbarkeitsmanagement die notwendigen Informationen über die IT-Infrastruktur und deren Kapazität. Das **Continuity-Management** stellt dem Verfügbarkeitsmanagement Informationen über kritische Prozesse zur Verfügung. Entstehen (potenzielle) Verfügbarkeitsprobleme, so nimmt sich das **Problem-Management** dieser an. Bei störungsbedingen Ausfällen liefert das **Incident-Management** die notwendigen Daten, um die Verfügbarkeiten zu überprüfen. Für das **Service-Level-Management** spielt die Verfügbarkeit für die SLAs eine große Rolle. Schlussendlich initiiert das Availability-Management den Change-Prozess zur Durchführung von Änderungen und wird über geplante Änderungen informiert.

Die Aktivität des Availability-Managements beginnt mit der Ermittlung der Verfügbarkeitsbedürfnisse, bevor ein Service-Level-Agreement abgeschlossen wird (vgl. Abb. 3.34). In diesem Schritt wird definiert, wann ein IT-Service als nicht verfügbar gilt, welche Auswirkung ein nicht verfügbarer IT-

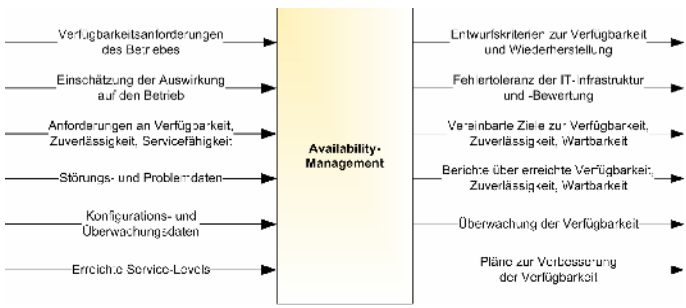

Abb. 3.34. Der Prozess des Availability-Managements nach [02]

Service hat, die Arbeitszeiten des Kunden und die Vereinbarungen über die Wartungen. Die nächste Aktivität nimmt sich der Planung der Verfügbarkeit an. Dabei werden Schwächen ausgewertet, um Fehler zu erkennen, und die Planung und andere Service-Prozesse optimiert. Die Aktivität der Erstellung eines Entwurfs der Wiederherstellbarkeit (engl. „Recovery“) befasst sich mit der Planung der Reaktion u. a. auf unplanmäßige Nichtverfügbarkeit und die Einbeziehung des Incident-Managements zur Kommunikation und verschiedener Verfahren. Als weitere Aktivität ist die der Wartung zu nennen (engl. „Planned Downtimes“), die sich mit der planmäßigen Nichtverfügbarkeit beschäftigt. Die letzten beiden Aktivitäten zielen auf die Erstellung eines Verfügbarkeitsplans und die Kontrolle mittels Messung und Berichtwesen. Das Availability-Management behilft sich für diese Aktivitäten verschiedener Methoden und Techniken wie CFIA, FTA, CRAMM etc., die in Tabelle 3.16 aufgeführt werden.

Tabelle 3.16. Methoden des Availability-Managements [09]

Methode	Verfügbarkeitsplanung	Verbesserung der Verfübarkeit	Messung und Berichterstattung
CFIA	×	×	×
FTA	×	×	
CRAMM	×	×	
SOA		×	
Erweiterter Störungslebenszyklus	×	×	×
Kontinuierliche Verbesserung		×	
TOP		×	

Für die Praxis ist es bei der Einführung eines Availability-Managements darauf zu achten, dass bekannte Ausfallzeiten und Termine bekannt gegeben werden sollten. Darüber hinaus spielt die Sicherheit eine große Rolle, die z. B. bei einer Denial-of-Service-Attacke Auswirkung auf die Verfügbarkeit hat. Das Verfügbarkeitsmanagement hat nicht die Aufgabe, die unterbrochenen Betriebsprozesse wieder aufzunehmen, da dies die Aufgabe des Continuity-Managements ist. Bei den entstehenden Kosten ist darauf hinzuweisen, dass mit der Zunahme der Verfügbarkeit die Gesamtkosten und die Kosten für präventive Maßnahmen exponentiell steigen, die Kosten für korrektive Maßnahmen aber stetig fallen. Daraus ergibt sich die Schlussfolgerung, dass bei der Realisierung einer hohen Verfügbarkeit es nicht anders geht, als die entstehenden Kosten mit einem hohen Preis zu vergüten. Bei der Implementierung des Availability-Managements können die kritischen Erfolgs- und Leistungsindikatoren aus Tabelle 3.17 helfen.

Tabelle 3.17. CSFs und KPIs des Availability-Managements

CSF	KPI
Geschäftsprozesse spezifizieren Anforderungen an Verfügbarkeit eindeutig	Anzahl und Auswirkung ausgefallener IT-Services und -Komponenten
Formalisierung dieser Spezifikationen durch das SLM	Performance der Zulieferer (UC)
Verständnis von Verfügbarkeit und Downtime zwischen Geschäftspartnern	Dauer der Nichtverfügbarkeit
Nutzen des Availability-Managements anerkennen	Häufigkeit der Nichtverfügbarkeit
	Prozentsatz der Verfügbarkeit pro Anwendergruppe

Zum Schluss dieses Kapitels sollen noch die Vorteile der Einführung des Availability-Managements zusammenfassend aufgelistet werden [02]:

- IT-Services entsprechen den vereinbarten Verfügbarkeitsanforderungen.
- Eindeutige Zuständigkeit für Verfügbarkeit innerhalb des Unternehmens.
- Aufgewendete Kosten werden gerechtfertigt.
- Einleitung der richtigen korrektiven Maßnahmen.
- Reduzierung von Häufigkeiten und Dauer der Nichtverfügbarkeit.

3.3.5 Continuity-Management

Im Gegensatz zum Availability-Management, wo es im Grunde um die Planung und Verbesserung der Verfügbarkeit von IT-Services geht, kommt das IT-Service-Continuity-Management (kurz: Continuity-Management) zum Einsatz, wenn ein Unternehmen einer Katastrophe begegnet. Eine Katastrophe wird verursacht von z. B. einem Feuerbrand, Blitzeinschlag, Einbruch oder Vandalismus, Entführung, Erpressung oder Sabotage. Neben diesen Ursachen können terroristische Gewalt und das Internet eine Katastrophe verursachen. Bei Letzterem denke man an gezielt verteilte Viren oder Trojaner und Denial-of-Service-Attacken (DoS).

Die Risikowahrscheinlichkeit für ein IT-Unternehmen ist, wie in Tabelle 3.18 angegeben, verteilt.

ITIL definiert eine Katastrophe als ein „Ereignis, das den Betrieb eines Service oder Systems in solch hohem Maße stört, dass häufig ein erheblicher Aufwand erforderlich ist, um den ursprünglichen Betriebsablauf wiederherstellen zu können“ [02]. Das Continuity-Management wirkt dabei präventiv. Existiert ein Notfallplan bzw. Kontinuitätsplan nicht, ist es im Fall

Tabelle 3.18. Risikoverteilung (Quelle: [06])

Risiko	Prozentueller Anteil
Diebstahl	35%
Virusbefall	20%
Sabotage	16%
Hardware	12%
Umgebung	7%
Software	4%
Höhere Gewalt	3%
Sonstige	3%

einer Katastrophe bereits zu spät. Aus diesem Grund sollte dieser Prozess nicht vernachlässigt werden. Das Motto „Es passiert immer den anderen, mir aber nicht“ ist für ein seriöses Unternehmen inakzeptabel. Das Continuity-Management definiert und plant alle Maßnahmen und Prozesse für unvorhergesehene Katastrophen. Es bildet einen Bestandteil des Business-Continuity-Managements und ist ständig in die Aktivitäten des Change-Managements involviert [o20]. Mittels einer Risikoanalyse wird die Wahrscheinlichkeit der zuvor erwähnten Risiken abgeschätzt. Auch hier gilt der wirtschaftliche Aspekt, Maßnahmen zu finden, die im angemessenen Verhältnis zum Aufwand, und somit zu den Kosten, stehen. Für die Erfüllung der Wiederherstellung kann ein externer Dienstleister als Recovery- und Backup-Provider beauftragt werden [05]. Der Fokus des Continuity-Managements liegt u. a. auf dem gesamten Unternehmensbereich, den Gebäuden, Räumen und Arbeitsplätzen und im Extremfall auf der Verlegung ganzer Rechenzentren und Standorte. Laut [06] ergeben sich für das Continuity-Management folgende Aufgaben:

- Überlebensfähigkeit eines Unternehmens nach Katastrophen nachhaltig gewährleisten (hier: Schadensbegrenzung).
- Bedrohungen und Risiken erkennen, einschätzen und verringern mittels Risikoanalysen.
- Erstellung eines Kontinuitätsplans zur kontrollierten und qualitätsgesicherten Wiederherstellung der IT-Services nach einem Katastrophenfall.

In einem K-Fall (Katastrophenfall) zählt jede Minute. Es muss ein Konzept vorhanden sein, das unnötige Bürokratie vermeidet, indem die autorisierten Zuständigkeiten klar definiert sind. Der Kontakt zum Krisen-Management und die restlichen Kommunikationswege müssen dabei problemlos, am besten direkt, hergestellt werden können. Darüber hinaus muss darauf geachtet werden, dass der Aufbewahrungsort der Notfallpläne bekannt und zugänglich ist [06]. Damit das Continuity-Management seinen Dienst ordnungsgemäß verrichten kann, müssen Schnittstellen zu anderen ITIL-Prozessen existieren. Anhand des **Service-Level-Managements** können die essentiellen Services ausfindig gemacht werden. Das **Availability-Management** unterstützt das Continuity-Management mit der Entwicklung und Implementierung von Präventivmaßnahmen. Die Information über die nach einer Katastrophe wiederherzustellende Infrastruktur liefert das **Configuration-Management** mit seiner Basiskonfiguration. Das **Capacity-Management** gewährleistet die Ressourcen für die Erfordernisse einer Organisation. Als letzter Prozess ist das **Change-Management** zu nennen, das dafür sorgt, dass die Notfallpläne stets aktuell sind, indem es das Continuity-Management in alle Änderungen einbezieht, die diese Pläne tangieren [02]. Die von ITIL vorgeschlagenen Gruppeneinteilungen können der Tabelle 3.19 entnommen werden.

Die Aktivitäten des Prozesses Continuity-Managements sind in Phasen eingeteilt, die in der Abb. 3.35 benannt werden.

Tabelle 3.19. Gruppierung von IT-Services (Quelle: [05])

Gruppe/Bezeichnung	Beschreibung
Alternative Ausfallmaßnahmen	Empfohlen werden Datenspiegelungen, redundante Systeme und Geräte.
Cold Standby	Es existieren separate Recovery-Räume und die notwendige Infrastruktur zur längerfristigen Wiederherstellung.
Immediate Standby	IT-Services müssen sofort wiederhergestellt werden; es existiert eine redundante Produktivumgebung (inkl. der Datenbestände).
Keine Aktion	Dienst ist als nicht kritisch eingestuft; es sind keine weiteren Maßnahmen notwendig.
Manuelles Recovery	Für den Fall, dass keine Automatismen für bestimmte Fälle existieren.
Warm Standby	Eine mögliche Umschaltung auf ein Backup-Rechenzentrum bzw. redundante Systeme für schnelles Recovery.

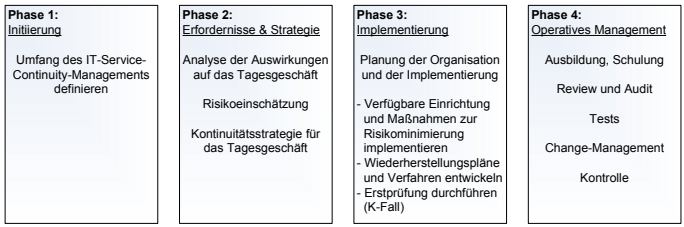

Abb. 3.35. Phasen des Continuity-Managements nach [06]

Die Implementierung eines Continuity-Managements hat in der Praxis gezeigt, dass mindestens die Schnittstellen zur CMDB, der DSL und ggf. andere Prozessinformationen vorhanden sein sollten, je nach Unternehmensanforderung. Vorteilhaft ist es auch, Standardvorlagen zu erarbeiten und umzusetzen und sicherheitsrelevante Daten an den jeweiligen Standorten zu

Tabelle 3.20. CSFs und KPIs des Continuity-Managements

CSF	KPI
Effektiv eingerichteter Continuity-Prozess	Anzahl nicht erreichter Continuity-Anforderungen
Begleitung und Engagement des gesamten Unternehmens	Anzahl der Mängel im Wiederherstellungsplan
Gute und moderne Ausstattung	Anzahl vertraglich vereinbarter Rahmenbedingungen, die nicht durch die Pläne abgedeckt werden
Schulung der am Prozess beteiligten Personen	Anzahl durchgeführter Notfallübungen
Regelmäßige, unangekündigte Tests des Wiederherstellungplans	Finanzielle Einbußen nach einer Katastrophe
	Kosten für den Prozess

replizieren. Wie bei einigen Institutionen ein Feueralarm probeweise durchgespielt wird (Notfallübung), so sollten auch Katastrophenfälle realistisch simuliert werden, um die Gegenmaßnahmen auf ihre Wirksamkeit zu prüfen.

In der Praxis wird der Sinn und Zweck eines Continuity-Managements oft verkannt. Das hat sicherlich damit zu tun, dass für solche Fälle die IT-Infrastruktur versichert ist [05]. Allerdings wird dabei außer Acht gelassen, dass nicht alle Folgeschäden ersetzt werden. Je länger ein Unternehmen nicht produktiv arbeitet, umso größer ist die Wahrscheinlichkeit, dass in den folgenden Jahren die Existenz des Unternehmens bedroht ist. Letztendlich muss jedes Unternehmen für sich entscheiden, ob die Kosten oder die Auswirkungen nach einer Katastrophe getragen werden können.

Bei der Implementierung eines Continuity-Managements können die in Tabelle 3.20 angegebenen kritischen Erfolgs- und Leistungsindikatoren behilflich sein.

Am Ende dieses Kapitels sollen die Vorteile eines implementierten Continuity-Managements aufgezeigt werden:

- Systeme werden mit vorheriger Überlegung wiederhergestellt.
- Gesteigerte Kontinuität wegen geringen Zeitverlusts durch schnelle Reaktionszeit.
- Minimale Unterbrechung der geschäftlichen Aktivitäten.

3.3.6 Security-Management

Es gibt eine bekannte Skizze der ITIL-Prozesse, deren Anordnung einem Haus gleicht – das ITIL-Haus. Während das Fundament das Configuration-Management bildet, ist der Service-Desk als Tür dargestellt. Das Security-Management ist außerhalb des ITIL-Hauses als ein Blitzableiter abgebildet. Diese Darstellung macht deutlich, wie das Security-Management zu verstehen ist und welche Aufgaben und Funktionen es beinhaltet.

Zunächst einmal sorgt dieser Prozess für einen definierten Schutz des Unternehmens und seiner Services. Die Sichtweise der Sicherheit ist die eines Service-Anbieters, in der das Security-Management für die strukturelle Integration in der IT-Organisation verantwortlich ist [02]. Die Sicherheit des internen Netzwerks (LAN) gegenüber externen Diensten spielt eine große Rolle [06], da Bedrohungen von außen abzuwehren sind. Strategische, taktische und operative Maßnahmen helfen Bedrohungen und Sicherheitslücken zu erkennen und zu klassifizieren [06]. Der Nutzen eines Security-Managements ist nicht direkt messbar. Wie bei einer Versicherung ist der tatsächliche Nutzen erst im Schadensfall konkret erkennbar. Als Grundlage für ein IT-Service-Management kann die Norm ISO 17799 herangezogen werden.

Das Ziel des Security-Prozesses ist die Erfüllung der Sicherheitsanforderungen in den SLAs usw. und die Bereitstellung eines gewissen IT-Grundschutzes, also der interne, minimale Sicherheitsanspruch. Diese Ziele werden mit dem CIA-Prinzip verfolgt. CIA bezieht sich auf die Daten und ist ein Akronym für Confidentiality (**Vertraulichkeit**), Integrity (**Integrität**) und Availability (**Verfügbarkeit**). Vorfälle innerhalb eines Security-Managements werden **Security-Incidents** genannt. Es handelt sich hierbei um Vorfälle, in denen das CIA-Prinzip verletzt wird. Aus diesem Grund sollte eine Organisation die Minimierung von Security-Incidents anstreben. Die so genannten **Policy-Statements** enthalten die Sicherheitsanforderungen des Kunden und müssen entsprechend in den SLAs, OLAs und UCs geplant und vertraglich festgelegt werden [06].

Das Security-Management beeinflusst auch andere ITIL-Prozesse. So meldet das **Incident-Management** die Security-Incidents und nimmt auch die Störungsmeldungen von IT-Systemen entgegen. Das **Configuration-Management** legt die Vertraulichkeit der CIs fest und verknüpft diese mit einem Maßnahmenkatalog. In der Ursachenforschung des **Problem-Managements** werden strukturelle Sicherheitsmängel gesucht und behoben. Das **Change-Management** ist für das Fortbestehen der Sicherheitslevel nach einem Change verantwortlich und enthält den Security-Manager als ein Mitglied im CAB. Das **Release-Management** ist für die Einführung von legaler, virenfreier Software, ausführlichen Test usw. zuständig. Die Sicherheitsanforderungen der SLAs müssen dabei jederzeit gewährleistet sein. Auch im **Service-Level-Management** geht es um Sicherheitsbedürfnisse und Sicherheitsmaßnahmen. Die restlichen ITIL-Prozesse tangieren das Security-Management nur gering.

Für jede Bedrohung wird ein Security-Incident erstellt. Erst dann ist der Schaden abschätzbar und wird für eine Wiederher-

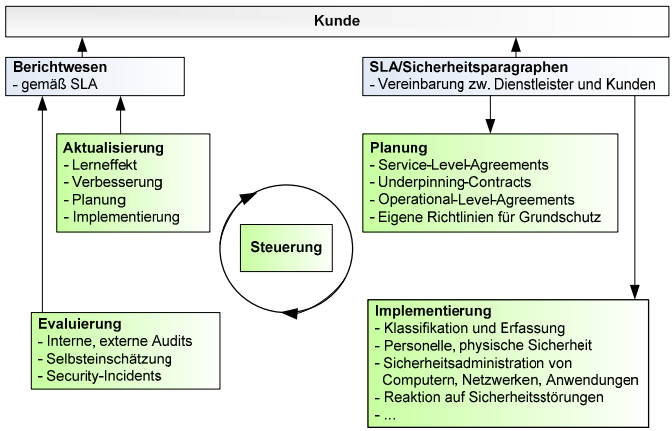

Abb. 3.36. Prozess des Security-Managements nach [02]

stellung korrigiert. Bedrohungen können mit vorbeugenden Maßnahmen wie Rechte- und Rollenkonzepten und Autorisierungsmechanismen verhindert werden. Datensicherungen und Kontinuitätspläne können den Schaden begrenzen. Entdeckt werden können Bedrohungen durch Monitoring mit Alarmfunktion und Antivirenprogrammen. Die Abb. 3.36 visualisiert die einzelnen Aktivitäten des Security-Managements.

Während der Planung der Sicherheit sind die Sicherheitsparagraphen der SLAs, OLAs und UCs ausschlaggebend. Hier muss eine Abstimmung mit dem Service-Level-Management erfolgen. Die Aktivität der Implementierung umfasst die Klassifizierung und Kontrolle von IT-Werkzeugen, die personelle Sicherheit und den Zugriffsschutz. Zweites beschäftigt sich mit der Förderung des Sicherheitsbewusstseins, Richtlinien für das Personal und Verpflichtungserklärungen der Mitarbeiter sowie Disziplinarmaßnahmen. In der Evaluierung wird die Implementierung überprüft und bewertet. Zu dieser Aktivität gehören interne und externe Überprüfungen und die Selbsteinschätzung.

Tabelle 3.21. CSFs und KPIs des Security-Managements

CSF	KPI
Akzeptanz, Beteiligung und Unterstützung des Managements	Anzahl durchgeführter Notfallübungen, Audits und Stichproben
Einbindung der Anwender bei der Erstellung des Secutrity-Prozesses	Anzahl und Schwere der inneren und äußeren Attacken
Klar definierte Zuständigkeiten	Kostenaufwand für Sicherheitsmaßnahmen
	Einhaltung der vereinbarten und gemessenen Service-Level

Bei Bedarf wird die Sicherheit in der nächsten Phase anhand der Auswertungsergebnisse aktualisiert. In wieweit die von einem Kunden geforderte Sicherheit erfüllt ist und welche Sicherheitsvorfälle aufgetreten sind, wird vom Berichtswesen des Security-Managements kommuniziert. Diese Aktivitäten erinnern an den PDCA-Zyklus, der durch immer wiederkehrende Aktivitäten eine Prozessoptimierung ermöglicht. Tabelle 3.21 gibt einen Überblick über die kritischen Erfolgs- und Leistungsindikatoren für die Implementierung eines Security-Managements.

4 Anhang

4.1 Checklisten

4.1.1 Was ist ITIL?

Historie

- ITIL steht für „Information Technology Infrastracture Library“ und wurde von der OGC (damals CCTA genannt) in den 80er Jahren im Auftrag der britischen Regierung entwickelt, um Effizienz und Effektivität zu erreichen.
- ITIL ist eine Vereinheitlichung der Analyseergebnisse, der so genannte „Best Practice“-Ansatz, der untersuchten britischen Behörden, die in einer Büchersammlung zusammengefasst ist.
- ITIL ist ein De-facto-Standard, d. h. weit verbreitet und allgemein anerkannt.
- ITIL definiert was und wann etwas zu tun ist, aber nicht das „wie“.

Vorteile

- Keine Neuerfindung des IT-Service-Gedankens.
- Fördert die Verständigung zwischen IT-Abteilungen innerhalb eines Unternehmens und unternehmensübergreifend mit Hilfe einer gemeinsamen Terminologie.

- Ausrichtung des IT-Services auf eigene Unternehmensanforderungen und die der Kunden
- Qualitätsoptimierung der erbrachten IT-Services
- Reduzierung der langfristigen Kosten von Dienstleistungen
- Jeder Prozess hat einen Verantwortlichen. Dadurch kann eine höhere Mitarbeiterzufriedenheit erreicht und die Personalfluktuation niedrig gehalten werden.
- ITIL kann für alle Unternehmen adaptiert werden.
- Optimierung der Kosten, Kommunikation, Kundenorientierung, Qualität und Transparenz.
- ITIL ist organisationsneutral, umfassend und detailliert, vollständig, Werkzeug-neutral und besitzt ein Rollenkonzept.

Nachteile

- ITIL ist keine umfassende Standardisierung, sondern nur ein (generischer) Best-Practice-Ansatz
- ITIL beschreibt, was zu tun ist, aber nicht wie es erreicht werden kann.
- Umsetzung eines ITSM auf Basis von ITIL benötigt externe Dienstleister oder Sekundärliteratur, die Kosten verursachen.
- Einige Methoden und Konzepte des ITIL-Frameworks sind nur dann sinnvoll, wenn die IT-Organisation eine bestimmte Größe aufweist.

Standards und Normen

- Der Standard ISO/IEC 2000, aus dem britischen Standard BS 15000 übernommen, macht es möglich, die Konformität des implementierten ITSM gegenüber dem ITIL-Grundgerüst zu belegen.
- Der Standard ISO/IEC 20000 enthält Anforderungen an ein professionelles ITSM und dient als messbarer Qualitätsstandard.

- Die erfolgreiche Umsetzung der ISO 20000 in einer Organisation kann zertifiziert werden.
- Der Standard ISO 20000 enthält den PDCA-Zyklus (nach Deming) zur Qualitätsverbesserung.
- Die Norm ISO 9001 beschreibt das Modell eines prozessorientierten Qualitätsmanagementsystems.

Publikationen und Revisionen

- ITIL-Revision 2 besteht aus sieben Kernbüchern:
  - Service Support,
  - Service Delivery,
  - Security Management,
  - ICT (Information and Communications Technology) Infrastructure Management,
  - Application Management,
  - The Business Perspective,
  - Software Asset Management.
- ITIL-Revision 3 besteht aus fünf Kernbüchern:
  - Service-Strategy,
  - Service-Design,
  - Service-Transition,
  - Service Operation,
  - Continual Service Improvement.
- Überarbeitungsprozess der ITIL v2 wird „ITL Refresh“ genannt.
- Das Ergebnis des ITIL-Refresh ist die neu strukturierte ITIL v3.
- Die neue ITIL-Revision 3 besteht zur Hälfte aus altem, zur Hälfte aus neuem Wissen (alle V2-Prozesse sind wieder in V3).
- ITIL v3 richtet sich noch ausdrücklicher nach dem Business-Nutzen.
- ITIL V3 ist mit dem Standard ISO/IEC 20000 abgestimmt.

4.1.2 ITIL-Managementbereiche – Einleitung

Vision, Ziele, Politik

- Durch definierte Visionen, Ziele und Politik kann die Qualität der Prozesse innerhalb des Unternehmens und die der angebotenen IT-Services steigen.
- Zur Vision gehört auch ein kurzer Abriss der Ziele, das Mission-Statement.
- Zielvorgaben werden nach den SMART-Vorgaben definiert.
- Die Politik ist die Gesamtheit der Entscheidungen und Maßnahmen zur Erreichung der Ziele.

Reifegrad, Prozessreifung, KPI

- Mit Hilfe einer Reifegradermittlung kann eine Organisation Verbesserungsstrategien und konkrete Pläne zur Umsetzung der Visionen entwickeln.
- Mit den CSFs (Critical-Success-Factors) und KPIs (Key-Performance-Indicators) stehen für die Messung qualitative und quantitative Leistungsindikatoren zur Verfügung.
- Die Kommunikation zwischen IT-Dienstleister und seinem Kunden sollte auf gleicher Ebene geführt werden, um Fehlkommunikation zu vermeiden (Stichwort: Reifegrad).
- Die Prozesse sollten in ihrer Reifung gesteigert werden. Das CMMI-Prozessmodell ermöglicht dabei die Klassifizierung der Reife von Prozessen.
- Der Erfolg und Nutzen einer ITIL-Implementierung lassen sich durch KPIs (Key-Perfomance-Indicator) ermitteln.
- Das generische ITIL-Prozessmodell: Die Prozessüberwachung hat Einfluss auf die Prozessausführung, die wiederum von den Prozessbedingungen (Ressourcen, Rollen) abhängig ist.
- ITIL-Prozesse verlaufen horizontal durch die Organisationshierarchie.

4.1.3 Service-Desk

- Ein Service-Desk stellt eine zentrale Anlaufstelle für Kunden und Anwender dar, was mit dem Begriff „Single Point Of Contact“ (SPOC) ausgedrückt werden kann.
- Ein Service-Desk ist kein Prozess, sondern vielmehr eine Funktion, die alle Prozesse des Service-Supports koordiniert.
- Ein Service-Desk bildet Teile des Incident-Managements operativ ab. Er nimmt Störungen bzw. Incidents entgegen und macht Services erst abrufbar.
- Ein Service-Desk hat vier Ausprägungen: „Call Center“, „Unksilled Service Desk“, „Skilled Service Desk“ und „Expert Service Desk“.
- Für die Service-Desk-Realisierung liegen drei Lösungen vor: lokal bzw. dezentral, zentral und virtuell.

4.1.4 Incident-Management

- Das Incident-Management ist für eine schnellstmögliche Wiederherstellung des normalen Service-Betriebs bei minimaler Behinderung der Geschäftsprozesse zuständig.
- Neben Störungen werden auch Anfragen (Service-Requests) der Anwender über den Service-Desk erfasst.
- Als weitere Leistung ist der in vereinbarten Zeitintervallen dem Anwender zu unterrichtende Status der Fehlerbeseitigung vorgesehen.
- Jeder aufgegebene Incident bleibt für seinen gesamten Lebenszyklus im Besitz des Incident-Managements (Owner).
- Der Prozess Incident-Management besitzt einen Incident-Manager, der für eine reibungslose und effektive Funktionsfähigkeit zuständig ist, in dem hierarchische Eskalationen eingeleitet werden und eine Beziehung zum SLM besteht (Leistungsvereinbarungen).

- Ein Incident wird für seine Weiterbearbeitung klassifiziert, d. h. kategorisiert und mit einer Priorität versehen. Letzteres setzt sich zusammen aus der Dringlichkeit und der Auswirkung einer Störung.
- Für einen Incident existieren hierarchische und funktionale Eskalationen.
- Ein Incident kann zu einem Problem werden, muss es aber nicht zwangsläufig. Ein Incident kann bereits geschlossen sein, auch wenn das Problem weiterhin offen bleibt.
- Probleme (Unknown-Errors) und bekannte Fehler (Known-Errors) sollten für das Incident-Management bereitgestellt werden.

4.1.5 Problem-Management

- Das Problem-Management wird für die Minimierung von Auswirkungen der Incidents und Problems, bedingt durch Fehler in der IT-Infrastruktur, eingesetzt.
- Das Problem-Management kommt zum Einsatz, wenn Störungen gemeldet werden, deren Ursache unbekannt ist (*reaktiv*). Befasst sich das Problem-Management mit der Ursachenforschung, um womögliche Störungen präventiv vorzubeugen (Trendanalyse), so spricht man von einem *proaktiven* Problem-Management.
- Ein Problem stellt eine Störung mit unbekannter Ursache dar. Deswegen ist ein Problem ein unbekannter Fehler (engl. „Unknown-Error“). Ein bekannter Fehler (engl. „Known-Error“) ist ein Problem, dessen Ursache erfolgreich festgestellt wurde.
- Das Problem-Management arbeitet parallel zum Incident-Management. Das bedeutet, dass zu einem Incident ein neues Problem-Ticket eröffnet werden kann. Beide Prozesse besitzen dabei einen unabhängigen Status, d. h., ein Problem-

Ticket kann offen sein, obwohl der Incident dazu bereits geschlossen ist.
- Während beim Incident-Management eine möglichst schnelle Behebung der Störung angestrebt wird (Zeitmangel), besitzt das Problem-Management genügend Zeit, um die Ursachen von Störungen zu ergründen und diese zu eliminieren.
- Die erworbenen Erkenntnisse des Problem-Managements fließen in das Change-Management in Form von RfCs (Request-for-Change) ein, da die Lösung der Störungen sich größtenteils auf die IT-Infrastruktur auswirken.
- Das Problem-Ticket kann erst dann geschlossen werden, wenn die Evaluierung bzw. der Post-Implementation-Review (PIR) durchgeführt worden ist.
- Ein Problem-Manager hat die Aufgabe, bei der Entwicklung und Pflege von Problem- und Fehlerbehandlungen mitzuwirken, indem er u. a. die Effektivität und Effizienz beurteilt. Er ist für die Beschaffung von Managementinformationen und der nötigen Ressourcen zuständig.

4.1.6 Configuration-Management

- Das Configuration-Management stellt allen anderen Prozessen ein logisches Modell der IT-Infrastruktur zur Verfügung.
- Dazu werden die einzelnen Elemente, die so genannten Configuration-Items (CIs), und deren Beziehungen untereinander in einer Datenbank, der Configuration-Database (CMDB), verwaltet.
- Die CMDB stellt die wichtigste Informationsquelle für das ITSM dar. Sie ist überwiegend objekthierarchisch strukturiert.
- Sämtliche zu kontrollierenden IT-Komponenten (E-Mails, Dokumentationen, Server etc.) werden in die CMSB aufgenommen. Nur dann können die CIs einen Prozess durchlaufen.

- Ein Config-Management kann aus einem Asset-Management entstehen.
- Damit ein Configuration-Item systemweit eindeutig identifizierbar ist, besitzt dieses eine eindeutige Referenznummer bzw. einen Item-Key (Schlüssel).
- Eine gute CMDB ist definiert durch die Ausgewogenheit zwischen Umfang (Scope) und Detaillierungsgrad (CI Level).
- Das Configuration-Management umfasst fünf Aktivitäten:
  - Planung,
  - Identifizierung,
  - Kontrolle,
  - Statusüberwachung,
  - Verifizierung und Audits.

4.1.7 Change-Management

- Das Change-Management soll die Auswirkungen von änderungsbedingten Störungen für den IT-Service minimieren.
- Dies gelingt durch die Bereitstellung standardisierter Prozeduren und Methoden für eine effiziente und wirtschaftliche Implementierung autorisierter Changes mit kleinstmöglichem Risiko für die bestehende und für die neue IT-Infrastruktur.
- Jede Änderung an einem Configuration-Item muss genauestens auf ihre Notwendigkeit und Auswirkung auf das Gesamtsystem (engl. „Change-Impact“) geprüft, später geplant, organisiert und überwacht werden.
- Change wird als Synonym für Neuerungen und Verbesserungen, Änderungen oder Korrekturen der IT-Infrastruktur verwendet.
- Ein Change oder RfC wird genehmigt, dokumentiert und die Ausführung überprüft (engl. „Review“).

- Standard-/Routine-Changes und Service-Requests müssen lediglich erfasst und dokumentiert werden.
- Reguläre Changes bzw. RfCs verlangen nach einer Abschätzung, Freigabe, Planung und Kontrolle in der Umsetzung.
- Einige Änderungen bedeuten einen großen Aufwand, wodurch einige Vertragskunden betroffen sein können. Hierzu stellt das Change-Management dem Service-Level-Management den PSA (Projected-Service-Availability)-Bericht zur Verfügung, der auch einen Zeitplan (Forward-Schedule-of-Change) beinhaltet.
- Der Change-Manager nimmt sich der Standardänderungen und einfachen RfCs an.
- Ein Change-Koordinator kann die Planung und Koordinierung der Änderungen einzelner Bereiche übernehmen.
- Das Change-Advisory-Board (CAB) kommt in Einsatz, wenn umfangreiche oder kritische Änderungsanträge vorliegen. Es kann bei dringenden Fällen durch ein Emergency-Committee (EC) stellvertretend eintreten.

4.1.8 Release-Management

- Das vom Change-Management autorisierte Release-Management führt Änderungen in Form von Releases aus.
- Das Release-Management besitzt einen ganzheitlichen Blick auf die Änderungen an IT-Services.
- Es beachtet technische und nicht-technische (organisatorische) Aspekte eines Release.
- Für eine weitgehende homogene IT-Infrastruktur und die Vereinfachung der Administration werden im Release-Management qualitätsgesicherte Standards und Grundkonfigurationen (engl. „Baselines“) erarbeitet.
- Die produktive Umgebung stellt einen isolierten Bereich dar. Das Release-Management darf nur im Auftrag des

Change-Managements mit Standardverfahren diese Umgebung durch Rollout oder Rollin ändern.

- Ein Release wird in drei Formen unterteilt:
  - Major-Release,
  - Minor-Release,
  - Emergency-Release/-Fix.
- Das Release-Management kennt drei Arten für ein Release:
  - Delta-Release,
  - Full-Release,
  - Package-Release.
- Die DSL (Definitive-Software-Library) stellt einen sicheren Aufbewahrungsort aller autorisierter Versionen dar.
- Das DHS (Definitive-Hardware-Storage) kann als Vorrats- und Ersatzteillager geprüfter wichtiger Hardwarekomponenten (Basiskonfiguration) gesehen werden.
- Aktivitäten des Prozesses Release-Managements:
  - Release-Policy definieren und Release-Planung.
  - Release-Build erstellen.
  - Test und Abnahme des Release.
  - Planung eines Rollout.
  - Organisatorische Aspekte planen.
  - Rollout durchführen.

4.1.9 Service-Level-Management

- Das Service-Level-Management beschäftigt sich mit den strategisch-taktischen Aspekten eines IT-Dienstleisters.
- Das Service-Level-Management überprüft und überwacht die Qualität und Aktualität der Services mit Hilfe von Optimierungszyklen. Seine Aufgabe ist es auch, Verhandlungen mit internen und externen Dienstleister zu führen, um SLAs zu ermöglichen.

- Für die Realisierung der IT-Dienstleistungen ist aber der Service-Desk verantwortlich.
- Gegenstand des SLMs sind die Service-Level-Agreements (SLAs), also Vereinbarungen zwischen Dienstanbietern und Dienstabnehmern bezüglich der Qualität und Quantität des Service-Managements. SLAs können sich auf externe Kunden oder unternehmensinterne IT-Organisationen beziehen.
- Grundlage für die SLAs bilden abgeschlossene Verträge, die oft die SLAs als Hauptbestandteil aufnehmen.
- Die SL-Agreements erlauben eine Beurteilung der IT, wenn notwendige Angaben und Zielsetzungen enthalten sind. Beide Partner kennen somit den Aufwand und die Kosten einer IT-Dienstleistung genau.
- Die von einem Dienstleister angebotenen Leistungen und ihre Merkmale, Komponenten und Kosten, werden in einem Dienstleistungskatalog, dem so genannten Service-Katalog, definiert.
- Die nicht technisch verfassten Service-Level-Requirements (SLRs), die mit einem Lastenheft vergleichbar sind, enthalten den vom Kunden geforderten Leistungsumfang, die notwendigen Ressourcen und die Kosten.
- SLRs werden in Service-Specsheet (vgl. Pflichtenheft) übersetzt. Sie enthalten die technische Beschreibung von IT-Services, beschreiben die Kundenwünsche detaillierter und beschäftigen sich mit den daraus entstehenden Konsequenzen für den Dienstleister.
- Ein Underpinning-Contract (UC) ist ein Absicherungsvertrag gegenüber einem externen Lieferanten.
- Ein Operational-Level-Agreement (OLA) ist eine weitere Beschreibung eines UCs. Ein OLA wird mit internen Organisationseinheiten abgeschlossen.
- Für die Verbesserung der IT-Services steht dem SLM ein Service-Verbesserungsprogramm (Service-Improvement-Program, kurz: SIP) zur Verfügung.

- Das Service-Level-Management kann mit Hilfe eines Service-Qualitätsplans (SQP) auf alle notwendigen Management-Informationen zur Steuerung der IT-Organisation und externer Lieferanten (Provider) zugreifen.
- Verrechenbare Kosten entstehen als Ergebnis der Service-Achievements (SA).

4.1.10 Financial-Management

- Das Financial-Management beschäftigt sich nicht mit Unternehmens-Controlling oder Finanzbuchhaltung, sondern ausschließlich mit der IT-Umgebung.
- Kosten werden überwacht, den verursachenden Organisationseinheiten zugeordnet und verrechnet.
- Das Financial-Management greift auf die Finanzbuchhaltung zurück, um eine Budgetplanung, Kostenkontrolle und die Leistungsverrechnung zu ermöglichen.
- Das Financial-Management trifft Schätzungen über die erforderlichen Finanzmittel mittels der Finanzplanung bzw. des Budgeting.
- Die Kostenrechnung bzw. das Accounting dient der Ermittlung und Zuordnung von Kosten für einen bestimmten Service pro Anwender.
- Bei der Leistungsverrechnung, oder auch Charging genannt, geht es um die Weiterverrechnung der Kosten auf Grund der tatsächlich bezogenen Leistungen.

4.1.11 Capacity-Management

- Im Capacity-Management wird aus Geschäftsanforderungen der Kapazitätsplan erstellt und dessen Einhaltung überwacht.

- Es sollen für die zu erbringenden Service-Level der Umfang und die Kosten ermittelt werden, um Kapazitätsengpässe zu vermeiden. Belastungs- und Auslastungsszenarien der IT-Infrastruktur werden in der Regel durchgeführt.
- Das Hauptaugenmerk liegt hierbei auf der Hard- und Software und dem Personal. Die Ressourcen sollen effizient eingesetzt werden.
- Panikkäufe sollen durch dieses Management bewusst vermieden werden.
- Das Capacity-Management besitzt die Capacity-Management-Database (CDB), in der Informationen aus dem laufenden Betrieb enthalten sind. Dies erlaubt ein rechtzeitiges Erkennen von Leistungsgrenzen der IT-Komponenten.
- Neben der CMDB erhält die CDB zusätzliche Informationen über den Workload (Leistung und Auslastung). Aus der Kapazitätsdatenbank lassen sich der Kapazitätsplan, die technischen Berichte und die Management-Berichte erstellen.
- Der proaktive Subprozess Business-Capacity-Management (BCM) trifft Vorhersagen über zukünftige Bedürfnisse und Anforderungen der Kunden.
- Der zweite Subprozess ist das Service-Capacity-Management (SCM), das im Wesentlichen die Nutzung von IT-Dienstleistungen bestimmt.
- Der dritte Subprozess Resource-Capacity-Management (RCM) hat die Aufgabe, die Nutzung der IT-Infrastruktur zu bestimmen und potenzielle Probleme zu erkennen.

4.1.12 Availability-Management

- Das Availability-Management dient der Optimierung der Nutzung und der Leistungsfähigkeit (Performance Management) der IT-Infrastruktur.

- Das Verfügbarkeitsmanagement ist für die Kontrolle der Service-Verfügbarkeit und die Sicherstellung der Wiederverfügbarkeit bei einem Ausfall zuständig. Es dient nicht einer Durchführung der Wiederherstellung der Verfügbarkeit.
- Aus den Geschäftsanforderungen werden ein allgemeines und ein servicespezifisches Verfügbarkeitsniveau definiert und die Umsetzung geplant.
- Für die Qualitätskontrolle werden die KPIs überwacht und ein Verfügbarkeitsplan erstellt.
- Durch Optimierung der Verfügbarkeit und die Erbringung der vereinbarten Service-Level kann eine höhere Kundenzufriedenheit erreicht werden, wovon der Unternehmenserfolg abhängt.

4.1.13 Continuity-Management

- Das (IT-Service-) Continuity-Management kommt in Einsatz, wenn ein Unternehmen einer Katastrophe begegnet. Es agiert präventiv.
- Der Fokus des Continuity-Managements liegt u. a. auf dem gesamten Unternehmensbereich, den Gebäuden, Räumen und Arbeitsplätzen und im Extremfall auf der Verlegung ganzer Rechenzentren und Standorte.
- Eine Katastrophe wird verursacht von zum Beispiel einem Feuerbrand, Blitzeinschlag, Einbruch oder Vandalismus, Entführung, Erpressung, Sabotage, terroristische Gewalt, das Internet und weitere.
- Eine Katastrophe ist laut ITIL ein „Ereignis, das den Betrieb eines Service oder Systems in solch hohem Maße stört, dass häufig ein erheblicher Aufwand erforderlich ist, um den ursprünglichen Betriebsablauf wiederherstellen zu können“ [02].

- Das Continuity-Management definiert und plant alle Maßnahmen und Prozesse für unvorhergesehene Katastrophen.
- Der Kontakt zum Krisen-Management und die restlichen Kommunikationswege müssen dabei problemlos, am besten direkt, hergestellt werden können.
- Systeme werden mit vorheriger Überlegung, d. h. mit Hilfe eines Notfall- bzw. Kontinuitätsplans, wiederhergestellt.

4.1.14 Security-Management

- Das Security-Management bietet die Sichtweise eines Service-Anbieters, in der es um strukturelle Integration in der IT-Organisation geht.
- Die Sicherheit des internen Netzwerks (LAN) gegenüber externen Diensten spielt eine große Rolle.
- Strategische, taktische und operative Maßnahmen helfen Bedrohungen und Sicherheitslücken zu erkennen und zu klassifizieren.
- Der Nutzen eines Security-Managements ist nicht direkt messbar.
- Das Ziel des Security-Prozesses ist die Erfüllung der Sicherheitsanforderungen in den SLAs, OLAs und UCs sowie die Bereitstellung eines gewissen IT-Grundschutzes (minimaler Sicherheitsanspruch des Unternehmens).
- Im Vordergrund stehen die Daten und die Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability) dieser (CIA-Prinzip).
- Vorfälle innerhalb eines Security-Managements werden Security-Incidents genannt. Es handelt sich hierbei um die Verletzung des CIA-Prinzips.

4.2 Aufgaben

4.2.1 Begriffserklärung

Was ist ein Prozess?

- Ein Prozess ist eine chronologische Abfolge von Schritten, die zur Erstellung eines Produktes erforderlich sind. Ein Prozess verarbeitet einen Input zum Output, ist zeitlich unbegrenzt und beliebig oft reproduzierbar.

Was ist ein Geschäftsprozess?

- Ein Geschäftsprozess besteht aus mehreren zusammenhängenden Aufgaben, die von einem oder mehreren Beteiligten durchgeführt werden, um ein Ziel bzw. einen Zweck zu erreichen.

Was versteht man unter einem Prozess- bzw. Geschäftsprozessmanagement?

- Unter diesem Management werden Geschäftsprozesse definiert und gestaltet, gesteuert, dokumentiert und verbessert. Zur Steuerung und Verbesserung werden Kennzahlen (quantitative, messbare Größen) benötigt. Es sorgt für Effektivität und Effizienz der Prozesse.

Was ist ein IT-Service?

- Ein IT-Service ist immateriell, unteilbar, zeitlich begrenzt, individuell, standortbezogen und kann nicht zurückgerufen werden.
- Ein IT-Service ist ein oder mehrere IT-Systeme, die einen Geschäftsprozess ermöglichen oder unterstützen und vom Kunden als zusammenhängendes Ganzes wahrgenommen werden.

Wie kann eine Qualitätssicherung eines Prozesses durchgeführt werden?

- Mit Hilfe des iterativen PDCA-Zyklus (nach Deming): Plan, Do, Check, Act.
- Weitere Methoden: Six Sigma, Total Quality Management (TQM), Quality Triology und das europäische EFQM-Modell

Was versteht man unter dem Begriff „Serviceprozess“?

- Ein Serviceprozess bzw. Service ist eine Kombination aus Produktion und Verbrauch, an dem Anbieter und Abnehmer gleichzeitig teilnehmen. Kunde und Anbieter können während der Erbringung Einfluss auf den Service ausüben. Ein Service kann also erst nach der Erbringung bewertet werden.

Was ist ein ITSM?

- ITSM steht für „IT Service Management“, das als Konzept und prozessorientiertes Modell anzusehen ist. Die Aufgaben des ITSM sind umfangreich und umfassen die Lieferung und Unterstützung der IT-Services, das Management der IT-Infrastruktur und der Applikationen und die Einhaltung der Geschäftsziele.

Was ist ein BSM?

- BSM steht für „Business Service Management“ und ist als Bindeglied zwischen dem Prozessmanagement und dem IT-Service-Management zu sehen, das eine bessere Zusammenführung des Business und der IT erlaubt.

4.2.2 ITIL-Revisionen

Nennen Sie einige der neuen Aspekte der ITIL-Revision 3.

- ITIL richtet sich noch ausdrücklicher nach dem Business-Nutzen.
- Der Fokus liegt auf dem Service Life Cycle – und erst in zweiter Linie auf den Prozessen.
- Mit ITIL V3 wird die Grundlage zu einem Balanced Scorecard geschaffen.
- Qualitätsmanagement auf Basis des Deming Quality Cycle stellt die lernende Organisation in den Mittelpunkt.
- ITIL V3 ist mit dem Standard ISO/IEC 20000 abgestimmt.
- Verbesserung in der Messbarkeit und Erbringung des Nachweises der echten Wertschöpfung.
- Alle V2 Prozesse sind wieder in V3.

4.2.3 ITIL-Managementbereiche – Einleitung

Warum sind für eine Organisation die Visionen, Zielen und Politik entscheidend?

- Durch definierte Visionen, Ziele und Politik kann die Qualität der Prozesse innerhalb des Unternehmens und die der angebotenen IT-Services steigen.

Was gehört zu einer Vision?

- Zur Vision gehört auch ein kurzer Abriss der Ziele und die dabei zu berücksichtigenden Werte: das Mission-Statement.

Welche Aufgabe hat die Unternehmenspolitik?

- Die Politik ist die Gesamtheit der Entscheidungen und Maßnahmen zur Erreichung, d. h. Konkretisierung und Realisierung, der Ziele.

Was ist eine Balanced-Score-Card (BSC)?

- Die BSC-Methode erlaubt es, aus den Zielen der Organisation oder der Prozesse die so genannten kritischen Erfolgsfaktoren (Critical-Success-Factors, CSF) abzuleiten. Im Anschluss daran werden die quantitativen Leistungsindikatoren (Key-Performance-Indicators, KPI) ermittelt.

Was ist ein KPI?

- KPI steht für „Key-Performance-Indicator" und ist ein quantitativer Leistungsindikator, der eine Variable darstellt, anhand derer man den „Fortschritt hinsichtlich wichtiger Zielsetzungen oder kritischer Erfolgsfaktoren innerhalb einer Organisation ermitteln kann." [02]

Mit welchem Modell lässt sich der Reifegrad eines Unternehmens bestimmen und welche Beziehung hat das CMMI-Modell dazu?

- Die Bestimmung des Reifegrads ist z. B. mit dem fünfstufigen Modell „European Foundation for Quality Management" (EFQM) möglich.
- Das CMMI-Modell (Capability-Maturity-Model-Integrated) ist ein prozessbezogenes Modell, womit die Reifung von Prozessen beschrieben wird. Fünf Ebenen können dabei erreicht werden, wobei die letzte die höchste ist.

4.2.4 Service-Desk

Ist ein Service-Desk ein Prozess oder eine Funktion?

- Ein Service-Desk ist kein Prozess, sondern vielmehr eine Funktion, die alle Prozesse des Service-Supports koordiniert.

Was ist mit „SPOC“ im Zusammenhang mit einem Service-Desk gemeint?

- Mit dem Begriff „Single Point Of Contact“ wird der Service-Desk als zentrale Anlaufstelle für Kunden und Anwender charakterisiert.

Was nimmt ein Service-Desk entgegen, was ist sein Hauptmerkmal?

- Ein Service-Desk nimmt z. B. Störungen, Verbesserungsvorschläge, Änderungswünsche, Support- und Bestellanfragen und Beschwerden auf. Dazu zählt auch die Bereitstellung von Dokumentationen.
- Das Hauptmerkmal ist die Entgegennahme von Incidents (Störungen). Ein SD macht die Services erst abrufbar.

Nennen Sie die unterschiedlichen Ausprägungen eines Service-Desks und grenzen Sie diese voneinander ab.

- Ein Call-Center nimmt Anrufe entgegen, erfasst diese und leitet sie weiter.
- Ein „Unskilled Service-Desk“ übernimmt die Aufgaben eines Call-Centers und ist zusätzlich um die Erstlösung einer Störung bemüht.
- Ein „Skilled Service-Desk“ übernimmt die Aufgaben eines Call-Centers und ist zusätzlich um eine erweiterte Lösung einer Störung bemüht.
- Ein „Expert Service-Desk“ übernimmt sämtliche Aufgaben eines „Skilled Service-Desk“, ist aber zusätzlich für die Behebung eines Incidents bemüht, setzt also mehr Wissen voraus.

Beschreiben Sie die Begriffe Incident, SRQ, Workaround, Problem (nach ITIL) und Known-Error.

- Ein Incident stellt eine Störung, die ein Weiterarbeiten verhindert, oder einen Service-Request dar.
- Ein Service-Request (SRQ) ist das Abrufen einer Dienstleistung, wie z. B. die Anforderung eines Dokumentes oder die Bereitstellung eines neuen PCs bei Neueinstellung.
- Ein Workaround ist eine Umgangslösung, die die Ursache des Problems nicht beseitigt, das Weiterarbeiten aber ermöglicht.
- Ein Incident kann zu einem Problem werden, wenn eine Analyse und Behebung der Störungsursache durchgeführt und eine Lösung ausgearbeitet wird.
- Ein Known-Error wird in einer zentralen Wissensdatenbank eingetragen, um bekannte Fehler und deren Ursachen und Lösungen dem Service-Desk zugänglich zu machen.

Welche Ziele werden mit einem Service-Desk verfolgt?

- Sein Einsatz soll
  - qualitativ hochwertige Unterstützung der Kunden/Anwender bieten,
  - die Kunden durch Steigerung der Zufriedenheit mit Hilfe von hoher Erreichbarkeit und schnellen Reaktionszeiten binden,
  - ein gutes Image aufbauen und die Mitarbeiterzufriedenheit steigern,
  - die nachgelagerten Abteilungen entlasten,
  - die „First Fix“-Rate (erste Lösung) steigern,
  - das Störungsaufkommen und unnötige Eskalationen minimieren,
  - die Servicekosten senken und
  - die Ressourcen effizient auslasten.

Welche Ausprägungen des Service-Desk sind Ihnen bekannt?

- Lokal/dezentral,
- zentral,
- virtuell.

4.2.5 Incident-Management

Was ist die Hauptaufgabe eines Incident-Managements?

- Das Incident-Management ist für eine schnellstmögliche Wiederherstellung des normalen Service-Betriebs bei minimaler Behinderung der Geschäftsprozesse zuständig.

Ist bei einem Incident-Management vorgesehen, dass der meldende Anwender innerhalb von vereinbarten Zeitintervallen über den Status seiner Störung informiert wird?

- Ja, diese Leistung ist so vorgesehen.

Welche Aufgabe hat der Incident-Manager?

- Er sorgt für eine reibungslose und effektive Funktionsfähigkeit des Incident-Managements. Er kann (hierarchische) Eskalationen anstoßen und muss mit dem Service-Level-Management (SLM) eng zusammenarbeiten.

Wie definiert ITIL den Begriff „Incident“?

- Eine Störung ist ein Ereignis, das nicht zum standardmäßigen Betrieb eines Service gehört und das tatsächlich oder potenziell eine Unterbrechung oder Minderung der Service-Qualität verursacht.

Was ist ein Service-Request (SRQ)?

- Ein Service-Request ist die Anfrage eines Anwenders zur Unterstützung, Service-Erweiterung, Lieferung, Information, zum Rat oder Dokumentation.

Wie sind in ITIL die Klassifizierung und Priorität definiert? In welchem Verhältnis stehen diese Begriffe zueinander?

- Die Priorität setzt sich zusammen aus der Auswirkung (engl. „impact“) und Dringlichkeit (engl. „urgency“) einer Störung. Die Priorität ist, neben der Kategorisierung einer Störung, ein weiterer Faktor für die Klassifizierung.

Was ist ein Workaround?

- Ein Workaround ist eine schnelle Umgangs- bzw. Alternativlösung, um die Störung zu umgehen, nicht aber deren Ursache zu ergründen (z. B. aus Zeitmangel).

Was versteht ITIL unter einem Problem?

- Die (unbekannte) Ursache für einen Incident wird „Problem“ genannt.

Was ist eine Eskalation und welche Ausprägungen gibt es davon?

- Eine Eskalation ist ein Mechanismus, der eine schnelle Behebung eines Incidents unterstützt. Sie wird angestoßen, wenn eine Störung nicht in erster Instanz oder innerhalb der vereinbarten Zeit behoben werden kann.
- In ITIL ist dies die funktionale, fachliche oder horizontale und hierarchische bzw. vertikale Eskalation.

4.2.6 Problem-Management

Fassen Sie kurz die Aufgaben bzw. Aktivitäten eines Problem-Managements zusammen.

- Im Mittelpunkt des Problem-Managements stehen die Ursachenforschung und die nachhaltige Beseitigung von Störungen (Incidents).
- Temporäre Lösungen (Workaraounds) und endgültige Lösungen bekannter Fehler (Known-Error) werden dem Incident-Management bereitgestellt.
- Die Behebung einer Fehlerursache kann beim Change-Management mit Hilfe eines so genannten Request-for-Change (RfC) beantragt werden.
- Die im Problem-Management definierten Aktivitäten setzen sich zusammen aus der Problem- und Fehlerbehandlung, des proaktiven Managements (Störungsvermeidung, Prophylaxe mittels Trendanalysen) und der Informationsbereitstellung für andere ITIL-Prozesse.

Welche Schnittstellen besitzt ein Problem-Management im Idealfall?

- Incident-Management (qualitativ gute Störungserfassung).
- Change-Management (kontrollierte Durchführung der RfCs).
- Configuration-Management (liefert Informationen über Infrastruktur).
- Availability (vereinbart Verfügbarkeitsstufen, verlangt Reports über Nichtverfügbarkeit).
- Capacity-Management (kann Probleme definieren, verlangt Reports von Ursachen bezüglich der Kapazität).
- Service-Level-Management (Qualitätsanforderung, Priorisierung von Problemen).

In welchem Verhältnis stehen die Begriffe Problem- und Error-Control mit dem Problem-Management?

- Problem-Control beschäftigt sich mit der Problembehandlung bzw. Problembearbeitung von Fehlern unbekannter Ursache (*unbekannte* Fehler).
- Das Error-Control steht für die Fehlerbehandlung *bekannter* Fehler.

Warum kann es wichtig sein, dass zu Anfang der Implementierung eines Problem-Managements ein multidisziplinäres Team hinzugezogen wird?

- Dadurch erreicht das Problem-Management die maximale Akzeptanz.
- Sämtliche wichtigen Informationen für jegliche Weiterbearbeitung eines Problems und die Schnittstellen zu anderen ITIL-Prozessen werden genauer definiert.
- Das Problem-Management wird optimal in die anderen Prozesse integriert.

Welche Vorteile weist ein Problem-Management auf?

- Fehler werden lokalisiert, dokumentiert und sind verfolgbar.
- Symptome und Lösungen von Störungen werden dokumentiert.
- Neue Störungen werden verhindert.
- Bessere Qualität und Beherrschung der IT-Services.
- Reflektives Lernen aus der Vergangenheit.
- Verbesserte Störungserfassung und Berichtswesen.
- Höhere Erfolgsquote im 1st-Level-Support.

4.2.7 Configuration-Management

Womit beschäftigt sich ein Configuration-Management?

- Das Configuration-Management stellt allen anderen Prozessen ein logisches Modell der IT-Infrastruktur zur Verfügung.

Was ist eine CMDB? Was bedeutet „Scope“ und „CI Level“ in diesem Zusammenhang?

- Eine Configuration-Management-Database ist eine große Karteikarte. Dazu werden die einzelnen Elemente der IT-Infrastruktur und deren Beziehungen untereinander in einer Datenbank (Configuration-Database, kurz CMDB) verwaltet.
- Scope und CI-Level meinen in diesem Zusammenhang den Umfang und Detaillierungsgrad der CMDB.

Was ist versteht man unter einem „CI“?

- Ein CI steht für ein Configuration-Item (Konfigurationselement) und entspricht einem Datensatz in der CMDB.

Welcher ITIL-Prozess liefert die wichtigsten und häufigsten inhaltlichen Beiträge für die Aktualisierung der CMDB?

- Es ist das Change-Management.

Kann das Configuration-Management mit dem Asset-Management gleichgestellt werden?

- Nein. Ein Asset-Management ist der Buchhaltung zuzuordnen und überwacht z. B. die Abschreibungen der Artikel. Im Configuration-Management hingegen sind Informationen über interne Zusammenhänge zwischen CIs hinterlegt. Änderungen an der IT-Infrastruktur werden hier dokumentiert.

Welche fünf Aktivitäten/Aufgaben/Tätigkeiten sind Ihnen für das Configuration-Management bekannt?

- Planung,
- Identifizierung,
- Kontrolle,
- Statusüberwachung,
- Verifizierung und Audits.

4.2.8 Change-Management

Welche Hauptaufgabe hat das Change-Management neben den anderen ITIL-Prozessen?

- Das Change-Management soll die Auswirkungen von änderungsbedingten Störungen für den IT-Service minimieren.
- Dies gelingt durch die Bereitstellung standardisierter Prozeduren und Methoden für die Implementierung von *autorisierten* Changes, mit kleinstmöglichem Risiko für die IT-Infrastruktur.

Darf der Change-Manager alle RfCs selbst bewilligen und durchführen?

- Dies darf er nur bedingt. Er darf lediglich Standard-Changes genehmigen. Andere Changes müssen je nach Klassifizierung (Priorität und Kategorie) vom CAB oder EC genehmigt werden.

Was ist ein Change?

- Ein Change definiert jegliche Änderung an der IT-Infrastruktur, d. h. an einem Configuration-Item. „Change“ kann als Synonym für Neuerungen und Verbesserungen, Änderungen oder Korrekturen verstanden werden.

Was versteht man unter Regular-Changes?

- Regular-Changes sind alle übrigen Änderungen, die auf Grund eines Request-for-Change erfolgen. Diese verlangen nach einer Abschätzung, Freigabe, Planung und Kontrolle der Änderung.

Welche Prioritäten kennen Sie im Rahmen des Change-Managements?

- Niedrig,
- mittel,
- hoch,
- dringend.

Wofür stehen die Kürzel FSC und PSA?

- Das PSA steht für „Projected Service Availability". Es stellt einen Bericht dar, der die Verfügbarkeit eines IT-Service während eines Change beschreibt. Er beinhaltet u. a. einen Änderungsplan bzw. -kalender, in dem die Durchführung der Changes verplant ist. Dieser Plan heißt „Forward Schedule of Changes", kurz FSC genannt.

Welche ITIL-Prozesse können für das Change-Management RfCs aufgeben?

- Incident-Management,
- Problem-Management,
- Release-Management,
- Capacity-Management,
- Service-Level-Management,
- Security-Management.

Skizieren Sie kurz die Aktivitäten des Change-Management.

- Einführung des Change-Management-Prozesses mit Hilfe des Configuration-Managements.
- Erfassen von RfCs.
- Akzeptieren und Filtern von RfCs.
- Klassifizieren (Kategorie, Priorität).
- Planen der Umsetzung.
- Koordinieren der Umsetzung.
- Evaluieren der Umsetzung/Änderung.
- Durchführen dringlicher Änderungen.

Wofür wird ein Backout- bzw. Fallback-Plan verwendet?

- Falls eine umgesetzte Änderung ein nichtfunktionsfähiges Produktivsystem verursacht, so kann durch eine vollständige oder partielle Umsetzung mit Hilfe eines solchen Backout-Plans der ursprüngliche IT-Service wieder hergestellt werden.

4.2.9 Release-Management

Welche Aufgaben hat das Release-Management?

- Festlegung von Release-Definitionen (Policies).
- Beaufsichtigung der Release-Erstellung.
- Genehmigung und Management von Releases.
- Steuerung der Release-Auslieferung und Verteilung.
- Pflege und Verwaltung des Hard- und Softwaredepots.
- Durchführung von Audits (mit Hilfe der CMDB).

Welche organisatorischen, d. h. nicht-technischen Aufgaben, übernimmt bei einem Release das Management?

- Das Release-Management ist in der Lage, Schulungsmaßnahmen einzuleiten, für die Abnahme eines Release zu sorgen und Änderungen bezüglich der SLAs, OLAs usw. mitzuteilen.

Ist das Release-Management für die Koordinierung der Einführung von Changes verantwortlich?

- Das Release-Management wird vom Change-Management dazu autorisiert, Changes umzusetzen. Die Koordinierung obliegt allein dem Change-Management, wobei das Release-Management die Vorgaben kritisch prüfen darf.

Welchen Ursprung hat ein Release? Wie wird es eingeleitet?

- Ein Release resultiert immer aus einem Change-for-Request. Es kann die eigene IT betreffen oder die Eigenentwicklung von Software.

Geben Sie jeweils ein Beispiel für die drei Unterteilungsformen eines Release.

- Major-Release: Einführung eines Applikationssystems (betrifft Gesamtunternehmen).
- Minor-Release: Eine Festplatte muss ausgetauscht werden.
- Emergency-Fix: Ein Programmierfehler stört den laufenden Betrieb.

Was ist eine DSL bzw. ein DHL?

- Die Definitive-Software-Library (DSL) stellt einen sicheren Aufbewahrungsort aller autorisierter Versionen dar. Die im Unternehmen produktiv eingesetzte Software (Eigenentwicklung, Fremdsoftware) existiert als eine archivierte Masterkopie.

- Das Definitive-Hardware-Store (DHS) kann als Vorrats- und Ersatzteillager geprüfter wichtiger Hardwarekomponenten (Basiskonfiguration) gesehen werden, die fehlerhafte Komponenten ersetzen oder für einen kurzfristigen Ausbau bei Kapazitätsengpässen verwendet werden können.

Für was ist der Release-Manager zuständig?

- Er hält den Kontakt zu dem Change- und Configuration-Manager und ist verantwortlich für die Einführung, Einhaltung und Weitererntwicklung des Prozesses.

4.2.10 Service-Level-Management

Welche Aspekte werden in einem Service-Level-Management behandelt? Welche Beziehungen sind hier Gegenstand?

- Ein SLM beschäftigt sich mit den strategisch-taktischen Aspekten eines IT-Dienstleisters.
- Der Gegenstand sind die Kundenbeziehungen eines Unternehmens, die in Form von Service-Level-Agreements (SLAs) existieren.

Können die SLAs eine Beurteilung der IT erlauben?

- Ja, indem die notwendigen Angaben (u. a. KPIs) und Zielsetzungen enthalten sind.

Mit einem SLM werden IT-Services und deren Durchführung definiert. Welcher Prozess bzw. welche Funktion ist für deren Realisierung zuständig?

- Der Service-Desk ist für die Realisierung der IT-Dienstleistungen verantwortlich, da er die Services erst abrufbar macht.

Wofür ist ein Service-Katalog sinnvoll? Stellt ein Service-Katalog ein Configuration-Item einer CMDB dar?

- In solch einem Katalog sind die Leistungen aller SLAs in einem Unternehmen wiederzufinden. Leistungserbringungen außerhalb des Service-Katalogs sind nicht zulässig.
- Es ist zumindest zu empfehlen, diesen Katalog als ein CI abzulegen, damit alle ITIL-Prozesse darauf zugreifen können.

Beschreiben Sie die Begriffe Service-Katalog, SLR und Service-Specsheet im Zusammenhang.

- Auf Grundlage eines Service-Kataloges werden die vom Kunden geforderten Service-Level-Requirements (SLRs), die notwendigen Ressourcen und die Kosten definiert.
- Ein SLR kann mit einem Lastenheft verglichen werden und ist nicht-technischer Natur.
- Ein SLR wird in ein Service-Specsheet übersetzt. Er enthält die technische Beschreibung von IT-Services, beschreibt die Kundenwünsche detaillierter und beschäftigt sich mit den daraus entstehenden Konsequenzen für den Dienstleister (u. a. Ressourcen). Ein Service-Specsheet entspricht einem Pflichtenheft und ist Bestandteil einer SL-Anforderung, kann aber, um den Rahmenvertrag zu entlasten, auch in ein gesondertes Dokument ausgegliedert werden.

Was ist die Besonderheit zwischen intern und extern abgeschlossenen Service-Level-Agreements? Welche Vertragsarten kennt das SLM?

- Externe SLAs gleichen den unternehmensinternen SLAs bis auf den nicht vereinbarten juristischen und optionalen kaufmännischen Teil.
- SLAs, die mit externen Lieferanten abgeschlossen werden, heißen aus Unternehmenssicht Underpinning-Contracts (UCs).

- Ein Operational-Level-Agreement stellt formal einen UC dar, der mit einer internen Organisationseinheit abgeschlossen wird. Ein OLA enthält meistens keine juristischen Vereinbarungen, der kaufmännische Teil ist hier optional.

Welche Aufgaben hat ein SL-Manager?

- Er erstellt und pflegt den Service-Katalog und formuliert anhand der Verträge (SLAs, OLAs und UCs) und Optimierungsprogramme ein effektives Service-Level-Management. Neben den verschiedenen Berichten wird im SLM die Verbesserung der IT-Organisation mittels Leistungsanalysen angestrebt.

4.2.11 Financial-Management

Womit beschäftigt sich das Financial-Management grundsätzlich nicht?

- Es beschäftigt sich nicht mit z. B. Unternehmens-Controlling oder Finanzbuchhaltung, sondern vielmehr mit den Kosten der IT.

Welche Aufgaben hat das Financial-Management?

- Kosten werden überwacht, den verursachenden Organisationseinheiten zugeordnet und verrechnet.
- Das Financial-Management stellt betriebswirtschaftliche Informationen zur Steuerung der IT-Organisation bereit, verwaltet die Erbringungskosten der zugesicherten Services, fördert wirtschaftliches Handeln, schafft Transparenz über Kosten und Leistungen.

Was bedeutet Budgeting in diesem Zusammenhang?

- Im Budgeting werden Schätzungen über die erforderlichen Finanzmittel mittels der Finanzplanung getroffen.
- Hierbei werden die tatsächlichen und die geschätzten Ausgaben miteinander verglichen. Es müssen ebenso laufende Projekte, der vergangene Geschäftsverlauf und die mittel- und langfristige Geschäftsplanung berücksichtigt werden.

Was versteht man unter einem Accounting?

- Mit Accounting ist die Kostenrechnung gemeint, die der Ermittlung und Zuordnung von Kosten für einen bestimmten Service pro Anwender dient.
- Grundlagen dafür sind die Kosten-Nutzen-Analyse und die ROI-Analysen.

Wie kann der Begriff „Charging" übersetzt werden und was steckt dahinter?

- Mit Charging ist die Leistungsverrechnung gemeint. Hier geht es um die Weiterverrechnung der Kosten auf Grund der tatsächlich bezogenen Leistungen. Es sollte einfach, verständlich, realistisch und fair sein.

Nennen Sie zwei Finanzplanungsmethoden des Budgeting.

- Incremental-Budgeting und Zero-Based-Budgeting.

Was wird unter dem Begriff „Chargable-Unit" verstanden?

- Es ist die kleinste Verrechnungseinheit, die sich ein Dienstleister bezahlen lassen kann. Diese Einheit orientiert sich am Bedarf.

4.2.12 Capacity-Management

Mit welchen Fragen setzt sich das Capacity-Management auseinander?

- Wie viel kostet die Anschaffung von Kapazitäten, um die geschäftlichen Anforderungen zu erfüllen?
- Wird die Kapazität effizient genutzt?
- Ist die Kapazität ausreichend für die künftige Nachfrage des Kunden?
- Wann ist die Performanz ausgereizt und wann sollte zusätzliche Kapazität angeschafft werden?

Wie werden mit dem Capacity-Management Panikkäufe auf Grund von Kapazitätsengpässen vermieden?

- Panikkäufe werden dadurch vermieden, dass das Einkaufen zunächst geplant wird. In einem Kapazitätsplan wird festgehalten, welcher Umfang und welche Kosten hinter den zu leistenden Service-Level stehen. Die Lasttests der IT-Infrastruktur und einzelner IT-Komponenten ermöglichen es, auf Kapazitätsengpässe vor deren Entstehung zu reagieren.

Was versteht man unter einem Demand-Management und welche Möglichkeiten ergeben sich daraus für ein Unternehmen?

- Das Demand-Management beschäftigt sich mit dem kundenseitigen und firmeninternen Bedarf. Es ist dadurch möglich, auf Kapazitätsnachfragen zu reagieren und diese zu beeinflussen. So kann z. B. ein manuell durchgeführter auslastungsstarker Datenbankzugriff (Erstellung eines Berichtes) in der Mittagszeit auf die Nacht verschoben werden, wo dieser dann gesteuert abläuft.

Nennen Sie einige Beispiele, in denen die Involvierung des Capacity-Managements ersichtlich wird.

- Bei der Einstellung eines neuen Mitarbeiters müssen geprüft werden, ob ein Drucker, Arbeitsplatzcomputer, die Berechtigungen zu Anwendungen und Systemen und Datenbanken bereitgestellt werden müssen.
- Einführung eines SAN: Ist es notwendig? Welcher Umfang an Kosten, Ressourcen und Aufwand ergeben sich daraus? Welcher Nutzen und welche Risiken bestehen für dieses Vorhaben?
- Störungen treten auf, deren Ursache ein Kapazitätsproblem ist.
- Das Capacity-Management liefert Audit-Berichte und gibt Service-Level-Empfehlungen.

4.2.13 Availability-Management

Nennen Sie die Hauptaufgaben eines Availability-Managements.

- Optimierung der IT-Infrastruktur bezüglich der Nutzung und der Leistungsfähigkeit.
- Kontrolle der Service-Verfügbarkeit.
- Sicherstellung der Wiederherstellung der Verfügbarkeit bei Ausfällen.
- Sicherstellung der Kundenzufriedenheit (implizit).

In welchem Format werden Verfügbarkeiten meistens angegeben. Geben Sie ein Beispiel.

- Die Verfügbarkeit wird oft im Format *HH*TT*WW* angegeben (Stunden am Tag, Tage in der Woche, Wochen im Jahr).
- Beispiel: 5 Tage von 7 bis 19 Uhr mit einem Ausfall von 1 Stunde: ((5 * 12) – 1) / (5 * 12) * 100 = 98,33%.

Welche Aufgaben hat der Manager dieser Disziplin?

- Er definiert und entwickelt den Availability-Prozess im Unternehmen.
- Greift bei unrealistischen Service-Levels korrigierend ein.
- Optimiert die Verfügbarkeit der IT-Infrastruktur.
- Erstellt die Berichterstattung zum Top-Management oder anderen ITIL-Prozessen.

Was bedeutet ein „hohes Maß“ an Verfügbarkeit?

- … dass der Anwender jeder Zeit oder im vereinbarten Rahmen über einen IT-Service verfügen kann.

Was ist der Vorteil von einem parallel geschalteten System für die Verfügbarkeit, im Vergleich zu einem seriellen System?

- Verwendet man für diese Systeme jeweils die gleichen Komponenten (Managed-Objects) mit den gleichen Ausfallwahrscheinlichkeiten, so erhöht sich nur für das parallele System die Gesamtverfügbarkeit.

Worum muss sich das Verfügbarkeitsmanagement nicht kümmern, weil diese Tätigkeit einem anderen Prozess obliegt?

- Das Verfügbarkeitsmanagement hat nicht die Aufgabe, die unterbrochenen Betriebsprozesse wieder aufzunehmen – dies ist die Aufgabe des Continuity-Managements.

4.2.14 Continuity-Management

Was ist ein Continuity-Management? Welche Aufgaben hat dieser Prozess?

- Das Continuity-Management ist ein Kontinuitätsmanagement, das im Fall einer Katastrophe zum Einsatz kommt. Es

soll die Überlebensfähigkeit eines Unternehmens nach Katastrophen mittels einer Schadensbegrenzung nachhaltig gewährleisten. Dabei werden mit Hilfe von Risikoanalysen Bedrohungen und Risiken bestmöglich erkannt, eingeschätzt und verringert. Das Ergebnis ist ein Kontinuitätsplan zur Kontrolle und qualitätsgesicherten Wiederherstellung der IT-Services nach einem Katastrophenfall.

Nennen Sie einige Risiken, gegen die sich ein IT-Unternehmen schützen sollte.

- Ein Unternehmen muss u. a. mit Diebstahl, Virusbefall, Sabotage, Hardwareausfall, Gefahren aus der Umgebung, Software bedingten Schäden und höherer Gewalt (Natur) rechnen.

Wie würden Sie den Begriff „Katastrophe“ definieren?

- Eine Katastrophe ist eine Begebenheit, die in den meisten Fällen mit einem erheblichen Aufwand bezüglich der Wiederherstellung verbunden ist. Der Betrieb wird dabei in einem hohen Maß gestört.

Wie werden in einem Continuity-Management die Risiken einer Katastrophe abgeschätzt und was ist dabei zu beachten?

- Die Wahrscheinlichkeit der Risiken wird mittels einer Risikoanalyse abgeschätzt. Weil z. B. für die Erfüllung der Wiederherstellung ein externer Dienstleister als Recovery- und Backup-Provider beauftragt werden kann, spielt hier auch der wirtschaftliche Aspekt eine große Rolle. Es müssen Maßnahmen gefunden werden, die im angemessenen Verhältnis zum Aufwand und somit zu den Kosten stehen.

Beschränkt sich das Continuity-Management nur auf die Wiederherstellung der IT-Infrastruktur?

- Die Wiederherstellung der IT-Infrastruktur ist sicherlich das Hauptziel des Kontinuitätsmanagements. Der Fokus liegt u. a. auf dem gesamten Unternehmensbereich, der Gebäude, Räume und Arbeitsplätze und im Extremfall auf der Verlegung ganzer Rechenzentren und Standorte.

Damit das Continuity-Management seinen Dienst ordnungsgemäß verrichten kann, müssen Schnittstellen zu anderen ITIL-Prozessen existieren. Benennen Sie diese Prozesse.

- Service-Level-Management,
- Availability-Management,
- Configuration-Management,
- Capacity-Management,
- Change-Management.

4.2.15 Security-Management

Welche Ziele verfolgt das Security-Management und wie können sie erreicht werden?

- Das Security-Management hat die Ziele, die Sicherheitsanforderungen in den SLAs, OLAs und UCs zu erfüllen sowie einen gewissen IT-Grundschutz bereitzustellen.
- Diese Ziele werden mit dem CIA-Prinzip verfolgt: Confidentiality, Integrity und Availability.

Was ist ein Security-Incident?

- Ein Security-Incident ist ein Vorfall, in dem das CIA-Prinzip verletzt wird. Das bedeutet, die Daten entsprechen nicht den Ansprüchen der Vertraulichkeit, Integrität oder der Verfügbarkeit.

Nennen Sie einige Maßnahmen, mit denen Bedrohungen entgegnet werden kann.

- Ein bereits entstandener Schaden muss abgeschätzt und korrigiert werden. Bedrohungen können mit vorbeugenden Maßnahmen wie Rechte- und Rollenkonzepte und Autorisierungsmechanismen verhindert werden. Datensicherungen und Kontinuitätspläne können den Schaden begrenzen. Entdeckt werden können Bedrohungen durch Monitoring mit Alarmfunktion und Antivirenprogrammen.

Zählen Sie die Aktivitäten in der richtigen Reihenfolge des Security-Prozesses auf.

- Steuerung,
- Planung,
- Implementierung,
- Evaluierung,
- Aktualisierung.

5 Literaturverzeichnis

5.1 Literatur

[01] Heide Balzert, „Lehrbuch der Objektmodellierung: Analyse und Entwurf“, Spektrum Akademischer Verlag, Heidelberg, Berlin, 1999

[02] Jan van Bon, Annelies van der Veen, Mike Pieper, „Foundations in IT Service Management basierend auf ITIL“, 1. Auflage der 3. Ausgabe, itSMF, Van Haren Publishing, 2006

[03] Ullrike Buhl, „ITIL-Praxisbuch – Beispiele und Tipps für die erfolgreiche Prozessoptimierung“, Verlag mitp (Redline GmbH), Heidelberg, 2005

[04] Computerwoche, Ausgabe 26/2007

[05] Wolfgang Elsässer, „ITIL Einführen und Umsetzen (Leitfaden für Effizientes IT-Management durch Prozessoptimierung)“, 2. erweiterte Auflage, Hanser Verlag, München, 2006

[06] Alfred Olbrich, „ITIL kompakt und verständlich“, 3. Auflage, Vieweg & Sohn Verlag, Wiesbaden, 2006

[07] Helmut Schiefer, Erik Schnitterer, „Prozesse optimieren mit ITIL“, 1. Auflage, Vieweg-Verlag, Wiesbaden, 2006

[08] Jan van Bon, Marianne Nugteren, Selma Polter, „ISO/IEC 20000, das Taschenbuch“, 1. Auflage der 1. Ausgabe, itSMF, Van Haren Publishing, 2006

[09] Rüdiger Zaranekow, Axel Hochstein, Walter Brenner, „Serviceorientiertes IT-Management (ITIL-Best-Practices und -Fallstudien)“, Springer Verlag, Berlin Heidelberg, 2005

5.2 Online-Quellen

[o01] Die Datenverwaltung steht vor historischen Herausforderungen, http://www.computerwoche.de/nachrichten/591899/?ILC-RSSFEED&feed=591899%20rssnews

[o02] Exagon will Schwächen von ITIL V 3 mit SelfCheck-Tool umgehen, http://www.computerwoche.de/knowledge_center/it_services/596384/?ILC-RSSFEED&feed=596384%20rssnews

[o03] Itil V3 ab Januar in Deutsch, http://www.computerwoche.de/knowledge_center/it_services/597022/?ILC-RSSFEED&feed=597022%20rssnews

[o04] Herbert Falk, Qualitätsmanager, Qualität & Norm, http://www.o04.info/allgemein/modell.htm

[o05] ITIL = TMTLA?, http://itil-blog.de/index.php/2006/08/26/itil-tmtla/

[o06] Neue Thesen des ITIL-Skeptikers, http://itil-blog.de/index.php/2006/08/26/neue-thesen-des-itil-skeptikers/

[o07] IT-Service-Management, http://www.itil.org/de/itilv2-itservmgmtprozesse/itilv2-itservicemanagementprozesse.php

[o08] ITIL V3 – Service Life Cycle, http://www.itil.org/de/itilv3-servicelifecycle/index.php

[o09] ITIL V3-V2 Mapping, http://www.itil.org/de/itilv3-servicelifecycle/itilv3-v2mapping.php

[o10] ITIL Refresh: Scope and development plan, 2006, http://www.itil.co.uk/scope_web.pdf

[o11] Weshalb wurde ITIL entwickelt, http://www.itsmf.de/bestpractice/weshalb.asp

[o12] Der Nutzen von ITIL, http://www.itsmf.de/bestpractice/nutzen.asp

[o13] IT-Service-Management-Studie 2006, http://www.materna.de/nn_1442/nsc_true/DE/Presse/de/BUI/2006/MATERNA_20stellt_20IT-Service-Management-Studie_202006_20vor.html__nnn=true

[o14] IT Infrastructure Library (ITIL), Background, http://www.ogc.gov.uk/guidance_itil.asp, http://www.ogc.gov.uk/guidance_itil_4672.asp

[o15] Initiativen des IT-Service-Managements, Universität St. Gallen, 30.06.2004, http://www.pascal-sieber.ch/Files/cno/fg-ict-040908-axel-hochstein.ppt

[o16] Service-oriented IT Management: Benefit, Cost and Success Factors, Universität St. Gallen, 2005, http://itservicetoday.blogs.com/itil/files/Service_Orientated_IT_Management_ITIL.pdf

[o17] ISO 9000, http://www.quality.de/lexikon/iso_9000.htm

[o18] Business Service Management, http://de.wikipedia.org/wiki/Business_Service_Management

[o19] Capability Maturity Model Integration, http://de.wikipedia.org/wiki/Capability_Maturity_Model_Integration

[o20] IT Infrastructure Library (ITIL), http://de.wikipedia.org/wiki/ITIL, letzter Zugriff: April 2007

[o21] IT Infrastructure Library (ITIL), http://de.wikipedia.org/wiki/ITIL, letzter Zugriff: Juni 2007

[o22] Prozessmanagement, http://de.wikipedia.org/wiki/Prozessmanagement

6 Abkürzungsverzeichnis

ADT	……	Average Downtime
AFR	……	Annual Failure Rate
AST	……	Agreed Service Time
BCM	……	Business Capacity Management
BS	……	British Standard
BSC	……	Balanced Score Card
BSI	……	British Standards Institution
BSM	……	Business Service Management
CAB	……	Change Advisory Board
CCTA	……	Central Computer and Telecommunications Agency
CDB	……	Capacity Database
CEN	……	Comité Européen de Normalisation
CIO	……	Chief Information Officer
CMDB	……	Change Management Database
CMMI	……	Capability Maturity Model Integration
CPU	……	Central Processing Unit
CW	……	Computerwoche
DHS	……	Definitive Hardware Storage
DSL	……	Definitive Software Library
DT	……	Downtime
EC	……	Emergency Committee

EFQM	.....	European Foundation for Quality Management
EN	.....	Europäische Norm
eTOM	.....	enhanced Telecom Operation Map
FAQ	.....	Frequently Asked Questions
FSC	.....	Forward-Schedule-of-Change
GPM	.....	Geschäftsprozessmanagement
ICT	.....	Information & Communications Technology
IEC	.....	International Electrotechnical Commission
IP	.....	Internet Protokoll
ISO	.....	International Organization for Standardization
IT	.....	Informationstechnologie
ITIL	.....	IT Infrastructure Library
ITSM	.....	IT Service Management
ITSMF	.....	IT Service Management Forum
KPI	.....	Key Performance Indicators
LAN	.....	Local Area Network
MO	.....	Managed Objects
MOF	.....	Microsoft Operations Framework
MTBF	.....	Mean time between Failures
MTBSI	.....	Mean time between System Incidents
MTTR	.....	Mean time to repair
OGC	.....	Office of Government Commerce
OPL	.....	Operational Level Agreement
PC	.....	Personal Computer
PDCA	.....	Plan, Do, Check, Act
PRINCE	.....	Projects in controlled Environments
PSA	.....	Projected-Service-Availability
QM	.....	Qaulitätsmanagement
RCM	.....	Resource Capacity Management

RfC	……	Request for Change
ROI	……	Return On Invest
SA	……	Service Achievement
SAN	……	Storage Attached Network
SC	……	Service Catalog
SCM	……	Service Capacity Management
SIP	……	Service Improvement Program
SLA	……	Service Level Agreement
SLR	……	Service Level Requirement
SOA	……	Serviceorientierte Architektur
SPOC	……	Single Point Of Contact
SPOF	……	Single Point Of Failure
SQP	……	Service Quality Plan
SRQ	……	Service Request
SSS	……	Service Specification Sheet/Specsheet
TCO	……	Total Cost of Ownership
TCP/IP	……	Transmission Control Protocol/Internet Protocol
TQM	……	Total Quality Management
UC	……	Underpinning Contract
UHD	……	User Helpdesk

7 Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z