PEARSON Education

Nadin Ebel

ITIL
Basis-Zertifizierung

Grundlagenwissen und Zertifizierungsvorbereitung für die ITIL Foundation-Prüfung

ADDISON-WESLEY

ACT®

ITIL-Basis-Zertifizierung

Nadin Ebel

ITIL-Basis-Zertifizierung

Grundlagenwissen und Zertifizierungsvorbereitung für die ITIL Foundation-Prüfung

ADDISON-WESLEY

An imprint of Pearson Education

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

Bibliografische Information Der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über *http://dnb.ddb.de* abrufbar.

10 9 8 7 6 5 4 3 2 1

08 07 06

ISBN-13: 978-3-8273-2352-1
ISBN-10: 3-8273-2352-5

Lektorat:	Sylvia Hasselbach, shasselbach@pearson.de
Korrektorat:	Michelle Kottemann, Bonn
Fachlektorat:	Michael Meyer, Helmut Corsten
Umschlaggestaltung:	Marco Lindenbeck, mlindenbeck@webwo.de
Herstellung:	Philipp Burkart, pburkart@pearson.de
Satz und Layout:	mediaService, Siegen
Druck und Verarbeitung:	Bercker Graph. Betrieb, Kevelaer

Printed in Germany

Inhaltsübersicht

Inhaltsverzeichnis

Für DON

Wer jeden Tag sagen kann: „Ich habe gelebt", dem bringt jeder Morgen einen neuen Gewinn.

(Seneca)

Vorwort

ITIL steht als Abkürzung für IT Infrastructure Library. Wie der Name vermuten lässt, handelt es sich hierbei um eine Sammlung von Büchern, eine Bibliothek. Die ITIL-Bände beschäftigen sich jeweils mit einem Bereich des Themenkomplexes IT Service Management. Alles dreht sich darum, die Qualität der IT Services zu verbessern und dies im Sinne des Unternehmens und der damit verbundenen Geschäftsziele. Es geht um den messbaren Beitrag zum Geschäftserfolg. Unter dem Gesichtspunkt von zielgerichteten, geschäftsprozessorientierten, benutzerfreundlichen und kostenoptimierten IT-Dienstleistungen müssen Prozesse, Menschen und Technologien Hand in Hand arbeiten und aufeinander abgestimmt werden.

Die Vorgaben von ITIL in allen denkbaren Bereichen der IT-Dienste wollen nicht als eine Religion verstanden sein. Vielmehr sollte die IT-Praxis immer wieder anhand der vorher niedergelegten Umsetzungsplanung überprüft werden, Praxiserkenntnisse wiederum sollten den Plan modifizieren dürfen.

Klingt Ihnen zu abstrakt? Aber eigentlich sind Sie dem Thema ITIL schon mehr oder weniger oft begegnet. Oder Ihnen ist die Abwesenheit dieses Leitfadens während Ihrer täglichen Arbeit schmerzhaft aufgefallen, vielleicht ohne dass Sie sich dessen wirklich bewusst geworden sind.

- Vielleicht dann, wenn Anwender Ihnen als Administrator die Türen einrennen? Sie einen Anruf mit Anfragen, Problemschilderungen oder Anforderungen nach dem anderen entgegen nehmen? Das Telefon nicht stillsteht und Sie aufgrund dessen nicht in Ruhe und konzentriert arbeiten können? Kurz: Sie werden mit direkten Anfragen und vermeintlichen Problemschilderungen überhäuft? Der Service Desk sollte im Gegensatz zur Fachabteilung als Anlaufstelle fungieren.
- Wünschen Sie sich in solchen Momenten eine Anlaufstelle, die Anrufe von Anwendern oder Kunden entgegennimmt und diese bearbeitet? ITIL nennt eine solche Funktion Service Desk und ordnet diesen Tätigkeiten den Prozess des Incident Management zu.
- Fehlersuche. Ein leidliches Thema. Fehler sind Ursachen von mehr oder weniger offensichtlichen Problemen. Da Fehler die Angewohnheit haben, immer wieder aufzutauchen, wenn die Fehlerursache nicht beseitigt wird, schadet es nicht, Fehlerursachen und Workarounds zu dokumentieren. Sie müssen die Ursachen beseitigen, proaktiv und präventiv darauf hinarbeiten, dass Fehler und Probleme in Zukunft weniger oft, nicht unvorbereitet und, wenn es geht, gar nicht mehr auftreten. Diese Themen sind als Prozess unter ITIL dem Problem Management zugeordnet.
- Sie haben Fragen zur bestehenden Infrastruktur, weil Sie Synergien mit Ihren Anwendungen schaffen möchten? Sie planen Erweiterungen oder müssen konsolidieren? Sie möchten Ihre Daten im SAN ablegen, haben aber keine Ahnung, wie viel Platz dort noch vorhanden ist? Dann wäre es doch toll, wenn irgendjemand ver-

bindliche Aussagen über die vorhandene IT-Infrastruktur in Ihrem Unternehmen oder beim Kunden machen könnte. Mit Hilfe des Configuration Management als ITIL-Prozess sollte das kein Problem sein.

- Sie möchten Notfälle überstehen und Vorkehrungen für Stromausfälle und andere Katastrophen treffen? Unter ITIL kümmert sich das IT Service Continuity Management darum.

Egal, ob es darum geht, Finanzen zu planen und zu kontrollieren (Financial Management), Verfügbarkeit von IT-Dienstleistungen zu kontrollieren und anzupassen (Availability Management) oder Kundenverträge und Lieferantenverträge zu vereinbaren und zu kontrollieren (Service Level Management), ITIL bietet den Rahmen für individuelles IT Service Management.

Motivation

Bei der Auseinandersetzung mit dem Thema ITIL und IT Service Management bin ich bei meiner Arbeit als IT Consultant mit unterschiedlichen Themen und Prozessen in Berührung gekommen. In meinen Augen ist es entscheidend, zu verstehen- sich darüber im Klaren zu sein, dass ITIL ein Rahmenwerk, eine Empfehlung, ein Werkzeug für das Unternehmen ist und keinen Selbstzweck darstellt. Unternehmen leben in großer Abhängigkeit von ihrer IT und viele Mitarbeiter sind sich leider noch immer nicht im Klaren darüber, was Dienstleistung bedeutet und dass Serviceorientierung keine Schande ist.

Viele Organisationen und Abteilungen spiegeln leider genau diesen Misstand wider. Das hat zur Folge, dass Probleme mehrfach und lange bearbeitet werden, da keine Dokumentation über frühere Probleme und deren Lösung existieren, was alle Beteiligten viel Arbeitszeit kostet. Ausfälle der IT Services, die immer wieder auftreten, v.a. da Systeme überlastet sind oder Änderungen fehlschlugen, bedeuten nicht nur einen Imageschaden der IT bzw. der entsprechenden Abteilung oder des Dienstleister im Unternehmen. Diese Ausfälle können gegebenenfalls sogar Schadensersatzansprüche nach sich ziehen.

Gerade das Durchführen von Änderungen (Changes) an und in der IT-Infrastruktur ist eine der häufigsten Fehlerquellen. Es fehlt an einer zentralen Planung und Überwachung. Nachgelagerte Fehler, die an anderer Stelle sichtbar werden, können nicht zugeordnet werden. Nicht nur in einem solchen Fall dauert die Informationssuche sehr lange, weil keine zentralen Informationen vorliegen und keine definierten oder bekannten Anlaufstellen oder Kommunikationssysteme existieren.

Die Erweiterung der Systeme erinnert oft an nächtliche Panikkäufe von Kneipenwirten. Da wird an der Tankstelle zu überhöhten Preisen und weil niemand vorab die Trinkvorräte kontrolliert und zu gegebener Zeit nachgefüllt hat, schnell eine Flasche einer Spirituosen-Marke gekauft, weil der Stammtisch die letzte verbleibende Flasche gerade geleert hat. Genauso sind Organisationen auf neue Anforderungen oder gar Katastrophen vielfach nicht vorbereitet, da zu wenig Planung im Vorfeld stattgefunden hat.

Doch notwendige Analysen der Ausgangssituation und die dazugehörige Projektplanung bringen wenig, wenn die Akzeptanz für die Thematik im Unternehmen nicht vorhanden ist. Jedes Sollkonzept ist zum Scheitern verurteilt, wenn die notwendige Sensibilisierung unter den Mitarbeitern im Konzern scheitert.

Für die meisten Mitarbeiter, die sich gegen neue Methoden wehren („Brauchen wir nicht. Bisher haben wir das auf gewohnte Weise gemacht und das lief auch so!“) ist ITIL eher ein Unwort denn ein Hilfsmittel zur Verbesserung der Serviceleistung. Zum Glück ist dem nicht so und alle, die sich mit dem Thema an dieser Stelle auseinandersetzen, sind (bereits) anderer Meinung. In meinen Augen ist Serviceorientierung ein Muss, das ständig optimiert werden kann.

Bei meiner Zertifizierungsvorbereitung im Jahre 2004 für die ITIL Foundation-Prüfung habe ich während der Recherche nur wenige aussagekräftige Seiten im Internet gefunden, die sich mit einem möglichen Fragenspektrum, ihrer Form und der geforderten Detailtiefe beschäftigten. Selftests gab es damals nur von einem englischsprachigen Anbieter. Fachliteratur war rar. Inzwischen hat sich das Bild gewandelt. Auf der Basis meiner eigenen Prüfungsvorbereitung habe ich im Jahr 2005 ein kostenloses eBook zur Vorbereitung auf die ITIL Foundation-Prüfung erst auf meiner eigenen Webseite und dann auf der Homepage meines Arbeitgebers, der ACT IT Consulting & Services AG, knapp ein Jahr lang bereitgestellt. An dieser Stelle nochmals ein dickes Danke an Birgit Enkel für das damalige Korrekturlesen.

Nach viel positivem Feedback, einer großen Anzahl von Mails und zahlreichen Verbesserungsvorschlägen ist es nun doch zu einer Veröffentlichung in Buchform gekommen.

Aufbau und Intention

Das vorliegende Buch führt Sie Schritt für Schritt an die Inhalte der IT Infrastructure Library heran. Die Themen in den ersten Kapiteln beschäftigen sich mit dem Aufbau einer Wissensbasis in Bezug auf ITIL und IT Service Management. Es geht um die Erläuterung von grundlegenden Begriffen, einen Überblick über die ITIL-Historie, die ITIL-Motivation, Aufgaben und Ziele. Sie bekommen einen umfassenden Überblick geboten, der Ihnen als Basis für die nachfolgenden Erläuterungen dienen soll.

Damit Sie wissen, wie die ITIL Foundation-Zertifizierungsprüfung aufgebaut ist und welche weiteren Zertifizierungsmöglichkeiten es im ITIL-Bereich gibt, finden Sie in *Kapitel 4, ITIL Foundation-Zertifizierung* ein Buchkapitel, das sich mit diesen Fragen auseinander setzt. So wissen Sie bereits vorab, was Sie während der Prüfung erwartet.

Danach folgt der Einstieg in den ITIL-Subset Service Support mit einem allgemeinen Überblick zum Thema. Den Prozessen dieses Themenkomplexes habe ich jeweils einzelne Kapitel gewidmet. Als Abschluss zum Thema Service Support folgen einige spezifische Kontrollfragen mit Lösung und Kommentar. So können Sie das Gelernte direkt überprüfen. Analog dazu schließen sich die ITIL-Prozesse des Service Delivery an. Den Abschluss bildet ein Katalog von Beispielfragen zur ITIL-Basis-Zertifizierung und ein Glossar.

Sie werden in diesem Buch viele Erklärungen eines Themas aus unterschiedlichen Perspektiven vorfinden. Dadurch werden sich die Inhalte besser einprägen und es soll Ihnen helfen, die Zusammenhänge im IT Service Management besser zu verstehen.

Vielen Dank an Michael Meyer und Helmut Corsten für das Fachkorrektorat und die Unterstützung bei der Grafikerstellung. Des Weiteren ein dickes Danke und viele Grüße an Speedy (Starbucks), Birgit („Weekend“), Katinka (Die griechische Ägäis wartet!), Yasemin & Jürgen, Jessica & Holger, Tim & Sandra, Kah mit Paulinchen und Basti, Pia mit Nikita, Yara und Pit, Janet & Rocco mit Herbie, Kerstin Sch. und Rubinio, meine Eltern, Holger & Beate, Markus B., Roman, Lisa & Olli, Patrizia T. und Sven & Markus. Danke auch an meine Kollegen von der ACT AG und meinen Vorgesetzten Harald Justen sowie meine Lektorin Sylvia Hasselbach, an Rainer Fuchs und Boris Karnikowski von Addison-Wesley.

Feedback, Rückfragen oder Kritik sind herzlich willkommen und können per eMail (*info@nell-it.de*) an mich herangetragen werden.

1 ITIL und IT Service Management

Die IT ist heutzutage aus Unternehmen nicht mehr wegzudenken und häufig nicht mehr nur ein Support-Bereich, sondern selbst Teil des Kerngeschäfts. Eine der Hauptforderungen unserer Zeit ist die konsequente Ausrichtung der IT-Dienstleister auf die Bedürfnisse ihrer internen und externen Kunden. Damit stehen IT-Unternehmen und –Abteilungen vor der Aufgabe, ihren Betrieb, aber auch die von ihnen betreute Infrastruktur so performant und kostengünstig wie möglich zu managen sowie die bereitgestellten Services verursachungsgerecht zu verrechnen. Gleichzeitig sind die IT-Bereiche, deren Infrastrukturen und Prozesse historisch gewachsen, stark technikgetrieben und ineffizient.

Um den Schritt in Richtung Systematisierung und Professionalisierung zu gehen, nutzen IT-Abteilungen und -Unternehmen die ITIL-Sammlung. Mit Hilfe der ITIL Best Practices gelingt die Wandlung zum umfassenden IT Service-Provider, der sich an den Geschäftsprozessen des gesamten Unternehmens orientiert.

Effizient und effektiv

- Effektiv: Effekt (Wirkung, Erfolg): tatsächlich, wirklich bzw. wirkungsvoll (im Verhältnis zu den eingesetzten Mitteln), lohnend
- Effizient: „besonders wirtschaftlich", „leistungsfähig"

Beispiel: Eine Hausfrau kann effizient mit ihrem Geld umgehen. Dagegen putzt sie besonders effektiv, wenn sie Essigreiniger verwendet.

ITIL (IT Infrastructure Library) ist eine über viele Jahre entstandene und gewachsene Sammlung von Best Practise-Anleitungen zur Darstellung von Prozessen, die der Aufrechterhaltung der vereinbarten IT-Aktivitäten dienen. Dies geht einher mit dem Erbringen und Verwalten von IT-Dienstleistungen für das Unternehmen. ITIL bietet als Bibliothek mit seinen Kapiteln zu den unterschiedlichen Management-Bereichen die Basis dafür und hängt eng mit dem Begriff des IT Service Management zusammen. Hinter diesem Begriff verbirgt sich das Bündel aller Maßnahmen und Aktivitäten, um Qualität und Quantität von IT Services optimal und zielgerichtet zu planen, zu überwachen und zu steuern.

Alles dreht sich darum, die Qualität der IT Services zu verbessern und das im Sinne des Business und der damit verbundenen Geschäftsziele. Services kommen in Interaktion mit Service-Erbringer und Service-Abnehmer zustande. Eine Bewertung des Service ist erst nach der Erbringung möglich. Unter der Qualität eines Service ist der Umfang bzw. das Ausmaß zu verstehen, in dem ein Service den Anfor-

derungen und Erwartungen eines Kunden entspricht. Es geht um den messbaren Beitrag zum Geschäftserfolg. Unter diesem Gesichtspunkt von zielgerichteten, geschäftsprozessorientierten, benutzerfreundlichen und kostenoptimierten IT-Dienstleistungen müssen Prozesse, Menschen und Technologien Hand in Hand arbeiten und aufeinander abgestimmt werden.

Der Begriff „IT Service"

IT Service als wichtiger Begriff bezeichnet die Summe aller technischen und nicht-technischen Interaktionen zwischen Kunden- und Dienstleisterseite.

Die Prozesse bilden das Herzstück des IT Service Management. Sie stellen die Grundlagen der Aktivitäten dar, die in den ITIL-Kapiteln beschrieben werden, um die vereinbarte Qualität der IT Services zu leisten. Dies bezieht sich auf die operativen Prozesse des Service Support und die taktischen Prozesse des Bereiches Service Delivery. Prozesse werden generell als definierte Abläufe bzw. Aktionsfolgen in einem System mit einem bestimmten Ziel verstanden. Es geht um die Beantwortung der Frage: „Was ist zu tun?" Über einen Prozess geht aus einem definierten Input ein zu erwartender Output hervor (*siehe Abbildung 1.1*). Es existieren unterschiedliche Prozessarten in einem Unternehmen. Dazu gehören Managementprozesse im Bereich Personalentwicklung, unterstützende Prozesse wie die ITIL-Prozesse oder Geschäftsprozesse im Bereich der Produktion. Es geht stets darum, einen Mehrwert zu schaffen. Prozesse bleiben konsistent und sind von Verfahren und Funktionen unabhängig. In Bezug auf Funktionen dreht sich alles um die Beantwortung der Frage „Wie ist etwas zu tun?".

Der Begriff „Prozess"

Ein Prozess ist nach ISO 8402 durch folgende Eigenschaften charakterisiert:

- Er besteht aus einer Menge von Mitteln und Tätigkeiten. Zu den Mitteln können Personal, Geldmittel, Anlagen, Einrichtungen, Techniken und Methoden gehören. Diese Mittel und Tätigkeiten stehen in Wechselbeziehung.
- Ein Prozess erfordert Eingaben.
- Ein Prozess gibt Ergebnisse aus.

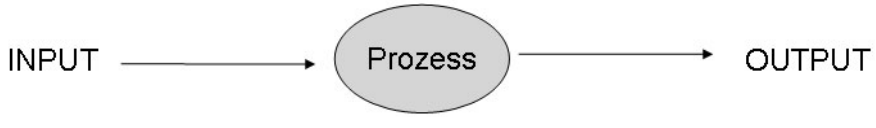


Abbildung 1.1: Prozessdarstellung

Ein Prozess stellt ein Vorgehensmodell für immer wiederkehrende Abläufe dar.

ITIL steht also nicht für sich und als Selbstzweck der Begrifflichkeiten im Raum, sondern berücksichtigt sowohl die komplexe heutige IT-Welt als auch die Geschäftsziele des Unternehmens. Ganz wichtig ist dabei die kundenorientierte Sichtweise.

Der Begriff „Qualität"

Qualität wird laut ISO 402 als Gesamtheit der Eigenschaften und Kennzeichen eines Produkts bzw. eines Service verstanden, die zur Erfüllung der festgelegten oder selbstverständlichen Bedürfnisse wichtig ist.

Ihren Ursprung hat die Beschreibung ITIL (IT Infrastructure Library) in Großbritannien, als Anfang der 80er Jahre die Behörde Central Computer and Telecommunications Agency (CCTA) ein Konzept in Auftrag gab, um die regierungsinterne IT transparenter organisieren zu können – und genau das leistet ITIL auch in der freien Wirtschaft. ITIL wird als wichtig erachtet und es gilt in den deutschsprachigen Ländern, den Niederlanden und natürlich Großbritannien als De-facto-Standard. Dies gilt vor allem aufgrund der einheitlichen Nomenklatur, die bislang abstrakte Fragen der IT-Dienste konkret fassbar macht.

Aber ähnlich wie am Anfang vieler früherer Schlagworte, beispielsweise der ISO-Norm, wissen viele noch nicht, was sich hinter den vier Buchstaben verbirgt. ITIL ist kein fester Standard, keine Norm wie ISO 9000/9001, sondern lediglich eine Bibliothek von niedergeschriebenen Best Practise-Empfehlungen mit definierten Begriffen und Prozessbeschreibungen. Es ist ein generisches Modell. Viele Experten vergleichen ITIL mit einem Skelett. Dieser Leitfaden ist ein Rahmen, der dem Körper Halt und Rückgrat bietet. Das Fleisch, die Organe und die Funktionalität muss jede IT-Abteilung, jeder IT-Dienstleister und jeder Mitarbeiter beisteuern. Im Laufe der Zeit müssen die Muskeln trainiert, die Gesundheit, die Seele und der Geist geschützt und gefördert werden. Und ganz wichtig: Alle müssen mit dem Herzen dabei sein. Das mag sich zwar kitschig lesen, entspricht aber den Tatsachen.

1.1 ITIL? Kenn' ich nicht?!

Das Regelwerk ITIL hat sich inzwischen als Orientierungshilfe für die Unternehmens-IT vielfach bewährt und ist mehr als eineals eine Orientierungshilfe für die Abbildung von IT-Prozessen. Trotz seines Ursprungs in den 80er Jahren ist ITIL für viele IT-Abteilungen noch neu. Die zahlreich angebotenen Kurse deuten jedoch darauf hin, dass der Best Practice-Ansatz von ITIL auch in Deutschland zunehmend Verbreitung findet. Gab es bis vor einigen Jahren noch keine deutschsprachige aussagekräftige und lesenswerte Literatur bis auf das Standardwerk der itSMF, sieht es heute schon anders aus.

Was ist das itSMF?

Das Information Technology Service Management Forum stellt die weltweit einzige unabhängige und international anerkannte Organisation für IT Service Management. Das itSMF hat es sich zum Ziel gesetzt, als unabhängiger und nicht kommerzieller Verein die aktuellen Erkenntnisse und Methoden im Bereich des IT Management zu fördern und bekannt zu machen. Es bietet, von Unternehmen für Unternehmen, eine Plattform zum Austausch von Informationen und Erfahrungen. 1991 wurde das IT Service Management Forum in England gegründet. itSMF Deutschland widmet sich der Förderung und Weiterbildung im Bereich des IT Service Management in Deutschland.

Das ITIL-Kompendium in englischer Sprache (*siehe Abbildung 1.2*) besteht aus den folgenden Veröffentlichungen:

- The Business Perspective: Diese Veröffentlichung stellt das Bindeglied zwischen dem IT Service Management und den Geschäftsanforderungen dar. Die Anforderungen des Geschäfts an die IT werden ermittelt und daraus die strategischen Anforderungen an die IT-Dienstleistungen abgeleitet.
- Planning to Implement Service Management: Diese Veröffentlichung hilft dem Service Provider, ein praxisorientiertes IT Service Management einzuführen, und ermöglicht es gleichzeitig dem Dienstleistungsempfänger, seine Anforderungen IT-gerecht zu formulieren.
- Information and Communications Technology (ICT) Infrastructure Management: „Information and Technology Infrastructure Management" beschreibt die Planung, Einführung, die Auslieferung und den Betrieb der IT Infrastruktur-Komponenten.
- Security Management: Der Prozess „Security Management" ermöglicht die Implementierung eines IT-weiten Prozesses zur integrierten Steuerung aller sicherheitsrelevanten Aspekte in der IT.
- Application Management: Der Prozess „Application Management" ist für das Management von Applikationen über ihren gesamten Lebenszyklus hinweg verantwortlich. Außerdem definiert er die Interaktion mit den Prozessen der Veröffentlichungen „ICT Infrastructure Management", „Service Support" und „Service Delivery".
- Service Support und Service Delivery: Diese beiden Veröffentlichungen bilden das Kernstück des IT Service Management. Sie beschreiben jeweils fünf Prozesse, die entsprechend als Service Support- und Service Delivery-Prozesse bezeichnet werden sowie die Funktion des Service Desk.

Die OGC als Nachfolgerin der CCTA bietet mit ihren in rund 45 Büchern veröffentlichten IT-Prozessen die umfangreichste bisher veröffentlichte Prozessdefinition für den Aufbau einer IT Service-Organisation. Dieses Kompendium hat sich seit seiner Entstehung Ende der 80er Jahre zu einem De-facto-Standard entwickelt, der auch in Deutschland immer stärkere Beachtung findet.

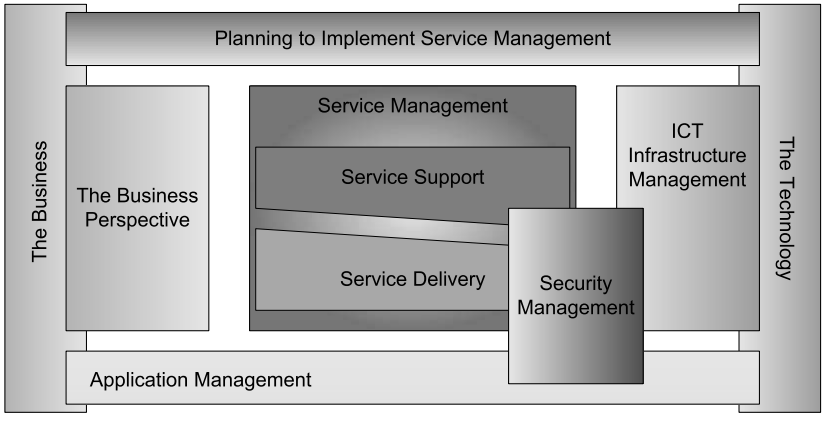


Abbildung 1.2: Bereiche des Original-ITIL-Kompendiums nach OGC

Der Nutzungsgrad von ITIL erweist sich als unterschiedlich stark ausgeprägt. Während einige Unternehmen ITIL nur in einzelnen Disziplinen einsetzen, nutzen es andere bereits in mehreren oder gar allen. Die Vorteile der Nutzung erscheinen durchaus eindeutig: Im Mittelpunkt steht die Erhöhung der Effizienz, gefolgt von der damit einhergehenden Kostensenkung und der Erhöhung der Kundenzufriedenheit. Nachteile zeigen sich vor allem durch den als zu hoch empfundenen Verwaltungsaufwand. In der Regel wird ITIL mit Hilfe eines Top-down-Ansatzes im Unternehmen realisiert. Die Unterstützung des Managements liegt dabei in der Hoffnung auf eine erhöhte Kundenorientierung begründet.

Mit der Service-Architektur und der IT Service Management-Organisation mit definierten Zuständigkeiten sind die Vorbedingungen erfüllt, die Best Practice-Ansätze von ITIL auf einer guten Grundlage nutzen zu können. Es gilt allerdings ein paar Regeln zu beachten: Es hat sich bewährt, ITIL aus der Kundenperspektive einzuführen und außerdem zuerst dort, wo großer Handlungsbedarf besteht.

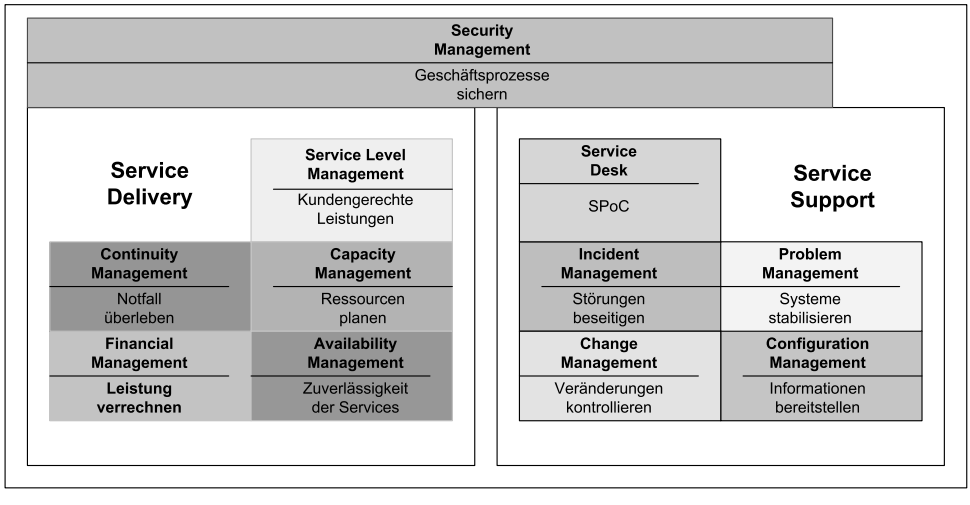


Abbildung 1.3: Einführung von ITIL

Steigende Anforderungen bei knapper werdenden Budgets haben zu einem Bedarf an bewährten Methoden im IT Service Management geführt. Das hat der IT Infrastructure Library (ITIL) zum Durchbruch verholfen. ITIL liefert zwar ein Prozessmodell, das definiert, was getan werden muss, sagt jedoch wenig dazu, wie die Prozesse in eine bestehende IT-Organisation eingeführt werden können. Dies ist aber gleichzeitig der große Vorteil dieses Modells, das sich der IT-relevanten Prozesse in den Unternehmen annimmt, ohne die Technologie zu stark in den Vordergrund zu stellen. Schließlich wird auf diesem Wege jedem Unternehmen hinreichend Flexibilität eingeräumt, um die notwendigen Veränderungen einzuleiten. Das Ziel bleibt jedoch bei allen Implementierungen von ITIL gleich: Sicherstellung von Betrieb, Sicherheit und Verfügbarkeit von Services unter Rücksichtnahme auf Kunden- und Serviceorientierung sowie Wirtschaftlichkeit bzw. Reduktion der Kosten. ITIL unterstützt die Ziele des Unternehmens, dabei gilt es nicht, ITIL als starre Schablone den Unternehmen aufzudrücken. Es ist und bleibt eine Sammlung von Best Practices, von erprobten Methoden für die Verbesserung der IT Services.

Einer der häufigsten Faktoren, die zum Scheitern oder zu enttäuschenden Ergebnissen bei der ITIL-Umsetzung führen, ist ein gewisser „Perfektionismus“, ein allzu starres Festhalten an den ITIL-Regeln. Wer hier zu viel auf einmal haben möchte, läuft Gefahr, sich zu verrennen oder bürokratische Strukturen aufzubauen, die im Alltagsgeschäft eher hinderlich als fördernd sind. Das ITIL-Regelwerk beruht nicht umsonst auf einer geschäftsorientierten Sicht der IT, es soll vor allem andere Prozesse unterstützen und die IT transparent machen, um sie in eine vernünftige Relation zu den Geschäftsprozessen zu bringen. Wird dies beachtet, bietet das Framework ein großes Potenzial zur Verbesserung von Prozessen.

1.2 (Noch) kein bunter Hund

ITIL-Einführung heißt, dass einer oder mehrere der häufigsten zehn Prozesse, die in der IT intern und extern vorkommen können, nach Vorgaben umgesetzt werden. Diese Vorgaben stehen als Best Practices im Raum und kommen heute meist von Großunternehmen, die den beschriebenen Prozess angepackt und Erfahrungen damit gesammelt haben. Als solches sind diese Best Practices aber nicht fest gemauert, sondern können ersetzt werden, was den Charakter der ITIL-Prozesse sehr offen und flexibel macht. Gemeint sind Funktionen und Prozesse wie Change Management, Incident Management, Service Desk oder auch Financial Management for IT Services (*siehe Abbildung 1.4*).

Zum Bekanntheits- und Verbreitungsgrad von ITIL erschienene Studien zeigen ein geteiltes Bild. Sie machen deutlich, dass sich ITIL zunehmender Beliebtheit erfreut, in manchen Unternehmen aber zum Teil noch gänzlich unbekannt ist. Laut einer Umfrage von Exagon Consulting, die im e-commerce-Magazin am 07.06.2006 erwähnt wurde, wollen zwei Drittel der größeren Unternehmen ihre IT-Prozesse bis 2008 nach dem ITIL-Framework gestalten. Derzeit wird ITIL laut der Erhebung durch Exagon bereits von 37 Prozent dieser Firmen zur Optimierung der IT-Prozesse genutzt, 31 Prozent planen die Umsetzung bis 2008. Befragt wurden in der Studie 318 Unternehmen mit über 100 Millionen Euro Umsatz.

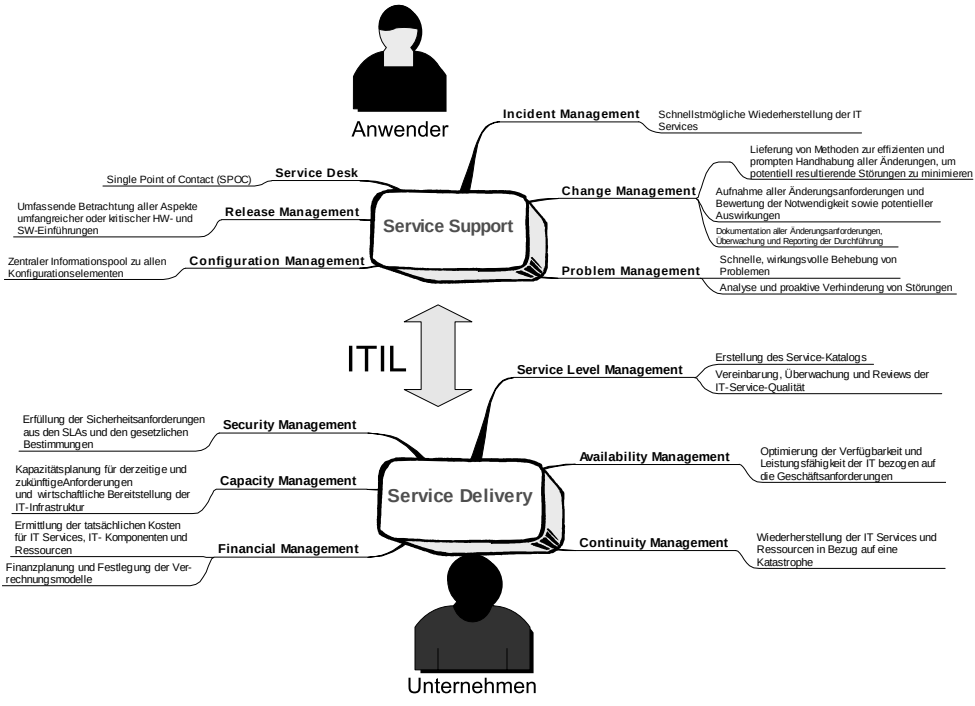


Abbildung 1.4: ITIL-Prozesse im Zusammenspiel

Einer der größten Vorteile wird in der Standardisierung gesehen: ITIL führt zu einer einheitlichen Sprach-, Vorgehens- und Denkweise und bietet Lösungsmodelle, die sich bereits in der Praxis bewährt haben. Dies bringt den Unternehmen eine gewisse Planungs- und Prozess-Sicherheit. Auch die Flexibilität wird hervorgehoben. Da das ITIL-Regelwerk kein Dogma darstellt, können alle Vorgaben flexibel und individuell angepasst werden. Gleichzeitig erhöht sich die Transparenz der IT-Prozesse, da diese mit Hilfe von ITIL genau definiert sind. Bei den meisten der Unternehmen ist ITIL daher in Form von Vorschriften oder Verfahrensanweisungen verankert. Es ist als Top-down-Ansatz vorgeschrieben und bekommt die notwendige Management-Unterstützung, damit das Regelwerk auch tatsächlich im Unternehmen „gelebt" werden kann. Ohne diese Unterstützung ist es wie jede Unternehmensphilosophie zum Scheitern verurteilt. Die Stärkung des ITIL-Bekanntheitsgrades ist es auch, die bei den Unternehmen auf der Wunschliste sehr weit oben zu finden ist. Gefragt ist ein stärkeres und intensiveres Marketing. Besonderer Wert wird diesbezüglich darauf gelegt, dass den Kunden der Mehrwert der ITIL-Nutzung kommuniziert wird. Neben dem Wunsch nach einer verstärkten und verbesserten Kommunikation besteht die Nachfrage nach einem Instrument zur Messung des ITIL-Erfolgsbeitrages. Ziel ist es, dass sich ITIL als Standard durchsetzt. Auf Basis der erschienenen Studien kann ITIL eine positive Entwicklung prognostiziert werden.

Jedes Unternehmen sollte sich aber bewusst sein, dass ITIL kein Zaubermittel darstellt. Es ist weder in der Lage, die Organisation zu verändern, noch die Services zu definieren, die Mitarbeiter zu motivieren oder fertige Lösungen anzubieten. Es bietet

lediglich unterstützende Prozesse an. Was das jeweilige Unternehmen daraus macht, ist seine Sache.

ITIL ist viel mehr als nur eine Buchreihe, es steht für eine IT Service-Philosophie, deren Rahmenwerk in weltweiter Zusammenarbeit von verschiedenen Organisationen, Spezialisten und der Industrie permanent weiterentwickelt wird.

1.3 ITIL und seine Prozesse

Die ITIL beschreibt als Buchreihe (Library) das IT Service Management in Form von Best Practices. Organisationen und Unternehmen soll durch diese umfassende Dokumentation zur Planung, Erbringung und Unterstützung von IT-Serviceleistungen ein zukunfts- und kundenorientierter Weg aufgezeigt werden, ihre IT-Organisation neu zu gestalten. Neben dem Kernbereich von ITIL, dem Infrastructure Management ICTIM, werden in der Praxis vor allem die zehn Managementbereiche des Service Support und Service Delivery umgesetzt (*siehe Abbildung 1.5*).

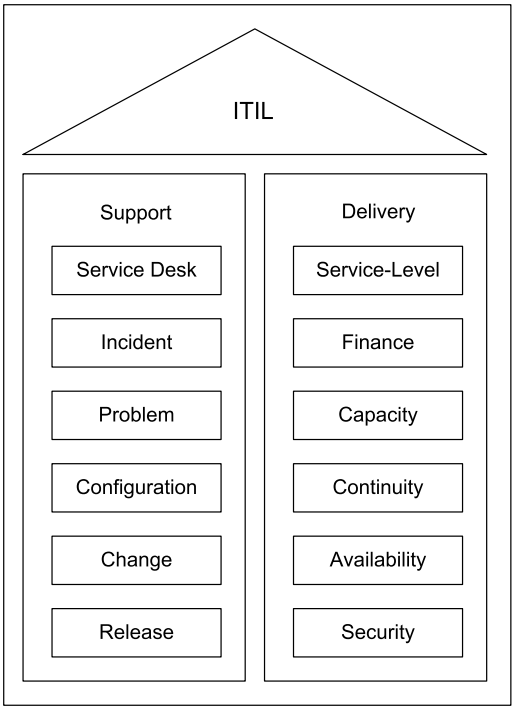


Abbildung 1.5:
ITIL-Kernprozesse

Aufgrund der Heterogenität der verschiedenen Unternehmen beschreibt ITIL nicht das „Wie“, also die Umsetzung der Best Practices-Vorschläge, sondern das „Was“, die Inhalte, Prozesse und Ziele innerhalb der IT-Organisation und kann dadurch leicht auf die individuellen Bedürfnisse eines Unternehmens zugeschnitten werden. ITIL bietet eine Vielzahl an Vorteilen und garantiert durch langjährige Praxiserfahrungen eine hohe Zuverlässigkeit. Vieles deutet auch darauf hin, dass der ITIL-Standard in Zukunft an Bedeutung gewinnen wird. ITIL wird bereits heute, vor allem in größeren Unternehmungen, erfolgreich umgesetzt.

1.3.1 Qualität

Jede neue Technologie oder Methode findet wenig Anklang, wenn sie nicht durch die richtigen Prozesse und Mitarbeiter unterstützt wird. Es gilt also, dass sich das Unternehmen zuerst über die anzuwendende Alignment- und Service Management-Strategie im Klaren sein muss, um dann die benötigten Tools zusammenzustellen und die Prozesse zu automatisieren. Genauso wichtig ist es zu verstehen, dass wir hier nicht über einen einzigen isolierten Prozess sprechen, sondern über eine ganze Kette von integrierten und miteinander verbundenen Prozessschritten.

Dabei spielen die gleich bleibende Qualität zu vertretbaren Kosten und die Qualitätssicherung eine wichtige Rolle. Die Gesamtqualität stellt sich dabei als Ergebnis aus den jeweiligen Qualitäten der einzelnen Teilprozesse dar, aus denen der gesamte Prozess besteht. Sowohl die einzelnen Teilprozesse als auch deren Qualitätsanteile üben eine gegenseitige Wechselwirkung aus. Für die Qualitätssicherung im Sinne einer ständigen Prüfung der Qualität und der daraus abgeleiteten Intention, die Qualität mindestens konstant zu erbringen, bietet der Qualitätskreis von Deming ein hilfreiches und simples Modell. Dieses stellt die Qualität in den Vordergrund und beschreibt eine kontinuierliche Qualitätsverbesserung durch einen Zyklus, der als „Plan-Do-Check-Act" (PDCA-Modell) bezeichnet wird (*siehe Abbildung 1.6*). Dabei beginnt Deming mit dem Schritt „Plan", der den gegenwärtigen Sachstand auf Verbesserungspotentiale überprüft und einen Plan zur Qualitätsverbesserung entwickelt. Bei der Analyse von Schwachstellen und Verbesserungspotenzialen ergeben sich meist konkrete Änderungsmaßnahmen zur Verbesserung der betrachteten Prozesse. Diese Änderungsmaßnahmen werden dann im Umsetzungsabschnitt „Do" durchführt.

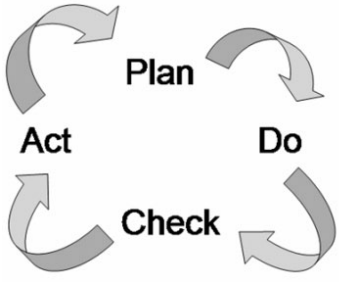


Abbildung 1.6:
Qualitätskreis von Deming

Nachdem eine Veränderung eingetreten ist, muss überprüft werden, ob die Veränderungen positiv verlaufen sind. In Bezug auf die vorher definierten Ziele wird kontrolliert, ob Seiteneffekte aufgetreten und wie diese zu bewerten sind. Im letzten Teil werden Maßnahmen zur Korrektur der festgestellten Abweichungen, Plan-Änderungen oder Verbesserungen im Qualitätsmanagementsystem durchgeführt, um das vorher definierte Ziel zu erreichen. Wird das „Qualitätsrad" stetig weitergedreht, so ergibt sich mit der Zeit automatisch eine Verbesserung der vorgefundenen Produktions- oder Geschäftsprozesse. Dabei sollten die Ergebnisse stets kritisch und offen betrachtet werden. Im Bedarfsfall sollte nicht gezögert werden, durchgeführte Änderungen schnell wieder zurückzunehmen, falls diese nicht die erwünschten Ergebnisse zeigen.

1.3.2 Prozessmanagement

Prozessmanagement ist mittlerweile fester Bestandteil der IT. Best Practices wie ITIL haben längst Einzug in moderne IT Management-Büros gehalten. Service Management organisiert die Kommunikation zwischen Anwender und IT-Servicemitarbeiter und ist die wesentliche Herausforderung für den sicheren und wirtschaftlichen IT-Betrieb. Es schließt die Lücke zwischen Kunden, IT-Abteilung und Dienstleistern.

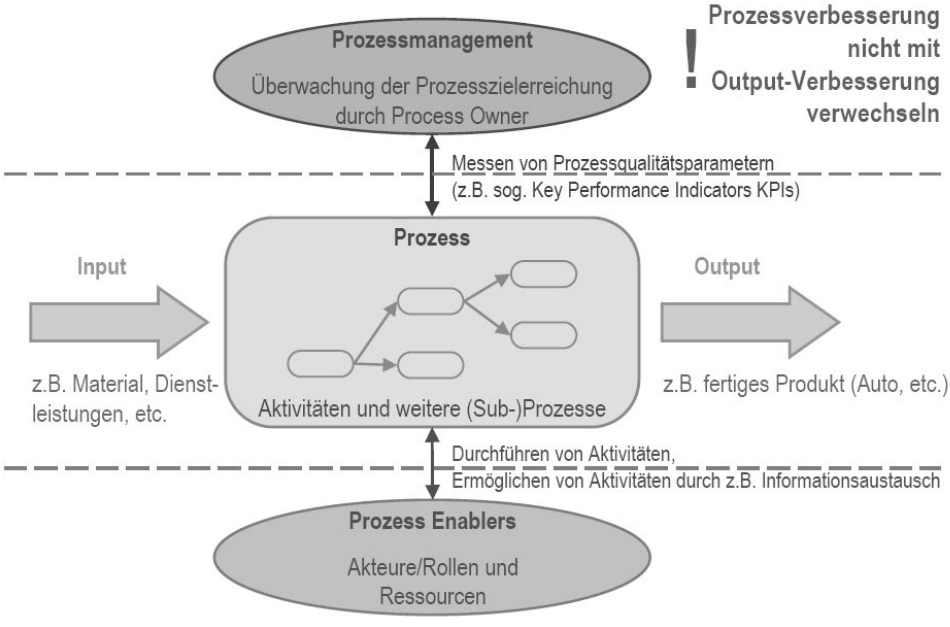


Abbildung 1.7: Prozessmanagement

Unternehmen und Organisationen werden durch den intensiven Wettbewerb und die Notwendigkeit von Veränderungen dazu gezwungen, das Niveau und die Qualität des Services, den sie ihren Kunden bieten, stetig zu erhöhen. Alle Produkte und Dienstleistungen eines Unternehmens entstehen durch seine Prozesse. Die Optimierung und konsequente Ausrichtung der Prozesse auf Kunden ist eine ständige Aufgabe der Unternehmen. Prozessmanagement ist nicht „Steuerung" von Prozessen, wie der Begriff „Management" nahe legen würde, sondern die Gestaltung von Prozessen mit dem Ziel der Vereinfachung und Verbesserung. Ein Prozess sollte effizient und effektiv sein. Basis der einzelnen Prozesse bilden Aktivitäten. So entstehen Prozessketten, die messbare Ergebnisse liefern (*siehe Abbildung 1.7*). Hier helfen Leistungsindikatoren (Kennzahlen).

Leistungsindikatoren (KPIs)

Um die Prozessqualität beurteilen zu können, sind klar definierte Parameter und messbare Ziele nötig, sog. Leistungsindikatoren (auch: Key Performance Indicators, KPI). Mehr zum Thema Leistungsindikatoren erfahren Sie in *Kapitel 2.1.6, Werkzeuge und Tools*.

Die Betrachtung des einzelnen Prozesses an sich ermöglicht die gezielte Optimierung. Der Prozessinhaber (Process Owner) ist für das Ergebnis des Prozesses verantwortlich, wohingegen der Prozessverantwortliche (Process Manager) für die Einrichtung und Durchführung zuständig ist.

2 ITIL und ICTIM im Überblick

Welch großen Stellenwert die Informationstechnologie (IT) in den letzten Jahren für den Erfolg eines Unternehmens hatte, sollte nicht unbekannt sein. Die IT unterstützt die Unternehmen nicht nur in der Umsetzung der Strategie, sondern ist zunehmend gefordert, neue Geschäftsfelder zu ermöglichen und den sich ändernden Anforderungen mit angemessener Reaktionszeit zu begegnen. Als Konsequenz und auch für die eigene positive Positionierung innerhalb der Unternehmen muss sich die IT zu einem Servicelieferanten wandeln.

Genau dieser Anforderung kommt die Entwicklung rund um den Begriff IT Service Management (ITSM) entgegen. IT Service Management stellt Prozess-, Kunden-, Kosten- und Leistungsorientierung in den Vordergrund. Damit werden langfristig sowohl die Kosten gesenkt als auch die Produktivität erhöht, nachhaltig und ohne negative Seiteneffekte auf das Kerngeschäft. Voraussetzung dafür ist die Bereitschaft des Managements und der Mitarbeiter zum Wandel in Richtung Kunden- und Serviceorientierung innerhalb des Unternehmens. Dies wird auch als Service- bzw. Unternehmenskultur bezeichnet. Hat sich eine Organisation für die Einführung von ITSM entschieden, gilt es, bestehende Leitgedanken, Strukturen und Abläufe zu hinterfragen und ggf. anzupassen, um interne Barrieren aus dem Weg zu räumen. Aus diesem Grund ist es überaus wichtig, dass das Management die Entscheidung trägt, aber auch gleichzeitig dafür sorgt, dass alle Beteiligten am gleichen Strang ziehen.

Die Standardisierung hat auch vor der IT nicht Halt gemacht. Nachdem der Standardisierungsgrad im Bereich der Hard- und Software mittlerweile ein konkretes Niveau erreicht hat, konzentriert sich die Standardisierung mittlerweile auf die IT-Prozesse. Der End-to-End Servicegedanke hält Einzug in die Unternehmen. IT-Prozesse werden qualitativ und quantitativ messbar.

Es gibt einige Vorschläge für prozessorientierte Vorgehensmodelle, mit denen ITSM konzipiert und strukturiert werden kann. Ein wichtiges und weit verbreitetes Rahmenwerk für die Konzeption, Steuerung und Optimierung der Geschäftsprozesse im ITSM ist ITIL. Es bietet die Grundlage zur Verbesserung von Einsatz und Wirkung der eingesetzten IT-Infrastruktur. Das ITIL Basis-Framework besteht aus den 10 ITIL-Prozessen, die in den Büchern „Service Support“ und „Service Delivery“ (fünf Support-Prozesse, fünf Delivery-Prozesse) dargestellt werden (*siehe Abbildung 2.1*). Für viele zählt das Kapitel „Service Desk“ als Funktionsbeschreibung auch dazu.

Diese Bücher enthalten Zielsetzungen und Beschreibungen der ITIL-Bereiche in Form von Prozess- und Funktionsbeschreibungen sowie die Darstellung der Beziehungen zwischen ihnen. Dazu gehören Aufgaben, Implementierungshinweise, Schwierigkeiten, die bei der Umsetzung entstehen können und der Nutzen aus der Einführung der ITIL-Aktivitäten. Diese Prozessbeschreibungen bieten damit einen geeigneten Rahmen für individuelles IT Service Management, sind aber keine Anleitung im engeren Sinne und können bei der Implementierung unternehmensspezifisch konkretisiert werden. Der damit geschaffene Freiraum und die Flexibilität für das jeweilige Unternehmen erscheint dem einen als Fluch und fehlende Konkretisierung, anderen ist dies eher willkommen als die starre Vorgabe von Normen und harten Vorschriften.

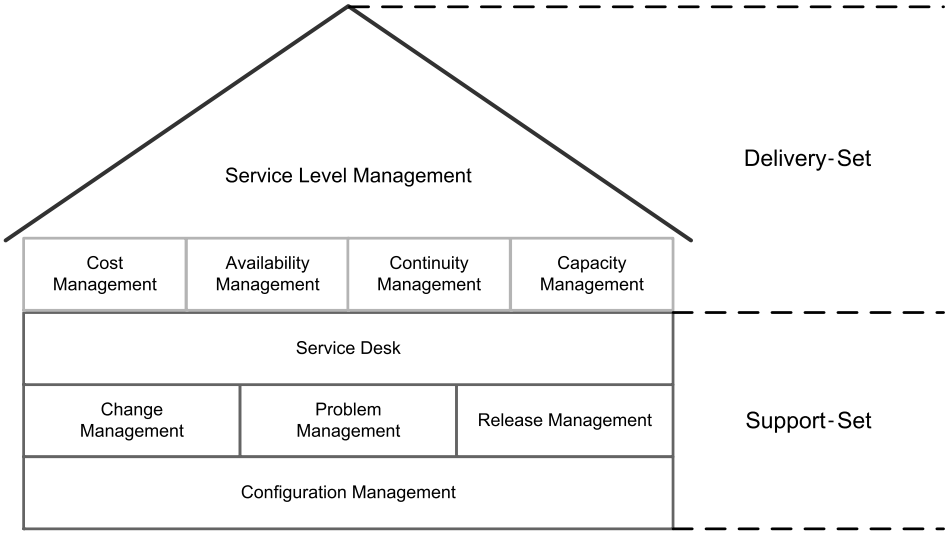


Abbildung 2.1: Das ITIL-Haus

Neben den erwähnten Prozessbeschreibungen gibt es noch weitere Veröffentlichungen zu anderen IT-spezifischen Themen. Die neue ITIL Library (siehe auch *Kapitel 1.1, ITIL? Kenn' ich nicht?!*) besteht aus den folgenden Gebieten:

- The Business Perspective (strategische Ebene)
- Applications Management (taktische Ebene)
- Security Management (taktische Ebene)
- Service Delivery (taktische Ebene)
- Service Support (operative Ebene)
- Infrastructure Management (ICT) (operative Ebene)

Die ITIL-Bücher sind heute Eigentum des OGC (Office of Government Commerce). Die OGC ist eine 2001 ins Leben gerufene Dachorganisation, der u.a. die CCTA unterstellt wurde.

Organisationen und ITIL

EXIN ist eine niederländische Stiftung, die außerhalb des englischsprachigen Raums für die Abnahme der offiziellen Zertifizierungsprüfungen zuständig ist. EXIN führt selbst keine Schulungen durch, um diese Unabhängigkeit zu gewährleisten. Für Deutschland übernimmt die TÜV Akademie GmbH diese Aufgaben.

Die ITIL-Revision 2 hat mit dem ICT Infrastructure Management vier weitere wichtige Bausteine erhalten. Mit den Managementbereichen

- Design and Planning,
- Deployment,
- Operations und
- Technical Support

wird das bisher bekannte IT Service Management um die operativen Prozesse des IT-Betriebs ergänzt. Damit werden bisherige Fragestellungen zur Verteilung von Aufgaben transparent, die oft als ungeklärt oder frei entscheidbar kommuniziert wurden.

ITIL 3

ITIL 3 wird von der OGC vorangetrieben, nachdem die Veröffentlichungen von ITIL 2 bereits breite Akzeptanz erfahren haben. Ziel der neuen Versionen sind Veröffentlichungen einer überarbeiteten Bibliothek bis zum Jahre 2007. Die OGC als Dachorganisation von ITIL hat dafür ein eigenes Großprojekt initiiert: das ITIL Refresh-Projekt. Der entsprechende Public Scoping-Report stellt den bisherigen Projekt-Verlauf, die weitere Planung und die bisherigen Ergebnisse dar. Die neue IT Infrastructure Library wird sich stärker am Begriff des Service Lifecycle ausrichten. Dementsprechend werden fünf neue Kernbücher mit den folgenden Titeln erscheinen:

- Service Strategy
- Service Design
- Service Transition
- Service Operations
- Continual Service Improvement

(Fortsetzung)

Der Themenbereich Service Strategy kann als Einstiegspunkt und zentrale Veröffentlichung der Reihe angesehen werden. Die Publikationen aus dem ITIL-Kompendium werden in insgesamt vier Schüben („Tranches“) erscheinen:

- Tranche A (bis Herbst 2006)
  - Integrierte Prozess-Grafiken
  - Glossar
  - High-Level-Einführung
  - What's new
- Tranche B (Februar 2007)
  - die Kernbücher zum Thema Service Lifecycle
- Tranche C (kontinuierlich nach Veröffentlichung der Kernbücher)
  - Pocket Guides
  - Case Studies
  - Vorlagen
  - Ausbildungshilfen
- Tranche D (Sommer 2007)
  - Executive Introduction to Service Management als ITIL-Einführung für die Zielgruppe im Management

2.1 Was ist ITIL?

Bei der grundsätzlichen Frage, wie IT-Umgebungen aufgebaut und betrieben werden sollen, tauchen diverse Schlagworte immer wieder auf. Dazu gehören ITIL, ITSM, BS15000 und neuerdings auch ICT. Bei all diesen miteinander in Verbindung stehenden Ansätzen in Bezug auf Prozesse und auch das IT Service Management ist eine Voraussetzung für die erfolgreiche Umsetzung die unabdingbare Bereitschaft zum Wandel in Richtung Kunden- und Serviceorientierung. Dies bedingt in vielen Unternehmen eine Anpassung der vorherrschenden Servicekultur. Mit Hilfe von ITIL soll zudem eine eindeutige Begriffswelt im Service Management-Bereich geschaffen werden. So wissen Anwender und Kunden, was sie von einer IT-Organisation und ihren Dienstleistungen erwarten können. Dies ermöglicht ein gemeinsames und allgemeines Verständnis der Aufgaben von Seiten der IT-Betreiber. Letztendlich sprechen alle Beteiligten die „gleiche Sprache“.

Dieser Aufgabe kam Ende der 80er Jahre die CCTA (Central Computer and Telecommunications Agency) durch die Veröffentlichung der ITIL-Dokumentationen nach. Dabei wurden die dokumentierten Prozesse nach dem Best Practice-Ansatz optimiert. Das Potenzial von ITIL vergrößerte sich, als die aus den behördlich geprägten Strukturen stammende Beschreibung den Bedürfnissen der Industrie angepasst wurde. Durch diese Öffnung wurde ITIL zu dem international anerkannten De-facto-Standard. Im Gegensatz zum De-jure-Standard, der über ein Normungsinstitut offiziell abgesegnet wird, stützt sich ein De-facto-Standard auf seine Verbreitung.

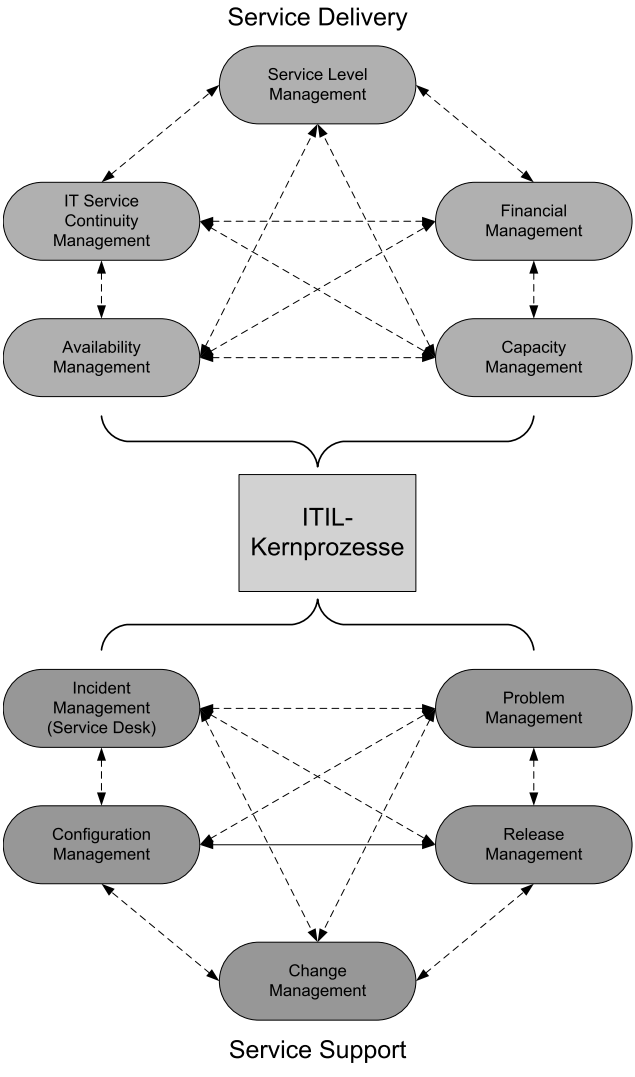


Abbildung 2.2: ITIL-Übersicht: Prozesse und Funktion

Die ITIL-Bibliothek umfasste ursprünglich mehr als 40 Bücher, die dann in Bezug auf Service Support (Betrieb von IT-Diensten) und Service Delivery (Bereitstellung von IT-Diensten) als Kern zusammengefasst wurden (*siehe Abbildung 2.3*). Sie beschreiben die Anforderungen, die notwendig sind, um IT-Dienstleistungen auf effektive Weise bereitzustellen. Während andere IT-Standards sich in erster Linie mit der Kompatibilität von Produkten und Services auseinandersetzen, handelt es sich bei ITIL um eine Regelsammlung zur Prozesseinführung und -verbesserung in einer sehr umfassenden Form.

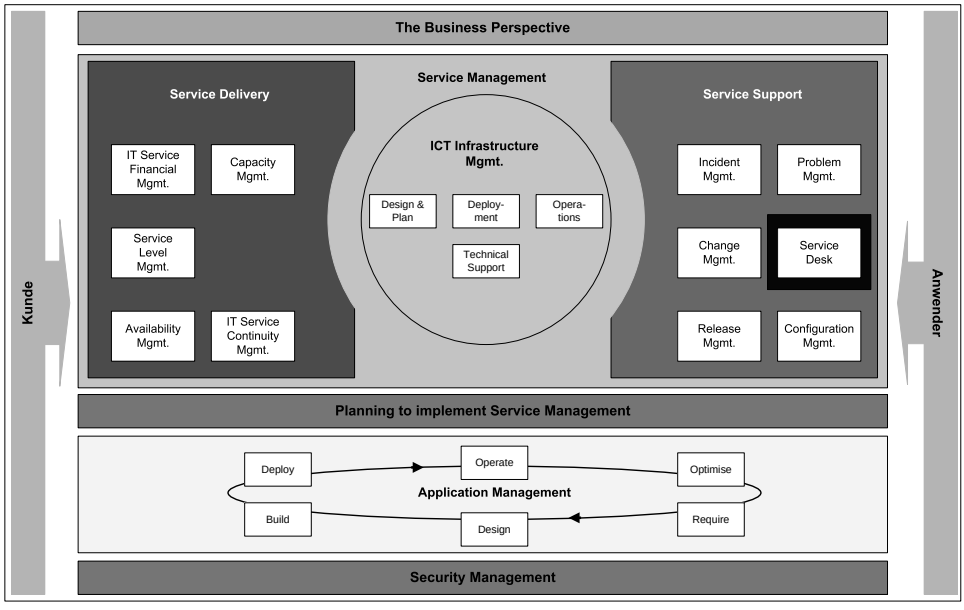


Abbildung 2.3: ITIL im Sinne des Service Management

ITIL liefert nicht das „Wie“, sondern das „Was“ zur Erbringung einer bedarfsgerechten IT Service-Leistungserbringung. Daher muss ein Unternehmen die Modelle und Vorgaben aus der ITIL-Bibliothek zunächst an seine jeweiligen Bedürfnisse anpassen. Die Über- und Umsetzung muss die Organisation jedoch selber leisten. Bereits bestehende Serviceprozesse berücksichtigt das Regelwerk ebenso wenig wie den Umstand, dass unterschiedliche Produkte unterschiedliche Anforderungen und Prozesse mit sich bringen. Hier ist zwischen Flexibilität und geringem Detaillierungsgrad abzuwägen. Aus diesen Gründen wird ITIL als Framework bezeichnet. Es gibt lediglich den Rahmen vor, den sich die Unternehmen als Schablone und Empfehlungsgrundstock zunutze machen können.

2.1.1 Historie des ITIL

Bereits Anfang der 80er Jahre suchten Mitarbeiter des britischen Staates im Auftrag der damaligen (Thatcher-)Regierung nach Möglichkeiten, um die Kosten der IT im staatlichen Bereich zu reduzieren. Ziel waren höhere Effizienz und geringere Kosten, ohne dabei die Entwicklungs- und Innovationskraft der neuen Technologien zu gefährden.

Das Projekt wurde als Government Information Technology Infrastructure Management Method (GITIMM) vorgestellt und 1986 offiziell gestartet. 1988 wurde von der GITIMM-Gruppe ein Benutzerforum installiert, aus dem sich später das itSMF (IT Service Management Forum) entwickelte. Im Rahmen der eigentlichen GITIMM-Entwicklung, die durch reichhaltigen Erfahrungsaustausch mit dem privaten Sektor begleitet wurde, ist die auch heute noch aktuelle Unterscheidung zwischen Maßnahmen für Service Support und Service Delivery entstanden. Etwa zeitgleich wurde das GITIMM-Projekt umbenannt. Die alte GITIMM lebte als IT Infrastructure Library (ITIL) weiter.

In den Folgejahren entwickelte sich ITIL als Maßstab der Leistungserbringung in privaten Unternehmen und ITSM (IT Service Management) etablierte sich zu einem Begriff, der als Sammelbecken für alle Maßnahmen der Beteiligten rund um ITIL Verwendung fand. Mitte der 90er Jahre kristallisierte sich itSMF als herstellerunabhängiges und neutrales Gremium mit der Aufgabe heraus, Prinzipien und Leitlinien im ITSM zu verbreiten und eine Plattform für den Informationsaustausch zu bilden.

2.1.2 Warum ITIL?

IT Service Management bedeutet, die Qualität und Quantität des IT Service zielgerichtet, geschäftsprozessorientiert, benutzerfreundlich und kostenoptimiert zu überwachen und zu steuern. Dies heißt, dass die Gesamtheit aller zur Abwicklung des Geschäftsprozesses eingesetzten Ressourcen der unternehmensinternen IT zur Optimierung der Betriebsabläufe herangezogen werden. Der Zweck der IT begründet sich somit in der optimalen Unterstützung der Geschäftsprozesse bei der Erreichung der Unternehmensziele.

Der große Nutzen von ITIL besteht in der Qualitätsverbesserung auf allen Organisationsebenen. ITIL beschreibt ein systematisches und professionelles Vorgehen für das Management von IT-Dienstleistungen. Die Library stellt nachdrücklich die Bedeutung der wirtschaftlichen Erfüllung der Unternehmens-Anforderungen in den Mittelpunkt. ITIL ist niemals Selbstzweck. Die Arbeit nach den in ITIL beschriebenen „Best Practice"-Prozessen bringt der Organisation folgende Vorteile:

- Unterstützung der Geschäftsprozesse und der Aufgaben der daran beteiligten Mitarbeiter
- Definition von Funktionen, Rollen und Verantwortlichkeiten im IT Service-Bereich
- Weniger Aufwand bei der Entwicklung von Prozessen, Prozeduren und Arbeitsanweisungen
- Flexible IT-Dienstleistungen, die den Anforderungen des Business entsprechen
- Höhere Kundenzufriedenheit durch bessere und messbare Verfügbarkeit und Performance der IT-Servicequalität
- Höhere Produktivität und Effizienz durch den gezielten Einsatz von Wissen und Erfahrung
- Basis für eine Quality-Management-Systematik im IT Service Management
- Höhere Mitarbeiterzufriedenheit und niedrigere Personalfluktuation
- Bessere Kommunikation und Information zwischen den IT-Mitarbeitern und ihren Kunden (Business IT Alignment) durch die Benutzung der gleichen Sprache sowie durch aktuellen Informationsaustausch
- Training und Zertifizierung der IT Service Professionals
- Internationaler Erfahrungsaustausch

Diese Punkte erscheinen natürlich nicht nur kleinen Unternehmen als Notwendigkeit. Auch die Frage der externen Vermarktung von IT Services bzw. die Betrachtung der Wettbewerbstauglichkeit der IT-Abteilungen sind von Interesse und stehen vermehrt im Brennpunkt (z.B. IT-Outsourcing).

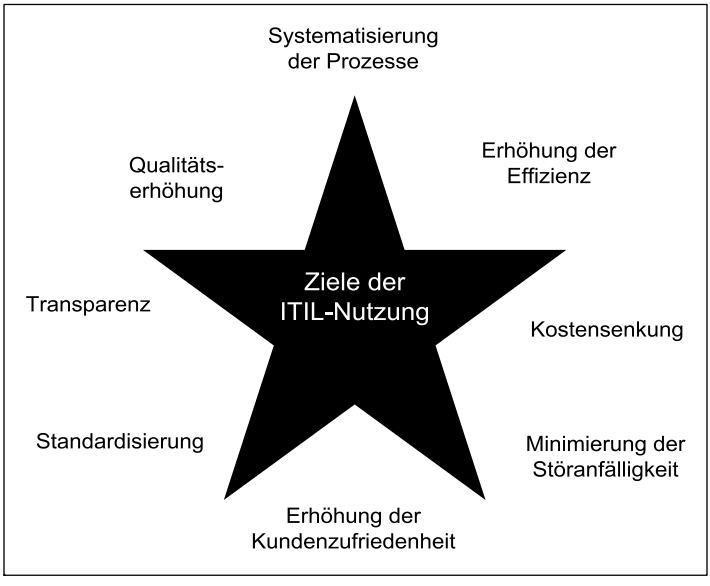


Abbildung 2.4: Ziele der ITIL-Nutzung

IT als Servicegeschäft zu betrachten, sollte vorrangiges Ziel der Angestellten und Betreiber in diesem Bereich sein. Sie sollten in der Lage sein, sich in den Dienst des Anwenders zu stellen und den Blick auf das eigentliche Geschäftsziel zu richten.

Im Laufe der vergangenen Jahre gab es eine regelrechte Ausgründungswelle von IT-Konzerntöchtern und/oder die Zuwendung zum Thema IT-Outsourcing. IT Services wurden zu Serviceeinheiten gebündelt; oft entstanden sie durch Zusammenlegung mehrerer IT-Bereiche, meist sogar über Standorte hinweg. Auch die Aufsplittung der Aufgaben auf Spezialisten für die IT-Infrastruktur und für IT-Anwendungsservices ist anzutreffen. Geführt werden entweder als Profit- oder Cost-Center oder als rechtlich selbstständige Unternehmen mit unternehmerischem Freiraum. Trotzdem muten diese Aktivitäten kaum mehr als der Auftakt zur Restrukturierung der IT-Aufgaben an. IT-Unternehmen, sofern sie Drittmarktkunden bedienen, wetteifern mit unterschiedlichen Konkurrenten, die jeweils spezifische Stärken aufweisen. Global agierende Anbieter, die standardisierte Dienstleistungen zu attraktiven Preisen anbieten, teilen sich den Markt mit Spezialisten, die sich auf Nischen nach Branchen oder Fachgebieten konzentrieren und nicht dem Ehrgeiz verfallen, jeden Service optimal anbieten zu können. Es besteht demnach eine Marktstruktur, wie sie für reife Märkte typisch ist. In diesem Umfeld muss ein IT-Serviceanbieter seinen Weg finden und erfolgreich beschreiten. ITIL ist ein mögliches Werkzeug in diesem Dschungel, das oftmals Ordnung in einen Wald bringt, den viele IT-Leute vor lauter Bäumen nicht mehr zu sehen scheinen. Denn letztendlich geht es doch darum, den Servicegedanken in (möglichst) optimaler Art und Weise im Kundenumfeld umzusetzen.

ITIL erspart Unternehmen die Mühe, neue Konzepte zu suchen und eigene Lösungen zu erarbeiten, da sich die Modelle bereits in der Praxis bewährt haben und so eine gewisse Planungs- und Prozesssicherheit bieten – auch wenn entsprechende individuelle Anpassungen und Anforderungsumsetzungen notwendig sind.

2.1.3 ITIL-Kernprozesse

ITIL und die Arbeit der OGC bzw. CCTA stehen nicht losgelöst von der Arbeit benachbarter Institutionen. Auch andere Bereiche haben sich bereits mit ITIL und seinem Nutzen auseinandergesetzt. Das British Standard Institute (BSI; vergleichbar dem Deutschen Institut für Normung DIN) spricht in seiner Beschreibung des BS 15000 von zehn „ITIL-Disziplinen“, die es zu erfüllen gilt. Dabei findet eine grundlegende Unterscheidung zwischen Service Support und Service Delivery statt. Gleichzeitig ist es aber so, dass die ITIL-Bibliothek nicht auf diese Bereiche beschränkt bleibt (*siehe Abbildung 2.5*). Für ein effizientes IT Service Management und dessen Zertifizierung sind die folgenden Dokumente zu berücksichtigen:

- IT Infrastructure Library (ITIL): Best Practice für IT Service Management. Die folgenden Dokumente geben eine Übersicht der ITIL-Oberbereiche:
  - Service Support
  - Service Delivery
  - Planning to Implement IT Service Management
  - Application Management
  - ICT Infrastructure Management
  - Security Management
  - The Business Perspective

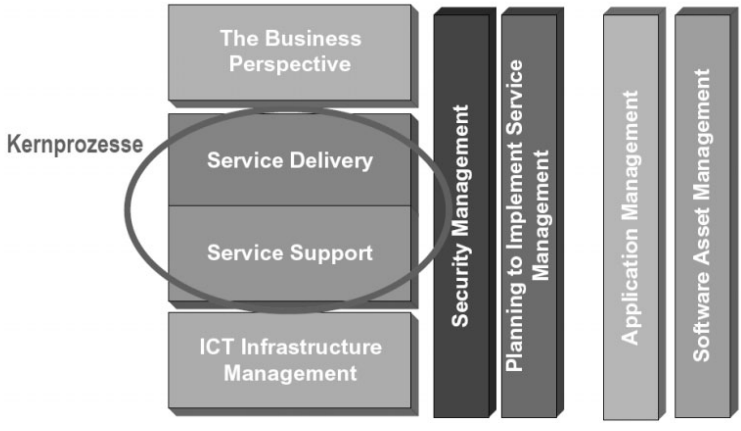


Abbildung 2.5: ITIL-Kernprozesse

- BS 15000-1:2002: IT Service Management: Specification for Service Management. Dieses Dokument referenziert vornehmlich auf die ITIL-Dokumente.

- BS 15000-2:2003: IT Service Management. Code of Practice for Service Management. Dieses Dokument beinhaltet Hinweise für das praktische Anwenden der Norm BS 15000-1.
- PD 0005:2000: IT Service Management. A Manager's Guide. Dieses Dokument enthält Management Erklärungen zur Umsetzung des BS 15000-Standards.
- PD 0015:2002: IT Service Management. Self-Assessment Workbook. Dieses Dokument dient Unternehmen, die sich nach BS 15000 zertifizieren lassen möchten. Es beinhaltet Fragen, die für eine Selbstbeurteilung der aktuellen Situation im Unternehmen hilfreich sind.

Bei der Erstellung der britischen Standards für das IT Service Management ist das BSI bestrebt, sich an die IT Infrastructure Library der OGC zu halten, um so die Dokumente konsistent zu halten.

BS 15000

BS 15000 ist ausgerichtet an den Prozessbeschreibungen, wie sie durch die IT Infrastructure Library (ITIL) des Office of Government Commerce (OGC) beschrieben sind, und ergänzt diese.

> *„BS 15000 ist ein allgemein anerkannter Standard, mit dem jede IT-Organisation dem Unternehmen beweisen kann, dass die Service Delivery-Prozesse nach den Best Practice-Richtlinien ausgeführt werden." – Gartner*

Offiziell bekannt gegeben wurde der BS 15000 am 6. November 2000 auf der Konferenz des IT Service Management Forums (itSMF) in Birmingham, England. Seit dem 1. Juli 2003 wurde das BS 15000-Zertifizierungsschema formell veröffentlicht. BS 15000 wendet sich sowohl an die Anbieter von IT Service Management-Dienstleistungen als auch an die Branchen, die ihre IT-Aufgaben entweder outsourcen oder selbst managen. Basierend auf ITIL spezifiziert Service Management-Prozesse und bildet gleichzeitig eine Basis für die Durchführung entsprechender Assessments.

BS 15000 spezifiziert eine Reihe zusammenhängender Managementprozesse und soll die Grundlage für die Auswertung des gemanagten Services bilden. Relationship Management (als Kernaspekt des Service Support) wird mit diesem Standard angesprochen, insbesondere für Branchen, die Qualitätsservice liefern oder benötigen. Diese Publikation eines Code of Practice wurde von BSI und itSMF in Zusammenarbeit mit dem OGC und weiteren Beteiligten ausgearbeitet. Das itSMF und das BSI sind auch die führenden Organisationen, die daran arbeiten, einen neuen messbaren Standard für die Industrie einzurichten, der auf der IT Infrastructure Library (ITIL) basiert.

Die einzelnen ITIL-Bücher bieten erweiterte Informationen zu den Themen, die im Code of Practice angesprochen werden, und jedes von ihnen wird durch das Taschenbuch für Service Management des itSMF unterstützt. Ergänzt wird das Ganze durch einen Code of Practice for IT Service Management (Verfahrensregeln) im DISC PD 0005:1998.

IT-Dienstleister und IT-Betreiber können mit Hilfe eines ITIL/BS-15000 Assessment die Leistungsfähigkeit ihrer IT-Prozesse in ausgewählten Prozessbereichen ermitteln und generelle Schwachstellen von IT-Prozessen innerhalb ihrer Organisation aufdecken. Darüber hinaus sind sie in der Lage, aktive Unterstützung der Führungsverantwortlichen für operationale Verbesserungsmaßnahmen der IT-Infrastruktur zu erhalten und ihre IT-Infrastruktur transparenter zu gestalten.

2.1.4 Service Support und Service Delivery

In den beiden historischen Hauptkategorien (Service Support und Service Delivery) sowie mehreren Unterkategorien wird beschrieben, welche Rollen und Verantwortlichkeiten eine IT-Abteilung erfüllen sollte (*siehe Abbildung 2.6*). Im Bereich Support geschieht dies in Bezug auf die folgenden Kapitel:

- Configuration Management
- Problem Management
- Change Management
- Incident Management
- Release Management

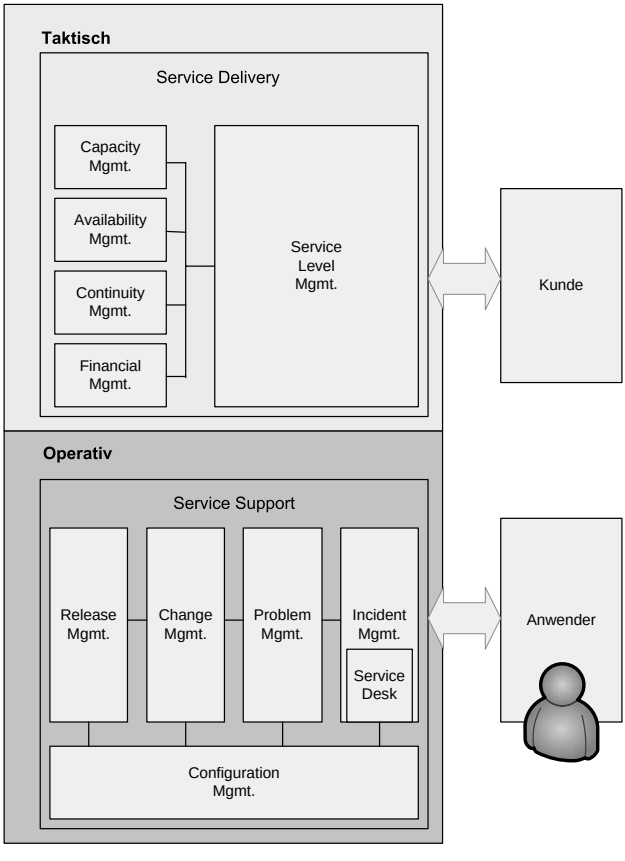


Abbildung 2.6:
Prozesse nach ITIL

Im Bereich Service Delivery wird unterschieden zwischen:

- Service Level Management
- Capacity Management
- Continuity Management
- Availability Management
- Financial Management

Dem Thema Service Desk kommt dabei eine Sonderrolle zu, da es sich um eine Funktion und nicht um einen Prozess handelt.

Auch das Security Management nimmt eine Sonderstellung ein, da es nicht innerhalb des Kernprozesses Service Delivery zu finden ist. Diesem Prozess wurde ein eigenes Buch gewidmet. Grob kann es jedoch dem Bereich Service Delivery zugeordnet werden. Für die ITIL-Basis-Zertifizierungsprüfung wird das Security Management den Kernprozessen zugeordnet.

Im Folgenden werden die IT Service Management-Prozesse von ITIL kurz erläutert:

- Service Desk (Funktion): Das Service Desk stellt die Erreichbarkeit der IT-Organisation sicher. Es ist die einzige Schnittstelle (Single Point of Contact, SPOC) zum Anwender, hält ihn auf dem Laufenden und steht für Rückfragen zur Verfügung. Es koordiniert die benachbarten Supporteinheiten und kann Aufgaben aus anderen Prozessen übernehmen, z.B. Incident Management, Change Management, Configuration Management. Das Service Desk selber ist kein Prozess, sondern eine Funktion der IT Service-Organisation.

  Es werden neben Störungen auch alle Anfragen (Service Requests) der Anwender über ein Service Desk erfasst, erste Hilfestellung geleistet und gegebenenfalls die weitere Bearbeitung in den nach folgenden Supporteinheiten koordiniert. Des Weiteren stellt das Störungsmanagement der Geschäftsführung Managementinformationen zur Verfügung.

- Incident Management: Das Incident Management hat die Aufgabe, einen ausgefallenen oder beeinträchtigten, sprich qualitativ verschlechterten Service dem Anwender so schnell wie möglich wieder in vereinbarter Qualität zur Verfügung zu stellen (*siehe Abbildung 2.7*).

  Hier ist die Beseitigung der Ursache zweitrangig; auch eine Störungsumgehung zählt (aus der Sicht des Anwenders) als Beseitigung der Störung. Es geht darum, den IT-Service so schnell wie möglich wiederherzustellen und die Störungen zu erfassen.

- Problem Management: Das Problem Management unterstützt das Incident Management, indem bei auftretenden Störungen die eigentlichen Ursachen analysiert und anschließend nachhaltig beseitigt werden können. So werden Lösungen entwickelt und zur Umsetzung an das Change Management weitergeleitet.

  Auch die Dokumentation der bekannten Fehler und deren Beseitigung gehört zu den Aufgaben dieses Prozesses, der damit wiederum die Effizienz des Service Desk steigern kann. Zudem befasst sich das Problem Management mit der Störungsvermeidung (proaktives Problem Management) durch Trendanalyse, Monitoring

oder weitere vorbeugende Maßnahmen. So wird das Problem Management in die drei Bereiche Problem Control, Error Control und proaktives Problem Management unterteilt (*siehe Abbildung 2.8*).

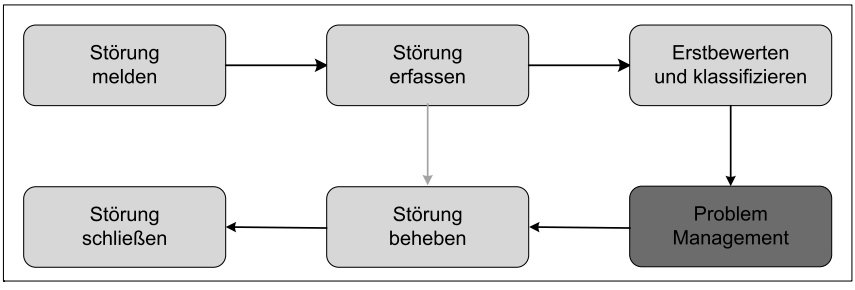


Abbildung 2.7: Incident Management

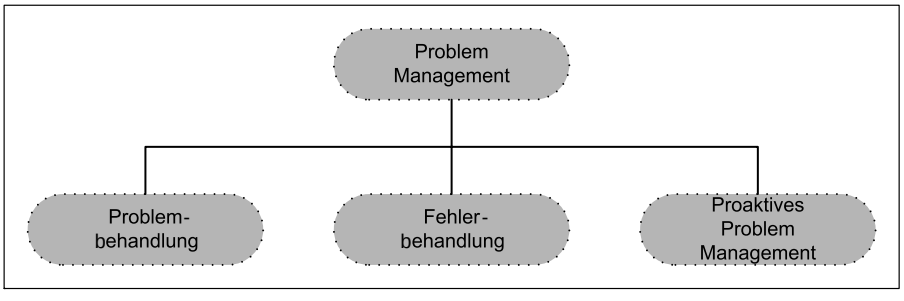


Abbildung 2.8: Problem Management

Es geht bei diesem Prozess um die Ursachenforschung. Ist die Ursache bekannt, ist zu entscheiden, ob die Beseitigung der Problemursache über einen Change beseitigt werden muss.

- Change Management: Hier werden Änderungen an der IT-Infrastruktur und ihren Komponenten (Configuration Items) autorisiert und dokumentiert, die der Problemlösung dienen oder aufgrund von Reaktionen auf neue Kundenanforderungen und Geschäftsabläufen angestoßen werden. Die Reihenfolge der einzelnen Schritte wird geplant und kommuniziert, um eventuelle Überschneidungen rechtzeitig zu erkennen. Dabei spielt neben dem Change-Manager das Change Advisory Board (CAB) eine wichtige Rolle. Nach erfolgter Autorisierung der Änderung ist es Aufgabe des Change Management-Prozesses, die Koordination der Durchführung und die Abnahme der Änderungen durch den Kunden sicherzustellen. So ist es möglich, den Änderungsprozess zu kontrollieren und Auswirkungen auf den produktiven Betrieb zu minimieren.

- Configuration Management: Die für das IT Service Management notwendigen Informationen werden als servicerelevante IT-Komponenten vom Configuration Management registriert, verwaltet und anderen Service Management-Prozessen bereitgestellt. Dabei geht es auch um ihre Beziehungen zueinander, die vom Configuration Management in einer Datenbank (Configuration Management Database, CMDB) erfasst und beschrieben werden (*siehe Abbildung 2.9*). Sie beinhaltet Informationen zu eingesetzter Hardware, Software, Dokumentationen, Prozessen und Prozeduren und stellt diese mit logischen Verknüpfungen zur Verfügung, die weit über eine reine Inventarisierung hinausgehen. Dem Configuration Management fällt damit eine zentrale Rolle zu. Ziel des Konfigurationsmanagements ist die Unterstützung anderer ITIL-Funktionen durch die Bereitstellung eines möglichst detaillierten Modells zur Abbildung der IT-Infrastruktur.

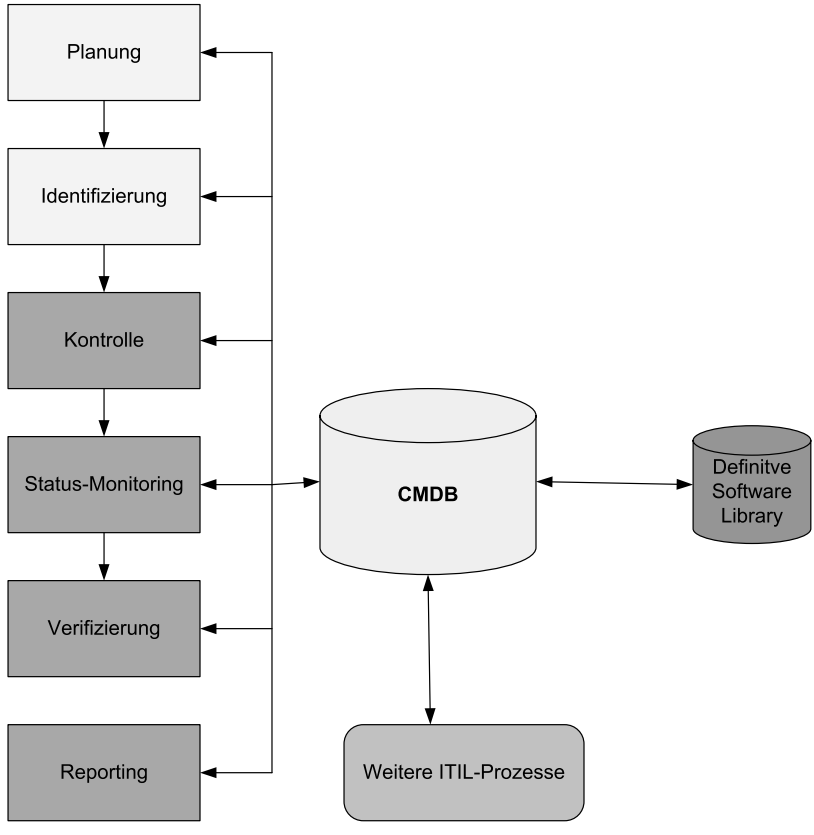


Abbildung 2.9: Configuration Management und die zentrale Rolle der CMDB

Bei seiner Aufgabe muss das Configuration Management daher deutlich über das Asset Management hinausgehen, da nicht nur die Vermögenswerte bilanztechnisch (im Sinne einer Inventarisierung) erfasst werden, sondern auch Daten wie Standort, Verknüpfung mit anderen Komponenten, Spezifikationen etc. erforderlich sind.

- Release Management (auch Control & Distribution genannt): Durch die kontrollierte Verteilung, Installation und Wartung von Soft- und Hardware (*siehe Abbildung 2.10*) soll sichergestellt werden, dass nur autorisierte, kompatible und einheitliche Versionen im Einsatz sind. Zudem steuert das Release Management die Einführung dieser Items, so dass beispielsweise Anwender und Servicemitarbeiter sich rechtzeitig auf die Änderung einstellen können (z.B. Rolloutverfahren) und die Anzahl der Änderungen gering gehalten wird (z.B. durch Releasepakete). Durch die Zusammenarbeit mit dem Configuration Management können Dokumentationen zeitnah aktualisiert werden. Außerdem sind die Mitarbeiter in einer homogenen Softwarelandschaft in der Lage, falsche Versionen, nicht genehmigte Kopien, illegale Software, Viren und unerlaubte Eingriffe leichter zu erkennen.

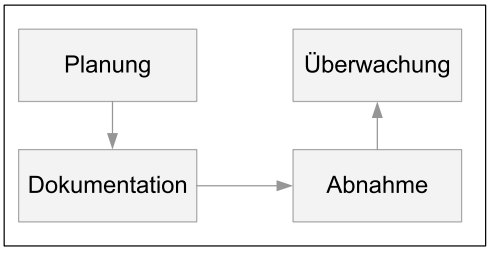


Abbildung 2.10:
Release Management

- Service Level Management: An der Schnittstelle zum Kunden werden hier die Serviceanforderungen aufgenommen und deren Umsetzung mit der IT Service-Organisation (Operational Level Agreements, OLA) sowie externen Dienstleistern (Underpinning Contracts, UC) abgesichert. Auf dieser Basis werden die Service Level Agreements (SLAs) mit dem Kunden vereinbart. Ein SLA regelt in wenigen, nicht technischen Worten u.a. die Rechte und Pflichten sowohl für den Servicegeber als auch für den Servicenehmer. Es dokumentiert die Serviceparameter, Kennzahlen und Zielwerte, beschreibt die Messverfahren und definiert den Gültigkeitszeitraum etc. Grundlagen für die Erstellung der SLA ist der Servicekatalog. Zum Service Level Management gehören zudem die Überwachung der Dienstleistungsqualität und eine entsprechende Berichterstattung (Reporting).
- Availability Management: Hier werden die Anforderungen aus den SLAs in einen Plan zur Erhaltung der Service-Verfügbarkeit umgesetzt. Dies wird erreicht, indem mögliche Ausfälle auf Basis von Analysen vorausberechnet werden, deren Risiko bewertet und dann entsprechende Maßnahmen zur Sicherung der geforderten Verfügbarkeit entworfen und umgesetzt werden. Dazu gehören auch das Absichern durch Supportverträge mit Lieferanten, rechtzeitige Initiierung von Changes sowie die Optimierung der IT-Infrastruktur und der dazugehörigen Arbeitsabläufe.
- Capacity Management: Das Capacity Management erstellt aus den Geschäftsanforderungen (z.B. Antwortzeiten) den notwendigen Service-Bedarf und leitet darauf basierend einen Ressourcenplan ab. Dabei wird in der Regel in Bezug auf Business, Service und Resource Capacity Management unterschieden.

  Unter Einbeziehung der Ergebnisse aus Lasttests (Performance Management) wird eine optimale Lastverteilung auf die bestehenden Systeme ermittelt und mit Hilfe von Tuning und Workload Balancing sichergestellt. Weitere Aufgaben sind Application Sizing, Service Modellierung und Bedarfsmanagement (Demand Management).

- IT Service Continuity Management (ITSCM): Die Aufgabe des IT Service Continuity Management besteht darin, basierend auf einer Risikoanalyse schützenswerte IT-Vermögenswerte zu identifizieren, risikosenkende Maßnahmen zu ergreifen und einen Notfall-Plan zu erstellen, so dass bei Eintritt eines solchen Notfalls der Service kontrolliert wieder in Betrieb genommen und aufrecht erhalten werden kann. Dabei ist ITSCM in dem übergeordneten Prozess Business Continuity Management eingebettet. Die Notfallmaßnahmen sind dem Change Management unterstellt und müssen regelmäßig überprüft werden.
- Financial Management for IT Services (Cost Management): Der Prozess Financial Management for IT Services umfasst Budgetierung, Kostenrechnung (Accounting) und Leistungsverrechnung (*siehe Abbildung 2.11*).

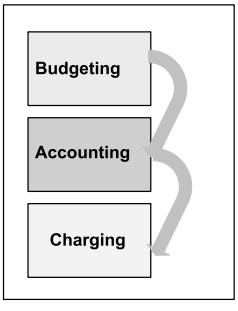


Abbildung 2.11:
Financial Management

Ziel der Kosten- und Leistungsverrechnung ist es, die zur wirtschaftlichen Steuerung der IT Services tatsächlich entstandenen Kosten transparent aufzuzeigen und dem Kunden die erbrachte Leistung in Rechnung zu stellen. So kann die Effizienz des Einsatzes der IT-Infrastruktur direkt gemessen werden. Besondere Bedeutung hat dieser Aspekt durch die Betrachtung der TCO (Total Cost of Ownership) bekommen.

- Security Management: Dieser Bereich entstammt ursprünglich dem Service Delivery-Set und ist wegen seiner historischen Bedeutung eng damit verknüpft (*siehe Abbildung 2.12*). IT Security Management beschäftigt sich mit der Einführung und Umsetzung eines definierten Sicherheitsniveaus für die IT Services. Um die internen und kundenspezifischen Wünsche des benötigten Sicherheitslevels zu ermitteln, ist eine Risikoanalyse notwendig. Der interne, minimale Sicherheitsanspruch wird dabei als IT-Grundschutz bezeichnet. Darüber hinausgehende Sicherheitsbedürfnisse des Kunden müssen individuell herausgearbeitet werden.

  Das Security Management befasst sich also mit dem weiten Gebiet des Datenschutzes und der Datensicherheit. Während sich der Datenschutz mit der Absicherung der Daten vor unberechtigtem Zugriff oder unberechtigter Verwendung befasst, ist es Aufgabe der Datensicherheit, die technische Unversehrtheit der Daten zu sichern. Das Sicherheitsmanagement umfasst sowohl organisatorische als auch technische Elemente.

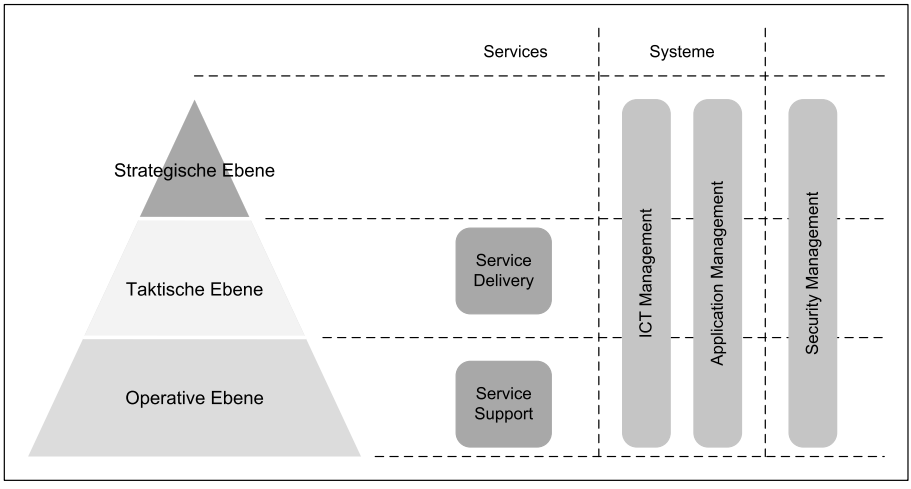


Abbildung 2.12: Einordnung des Security Management

- Risikomanagement (Risk Management): Das Risikomanagement gehört nicht zu den Kernfunktionen von ITIL, ist aber wegen seiner zentralen Bedeutung für die IT mit dessen Funktionen eng verknüpft. Es handelt sich hierbei um ein Überwachungssystem, das als Frühwarnsystem vor Entwicklungen warnen soll, die den Fortbestand der Organisation gefährden oder sich zumindest wesentlich auf die Vermögenslage der Organisation auswirken. Ein Risikomanagement muss, um seinen Zweck voll erfüllen zu können, die Organisation ganzheitlich betrachten und geht daher über die IT hinaus. Das Risikomanagement stellt zum Beispiel der Notfallplanung wichtige Informationen zur Risikoanalyse zur Verfügung.

Bei Support-Prozessen wie Incident Management und Problem Management hat sich ITIL laut zahlreicher Studien bereits etabliert. Je weiter sich der Betrachter jedoch vom Anwender-Support entfernt, desto geringer ist oft der Reifegrad der Prozesse. Das gilt für das Change Management und mehr noch für das Release Management. Erst ansatzweise implementiert erscheinen die Disziplinen, die sich auf den Applikationsbetrieb ausrichten. Unter den Service Delivery-Prozessen, die dafür sorgen sollen, dass die IT-Leistung tatsächlich dem Bedarf der Kundenorganisation entspricht, ist das Service Level Management relativ gut ausgeprägt. Das gilt auch für Prozesse zur IT-Sicherheit wie Availability Management und IT Service Continuity Management.

2.1.5 ITIL-Einführung im Unternehmen

ITIL schafft die Möglichkeit, die Prozesse im IT Service Management übersichtlich und transparent darzustellen, so dass sich der Überblick vor allem bei komplexen Prozessen verbessert, die über die Grenzen von Zuständigkeitsbereichen wie z.B. Fach- und IT-Abteilungen hinausgehen. Zudem wird ITIL als Prozesslandschaft gesehen, die als Grundlage und Voraussetzung für eine nachhaltige Prozessverbesserung dient. Sie sollten sich jedoch der Tatsache bewusst sein, dass ITIL kein

Selbstzweck ist. Halten Sie nicht zu starr an den ITIL-Empfehlungen fest, sondern nehmen Sie diese als Framework an. Das ITIL-Regelwerk soll vor allem Prozesse unterstützen und sie transparent machen, um sie in eine adäquate und sinnvolle Relation zu den Geschäftsprozessen zu setzen.

Die Einführung dieser Prozesse zum IT Service Management mit Hilfe von ITIL stellt hohe Anforderungen an alle Beteiligten und das Unternehmen und erstreckt sich stets über einen längeren Zeitraum. Die Gestaltung neuer Prozesse setzt eine Analyse der bestehenden Abläufe voraus. Dies gestaltet sich in vielen Fällen schwierig, wenn die Verfahrensweisen bisher unzureichend dokumentiert und unterschiedliche Begriffswelten verwendet wurden. Im nächsten Schritt sind die Anforderungen der Nutzer zu erheben. Dazu müssen die Vorstellungen der Nutzer in präzisen Service Level Agreements fixiert werden. Wenn die Prozesse definiert wurden, die zur Erfüllung der Anforderungen notwendig sind, müssen die Prozessverantwortlichen mit den nötigen Schwerpunkten geschult werden, um die Prozesse anschließend einzusetzen.

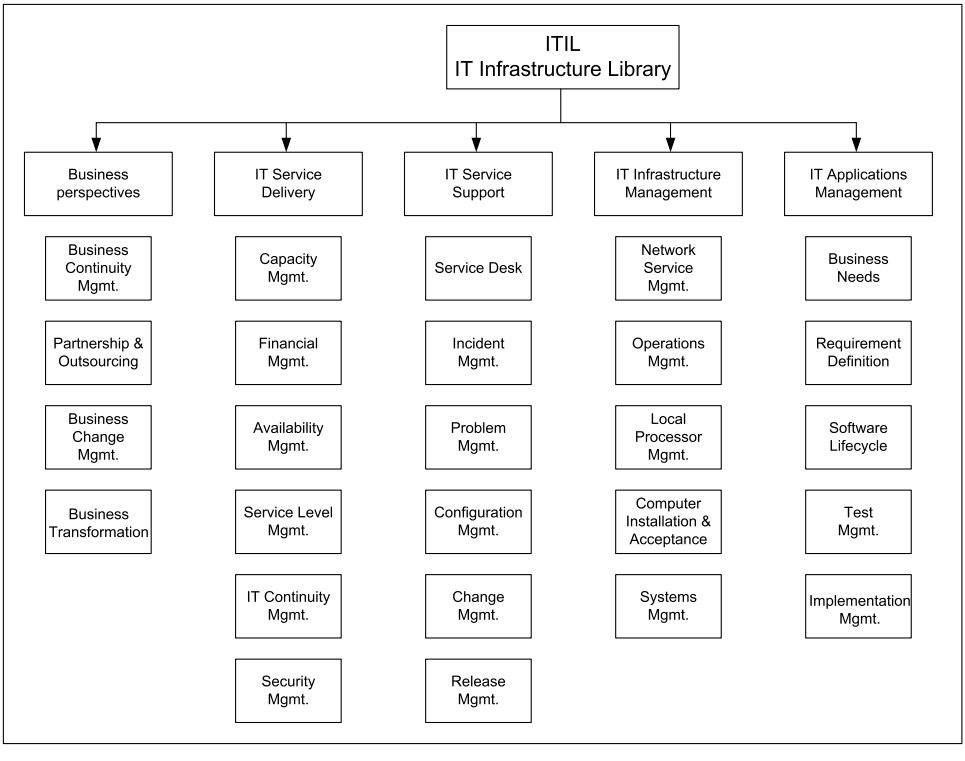


Abbildung 2.13: ITIL-Baum

Die einzelnen Prozesse werden in den meisten Fällen schrittweise eingeführt, indem nach und nach bestehende Vorgehensweisen durch ITIL-konforme Prozesse abgelöst werden. Die wenigsten Unternehmen sehen die Notwendigkeit, alle zehn ITIL-Prozesse plus Service Desk-Funktion einzuführen. Diese Einschätzung kann

auch durchaus korrekt sein. ITIL soll als Leitfaden (Best Practice) genutzt werden, dort, wo es um die Beseitigung von Schwachstellen und die Optimierung von Prozessen geht.

Die Umsetzung dieses Vorgehens ist im Unternehmen in jedem Fall als Projekt aufzusetzen. Zur Steuerung ist eine geeignete Projektmanagement-Methode zu nutzen. Eine Untersuchung des CIO-Magazins vom 13.7.2004 zeigte, dass bei 70 % der ITIL-Einführungen der Zeitplan überschritten wurde. Bei 45 % der Projekte wurde er um 10 bis 50 % überschritten, bei 5 % der Projekte sogar um 100 bis 300 %. ITIL empfiehlt, zur Umsetzung dieser Projekte auf die skalierbare, flexible Projektmanagement-Methode PRINCE2 zurückzugreifen.

PRINCE2

PRINCE2 (PRojects IN Controlled Environments) ist eine strukturierte Methode für effektives Projektmanagement und der tatsächliche Standard innerhalb der britischen Behörden. International ist die Methode weit verbreitet und anerkannt, sowohl innerhalb der privaten als auch der behördlichen Sektoren. Sie wurde im Jahre 1996 eingeführt. Laut PRINCE2 wird der Projektmanagementprozess in acht Hauptprozesse unterteilt. Diese Unterteilung basiert auf den Phasen innerhalb eines Projekts und auf den verschiedenen Verantwortlichkeiten. Jeder Hauptprozess wird weiter unterteilt in Subprozesse.

Ein Mehrwert für den einzelnen Mitarbeiter liegt in der anschließenden international anerkannten Mitarbeiter-Zertifizierung. Hier gibt es verschiedene Stufen der Zertifizierung.

Trotz seines Ursprungs in den 80er Jahren ist ITIL für die meisten IT-Abteilungen noch neu. Die zahlreich angebotenen Kurse und Publikationen deuten jedoch darauf hin, dass der Best Practice-Ansatz von ITIL auch in Deutschland zunehmend Verbreitung findet. Studien, die auf die Verbreitung, Nutzungsmotive sowie die organisatorische Verankerung von ITIL in deutschen Unternehmen schließen lassen, werden immer stärker fokussiert und auch in den Fachmedien verbreitet. Vor zwei Jahren waren solche Publikationen dagegen eher rar gesät.

Aus den aktuellen Veröffentlichungen in den Fachmedien wird deutlich, dass sich der Nutzungsgrad von ITIL als unterschiedlich stark ausgeprägt präsentiert. Während einige Unternehmen ITIL nur in einzelnen Disziplinen einsetzen, nutzen andere bereits mehrere oder gar alle Prozesse, wie sie in ITIL beschrieben werden. Die Vorteile der Nutzung werden dabei sehr eindeutig genannt: Im Mittelpunkt steht die Erhöhung der Effizienz, gefolgt von der damit einhergehenden Kostensenkung und der Erhöhung der Kundenzufriedenheit. Nachteile zeigen sich vor allem durch den als zu hoch empfundenen Verwaltungsaufwand. In der Regel wird ITIL mit Hilfe eines top-down-Ansatzes im Unternehmen realisiert. Die Unterstützung des Managements liegt dabei in der Hoffnung auf eine erhöhte Kundenorientierung begründet.

Dabei hat sich der Fokus von ITIL verschoben: Lag in der Vergangenheit der Schwerpunkt auf Prozesseinführung und Normierung, rückt jetzt zunehmend die Wirtschaftlichkeit in den Vordergrund. Dabei darf nicht vergessen werden, dass sich diese Ziele über ITIL nur langfristig realisieren lassen.

2.1.6 Werkzeuge und Tools

In Bezug auf die Einführung und Verwendung von Tools, die die ITIL-Prozesse und -Funktionen unterstützen sollen, muss zunächst diskutiert werden, welche ITIL-Disziplinen das Unternehmen einführen möchte und in welcher Reihenfolge sie eingeführt und ausgeprägt werden. Bereits bei der Diskussion um die theoretischen ITIL-Grundlagen wird deutlich, dass z.B. i.d. Regel die Configuration Management Database (CMDB), eine Datenbank, die alle relevanten Informationen zu Infrastrukturkomponenten und deren Beziehung zueinander enthält, verwendet wird. Da diese Datenbank die IT-Umgebung in Bezug auf die existierenden Objekte (Configuration Items, CIs) und die dazwischen bestehenden Beziehungen abbildet, nutzen andere Prozesse diese Datenbank für für die eigenen Prozesse relevante Informationen. Mit Hilfe der zentralen Datenbank des Configuration Management können beispielsweise die Daten des Service Desk für Managementaufgaben ausgewertet bzw. als Verrechnungsgrundlage (Service Level Agreements) genutzt werden.

Diese Datenbank stellt ein essenzielles Werkzeug für das gesamte ITIL-Prozessportfolio dar. Sie ist das Herzstück der ITIL-Prozesse rund um das Configuration Management. Sie dürfen dabei allerdings nicht vergessen, dass daneben jeder ITIL-Bereich seine eigene Datenbank pflegen und betreiben kann, um dort die für die Umsetzung des Prozesses relevanten Informationen abzulegen (*siehe Abbildung 2.14*).

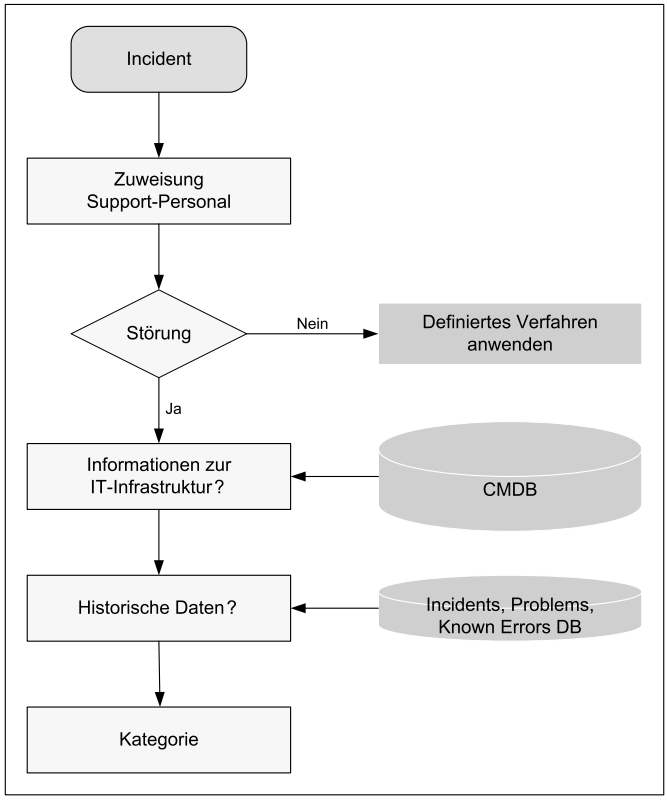


Abbildung 2.14: Datenbanken im Incident Management

Dabei muss betont werden, dass diese Datenbanken gleichzeitig kritische Erfolgsfaktoren darstellen:

- Die CMDB (Configuration Management Database) muss auf dem aktuellen Stand sein.
- Eine Known Error-Datenbank, in der Informationen zu bekannten Problemen, deren Lösungen oder entsprechende Workarounds abgelegt werden. Dies wird in den meisten Fällen über das Problem Management umgesetzt, die dem Incident Management bzw. Service Desk diese Informationen zur Verfügung stellen.

Doch auch die Prozesse des Bereiches Service Delivery kommen nicht ohne Werkzeuge aus. Es sind bereits ausgereifte Produkte erhältlich, um beispielsweise auf Basis der ITIL-Definitionen Service Levels festzulegen, diese an den Unternehmenszielen auszurichten und somit die Betriebskosten zu reduzieren. Wichtig ist dabei das reibungslose Zusammenspiel mit allen Tools weit über das reine Netzwerk- und Systemmanagement hinaus, so dass ein Unternehmen auch angrenzende Bereiche wie das Security Management oder die Softwareentwicklung einbeziehen kann. So stehen alle für das ITIL-Management erforderlichen Informationen konsistent zum Abruf bereit. Vorhandene Teillösungen sollten sich problemlos in die Gesamtlösung einbeziehen lassen. Auch für kleinere Umgebungen bietet sich bereits der Einsatz von entsprechenden Anwendungen an.

> Vielfach erscheint z.B. auch eine Verwendung des bereits in anderen Teilbereichen vorhandenen SAP-Systems oder von ERP-Systemen als sinnvoll. Es ist anzuraten, den Kontakt mit Unternehmen ähnlicher Branchen wie der eigenen zu suchen und von den dort gemachten Erfahrungen zu profitieren. Auch eine Recherche in entsprechenden Foren und bei unabhängigen Gesellschaften verspricht positive Anreize.

Nicht zu vernachlässigen sind Kennzahlen in Bezug auf Reporting und Monitoring innerhalb der ITIL-Prozesse. Dies bezieht sich vor allem auf Key Performance-Indikatoren (KPIs: wichtige Leistungsmesswerte), anhand derer jedes Unternehmen die passenden Qualitätskriterien für seine IT Services definieren und überprüfen kann. KPIs spielen eine Hauptrolle, weil sie die Qualität eines IT Services auf einen Blick charakterisieren. Zwar sind sie immer unternehmensspezifisch, doch meistens unternehmensübergreifend vergleichbar. Deshalb sollte eine Service Desk-Lösung für jede ITIL-Disziplin einen umfangreichen vordefinierten Satz von KPIs anbieten, aus dem jedes Unternehmen die für seine Zwecke relevanten Kennzahlen auswählen kann. Außerdem sollte es möglich sein, firmenspezifische Parameter einzubringen.

Effektive Werkzeuge sollten nicht nur die gesamte ITIL-Funktionalität aus Sicht der IT (Service Desk) abdecken, sondern auch den Anwendern, Systemanalytikern und Technikern als Informationsquelle dienen. Erreichen Anfragen über unterschiedliche Wege wie z.B. per Telefon, Fax oder E-Mail den zuständigen Mitarbeiter, sollten alle Informationen über den Zustand und den Fortschritt der Bearbeitung zentral verfügbar und abfragbar sein. Ausgefeilte Lösungen liefern zudem hilfreiche Zusatz-Features wie die Wissenssuche oder das Finden kompetenter Kandidaten für die Bearbeitung einer Anfrage. Häufig bietet sich hier die Einbindung von (vorhandenen) Prozess- und Workflow-Wegen an. Außerdem sollte das Management verschiedener

Servicetypen (inklusive Hinweise auf die Verletzung von Service Level-Agreements), Eskalationsmechanismen, Scoreboard-Features (schematische Erfassung der Bewertungen) und ein ausgefeiltes Benachrichtigungs- und Reporting-System möglich sein.

Eskalation

In ihrer eigentlichen Bedeutung bezeichnet die Eskalation eine durch Wechselwirkung hervorgerufene Steigerung eines (militärischen) Konfliktes. In der IT werden durch eine Eskalation Probleme, Themen, Entscheidungen oder Konflikte kontrolliert eine Ebene (horizontal oder vertikal) weitergereicht oder delegiert, wenn in einer Situation oder in einer Krise auf der aktuellen Ebene keine Lösung, Einigung oder Entscheidung möglich ist.

2.1.7 Key Performance-Indikatoren

Um die Prozessqualität beurteilen zu können, sind klar definierte Parameter und messbare Ziele nötig, so genannte Leistungsindikatoren (Key Performance Indicators, KPI). Sie sind Inhalt regelmäßiger (z.B. täglichen/wöchentlicher) Reports und werden über einen langen Zeitraum gesammelt und ausgewertet. Sie sind grundsätzlich eingebunden in ein unternehmerisches Steuerungssystem als Element eines Regelkreises, der sich mit den fundamentalen Elementen Messen (Erfassen, Berichten), Steuern (Zielvorgabe) und Regeln (Umsetzung, Realisierung) darstellen lässt. Welches Steuerungssystem das Management einsetzt, ist abhängig davon, welche Ziele es verfolgt.

Die Umsetzung der Reporting-Funktionalität wird in fast allen ITIL-Prozessen gefordert. Dies resultiert v.a. aus der Prämisse, dass IT-Serviceleistungen messbar gemacht werden müssen, um diese verbessern zu können. Im Bereich Incident Management (schnelle Behebung akuter Störungen oder Probleme) sollten zu den vordefinierten KPIs beispielsweise die Gesamtzahl der Incidents (Vorfälle) zählen, aber auch die mittlere Dauer bis zu ihrer Behebung oder Umgehung, der prozentuale Anteil von Incidents, der innerhalb der SLA-Vereinbarung beseitigt werden konnte, und die Anzahl von Incidents pro Support-Mitarbeiter. Die Gesamtzahl der Vorfälle kann direkt als ein Maßstab für die Stabilität der IT-Infrastruktur gelten, während die Zeit zu ihrer Behebung Aussagen über die Qualität des Incident- und Problem Management erlaubt. Der Prozentsatz innerhalb der SLA-Vereinbarung beseitigter Incidents gibt nicht nur Aufschluss über die Qualität des IT Services, sondern lässt sich auch für die Abrechnung nutzen.

Im Change Management wiederum zählen zu den Kriterien zum Beispiel die Anzahl von Änderungen pro Zeiteinheit insgesamt sowie pro Kategorie (Servicetyp, Konfiguration oder Region) oder pro Änderungsgrund (Anwender-Request, Systemerweiterung, Störungsbehebung oder Verbesserungsmaßnahme). Die Auswertung solcher KPIs macht beispielsweise auf einen Blick deutlich, wo sich instabile Hardware und Software befindet, welche Fachabteilungen mit ihrer Anwendung unzufrieden sind oder in welchem Maße die Zahl der Systemänderungen zu- oder abgenommen hat.

Für manchen IT-Manager dürfte allein schon die Information über die Zahl der Änderungen an der IT-Infrastruktur aufschlussreich sein, ist sie doch heute oftmals nicht oder nicht exakt verfügbar. Nicht zu vergessen: Changes kosten Geld, v.a. da komplexe Änderungen an der Infrastruktur oft von Mitarbeitern außerhalb der regulären Arbeitszeiten in extra dafür geschaffenen „Wartungsfenstern“ umgesetzt

werden. Auch eventuell nach Veränderungen an der Umgebung auftretende großflächige Probleme mit weitläufigen Auswirkungen durch Ausfälle kosten neben Geld auch die Zufriedenheit der Anwender. Weitere KPIs im Change Management sind daher auch die Zahl gescheiterter Änderungen (inklusive der dazugehörigen Gründe) bzw. die Anzahl von Incidents, die eine Änderung ausgelöst haben, oder die Anzahl der Incidents nach einem Change. Aus solchen Informationen lässt sich schnell ableiten, ob die IT-Abteilung Probleme an der Wurzel gepackt und beseitigt hat oder die Symptome nur an der Oberfläche kuriert bzw. ob Changes korrekt ohne negative Auswirkungen umgesetzt wurden.

Mithilfe solcher Key Performance-Indikatoren werden nicht nur das Fundament für die laufende Optimierung der ITIL-Prozesse gelegt, sondern auch eine tragfähige Basis für den weiteren Ausbau des Service Management geschaffen. So können Unternehmen die IT-Prozesse formen, die ihren geschäftlichen Anforderungen Rechnung tragen. Zweierlei ist dabei wichtig: Erstens sorgt ein ausbaufähiger Satz aussagekräftiger KPIs dafür, dass diese Optimierung vom ersten Tag an nachweisbar ist und etwaige Schwachstellen schnell deutlich werden. Zweitens sollten die eingesetzten Werkzeuge so standardkonform und offen sein, dass sie der kosteneffektiven Optimierung des Managements der IT Services dienen und ihr nicht im Wege stehen.

2.2 Was ist ICT Infrastructure Management?

ITIL wurde in einer so genannten Version 2.0 erweitert. Dies bedeutet, dass durch Umstrukturierungen und Erweiterungen der Kapitel neue Bereiche entstanden sind. Ein Teil davon ist das Information and Communication Technology Infrastructure Management (ICTIM). Dabei geht es darum, die Qualität der Information and Communication Technology (ICT) zu verbessern.

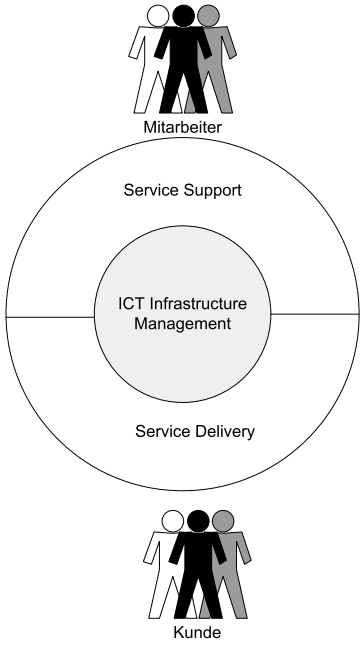


Abbildung 2.15:
ICTIM und ITIL in Relation

ICTIM umfasst in vier Managementbereichen alle Prozesse des Rechenzentrums (Data Center) bzw. der eigentlichen Erbringung von IT-Leistungen. Die ITIL-Revision 2 hat so mit dem ICT Infrastructure Management weitere wichtige Bausteine erhalten, die den Betrieb der IT-Infrastruktur, wie sie beispielsweise ein Rechenzentrum darstellt, abbilden. Mit den Managementbereichen Design and Planning, Deployment, Operations und Technical Support wird das bisher bekannte IT Service Management um die operativen Prozesse des IT-Betriebs ergänzt (*siehe Abbildung 2.16*). Damit werden bisherige Fragestellungen zur Verteilung von Aufgaben transparent, die oft als ungeklärt oder frei entscheidbar kommuniziert wurden.

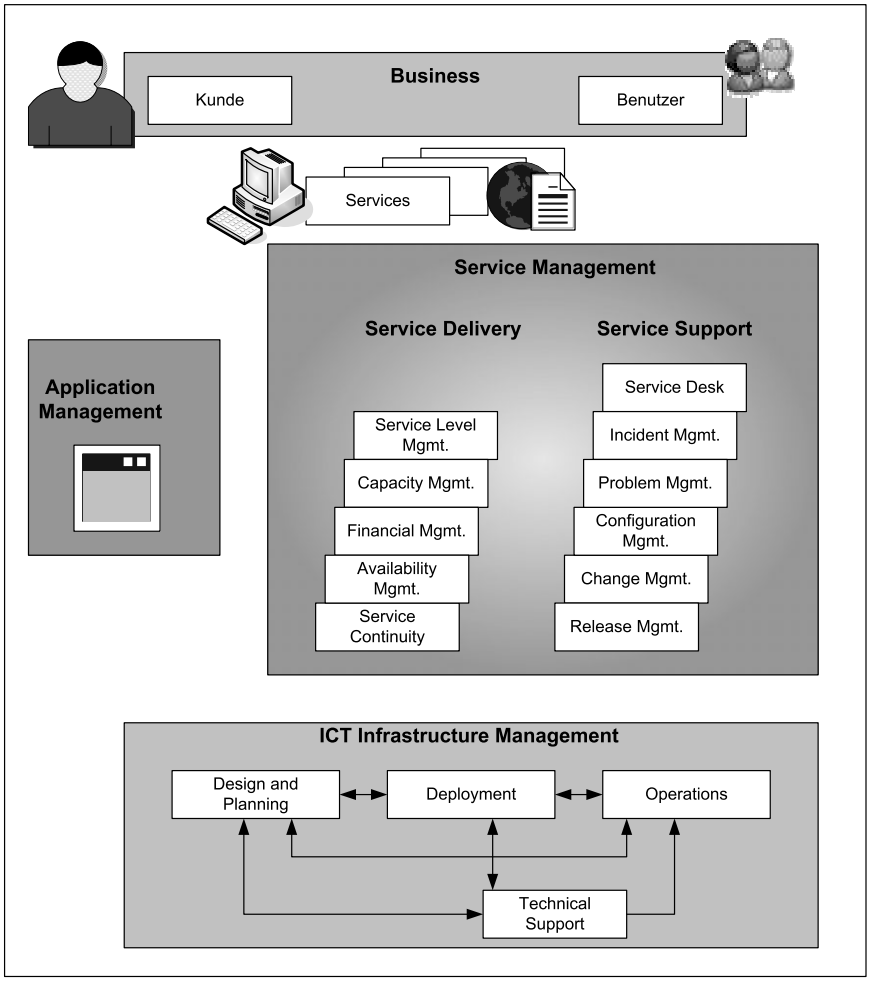


Abbildung 2.16: ITIL und ICTIM

Die Lösungen aus dem ICT Infrastructure Management schaffen in den Unternehmen so die Voraussetzungen für den Einsatz wertschöpfender Informations- und Telekommunikationstechnologie.

ICTIM sollte sich vergewissern, dass die Bedürfnisse der Kunden und Organisationseinheiten adäquat erfüllt sind. Gleichzeitig ist die Deckung der erforderlichen Kosten essenziell. Eine gute Planung, Verwaltung und Kontrolle sind Schlüsselpunkte, um zu gewährleisten, dass die Information Services (Informationsdienstleistungen) die Bedürfnisse kosteneffektiv erfüllen. Diese Aspekte werden mit Hilfe der ICTIM–Prozesse geführt, um den Prozess den allgemeinen Bedürfnissen anzupassen. Planung, Verwaltung und Kontrolle sind unbedingt erforderlich, um sicherzustellen, dass die passenden Ressourcen mit den richtigen Fähigkeiten und Kompetenzen zusammenkommen. Es geht also auch um personenbezogene Rollen, die so abgebildet werden.

Die Vorteile von ICTIM können gemessen werden und zeigen somit die Wirksamkeit der ICTIM-Prozesse anhand von verwertbaren Ergebnissen auf. ICTIM hilft den ICT-Diensten, effizienter und effektiver zu werden durch folgende Punkte:

- Verwalten von Veränderungen in der ICT-Infrastruktur
- Verwalten von Problemen
- Voraussehen von Problemen (und deren Lösungen)
- Unterstützung der ICT-Leitung, bessere Entscheidungen zu treffen
- höhere Produktivität von IT-Mitarbeitern in Schlüsselpositionen
- Erkennen neuer Technologien zur Kostenreduzierung und Dienstverbesserung
- Planen von Erweiterungen und Aufrüstungen

2.2.1 ICTIM-Aufgabenbereiche

Die ICTIM-Bereiche besitzen aufgrund ihrer Aufstellung und Definition zahlreiche Schnittstellen zu den unterschiedlichen ITIL-Disziplinen, so dass ICTIM vielfach als der Umsetzungsbereich für die Praxis angesehen wird.

Design and Planning

ICTIM Design and Planning umfasst die Entwicklung und Wartung von IT-Strategien und Prozessen für den Aufbau und die Einführung der entsprechenden IT-Infrastruktur-Lösungen im ganzen Unternehmen (*siehe Abbildung 2.17*). Hier geht es um eine technische Anlehnung an die strategische Ausrichtung des Unternehmens. Weitere Aufgaben sind:

- Koordination aller Aspekte von IT-Design und -Planung
- Bereitstellung eines einheitlichen Interfaces der IT-Planung für alle Geschäfts- und Serviceplaner
- Hilfestellung bei der Erstellung von Policies und Standards

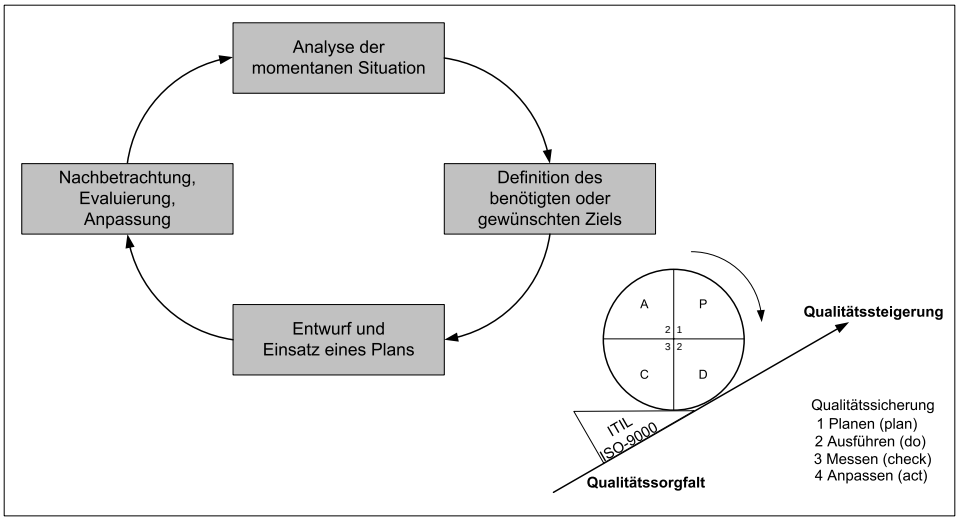


Abbildung 2.17: Design and Planning: ein Kreislauf (nach OGC)

Deployment

Deployment ist ein temporär aktiver Prozess und beinhaltet Projekt-Management-Verfahren, um neue Hard- und Softwarekomponenten in das Unternehmen einzuführen. Es bildet so das Bindeglied zwischen Development, Change Management, Operations und Technical Support (*siehe Abbildung 2.18*) und steuert über diese Bereiche hinweg die Entwicklung und Überführung neuer oder erweiterter Hard- und Software-Releases in die Produktion. Dieser Prozess kommt damit typischerweise im Rahmen von Change- oder Einführungsprojekten zur Ausführung. Ist die entsprechende Komponente in die Produktion überführt, wird sie dem Bereich Operations übergeben. Die folgenden Aufgaben werden über das Deployment abgewickelt:

- Pläne erstellen und pflegen, die den Rahmen für Projekte in Bezug auf Ziel, Zeitplanung und Ressourcen zur Einführung von neuen oder stark veränderten CIs beinhalten
- die benötigten Ressourcen zur Realisierung der entwickelten Pläne eruieren und Teams mit den entsprechenden Fähigkeiten zusammenstellen
- das Risk Management über den kompletten Zeitraum von Projekten verantworten
- Sicherstellen, dass die Erfahrungen und Erkenntnisse aus den Projekten dem IT-Betrieb, insbesondere Operations und Technical Support, in Form von aktuellen Dokumentationen zeitnah und vollständig zur Verfügung stehen, um eine reibungslose Übergabe und einen weitestgehend problemlosen Betrieb zu gewährleisten
- Änderungen entsprechend der Richtlinien oder nach den Projektvorgaben durchführen
- über den Status berichten und diesen dokumentieren

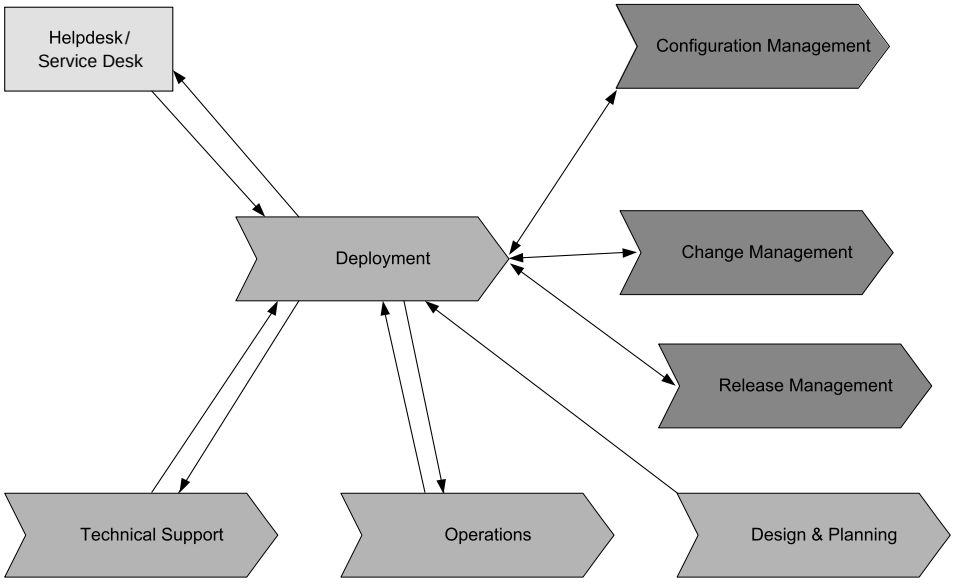


Abbildung 2.18: Der Deployment-Prozess im ICTIM und die Schnittstellen zu ITIL

Operations

Der Operations-Prozess umfasst alle Aktivitäten und Maßnahmen zur Bereitstellung und Instandhaltung der IT-Infrastruktur und der damit zusammenhängenden Services, entsprechend ihrem Bestimmungszweck. Dies

- ist die Basis für alle IT Services (Kerngeschäft),
- ist zentral für den täglichen Betrieb,
- ist Technik-fokussiert mit starken Anteilen von Steuerungs-, Controlling- und Monitoring-Prozessen,
- liefert grundlegende Informationen für alle Management-Bereiche (Status, Usage, MO).

Vielfach wird dieser Bereich als Second-Level-Support definiert, der dafür zu sorgen hat, dass das Tagesgeschäft läuft, Störungen und Probleme schnell behoben und die Bereitstellung des Services nicht beeinträchtigt wird.

Managed Objects

MO (Managed Objects) sind die Ressourcen der IT-Infrastruktur aus der Sicht der Geschäftsleitung.

Die Schnittstellen zu anderen Prozessen sind vielfältig, weswegen detaillierte Vereinbarungen (OLAs) und Abgrenzungen (Prozessdefinitionen) für die Erfüllung der Aufgaben essentiell sind.

Technical Support

Der Bereich Technical Support versteht sich als Aufbau von Kenntnissen über Evaluation, Unterstützung und Prüfung aktueller und zukünftiger IT-Infrastrukturlösungen. Er zielt auf eine Zentralisierung des technischen Know-hows, insbesondere der Erfahrungen und Informationen aus den Prozessen von Operations und Deployment, und der Unterstützung der Vision eines End-to-end-Services (*siehe Abbildung 2.19*). Mit Hilfe von Management-Tools bietet er analysierte und interpretierte Daten zum kontinuierlichen Report an Design and Planning. Der Prozess setzt sich zusammen aus folgenden Punkten:

- Erforschung und Entwicklung neuer Technologien
- Erstellung von Bedarfsfestlegungen und Ausschreibungen in Zusammenarbeit mit Design und Planung sowie Budgetplanung und -kontrolle, Materialbeschaffung und Lieferungs-Management
- Festlegung und Pflege von Freigabeverfahren und -richtlinien gemeinsam mit Deployment, beispielsweise zur betrieblichen Abnahme
- technische Referenzadresse für alle Berührungsbereiche zwischen IT und Dritten und als Third Line/Level Support
- technische Planung, Abwicklung und Steuerung aller Support-, Administrations- und Arbeitsfunktionen und -tools sowie Bereitstellung von Analyseergebnissen und Management-Reports zu allen Aspekten der IT-Infrastruktur inklusive der Pflege von Dokumentationen und Standardprozeduren

Der Technical Support wird oftmals als Third Level Support bzw. Center of Excellence bezeichnet.

Abbildung 2.19: Technical Support

Die Aktivitäten lassen sich in die drei funktionale Bereiche Research und Evaluierung, Projekte und Business as Usual (BaU) gliedern.

Herstellerspezifische Frameworks und Referenzprozessmodelle

ITIL dient auch als Basis proprietärer Ansätze unterschiedlicher Hersteller, die auf ITIL beruhen. In den letzten zwei bis drei Jahren zeigt sich ein zunehmendes Interesse an Referenzmodellen zur Umsetzung und Erreichung eines serviceorientierten IT-Managements. Dementsprechend wurde von den unterschiedlichsten Organisationen eine Fülle von Modellen entwickelt, die dabei helfen sollen, ein serviceorientiertes IT-Management zu gewährleisten. Diese herstellerspezifischen Frameworks und Referenzprozessmodelle wurden von Firmen wie HP, IBM oder Microsoft initialisiert und ausgebaut. Sie dienen als Initiatoren der jeweiligen Richtung, die durch die entsprechenden Berater bei der Zielgruppe verwirklicht werden. MOF als Microsoft Operations Framework (Microsoft) wird vorwiegend bei Kleinunternehmern und kleinen Mittelständlern umgesetzt, wogegen ITSM als IT Service Management von Hewlett Packard (HP) vorwiegend große Mittelständler bedient und ITPM als IT Process Model von IBM sich primär in Konzernen findet.

Vielfach liegt allerdings auch der Verdacht nahe, dass neben der Kundenunterstützung hinsichtlich Serviceorientierung und Mapping der ITIL-Prozesse die eigenen Produkte einfach ein Aufhänger gefunden wurde, aus dem Kapital geschlagen wird.

Im Gegensatz zu herstellerspezifischen Best Practice-Modellen wie das IBM IT Process Model (ITPM), das IT Service Management Model (ITSM) von HP oder das Microsoft Operations Framework Process Model (MOF) sind die ITIL-Bücher immer noch als die einzige nicht-proprietäre und öffentlich zugängliche Verfahrensbibliothek in diesem Bereich anzusehen.

IBM hat sich auch in Bezug auf die proprietäre IT Service Management-Abbildung seiner großen Leidenschaft der Umbenennung und Umstrukturierung hingegeben, wie Sie es wahrscheinlich bereits in Bezug auf das Portfolio der IBM kennen. Mittlerweile heisst dieser Ansatz nicht mehr ITPM, sondern PRM-IT, wobei die Bezeichnung für IBM Process Reference Model for IT steht.

3 Die ITIL Foundation-Zertifizierung

Über 30.000 Experten in mehr als 30 Ländern weltweit haben sich bereits im IT Service Management nach ITIL zertifizieren lassen. So können Unternehmen gezielt nach Mitarbeitern mit einer solchen Qualifikation suchen, um entsprechendes (Basis-)Know-how ins Unternehmen zu holen. Sie sollten allerdings nicht vergessen, dass dies nicht unbedingt konform ist mit dem gerühmten hohen Standard der Office of Government Commerce (OGC, früher CCTA), der in England und Holland stärker als im übrigen Europa verbreitet ist. Mitarbeiter mit einer ITIL-Basis-Zertifizierung verfügen jedoch mindestens über das Grundlagenwissen hinsichtlich ITIL, was die Prozesse, Begriffe und den Hintergrund dieses De-facto-Standards angeht.

Schließlich ist das Know-how der Mitarbeiter der erste und wichtigste Schritt zu einer erfolgreichen Einführung von IT Service Management. Steht nicht nur der kurzfristige Erfolg an erster Stelle, so ist eine einheitliche Sprache im Unternehmen unverzichtbar, auch als Ausgangsbasis für besser aufeinander abgestimmte und effizientere Prozesse im Hinblick auf die Zusammenarbeit mit Kunden und Zulieferern. In einer Organisation, in der sich ITIL bereits etabliert hat, besteht die Aufgabe der Abteilungen und der Mitarbeiter in der Überwachung, Qualitätssicherung und Verbesserung der Prozesse. Dies bezieht sich nicht nur auf die vorhandenen Mitarbeiter einer Organisation. Auch in Stellenausschreibungen wird ITIL zukünftig eine Rolle spielen; Kandidaten werden Kenntnisse und Erfahrung als Pluspunkt zugeschrieben.

Da ITIL ein wesentlicher Bestandteil des Qualitätsmanagements ist, gehören auch Qualifizierungsmaßnahmen und Zertifizierungen dazu, um bestimmte Qualitätsstandards zu erreichen. Das klassische ITIL-Curriculum umfasst dabei die Grundlagenschulung in Form der ITIL Foundation sowie die weiterführende Ausbildung zum IT Service Manager. Diese bezieht sich auf das Management bzw. die Practioneer-Weiterbildung für den operativen Bereich. So werden sowohl horizontal als auch vertikal in der Organisationsstruktur die notwendigen Kenntnisse aufgebaut, um ITIL einzuführen, voranzutreiben, zu verstehen und zu leben.

3.1 ITIL-Zertifizierungen

Nach internationalen Expertenmeinungen werden die ITIL-Ansätze in den nächsten Jahren Normcharakter erreichen. So heißt es in einem Artikel der Computerwoche online vom 16.04.2004: *„Von 125 Unternehmen, die ITIL einsetzen, erklären demnach rund 70 Prozent, das Framework biete einen strukturierten Ansatz zur Bereitstellung von Services und lohne den Aufwand durchaus. Die Studie, die Ende des Monats von*

Hornbill Systems veröffentlicht wird, ergab außerdem, dass 50 Prozent der ITIL-Anwender höhere Kundenzufriedenheit und/oder Kompetenz der IT-Abteilung erzielten ...“

Zur Qualifizierung der IT-Verantwortlichen werden die international anerkannten ITIL-Zertifikate vergeben. Wie in vielen anderen Bereichen gibt es auch in Bezug auf ITIL eine Reihe von Zertifizierungen, die nach Schwierigkeits- und Erfahrungsgrad gestaffelt sind (*siehe Abbildung 3.1*).

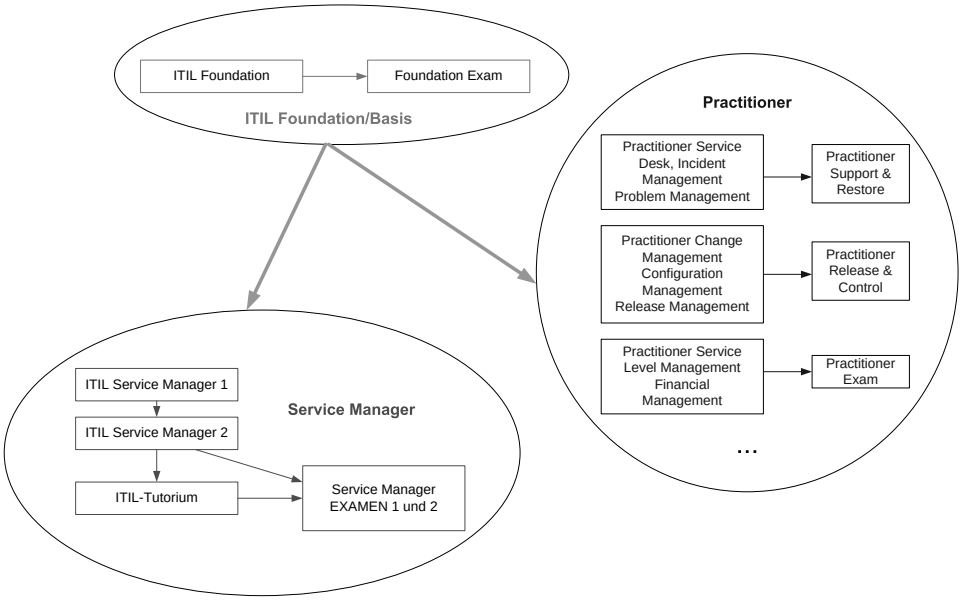


Abbildung 3.1: Das ITIL-Curriculum

Die Hoheit dieser Zertifizierungsprüfungen liegt nicht wie bei vielen anderen Zertifizierungen bei Thompson Prometric oder der OGC bzw. CCTA selbst. Das Office of Government Commerce (OGC) tritt lediglich als Träger von ITIL auf.

Einteilung der vorhandenen ITIL-Zertifikate:

- ITIL-Foundation: Das Foundation-Zertifikat umfasst nur die Management-Bereiche des IT Service Management (Service Support/Service Delivery/Security Management). Geprüft wird das Fachwissen in diesen Bereichen.
- ITIL Service Manager: Auch das Service Manager-Zertifikat umfasst nur die Management-Bereiche des IT Service Management, diese jedoch in vertiefter Form mit dem Nachweis eigenständiger Gestaltungskompetenz.
- ITIL Practitioner: Ergänzend zum Service Manager-Zertifikat wird ein operativer und nach Praxis-Gesichtspunkten ausgerichteter Managementbereich erarbeitet und geprüft.

Die ITIL-Zertifizierungsprüfungen für den angelsächsischen Raum werden von dem Information System Examination Board (ISEB) in englischer Sprache für Großbritannien, Irland und den British Commenwealth abgenommen. EXIN führt alle nicht-englischsprachigen Zertifizierungsprüfungen durch und ist somit auch für die ITIL-Prüfungen im deutschsprachigen Raum zuständig. EXIN ist eine von der holländischen Wirtschaft geförderte Stiftung. So bieten diese beiden Organisationen Examen auf der Grundlage von ITIL an. Beide sind nicht-proprietäre und nicht-profitorientierte Organisationen. Sie organisieren die Examen, bieten aber selbst keine entsprechenden Schulungen an. Sie arbeiten bei der Ausarbeitung der Prüfungen sehr eng zusammen.

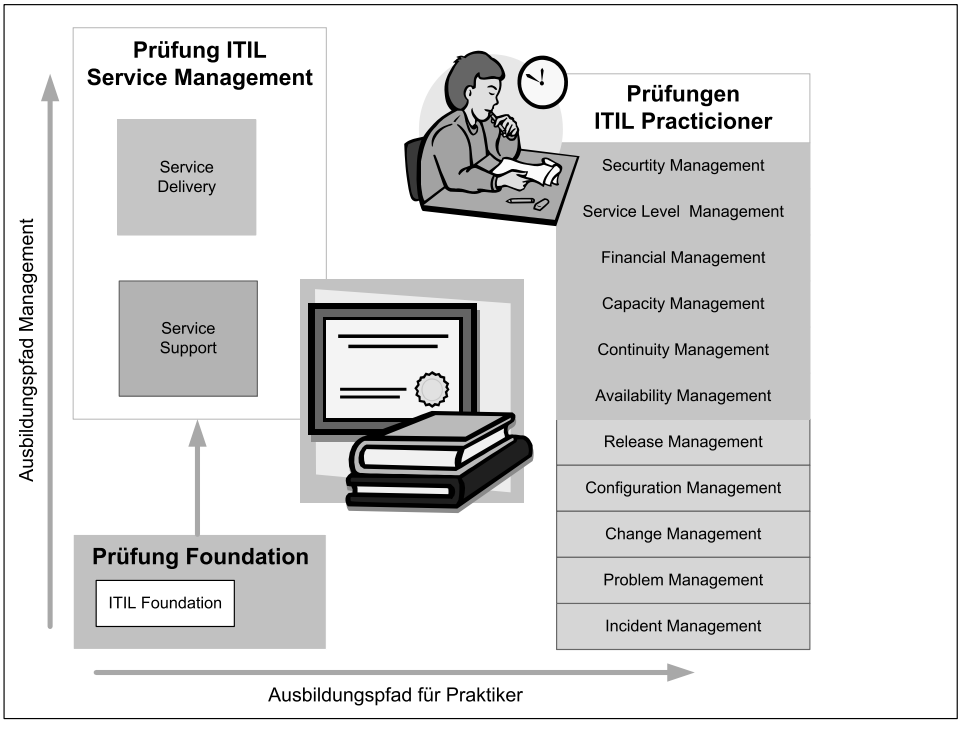


Abbildung 3.2: Ausbildungspfad nach EXIN/ISEB

Analog zu den Zertifizierungsprüfungen und anderen ITIL-Themen werden Schulungen angeboten. Diese unterscheiden sich jedoch sowohl bezüglich der anbietenden Institutionen, Trainer und Preise als auch teilweise der Inhalte erheblich. Veranstaltungen bei einer Dauer von 2 Tagen können durchaus den Betrag von 1.500 Euro übersteigen, während Sie bei anderen Veranstaltern lediglich eine Veranstaltungsgebühr von 150 Euro entrichten. Vor allem IHKs bieten von Zeit zu Zeit diese kostengünstigen Kurse an, die qualitativ nicht schlechter sind als die teure Konkurrenz. Maßgeblich ist stets der jeweilige Trainer. Zu der reinen Kursgebühr müssen Sie die Prüfungsgebühr des TÜV bezahlen – ca. 140 Euro – oder den entsprechenden Tagessatz des TÜV. Dieser hat die Abnahme der ITIL-Zertifizierungen in Deutschland von der EXIN übernommen.

ITIL-Schulungen, -Kurse oder –Seminare

Die ITIL Foundations-Schulung vermittelt die ITIL-Terminologie sowie die theoretischen Grundlagen zu den ITIL-Prozessen und bereitet damit auf die ITIL Foundations-Zertifizierung vor. Bei entsprechender Eigeninitiative, Selbststudium und Durchlauf von Testfragen ist eine entsprechende Schulung nicht unbedingt notwendig.

Das Foundation Zertifikat wiederum ist Voraussetzung für die folgenden Aufbau-Kurse: Die umfangreiche IT Service Manager-Ausbildung vertieft dieses Wissen durch Übungen und ergänzt es durch weitere Aspekte, die strategische und taktische Fragen des IT Service Management betreffen. Diese Schulung kann mit der Zertifizierung zum IT Service Manager abgeschlossen werden.

Die ITIL Practitioner-Ausbildung stellt eine Spezialisierungsmöglichkeit innerhalb der ITIL/ITSM-Ausbildung dar, bei der jeder Prozess einzeln behandelt wird. Mit Vertiefung der Prozesstheorie und entsprechenden Übungen sind diese Kurse vor allem für diejenigen gedacht, die später in diesem Prozess konkrete Rollen bzw. Aufgaben in ihrem Unternehmen übernehmen sollen.

Wer die jeweilige Zertifizierung erfolgreich abschließt, erhält ein offizielles Zertifikat von der TÜV Akademie GmbH und eine Anstecknadel (*siehe Abbildung 3.3*):

- Grün: Foundation
- Blau: Practitioner
- Rot: Service Manager

Abbildung 3.3:
Die ITIL-Zertifizierungsanstecknadeln

Das ITIL-Logo stellt die Form eines Diamanten durch vier kleine Diamanten dar. Im Sinne von EXIN steht der Diamant für die Kohärenz in der IT-Infrastruktur. Die vier kleinen Diamanten symbolisieren die vier Kernbereiche von ITIL: Service Support, Service Delivery, Infrastructure Management und IT Management. Möglich ist aber die Verwendung der Themen, die in den ITIL De-facto-Standard einbezogen wur-

den: die ITIL-Literatur (mit der OGC als Träger und Eigentümer), dem Anwenderkreis (repräsentiert durch das itSMF), das Prüfungsinstitut (wie etwa EXIN) sowie die Trainer und Anbieters von ITIL-Dienstleistungen wie Consulting.

3.1.1 ITIL Foundation-Zertifizierung

Das ITIL Foundation-Zertifikat ist die Basis der ITIL-Zertifizierungen und führt in das prozessorientierte IT Service Management ein. Darauf baut die Ausbildung zum zertifizierten Service Manager nach ITIL auf.

Es bestehen keine besonderen Voraussetzungen für die Zertifizierungsprüfung. Für das Ablegen der Prüfung zum Erwerb dieses Zertifikates ist keine Schulung zwingend erforderlich, allerdings ist der Besuch einer ITIL-Foundation-Schulung oder vergleichbarer Trainings anzuraten, wenn keinerlei praktisches oder theoretisches Vorwissen besteht.

Der Test zur Basis-Zertifizierung besteht aus 40 Fragen in Multiple Choice-Form, die innerhalb von 60 Minuten zu beantworten sind. In der Regel ist von den drei oder vier vorgegebenen Antwortmöglichkeiten nur eine Antwort richtig. Der Teilnehmer erhält den Prüfungsbogen mit den Fragen und Antworten, der vom TÜV-Mitarbeiter wieder eingesammelt wird, und einen Lösungsbogen. Auf diesem Vordruck sind die personenbezogenen Daten des Teilnehmers und die Lösung zu jeder Aufgabe einzutragen. Der ausgefüllte und abgegebene Vordruck wird dann anhand einer Lösungsschablone überprüft. Bestanden hat der Teilnehmer, wenn er von den insgesamt 40 Multiple Choice-Fragen 65 % (26 Fragen) richtig beantworten konnte. Während der Prüfung führt eine Mitarbeiterin bzw. ein Mitarbeiter des TÜV Aufsicht. Falls die Prüfung innerhalb einer Schulung stattfindet, hat der Trainer den Raum zu verlassen.

Themen der Prüfung sind:

- die Grundmotivation und die Zielsetzung der IT Infrastructure Library (ITIL)
- die Best Practices im IT Service und im Zusammenspiel zwischen IT-Serviceliferanten und IT-Kunden
- die ITIL-Terminologie und –Kernprozesse im Überblick
- das Zusammenspiel der einzelnen IT Service Management-Prozesse
- die Vorteile von ITIL für die IT Serviceorganisation
- Vertiefung des Verständnisses für die Prozessabläufe
- Grundlagenkenntnisse der ITIL-Einführungsstrategie

3.1.2 ITIL Practitioner

Der Practioner-Bereich der ITIL-Zertifizierung ist für den operativen Bereich und die entsprechenden Mitarbeiter gedacht, die sich tiefer in einzelne Prozesse einarbeiten wollen.

Nach der Prüfung und Zertifizierung für ITIL Foundation und ITIL Service Manager bietet die TÜV Akademie seit 2005 die Prüfung und Zertifizierung für das erste Ausbildungsmodul zum ITIL Practitioner für „IT Service Management Release and Control“, kurz IPRC an. Der Bereich „ITIL – Practitioner Service Level Mange-

ment (SLM)“ wird seit kurzem auch in deutscher Sprache angeboten. Daneben existieren folgende Practioner-Ausbildungsmöglichkeiten:

- ITIL Practitioner Support and Restore (Service Desk, Incident Management und Problem Management), kurz IPSR
- ITIL Practitioner Agree and Define (IPAD)
- ITIL Practitioner Plan and Improve (IPPI)

Die anderen Practitioner-Teile sind bis zur Freigabe durch den TÜV nur in englischer Sprache verfügbar. Insgesamt bezieht sich diese Zertifizierung auf die folgenden Prüfungen:

- ITIL Practitioner Configuration Management
- ITIL Practitioner Incident Management
- ITIL Practitioner Problem Management
- ITIL Practitioner Release Management
- ITIL Practitioner Change Management
- ITIL Practitioner Service Level Management
- ITIL Practitioner Financial Management
- ITIL Practitioner Capacity Management
- ITIL Practitioner Availability Management

Zertifizierungsprüfungen werden bisher (Stand Juli 2006) für das Modul IPRC, SLM und IPSR angeboten.

3.1.3 ITIL Service Manager

Aktuell setzen viele Unternehmen auf ITIL, um ihre IT-Prozesse in Richtung IT Service Management zu definieren und zu verbessern. Gerade IT-Manager in Schlüsselpositionen werden jetzt zum ITIL Service Manager ausgebildet, so dass sie die IT-Landschaft ihres Unternehmens absichern und zur Steigerung des Geschäftsnutzens ausrichten können.

Diese Zertifizierung richtet sich neben dem IT-Management an Projektleiter, die mit der Implementierung oder Koordination von IT-Management befasst sind. Das Ziel ist die Vermittlung des ITIL-Fachwissens. Dieses Wissen ist die Voraussetzung für die Einführung, den Betrieb und die systematische Weiterentwicklung der Prozesse in Bezug auf das ITIL Service Management. Um an dieser Zertifizierung teilzunehmen, muss der Teilnehmer bereits die ITIL Foundation-Zertifizierung erlangt haben. Aus diesem Grund wird diese Zertifizierungsform als mehrstufig bezeichnet.

Folgende Voraussetzungen für die Prüfungszulassung sind insgesamt zu erfüllen:

- bestandene ITIL Foundation-Prüfung (auch Voraussetzung für die Teilnahme an der Ausbildung)
- mindestens zwei Jahre Berufserfahrung/Praxis in den relevanten Themenbereichen
- Absolvierung der Ausbildung bei einem durch EXIN akkreditierten Schulungsunternehmen

- Die Ausbildung muss generell von einem akkreditierten Schulungsunternehmen nach den entsprechenden Vorgaben durchgeführt werden. Dazu gehört u.a. die Teilnehmerbewertung während des Seminars durch die Dozenten/Trainer in Form des sogenannten In-Course-Assessment (Gesamtbewertung). Nur wenn diese Beurteilung den Mindestvorgaben durch EXIN entspricht, erhält der Teilnehmer die Prüfungszulassung.

Mindestens 60 Seminarstunden sind vorgeschrieben. Am Ende der Ausbildung, die oft in Blöcken zu zwei-, vier- oder fünftägigen Veranstaltungen angeboten wird, wird die Prüfung abgelegt. Im Gegensatz zur Foundation-Prüfung, die eine geringe Durchfallquote aufweist, wird bei der Service Manager-Prüfung von durchschnittlichen Durchfallquoten berichtet, die bei rund 30 Prozent liegen.

Der Prüfling bearbeitet in jeweils drei Stunden zwei Prüfungskomplexe zu den Prozessen des Service Delivery und Service Support. Die Prüfung beruht auf Fragestellungen zu einer Fallstudie, die dem Prüfling einige Tage vor Prüfungsbeginn zugestellt wird. Die Aufgaben und Fragestellungen werden erst im Rahmen der Prüfung bekannt gegeben. Der generelle Ablauf lässt sich schematisch folgendermaßen darstellen: *Grundlagen des ITSM -> Service Management 1 -> Service Management 2 -> Zertifizierung als IT Service Manager*

Die bestandene Foundation-Zertifizierungsprüfung und ausgewiesene Praxiserfahrung ist Zulassungsvoraussetzung für das Service Manager-Examen. Es wird jeweils in einer schriftlichen, halbtägigen Klausur zu Service Support und Service Delivery abgelegt. Nach Bestehen dieser eintägigen Prüfung erhalten die Kandidaten den Titel „Manager in IT Service Management“.

4 Überblick Service Support

Der Bereich Service Support beinhaltet Themen und Prozesse zur Unterstützung und zum Betrieb der IT-Dienste. Gleichzeitig stellt er auch den Zugang der Benutzer und Kunden zum IT-Betrieb bereit. Hier sind die Prozesse angesiedelt, die sich vorwiegend mit der Erbringung von Services beschäftigen. Die unterschiedlichen Prozesse sind in sich abgeschlossen und bilden jeweils eine logische Einheit. Sie bieten jedoch untereinander Schnittstellen und Relationen sowie Verbindungen zu den weiteren ITIL-Prozessgruppen und IT-Disziplinen an. Diese Prozesse definieren die alltäglichen Funktionalitäten und Aufgaben des IT-Betriebes.

4.1 Beispielhafte Abläufe im Bereich Service Support

Ein alltägliches Beispiel stellt ein Anwender in seinem Arbeitsprozess am Rechner dar, der während seiner Arbeit mit einer Anwendung auf ein Problem stößt. Er kann entweder die gewohnte Tätigkeit in Bezug auf die vorhandene EDV gar nicht oder nur in eingeschränktem Maße verfolgen. Er ist weder in der Lage, sich das Problem intuitiv zu erklären, noch es selbst zu beheben. Gründe dafür sind unterschiedlich: fehlende Rechte, nicht vorhandene Kenntnisse oder Zuständigkeiten. Der Anwender nimmt demzufolge die ihm bekannten Kommunikationsmöglichkeiten in Richtung Service Support wahr, um das Problem von dort aus lösen zu lassen. Sein Ziel ist es, möglichst schnell problemlos weiterarbeiten zu können.

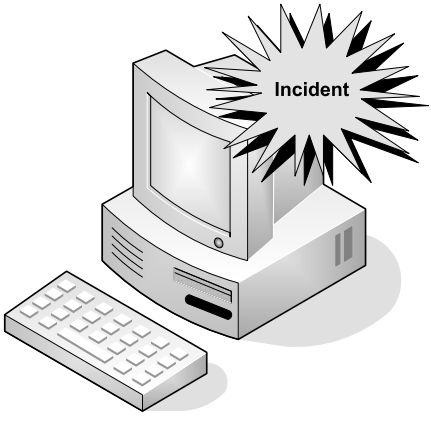


Abbildung 4.1:
Störungen, Unterbrechungen, …

Die Mitarbeiter des Service Desk repräsentieren als zentrale Ansprechpartner die Schnittstelle zwischen den Nutzern und dem IT Service Management. Sie nehmen Störungen (Incidents) und Anfragen entgegen und bilden die Schnittstelle zu den anderen IT Service Prozessen. Gleichzeitig garantiert das Service Desk die Erreichbar-

keit der IT-Organisation. Es ist die einzige Schnittstelle (Single Point of Contact/ SPoC) des Anwenders und hält ihn bei Bedarf auf dem Laufenden. Es koordiniert ggf. die nachfolgenden Supporteinheiten und übernimmt Aufgaben anderer Prozesse, z.B. Incident Management, Change Management, Configuration Management. Was hier deutlich werden soll: Das Service Desk stellt keinen Prozess dar, sondern vielmehr eine Funktions- oder Organisationseinheit. Aus diesem Grund kommt dieser Einheit eine Sonderrolle zu, die auch innerhalb des ITIL-Modells betont wird.

Das Incident Management dient der schnellstmöglichen Wiederherstellung des normalen Service-Betriebs. Die Priorität bei der Behebung einer Störung ergibt sich aus der Dringlichkeit bzw. einer Klassifizierung, mit der eine Störung behoben werden muss, und den Auswirkungen, die eine Störung für den Geschäftsablauf mit sich bringt.

Ein Incident ist jeder Vorfall, der eine Störung bzw. Minderung der Servicequalität hervorruft oder hervorrufen kann. Ein Problem ist die Ursache einer oder mehrerer Störungen.

Meist wird ein Incident als Problem deklariert, wenn er

- häufig auftritt,
- die Arbeit der Anwender/Kunden stark beeinträchtigt,
- die vereinbarten SLAs, also die Qualität des Service, gefährdet,
- das Incident Management keinen Workaround findet.

Störungen, deren Ursache nicht bekannt sind, werden im Rahmen des Problem Management analysiert. Es geht hier um die Ursachenforschung hinsichtlich eines Problems. Das Ergebnis kann kurzfristig eine vorübergehende Umgehungsstrategie (Workaround) sein, bis mittelfristig Wege zur Behebung (oft über einen Request for Change, RfC) wie das Einspielen eines FixPack, Patches o.Ä.) und Vorbeugung gefunden sind. Wichtig dabei ist, dass Probleme identifiziert, lokalisiert, diagnostiziert, dokumentiert und überwacht werden. Schnellschüsse aus der Hüfte, die nicht hinterlegt werden, nützen zwar für den Moment, einem entsprechenden Qualitätsanspruch wird so aber nicht Rechnung getragen. IT-Organisationen sollte es gelingen, durch proaktives Problem Management gezielt Störungen ihrer Services im Vorfeld zu erkennen und zu minimieren.

Das Configuration Management stellt ein logisches Modell der IT-Infrastruktur als Grundlage für alle IT Service Management-Prozesse zur Verfügung. Die Konfigurationsdatenbank (CMDB) ist die Basis für die Analyse von Störungen und Problemen sowie für die Planung von Änderungen an den IT-Systemen (*siehe Abbildung 4.2*). Bei Änderungen in der IT-Infrastruktur und den entsprechenden Komponenten werden von diesem Prozess aus die Änderungen an der CMDB umgesetzt. Das Change Management stößt diese Änderungen lediglich an.

Das Change Management plant und koordiniert die Durchführung von Änderungen an den IT-Systemen, die meist über das Problem Management angestoßen werden. Dazu werden geplante Änderungen bewertet, priorisiert und auf ihre Abhängigkeiten hin untersucht. Erhebliche Eingriffe in die IT-Infrastruktur werden an einen Entscheidungsausschuss, das Change Advisory Board (CAB), weitergege-

ben. Nach Erfolgsmeldung durch das Problem Management wird der RfC geschlossen. Das Change Management arbeitet sehr eng mit dem Problem Management und dem Release Management zusammen. Änderungen werden in vielen Fällen mit dem Projektmanagement der Entwicklungsprojekte abgestimmt und anschließend umgesetzt. Changes müssen nicht unbedingt aufgrund von Problemen oder Ausfällen eingebracht werden, sondern Veränderungen können auch aufgrund von langfristigen Zielen bezüglich Erweiterung von Funktionen, Diensten und anderen Verbesserungen an der IT-Infrastruktur vorkommen, die nicht immer unmittelbar registriert werden. Des Weiteren stellt das Change Management relevante Informationen und Berichte über die Änderung zur Verfügung.

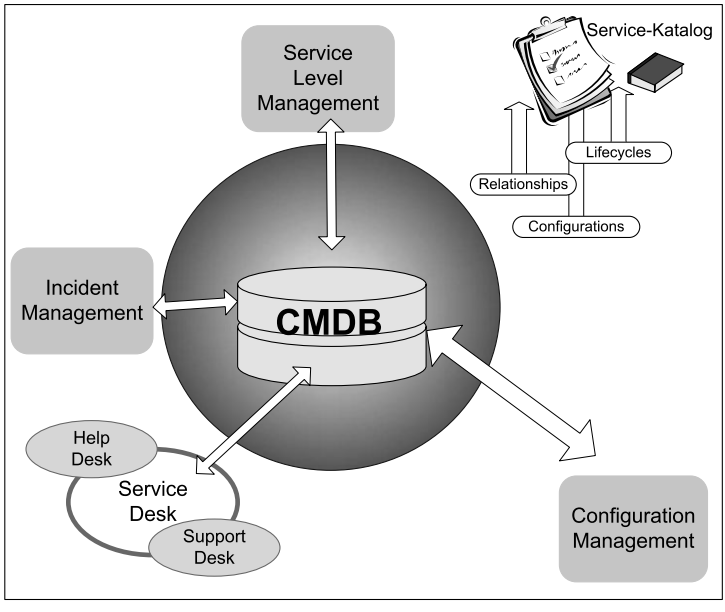


Abbildung 4.2: Dreh- und Angelpunkt im Service Support: Die CMDB

Abgrenzung zwischen Service Desk, Incident Management und Problem Management

Vielen ist die Einteilung des Service oder Help Desk als First Level-Anlaufstelle bereits ein Begriff. Dieser Einordnung sowie den Themen Second und Third Level Support wird an späterer Stelle Rechnung getragen.

Incident und Problem Management sind die Support-Prozesse für die Annahme und Behebung von Servicebeeinträchtigungen und damit ein entscheidender Faktor für die Zufriedenheit der Anwender bzw. Kunden der IT-Organisation. Incident Management wird vielfach von Service Desk-Mitarbeitern gesteuert, was aber keine zwingende Notwendigkeit darstellt, sondern oft aufgrund der Trennung von Aufgabenbereichen und Zuständigkeiten in großen Unternehmen meist gar nicht anders möglich ist. Daneben können und werden Spezialisten im Rahmen des einbezogen.

Das Release Management sorgt dafür, dass nur korrekte, autorisierte und getestete Komponenten für die Nutzung freigegeben werden. Dazu werden so genannte Releases gebildet und deren Einführung gesteuert. In der Regel werden nur Anwendungen im Unternehmen unterstützt, die innerhalb des Release Management freigegeben und über das Configuration Management in der CMDB dokumentiert werden. Hieraus bezieht das Service Desk bzw. Incident Management seine Informationen.

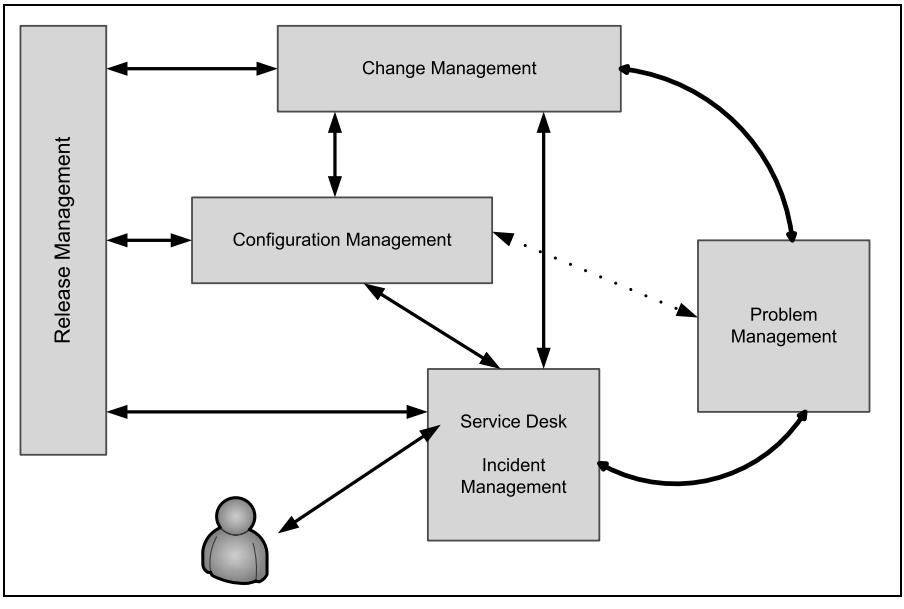


Abbildung 4.3: Interaktion im Service Support

Release

Ein Release stellt eine konsistente Menge von Software-Elementen dar, die als Ganzes die spezifizierten Anforderungen erfüllt.

4.2 Gliederung des Themenbereiches Service Support

Der ITIL-Bereich Service Support beschreibt die fünf Kapitel des ITIL-Modells:

- Service Desk
- Incident Management
- Problem Management
- Change Management
- Release Management
- Configuration Management

Die Reihenfolge ist dabei nicht unbedingt bindend, sondern je nach Einsatz im Unternehmen variabel in Bezug auf die jeweiligen Abhängigkeiten und Prozessflüsse.

Service Support und Service Delivery

Die taktische Ebene als Planung und Steuerung von IT-Dienstleistungen wird durch einen anderen ITIL-Themenkomplex repräsentiert, den Service Delivery (*siehe Abbildung 4.4*). Die operative Ebene stellt die Unterstützung von IT-Dienstleistungen als Service Support dar. Demzufolge steht dieser Bereich für den effizienten und kundenorientierten Betrieb von IT-Dienstleistungen.

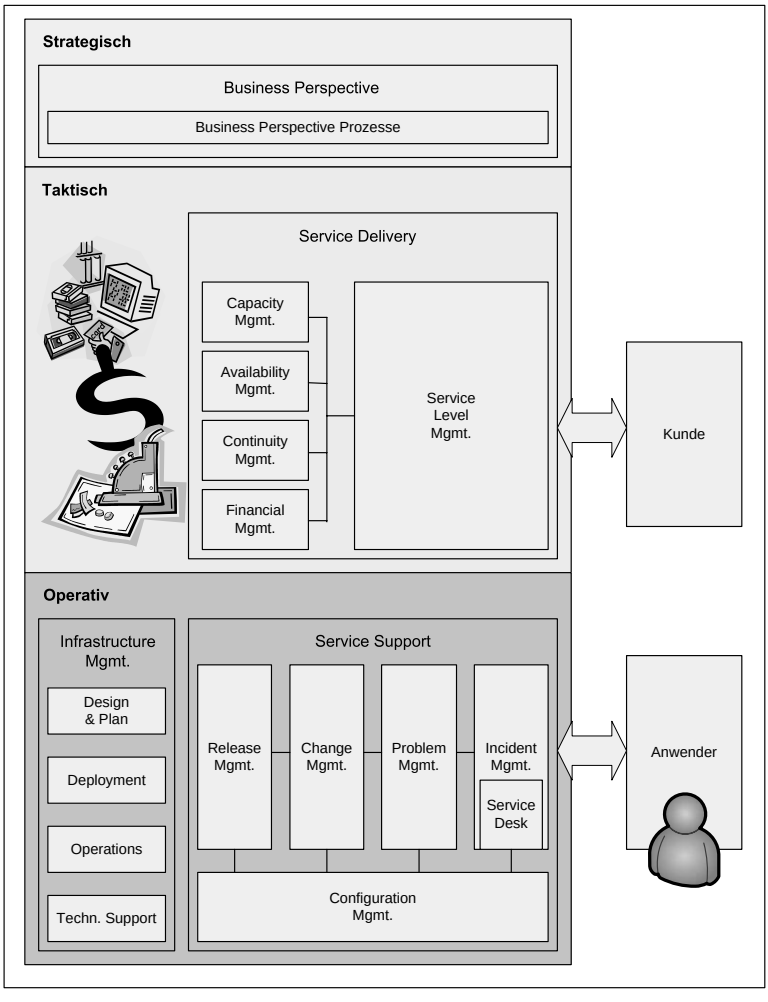


Abbildung 4.4: Aufteilung der ITIL-Bereiche

Anders gesagt: Der Service Support beschäftigt sich mit der täglichen Erbringung und Unterstützung von IT Services, Service Delivery befasst sich mit der mittel- bis langfristigen Planung, Beschaffung und Verbesserung der IT-Dienstleistung.

Neben dem selbstverständlichen Anspruch auf schnelle Störungsbehebung verlangen viele Kunden nach Folgendem:

- gleich bleibender Qualität der Dienstleistung(en)
- definiertem Service mit festgelegten Parametern
- Flexibilität und Schnelligkeit bei der Anpassung der Leistungen an geänderte Geschäftsanforderungen
- transparenten und klaren Kosten- und Abrechnungsstrukturen
- Messbarkeit des Beitrags zur Wertschöpfungskette

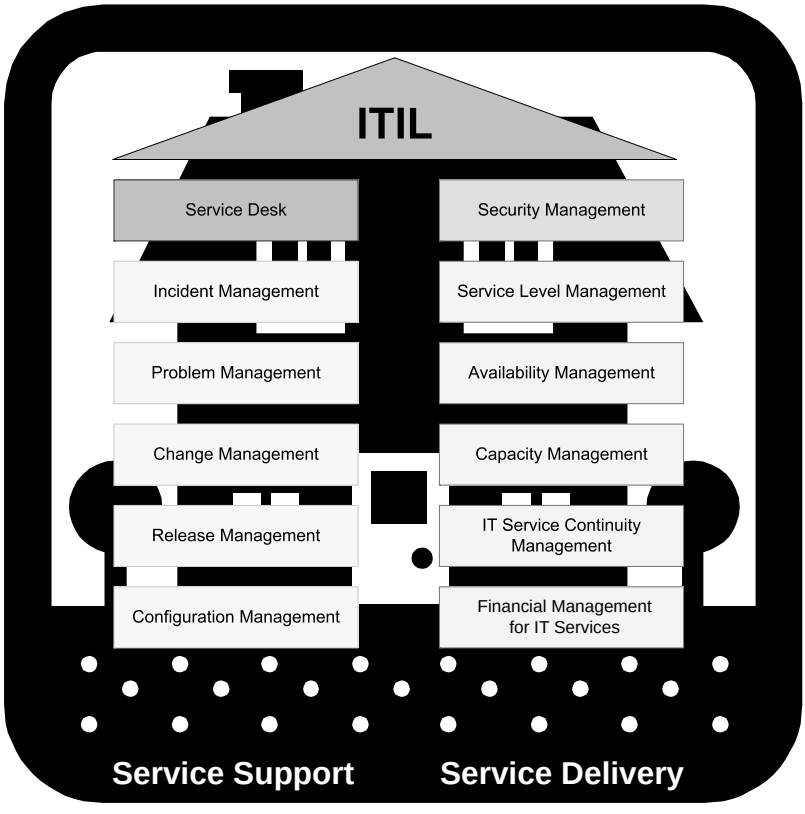


Abbildung 4.5: Unterscheidung Service Support und Service Delivery

Solchen Anforderungen kann man auf Seiten der IT-Dienstleister nicht alleine mit einem intensiveren Dialog begegnen. Die eigene Leistung lässt sich weiter steigern, wenn

- interne Prozesse optimiert und messbar sind,
- konsistente und vollständige Dokumentationen der Infrastruktur des Kunden vorliegen,
- Problemlösungen an den Ursachen und nicht an den Symptomen ansetzen,
- das Servicebewusstsein des IT-Personals gepflegt wird und
- gewünschte Anpassungen kosteneffizient und risikoarm durchgeführt werden.

Das Erreichen dieser Ziele steht im Fokus des professionellen IT Service Management, welches somit für IT-Dienstleistungsunternehmen ebenso bedeutsam wie unumgänglich ist.

Zu betonen sind die Seiteneffekte und Auswirkungen, die die Bereiche im Abschnitt Service Support untereinander und zu anderen ITIL-Bereichen haben. Als Beispiel bietet sich hier das Einbringen von Komponenten in die Live-Umgebung (Bereich Release-Management) an, welches auch die Bereiche Configuration und Change Management tangiert (*siehe Abbildung 4.6*).

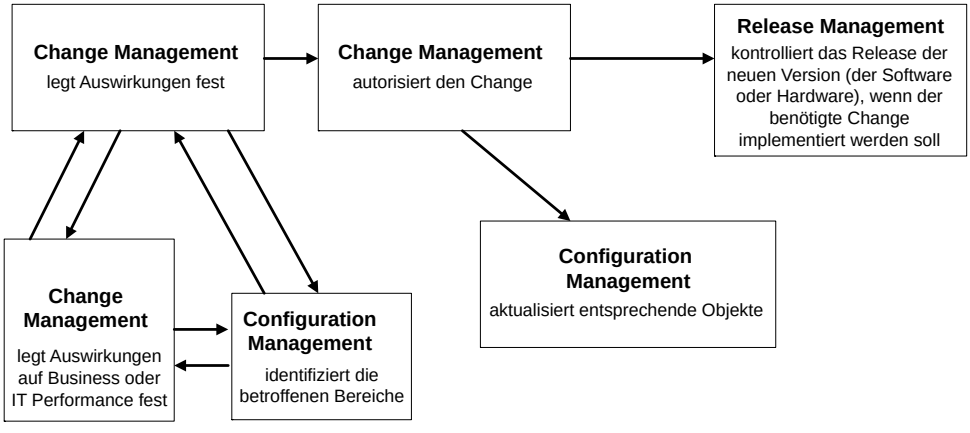


Abbildung 4.6: Beziehung zwischen unterschiedlichen Service Support-Bereichen

5 Service Desk

Der Service Desk stellt die primäre Kontaktstelle für sämtliche Belange rund um die IT Services zwischen dem Kunden und dem IT-Bereich dar. Dies beinhaltet die Help Desk-Funktionen und vielfach auch die Koordination von Change-Anforderungen, Service Level Management, Configuration Management und allen anderen Service Management-Prozessen von ITIL: Der Service Desk repräsentiert keinen Prozess, sondern eine Funktion innerhalb der Service-Organisation.

Um Kunden- und Geschäftsanforderungen in Hinblick auf den IT-Support zu erfüllen, existieren eine Reihe von Funktionen und Bezeichnungen, die Ihnen bestimmt schon einmal über den Weg gelaufen sind. Vielleicht haben Sie sich sogar schon gefragt, worin sich die einzelnen Namensgebungen unterscheiden:

- Call Center: Hier werden in der Hauptsache große telefonbasierte Gesprächsvolumina abgefangen. Dies ist vorwiegend aus dem Versicherungs- und Bankenumfeld bekannt.
- Help Desk: Der primäre Zweck des Help Desk liegt in der Verwaltung, Koordination und Lösung von Incidents, die so schnell wie möglich erfolgen soll, und zwar so, dass keine Anfrage verloren geht, vergessen oder ignoriert wird. Verbindungen zum Configuration Management und das Wissenstools für die Help Desk-Mitarbeiter sind vorhanden.
- Service Desk: Dieser erweitert im Grunde genommen die angebotenen IT-Dienste und stellt eine global-orientierte Leistung zur Verfügung, die zudem in die Service Management-Struktur integriert ist. Der Service Desk behandelt nicht nur Incidents, Probleme und Anfragen, sondern stellt eine Schnittstelle für weitere Aktivitäten zur Verfügung. Dies können Verbesserungsvorschläge von Seiten der Anwender für die alltäglichen Anwendungen und Tools sein, aber auch Themen wie Maintenance-Verträge, Software-Lizenzen, Service Level Management und andere ITIL-Bereiche. Vielfach werden Call Center und Help Desks in das Service Desk integriert, um die den Anwendern bzw. Kunden zur Verfügung gestellten Dienstleistungen auszuweiten und zu verbessern.

Das Service Desk ist fester Bestandteil der Aufbauorganisation einer Unternehmung. Damit wird auch verständlich, warum die verschiedenen ITIL-Prozesse innerhalb des Zuständigkeitsbereiches respektive Verantwortungsbereiches des Service Desk ablaufen können.

Die Entwicklung der IT-Dienstleistungen von der einfachen Batchverarbeitung hin zur komplexen Vernetzung von Technologien und Mitarbeiterbereichen hat neue Herausforderungen für das IT-Personal geschaffen. Aus einfachen Aufgaben sind komplexe Management-Funktionen entstanden. Der Service Desk stellt eine solche Aufgabe dar. War es früher durchaus noch möglich, wegen eines Problems den Supporter Ihrer Wahl anzurufen, ist heutzutage die Belastung des operativen

Personals derart groß, dass solche Störungen nicht mehr erwünscht sind. Die Anzahl Benutzer, die von IT-Dienstleistungen Gebrauch machen, wächst in jedem Unternehmen stetig an. Zudem sind die auftretenden Probleme oft schwierig nachzuvollziehen und komplex. Dies bedeutet, dass nicht nur die Anzahl der telefonischen Anfragen gestiegen ist, sondern auch, dass deren Inhalte höhere Ansprüche an die IT-Mitarbeiter stellen als früher.

Damit ist der Bereich, der für die Entgegennahme dieser Fragen verantwortlich ist, ein bedeutender Bestandteil des IT-Betriebes geworden. Seine Bedeutung wird auch in Zukunft steigen, da die erwähnte Entwicklung andauert. Service Desk-Mitarbeiter sind keine IT-DAUs ohne EDV-Know-how, auch wenn viele Mitarbeiter aus anderen Bereichen das gerne so sehen. Wer zwei Tage eine solche Tätigkeit hinter sich gebracht hat, wird das Ganze bestimmt in einem anderen Licht sehen. Nervenstärke und Serviceorientierung, schnelle Kategorisierungsfähigkeiten und ein breit gefächertes EDV-Allgemeinwissen sind hier unabdingbare Voraussetzungen. Und im Übrigen gibt es auch durchaus Experten-Service Desks, die sich nicht nur der Call-Annahme, sondern komplexen Problemlösungen widmen. Dies ist nicht die Regel, aber durchaus möglich.

Es gibt natürlich auch Negativbeispiele für Geschichten aus dem Bereich des Service Desk wie etwa der Text einer Anwenderanfrage, die in einem Ticket aufgenommen wurde: „User wünscht Zugriff auf eine Notes-Datenbank, die er mir aber nicht nennen konnte." – Schade!

Der Mensch im Service Desk

Wie überall sind im Service Desk motivierte und entsprechend den Anforderungen qualifizierte Mitarbeiter gefragt. Manchmal ist einem Kunden Verfügbarkeit wichtiger als Fachwissen. Oft liegt es eher am Kunden als an den Personen an sich, wenn es Probleme gibt, da Anforderungen bezüglich Know-how und Entwicklungsstand nicht klar definiert wurden. Im Vordergrund steht aber in jedem Fall die Forderung nach Freundlichkeit und Höflichkeit, was ganz wichtig in Hinblick auf die Akzeptanz durch die Anwender ist. Nicht nur die technische Kompetenz garantiert die Zufriedenheit des Kunden.

5.1 Service Desk nach ITIL

Der Service Desk stellt den „Single Point of Contact (SPoC)" in einer Service-Organisation. Mit Hilfe des Service Desk werden die Interessen der Kunden innerhalb der Service-Organisation repräsentiert. Eine Hauptaufgabe des Service Desk ist die Koordination und das Fungieren als zentrale Informationsstelle zwischen Kunden, internen Service-Organisationen und externen Providern.

Das Ziel dieser Funktion stellt sich als Unterstützung der vereinbarten Services und der Entlastung nachgelagerter Einheiten durch eine Art „Filterfunktion" dar. So wird eine selektive Weiterleitung der Anfragen, die in erster Instanz nicht gelöst werden können, vorgenommen. Deswegen fungiert der Service Desk als zentraler und primärer Ansprechpartner nach dem Prinzip „one face to the customer".

Die Festlegung der Service Desk-Struktur sowie deren personelle Besetzung hängen von einer Reihe von wichtigen Faktoren ab, welche die Form und Art des Unternehmens betreffen. Mit dem Wandel des Unternehmens muss auch die Struktur des Service Desk immer wieder angepasst werden. Grundsätzlich können folgende drei Service Desk-Strukturen unterschieden werden (*siehe Abbildung 5.1*):

- Zentraler Service Desk: Es gibt einen einzigen Service Desk, welcher für alle Organisationseinheiten, Niederlassungen und dezentralen Mitarbeiter zuständig ist. Der Vorteil liegt hier in der einfachen Handhabung und der Vereinheitlichung der Prozesse.
- Lokaler Service Desk: Jeder Standort oder jedes Departement in einem Unternehmen hat seinen eigenen lokalen Service Desk. Die Vorteile liegen in der optimalen Kundennähe und dadurch individuelleren Betreuungsmöglichkeiten.
- Virtuelle Service Desk-Organisation: Diese Art des Service Desk ist eine Mischform der beschriebenen Formen zentraler und lokaler Service Desk. Mit Hilfe der modernen Technologie können Informationen zentral gehalten und global zugänglich gemacht werden. Lokale Service Support-Einheiten unterstützen die Kunden vor Ort, wobei die zentrale Service Desk-Einheit für alle Anfragen sowie die Koordination der involvierten Service-Organisationen zuständig ist.

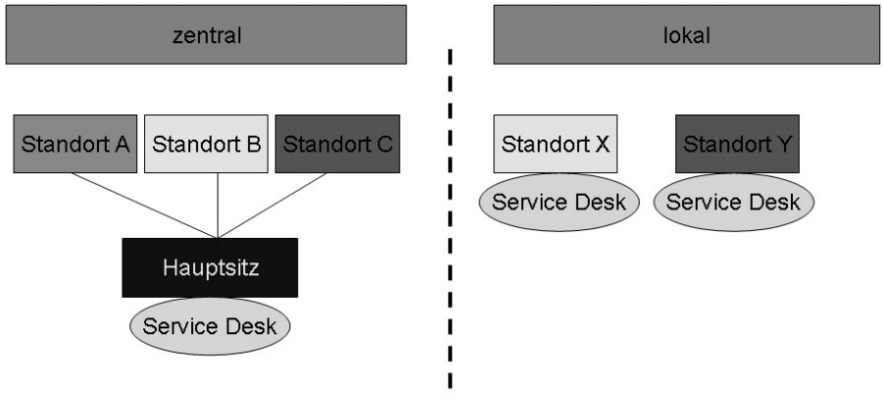


Abbildung 5.1: Unterscheidung lokaler und zentraler Help Desk

Es sollte stets nur ein einziger Ansprechpartner für den Erstkontakt der Anwender mit dem Service Desk aktiv sein. Zu beachten ist dabei, dass das Telefon nicht mehr das einzige Kommunikationsmittel darstellt. Es können Wünsche auch via Fax, eMail, Internet-/Intranetportale oder per Video-Request eintreffen und abgearbeitet werden. Letzteres ist eher die Ausnahme.

Die Bedeutung des Service Desk liegt speziell in seiner besonderen Rolle als Schnittstelle zwischen der IT und dem Endanwender. Damit repräsentiert der Service Desk die IT-Organisation gegenüber dem Kunden. Er stellt einen maßgeblichen Faktor für die Kunden- bzw. Anwenderzufriedenheit dar und ist somit auch von strategischer Bedeutung. Für den Anwender stellt dies oftmals die vielleicht wichtigste Funktion dar. Hier sitzen die Ansprechpartner für seine Fragen und oft auch die Personen, die ihm helfen und seine Probleme lösen.

Die Begriffe „Kunden“ und „Anwender“ werden in modernen Organisationen zunehmend als eine Einheit betrachtet. Kunden sind externe Partner und Anwender sind die internen Mitarbeiter. Beide arbeiten am System und haben somit dieselben Problemstellungen bezüglich des Supports.

Ein etwas grenzgängiges, aber trotzdem nicht zu vernachlässigendes Thema sind die Abrechnungsoptionen gegenüber dem Kunden. Dabei existieren die unterschiedlichsten Ansätze wie etwa Kosten pro Anruf (aufgeschlüsselt nach Problemtyp wie Desktop Service, Anwendung oder Upgradewunsch), Kosten auf Zeit und Material, Serviceanspruch basierend auf unterschiedlichen Supportverträgen und dementsprechenden Leistungen (Platin, Gold, Silber, Bronze), freier Service, Paket-/Fixleistungen als Overhead zum bereitgestellten IT Service.

5.2 Service Desk-Aufgaben und -Funktion

An dieser Stelle ist zu betonen, dass dem ITIL Service Desk gegenüber einem herkömmlichen Help Desk ein erweitertes Aufgabenspektrum zukommt. Es profitieren nicht nur die Anwender von einer zentralen Anlaufstelle, sondern auch die involvierten IT-Verantwortlichen und Service-Organisationen. Der Anforderungsbereich reicht von einer Störungsannahme, einer (eventuellen) Bearbeitung oder einem Weiterrouting über Statusberichte bis hin zur Lösung des Problems.

Status und Info: Feedback für den Kunden

Statusmeldungen an den Anwender zu geben ist keine zu vernachlässigende Aufgabe im Bereich des Service Desk. Dies ist nicht nur eine Bestätigung für den Kunden, dass sein Anliegen akzeptiert und aufgenommen wurde, sondern erspart auch unnötige Anforderungen an den Service Desk. Diese Statusmeldungen können aufgrund von diversen Aktivitäten und Zuständen der Anfrage in unterschiedlichen Ausprägungen ausgegeben werden.

Die Aufgaben für den Service Desk können sein (*siehe Abbildung 5.2*):

- einheitliche Kontaktstelle für die Kunden
- Registrieren und Nachverfolgen von Störungsmeldungen sowie Reklamationen
- laufende Information der Kunden betreffend Status und Fortschritt der Anfragen
- Durchführung einer ersten Prüfung der Kundenanfrage und Einleiten der Bearbeitung basierend auf den vereinbarten Service Levels
- Überwachung der Einhaltung der Service Level Agreements und ggf. Einleitung einer horizontalen (fachbezogenen) und/oder vertikalen (managementbezogenen) Eskalierung bei Gefahr der Nicht-Einhaltung der definierten Servicequalität
- formaler Abschluss der Anfragen inklusive Überprüfung der Zufriedenheit des Kunden, um sicher zu gehen, dass Probleme gelöst, Workarounds weitergegeben oder Anfragen beantwortet wurden

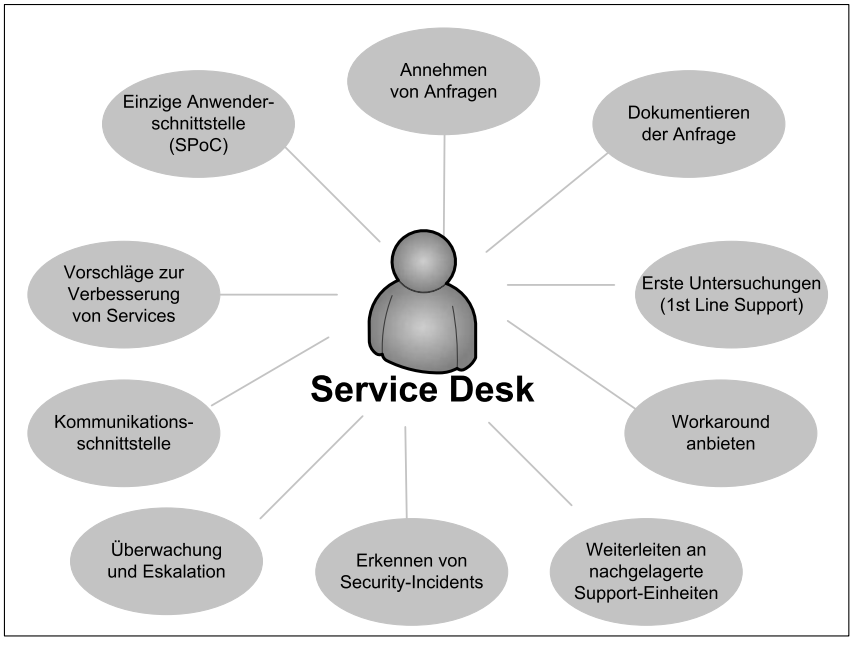


Abbildung 5.2: Vielfältige Aufgaben im Service Desk

- Koordination der nachgelagerten Second Level Support- sowie Third Party Support-Einheiten
- Bereitstellen von Management-Informationen zur Verbesserung der Servicequalität

Mancherorts ist das Service Desk auch für die Überwachung der Service Level Agreements (SLAs) oder Server Level Objectives (SLO) zuständig. Hier geht es um die Überwachung der Nachhaltigkeit und eine Art Problemlösungscontrolling auf Basis von vorab vereinbarten Richtwerten. In diesem Fall koordiniert der Service Desk die angrenzenden Support-Einheiten wie den Second Level Support und weitere Eskalations- und Lösungswege wie etwa Rufbereitschaften. Vielfach ist auch eine Einbindung des Bereiches Einkauf vorhanden.

Kurz und knapp: Mögliche Aktivitäten im Service Desk

- Jeder Anruf = Anfrage
  - Störungsmeldungen: Beeinträchtigung/Nicht-Verfügbarkeit
  - Service Request: Passwort zurücksetzen, Statusnachfrage
- Änderungen: Anstoßen von RfCs in Bezug auf Standardinstallationen/-bestellungen, Betreuung von Umzügen
- Bereitstellen von Informationen
  - z.B. aktiv bei Massenstörungen, Katastrophen, großflächigen Wartungs- oder Installationsarbeiten
- Überwachen der Infrastruktur: automatisiert oder aktiv

Der Nutzen ergibt sich aus folgenden Punkten:

- aktive Information der Anwender im Verlauf der Störungsbehebung
- Entlastung der Spezialisten durch Annahme und Beantwortung von Service Request
- Schaffung eines „Single Point of Contact“ und somit verbesserter Zugriff auf Informationen für die Anwender
- erweiterter Kundenfokus und pro-aktiver Ansatz bei der Service-Erbringung
- verbesserter Kundenservice und dadurch erhöhte Kundenzufriedenheit bzw. zufriedene Anwender durch professionelle und kompetente Hilfe
- schnellere und qualitativ bessere Abwicklung von Kundenanfragen
- verbessertes Teamwork und Kommunikation innerhalb der Service-Organisationen
- Reduzierung von negativen Auswirkungen auf das Unternehmen bei Störungs- und Problembearbeitung
- besser kontrollierte und verwaltete IT Infrastruktur-Komponenten
- verbesserte Nutzung der IT Support Ressourcen und dadurch erhöhte Produktivität
- verbesserte und aussagefähigere Management-Informationen für die Entscheidungsfindung
- Identifikation von Trainingsbedürfnissen des Kunden zur verbesserten Service-Nutzung

Die verantwortlichen Mitarbeiter und Abteilungsvorgesetzten erhalten in ad hoc gesetzten oder definierten Zeitabständen Informationen, Reportings und Übersichten, um die Servicequalität zu überwachen und weiter zu verbessern. Auch wiederkehrende Störungen werden erfasst, um gegebenenfalls Problemlösungen zu finden bzw. die betroffenen Einheiten schnell informieren zu können. Vielfach fallen nämlich an dieser Stelle schon Unregelmäßigkeiten der bereitgestellten Services auf, bevor sich diese massiv beim Kunden bemerkbar machen. Gehäufte Anrufe zu einem bestimmten Server oder einem Service weisen in der Regel auf ein Problem hin – sei es auf das entsprechende Objekt an sich (Printserver, Web-Anwendung) oder ein verwandter Service (Netzwerk).

Durch entsprechende automatisierte (Monitoring-)Tools kann die Arbeitsweise von einer rein reaktiven ausgeweitet werden auf eine proaktive Handlungsweise des Service Desk. Dabei ist es wichtig, dem Service Desk nur eingeschränkte Rechte einzuräumen.

In Hinblick auf auftretende Incidents ist reaktiv ein entsprechender Eskalations- bzw. Lösungsweg zu definieren und einzuschlagen, so dass die adäquaten Personen oder Service-Einheiten verständigt werden können und ein Eskalationsmanagement-Prozess angestoßen werden kann. Wichtig ist hierbei ein entsprechender Klassifizierungsrahmen.

Ohne korrekte Klassifizierung kann auf eine Anfrage nicht zufriedenstellend reagiert oder ein Problem nicht gelöst werden. Wenn diese Anforderungen nicht adressiert werden, gibt es auch niemanden, der sich darum kümmern kann. Also müssen Themen, die im Service Desk aufschlagen, spezifiziert werden – und das im Hinblick auf

- den Service oder das Equipment, zu dem der Incident gehört,
- damit verbundene SLAs oder SLOs,
- die nötige Auswahl der Person oder Gruppe, die den Incident bearbeiten soll,
- eine Abschätzung der Auswirkungen und der Priorität für den Geschäftsbetrieb,
- die Definition der Fragen, die dem Kunden gestellt werden müssen, um ein Problem einzugrenzen und die zur Weiterverarbeitung notwendigen Informationen zu erhalten,
- Kriterien die zur Zuordnung bereits bekannter Fehler oder Workarounds beitragen,
- eine Zusammenfassung und Definition der Aktionen, die zur Lösung beitragen (Lösungssammlung) bzw. Aufstellung entsprechender Schlüsselworte (*Problem existiert nicht mehr, Informationsgespräch, Kundentraining vonnöten, Kein Fehler gefunden, Change Request erforderlich, Reboot erforderlich*),
- die Definition einer ersten Reporting-Matrix zur Management-Information,
- Empfehlungen für Service-Verbesserungen,
- Schulungsbedarf bei Mitarbeitern oder den Anwendern.

Neben der Kommunikation zwischen dem Service Desk und dem Kunden ist aber auch Feedback und Kritik der angrenzenden Service-Einheiten in Bezug auf das Service Desk vonnöten. Dies dient einer Verbesserung der Problemannahme und Koordinierung. Diesbezüglich ist aus der Erfahrung zu betonen, dass es hier einen ständigen Optimierungsbedarf gibt. Aufgrund der zu betreuenden Items können vielfach Irritationen und Fehler auftauchen, die teilweise als schlicht menschlich zu werten sind, teilweise aber auch einem fehlenden Qualitätsbewusstsein von Mitarbeitern entspringen. Messkriterien sind:

- Erhöhte Kundenzufriedenheit
- Reduzierung der Störungs- und Beschwerde-Meldungen
- Reduzierung der Service-Kosten
- Bessere Koordination der IT Service-Aufgaben mit den involvierten internen und externen Stellen
- Höhere Motivation der Service-Mitarbeiter

Überwachung, Reporting und Leistungsindikatoren (KPI)

Mögliche Messpunkte sind die Anzahl eingegangener Incidents, die Anzahl abgeschlossener Incidents beim Service Desk und die Anzahl der nach Zeitraum XY noch nicht abgeschlossener Incidents. Letztlich stellt die Zufriedenheit des Kunden den wichtigsten Indikator dar.

Weitere Messfaktoren:

- Prozentsatz der im Service Desk behobenen Störungen
- Zahl der Anfragen und Verteilung
- Durchschnittlicher Zeitaufwand für die Lösung
- Zeitdauer bis Anruf entgegengenommen wird

5.3 Der Service Desk im ITIL-Gesamtzusammenhang

Grundvoraussetzung für das Funktionieren des Service Desk ist die Einbindung in die gesamte IT-Struktur und –Organisation. Er darf keine Insellösung sein. So wissen die Anwender, dass sie bei EDV-Problemen immer die gleiche Nummer wählen müssen und sollen. Positive Erfahrungen des Anwenders verstärken diesen Lerneffekt („Hier wird mir schnell geholfen!“). Dies führt dazu, dass sich die Bearbeitung von Aufgaben und der diesbezügliche Informationsfluss zentral steuern. Außerdem werden zentrale Ressourcen und Services adäquat genutzt.

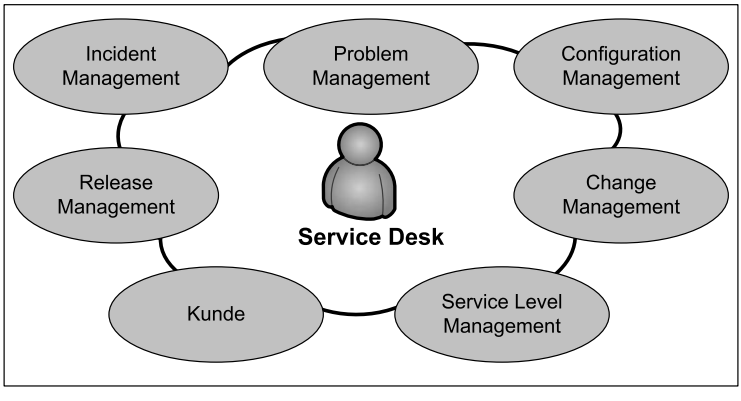


Abbildung 5.3: Service Desk im ITIL-Verbund

Bei ITIL nimmt der Service Desk eine wichtige und zentrale Stellung ein (*siehe Abbildung 5.3*). In den meisten Unternehmen findet sich die früher Benutzerservice oder Helpdesk benannte Organisation als Kommunikationsstelle zwischen der Informationstechnologie und den Benutzern oder Kunden. Der Service Desk selbst ist also kein ITIL-Prozess, sondern die Schaltstelle für die meisten ITIL-Prozesse. In erster Linie ist der Service Desk als Ansprechpartner für verschiedene Belange, Probleme und Anfragen seitens der Anwender/Nutzer zu sehen. Die Anfragen bzw.

die Meldungen von Störungen aller Art bei der IT-orientierten täglichen Arbeit müssen entgegengenommen, klassifiziert und dokumentiert sowie an die entsprechenden Stellen und Experten weitergeleitet werden. Auch die IT-Mitarbeiter nutzen die Möglichkeiten und das Wissen der Gruppe. Zumeist werden verschiedene Bearbeitungsstufen oder auch Eskalationsebenen unterschieden:

1. First Level für sofortige Lösungen durch das Call Center,
2. Second Level für komplexere und schwierigere Lösungen durch Teams oder Fachkräfte,
3. Third Level für das Einschalten von Experten bei spezifischen Problemen,
4. gegebenenfalls der Fourth Level für die Vergabe von Lösungsaufträgen an externe Stellen (Wartung, Garantiefälle etc.).

Diese Prozesse spielen eine zentrale Rolle für das Service Management. Auf die Integration der häufig isolierten Prozesse und Lösungen kommt es an. Der Service Desk ist das Sprachrohr und ein wesentlicher Sensor gegenüber dem Anwender. Hier werden vielfältige Informationen für andere Prozesse generiert, zum Beispiel für das Anforderungsmanagement von Services und Produkten, für die Leistungsprozesse im IT-Betrieb oder für das Service Level Management.

In welchem Umfang ein Service Desk die Anwender unterstützt, ist abhängig vom jeweiligen Unternehmen und den vorhandenen Aufgabendefinitionen. Laut ITIL entspricht das Service Desk eher dem First Level Support.

In verteilten IT-Organisationen ist das richtige Maß lokaler und zentraler Abwicklung zu finden. Konkurrierende Ziele wie Massenabwicklung trivialer Requests und qualifizierte Beantwortung anwendungsspezifischer Fragen erfordern eine strukturierte Organisation des Service Desk. Der hohe Umschlag an Prozessvorgängen erfordert hier zudem ausgefeilte Analyse- und Controlling-Instrumente. Wo der Service Desk im Outsourcing betrieben wird, führen die hohen Integrationsanforderungen zu komplexen Dienstleisterschnittstellen. Prozesse und Lösungen sollten hier nahtlos ineinander greifen. Des Weiteren sollten von Beginn an Zuständigkeiten und Prioritäten geklärt und kommuniziert werden. So müssen sich nicht unterschiedliche Stellen mit dem gleichen Problem herumschlagen, Anfragen nicht mehrfach beantwortet werden oder gar intern Lösungen erarbeitet werden, für die externe Supportverträge vorliegen.

Prozesse, die über die Funktion Service Desk abgebildet werden können

- Incident Management: Großteil, da die meisten Anfragen beim Service Desk Störungen sind → aufnehmen, überwachen
- Release/Change Management: bei Installationsprozessen
- Configuration Management: Korrekte Daten des Anwenders und der Ressourcen beim Service Desk abfragen/abrufen
- Service Level Management: Anfragen, Informationen über Standards und Leistungen, darüber hinausgehende Anfragen, …

Die wichtigsten Schnittstellen des Service Desk liegen im Bereich Incident Management, nachgelagertem Problem Management und Change Management sowie den Bereichen, die sich dem Configuration Management und Service Level Management verantwortlich zeigen (*siehe Abbildung 5.4*).

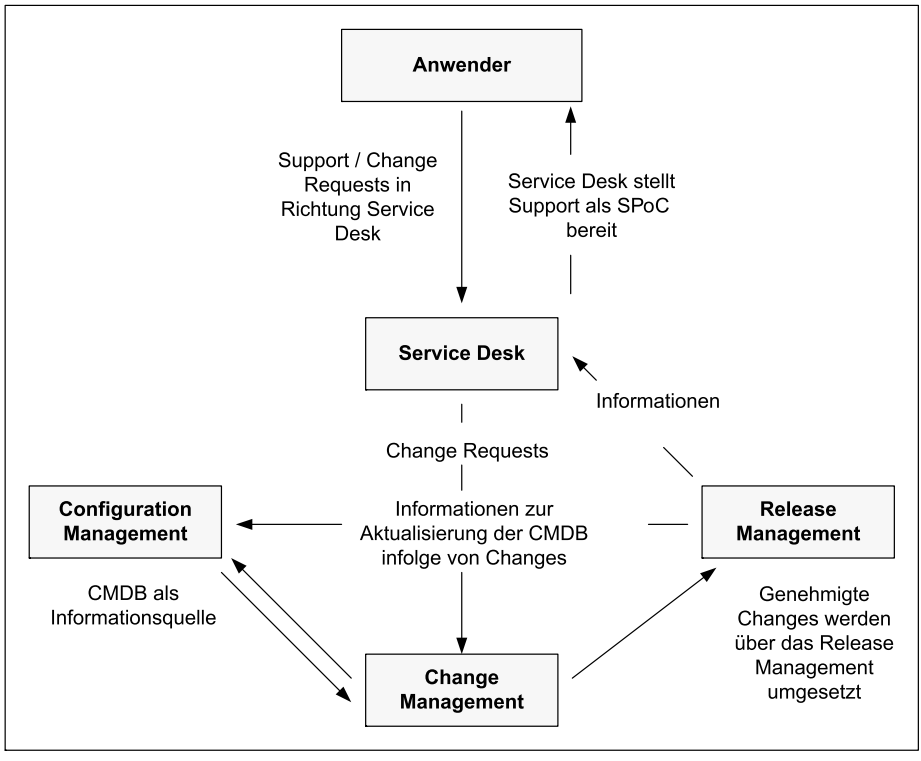


Abbildung 5.4: Interaktion mit den Prozessen des Service Support

Die Verbindungen zu den Einheiten aus dem Bereich Service Support erleichtern das Erkennen von Störungsursachen, da durch diese ein Überblick der betroffenen IT-Items zustande kommt. Hierbei nimmt die Configuration Management-Datenbank (CMDB) eine zentrale Rolle ein. Der Service Desk fragt die hier abgelegten Informationen ab und verwendet sie. Diese Datenbank ist die Basis der Tätigkeiten im Service Desk. Hier sind Informationen zum Anwender wie Stamm- und Kontaktdaten und Daten zu seinem Rechner (MAC-Adresse, IP, weitere Informationen zur Hardware) oder der entsprechenden Anwendungssoftware hinterlegt (*siehe Abbildung 5.5*).

Dies erfordert eine entsprechende Kommunikation und hilft so auch, sich anbahnende Probleme aufzudecken und künftige Störungen zu vermeiden.

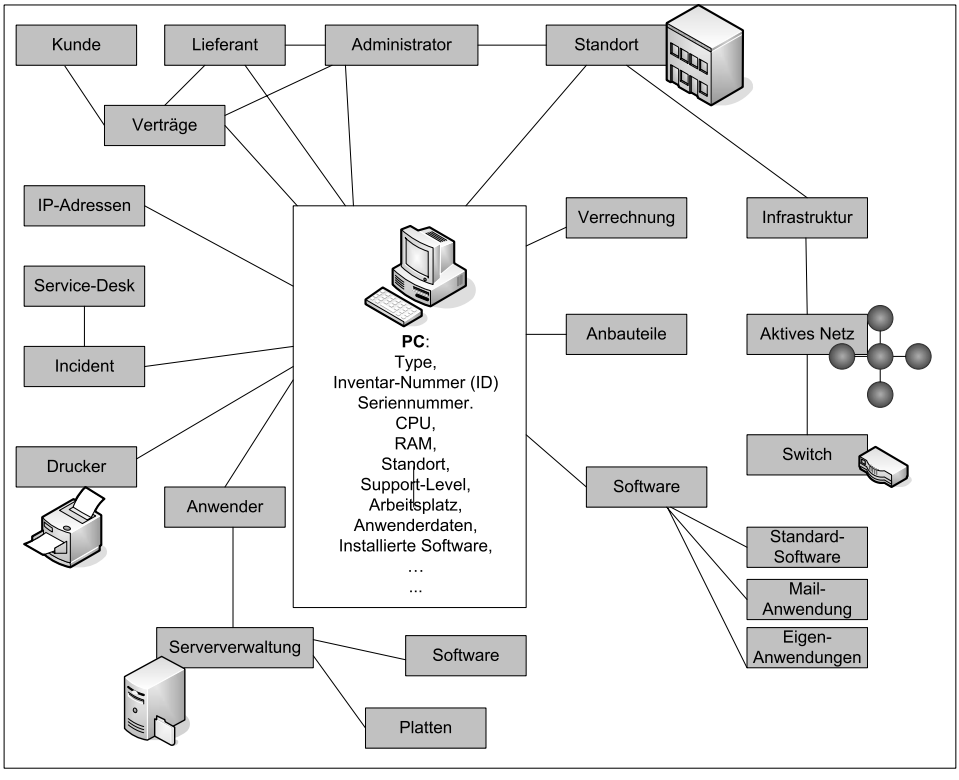


Abbildung 5.5: Die CMDB und die für das Service Desk relevanten Informationen

5.4 Tools

Nicht mehr wegzudenken aus dem Bereich Service Desk ist die Software, die zur Abwicklung von Aufgaben, Anforderungen und Funktionen zur Verfügung steht. Über dieses Instrument laufen die entsprechenden Prozesse und Workflow-Mechanismen. Dabei sind umfangreiche Reporting-Funktionen unerlässlich. Im Vordergrund steht aber stets die Frage, ob die eingesetzten Technologien die Anforderungen und Bedürfnisse des Kunden erfüllen. Nicht die neueste, sondern eine zuverlässige und anwenderfreundliche Technologie ohne böse Überraschungen ist gefragt. Hier geht es auch um die Frage, ob immer ein persönlicher Kontakt zum Service Desk-Mitarbeiter erfolgen muss oder ob der nicht-personalisierte Kommunikationsweg über Fax, eMail, Pager oder andere Tools erfolgen kann.

Der Person im Bereich Service Desk stehen neben den bereits genannten technischen Möglichkeiten, über die der Anwender Kontakt aufnimmt, weitere Werkzeuge zur Seite. Dazu gehören VOIP-Systeme, Wissens-, Such- und Diagnose-Tools sowie automatische Operations- und Netzwerk-Management-Tools. Hier stellt sich die Frage, ob Drittanbieter-Entwicklungen oder eigene Lösungen eingesetzt werden. Dies kann aber nur individuell und nicht pauschal beantwortet werden.

6 Incident Management

Incident Management ist ein Prozess aus dem Service Support-Set. Der Prozess umfasst weitgehend reaktive Aufgaben, mit denen sichergestellt wird, dass Störungen behoben werden und der Anwender so schnell wie möglich weiterarbeiten kann. Incident Management ist aber auch für verschiedene andere Prozesse von Bedeutung. Dieser Prozess stellt Informationen zu Störungen in der Infrastruktur zur Verfügung bzw. integriert diese Bereiche zur Lösungsfindung, falls das Incident Management nicht in der Lage ist, eine Störung selber zu beheben. Dann wird der Incident an einen anderen Prozess weitergegeben.

6.1 Incident Management nach ITIL

Das Incident Management ist für die schnellstmögliche Wiederherstellung des definierten Betriebszustands eines Service zuständig. Dabei werden meist neben Störungen auch alle Anfragen (Service Requests) der Anwender über ein Service Desk erfasst, erste Hilfestellung geleistet und gegebenenfalls die weitere Bearbeitung in den nachgelagerten Supporteinheiten koordiniert. Hinzu kommt die Aufgabe, den Anwender in vereinbarten Zeitintervallen über den Status der Fehlerbeseitigung zu unterrichten.

Incidents stellen Störungen dar. Es handelt sich dabei um Ereignisse, die nicht zum Standard-Betrieb gehören und tatsächlich oder potenziell eine Beeinträchtigung oder eine Minderung der Servicequalität darstellen. Das Incident Management muss die normale bzw. vereinbarte Dienstleistung (gemäß SLAs) in definierter Qualität so schnell wie möglich wieder herstellen, um negative Auswirkungen auf das Kundengeschäft zu minimieren. Ziel ist es, die Servicequalität und -Verfügbarkeit auf dem höchstmöglichen Level zu halten.

Incidents können in Bezug auf unterschiedliche Komponenten der IT-Umgebung auftreten:

- Hardware: System down, Drucker druckt nicht, Switchausfall
- Anwendungen: Dienst nicht verfügbar, Fehler in der Anwendung, kein Plattenplatz mehr

Der Service Request stellt einen Sonderfall dar und bezieht sich auf einen anderen Sachverhalt. Ein Service Request tritt in unterschiedlichen Ausprägungen auf und betrifft Fragen und Vorschläge zur Anpassung der Infrastruktur, Erweiterung der IT-Dienstleistungen, Installation von PCs, Software und Druckern (Request for Service, RfC). In den meisten Fällen liegt als Grund für den Kontakt des Incident Management keine Störung vor, sondern ein anders geartetes Anliegen.

Es gibt unterschiedliche Möglichkeiten, mit Service Requests umzugehen. In der Regel werden sie vom Incident Management aufgenommen, kategorisiert, klassifiziert und einem entsprechenden Anforderungsverfahren zugeordnet, das mit einem dahinter liegenden Workflow den entsprechenden Request erfüllen kann.

Service Request

Ein Service Request kann als Anfrage bezüglich Informationen, Ratschlägen oder Dokumentationen oder als Nachfrage nach einem vergessenen Passwort verstanden werden.

ITIL bezeichnet sowohl Störungen als auch Service Requests als Incidents. Störungen können ihre Ursache in verschiedenen Teilen der Infrastruktur finden. Vielfach werden Störungen durch den Anwender gemeldet.

6.1.1 Begriffe des Incident Management

Obwohl Incident Management einen wesentlichen Teil der Aufgaben des Service Desk darstellt, wird dieser Prozess nicht allein im Service Desk abgebildet. Incident Management liegt als Prozess horizontal in der Organisation und sorgt dafür, dass den Anwendern geholfen wird, die Registrierung und Steuerung von Störungen sorgfältig vorgenommen wird. Dabei werden Eskalationsfristen definiert und Incidents nach einer hierarchischen Symptomkategorisierung priorisiert, klassifiziert und gewichtet. Incidents können und müssen mit anderen Vorgängen verknüpft werden.

Der Unterschied zwischen Service Desk und Incident Management

Das Service Desk ist eine Funktion („Wie ist etwas zu tun?“), Incident Management der Prozess („Was ist zu tun?“). Im Grunde genommen kann der Service Desk dem Incident Management zugeordnet werden. In der Literatur und in Online-Quellen werden zu beiden Themen fast identische Beschreibungen angeboten, so dass eine Abgrenzung vielfach unmöglich erscheint. Natürlich ist es möglich, dass Service Desk und Incident Management über gleiche Abteilungen abgewickelt werden, so dass die Aufgaben identisch sind. Diese Erfahrung aus der Praxis hilft nicht bei der Differenzierung.

In der Prüfung wird oft explizit gefragt, welche *Funktion* bestimmte Aufgaben übernimmt. Hier ist aus der Fragestellung abzulesen, dass hier die Antwort „Service Desk“ richtig sein muss. Denn: *Der Service Desk ist die einzige im Service Support-Set beschriebene Funktion*, alles andere sind Prozesse! Wird nur nach dem entsprechenden *Prozess* gefragt, scheidet die Antwort „Service Desk“ aus, weil dies die *Funktion* darstellt.

Etwas kniffeliger wird es, wenn in der Aufgabenstellung gefragt wird, welcher *Prozess oder welche Funktion* eine bestimmte Aufgabe umsetzt oder für eine bestimmte Rolle zuständig ist. Hier müssen Sie prüfen, ob sich die beschriebene Tätigkeit wirklich den Prozessschritten aus dem Incident Management zuordnen lässt.

(Fortsetzung)

Wenn beispielsweise danach gefragt wird, welche Funktion oder welcher Prozess dafür zuständig ist, einen Incident zu klassifizieren, dann ist es das Incident Management. Dieser Prozessschritt ist aus der Definition der Prozessabfolge abzulesen. Wenn gefragt wird, welcher *Prozess oder welche Funktion* einen Telefonanruf des Anwenders entgegennimmt, dann ist es der Service Desk, da es sich um eine personalisierte Funktionsbeschreibung handelt, die nicht exakt auf die Prozessaktivitäten des Incident Managements abzubilden ist.

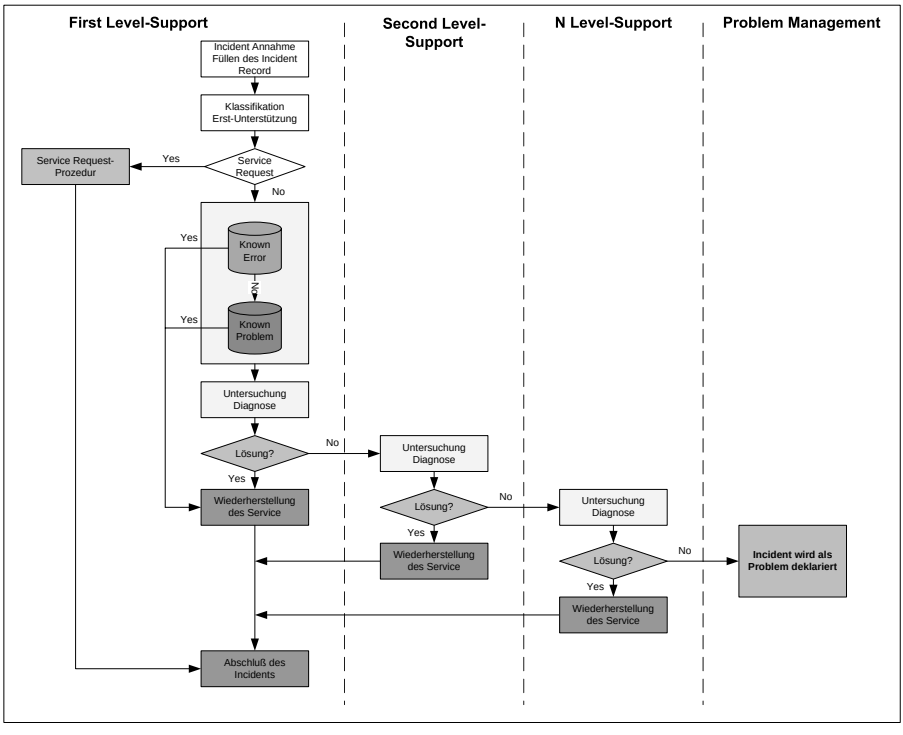


Abbildung 6.1: Prozessabfolge im Incident Management

Wenn danach gefragt wird, welcher Prozess oder welche Funktion einen Anwender zurückruft, um einen Status weiterzugeben, dann ist es das Service Desk. Diese Tätigkeit ist so nicht in der beschriebenen Form aus der Prozessabfolge des Incident Management abzulesen.

Oft hilft auch die Fragestellung, ob es um eine abstrakte Beschreibung (für das Incident Management) geht oder um konkrete, auf Personen abgebildete Tätigkeiten, die dem Single Point of Contact zugeordnet werden können.

Einige Begriffe tauchen in diesem Zusammenhang immer wieder auf:

- Problem: Die Ursache für einen oder mehrere Incidents wird Problem genannt. Die Analyse von Incidents (reaktiv) sowie die Beurteilung von Trends (proaktiv) lassen Probleme (Fehlerursachen) erkennen und sorgen im weiteren Verlauf für eine grundsätzliche Behebung bzw. Vermeidung von Störungen.
- Known Error/bekannter Fehler: Ist die Ursache einer Störung bekannt, diese aber noch nicht behoben, spricht man von einem bekannten Fehler. Um diese letztendlich zu beseitigen, ist eine Änderung (Change) der Software, Komponente oder der Infrastruktur erforderlich (*siehe Abbildung 6.2*). Da dies in vielen Fällen einige Zeit in Anspruch nimmt oder Updates vonnöten sind, die noch nicht zur Implementierung zur Verfügung stehen, wird dem Kunden eine temporäre Lösung (Workaround) angeboten. Dies löst nicht das eigentliche Problem, hilft dem Kunden aber, (mehr oder weniger eingeschränkt) auf gewohnte Art und Weise weiterarbeiten zu können, und verhindert Ausfälle.
- Workaround: Oftmals lassen sich Probleme (Störungsursache) nicht sofort lösen. Daher werden für bekannte Fehler Übergangslösungen erarbeitet, die dem Incident-Management zur Verfügung gestellt werden. Zum Beispiel kann die Benutzung eines anderen Printservers empfohlen werden, falls der primäre Server ausgefallen ist.

Abbildung 6.2: Zusammenhänge zwischen Incidents, Problemen, bekannten Fehlern und RfCs

- Impact ist das Maß, welches die Auswirkung der Störung auf den Service zum normalen (vereinbarten) Service Level ins Verhältnis setzt. Dabei geht es auch um die Folgen, die eine Störung auf das Tagesgeschäft des Anwenders hat.
- Die Dringlichkeit bezeichnet das Maß, in dem der Anwender bei der Ausübung seiner Tätigkeiten behindert wird. Incident Management legt diese Dringlichkeit in Absprache mit dem Kunden fest. Für ihn stellt die Dringlichkeit den maximal tolerierbaren Verzug der Störungsbeseitigung dar.
- Die Priorität definiert sich aus Dringlichkeit und Impact (Auswirkung). Falls gleichzeitig mehrere Störungen bearbeitet werden müssen, die nicht unmittelbar beseitigt werden können, muss die Arbeit priorisiert werden können. Die Zuordnung von Prioritäten basiert dabei hauptsächlich auf der Auswirkung einer Störung auf den Betrieb des Kunden (*siehe Abbildung 6.3*). Die Priorität gibt vor, in welcher Reihenfolge Störungen vorrangig zu bearbeiten und zu lösen sind.

  Eine Störung, von der ein einzelner Anwender in hohem Maß betroffen ist, kann somit eine höhere Priorität erhalten, als eine Störung, die die Arbeit von mehreren Anwendern in einer geringeren Auswirkung beeinträchtigt.

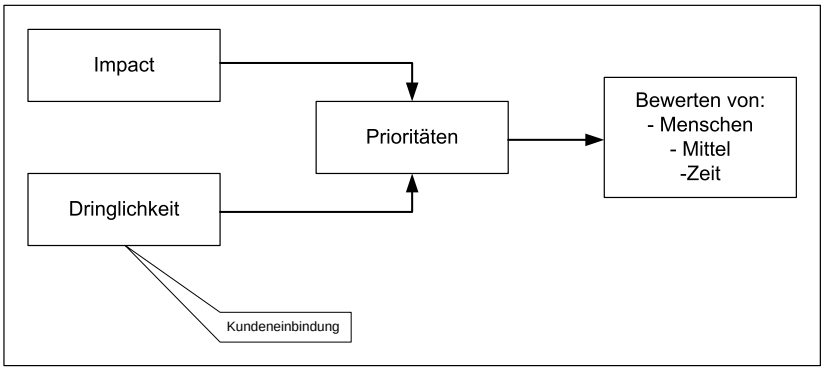


Abbildung 6.3: Größen zur Definition der Priorität

	Auswirkungen		
Dringlichkeit	**Niedrig**	**Mittel**	**Hoch**
Hoch	1	2	3
Mittel	2	3	4
Niedrig	3	4	5

Tabelle 6.1: Prioritätenfindung

Die Richtlinien für Impact-, Dringlichkeits- und Prioritätsbestimmung sollten in den SLAs stehen, ebenso die korrespondierenden definierten Lösungszeiten.

Priorität	Eskalationsstufe	Information intern	Information Eskalationsstufe
1	A	sofort	Sofort
2	B	XX Minuten	XX Minuten
3	C	X Stunden	X Stunden

Tabelle 6.2: Prioritätsstufen

Priorität 1 beschreibt den Gesamtausfall im Sinne eines Komplettausfalls des Systems. Kein Anwender kann im System arbeiten. Priorität 2 steht für einen Teilausfall, der den Ausfall einer wesentlichen Komponente des Systems darstellt. Ein großer Teil der Anwender kann nicht im System arbeiten oder ist in der Arbeit eingeschränkt. Priorität 3 wird für einen Einzelausfall verwendet, wenn ein Ausfall einer nicht wesentlichen Komponente des Systems die Ursache ist. Eine begrenzte Anzahl von Anwendern ist in ihrer Arbeit mit dem System beeinträchtigt.

- Kategorisierung/Klassifizierung (*siehe Abbildung 6.4*): Innerhalb einer Klassifizierung oder Kategorisierung wird der Incident einer bestimmten, unternehmensspezifischen Kategorie zugeordnet. Die Kategorisierung erfolgt nach den ersten Anzeichen (Indizien) der Störung, damit die mögliche Ursache schneller ermittelt werden kann. Netzwerk, Workstation, zentrale Verarbeitung oder die spezifischen Anwendungen können Beispiele einer möglichen Einteilung sein.

- Eskalation: Wenn sich herausstellt, dass eine Störung nicht innerhalb der im Service Level Agreement vereinbarten Zeit beseitigt werden kann (auf der Grundlage der Prioritätenregelung), müssen Maßnahmen ergriffen werden, um die Bearbeitung zu beschleunigen. Das kann bedeuten, dass mehrere Mitarbeiter mit entsprechenden Spezialkenntnissen darauf angesetzt werden. Jede Überschreitung der SLA-Parameter muss zudem dem verantwortlichen Management zur Kenntnis gebracht werden. Auf diese Art und Weise wird eine schnelle Behebung der Störung unterstützt. Dies wird als Eskalation bezeichnet.

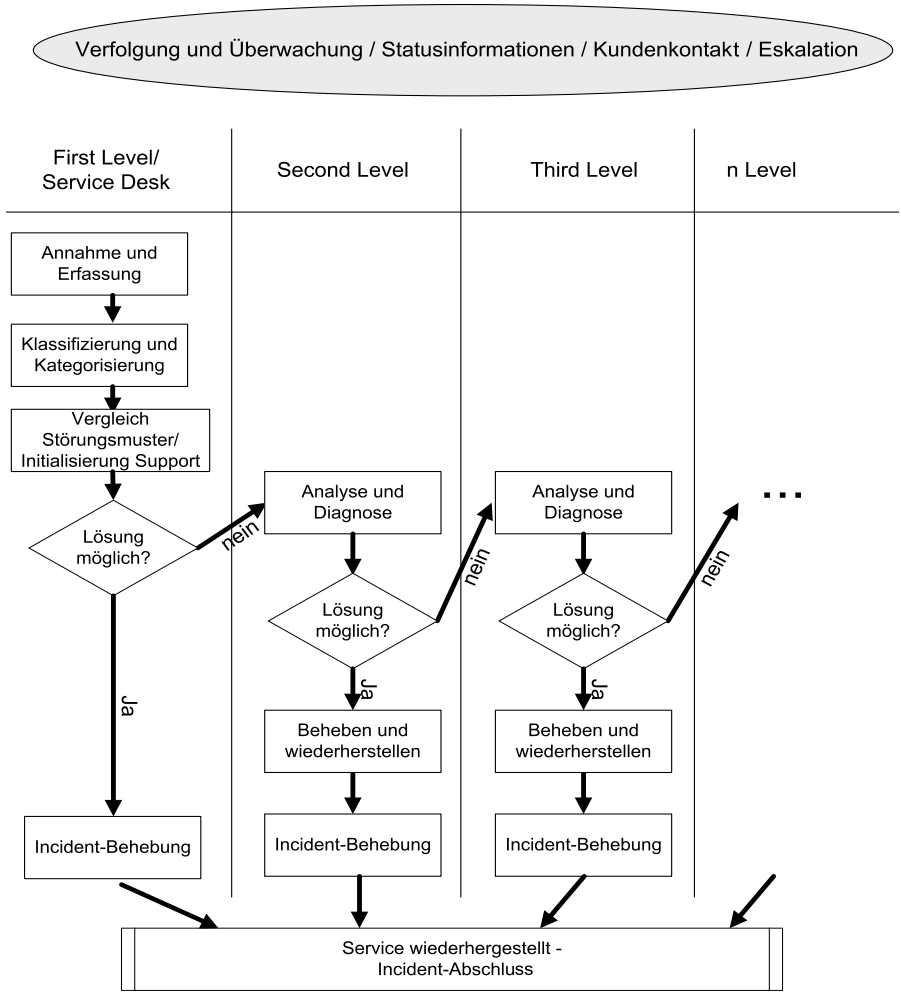


Abbildung 6.4: Abstufungen während der Incident-Behandlung

Bei der Eskalation wird unterschieden zwischen funktionaler und hierarchischer Eskalation:

- Funktionale Eskalation (horizontal): Hier handelt es sich nicht um eine Eskalation im eigentlichen Sinne, sondern vielmehr um ein Weiterleiten von Störungen an Spezialisten. Sie kommt also einer Anforderung an weiteren, dem Incident-Management nicht zugeordneten Personen gleich, um z.B. mehr Know-how, größere Erfahrung oder erweiterte Zugangsrechte innerhalb des Lösungsversuches bereitzustellen. Die funktionale Eskalation ist z.B. das Weiterleiten einer aufgenommenen Störung. Bei der funktionalen Eskalation wird auf detailliertere Kenntnisse oder Expertenwissen zugegriffen. Da dabei häufig hierarchische Grenzen überschritten werden müssen, kann es manchmal notwendig sein, erst hierarchisch zu eskalieren, um dann eine funktionale Eskalation folgen zu lassen.
- Hierarchische Eskalation (vertikal): Um die notwendige Unterstützung für die Sicherstellung eines oder mehrerer Prozesse zu erhalten, ist es unter Umständen erforderlich, hierarchisch zu eskalieren. Eine solche Eskalation ist auch denkbar, wenn Absprachen aufgrund bestehender Service Level Agreements in Gefahr geraten können. Sie wird auch dann notwendig, wenn die funktionale Eskalation nicht zum Erfolg führt, weil z.B. Befugnisse und Ressourcen nicht in ausreichendem Maße zur Verfügung stehen.

◆ Third Level, n Level Support: Mitarbeiter verschiedener Funktionen werden Support-Teams zugeteilt, für die sie zuständig sind. Diese Teams werden aufgrund ihrer Kenntnisse gebildet und eingestuft. Die Mitarbeiter der Support-Teams werden durch die funktionale Eskalation hinzugezogen.

  Das Service Desk stellt in der Regel die First Level-Abstufung dar, wobei der Second-Level Support oft auch als „Production Services", Produktionseinheiten oder die Mitarbeiter dort als Administratoren bezeichnet werden. Dazu zählen auch Netzwerk- und Servermanagement sowie die zentrale Datenhaltung. Entwickler, System-Ingenieure oder -Architekten, vielfach auch als „Engineering" betitelt, stellen den Third Level Support, gefolgt u.U. von extern hinzuziehenden Produkt- oder Hersteller-Spezialisten als Fourth Level.

6.2 Aktivitäten und Ziele des Incident Managements

An dieser Stelle soll vor allem verdeutlicht werden, dass das übergeordnete Ziel des Incident Management die Zufriedenheit der Anwender ist. Störungen von IT Services schnellstmöglich zu beheben, um dadurch negative Auswirkungen auf die Geschäftsprozesse des Kunden so gering wie möglich zu halten, ist ein vorrangiges Ziel des Incident Management. Im Interesse des Kunden bzw. aufgrund der geschäftlichen Erfordernisse zielt das Incident Management darauf ab, die Produktivität der Anwender (Mitarbeiter des Kunden) zu erhöhen und die Verfügbarkeit der IT Services zu verbessern.

Gleichzeitig unterstützt das Incident Management die IT-Organisation durch die verbesserte Überwachung der Leistungsfähigkeit gemäß SLA, durch sinnvolles Berichtswesen für das IT-Management und weitere ITIL-Prozesse. Hier gilt: Nur das, was gemessen wird, kann verbessert werden. Gerade im Incident Management bieten sich zahlreiche Reporting-Ansätze anhand der zu definierenden Leistungsindikatoren (KPIs) an.

Der Nachweis der vereinbarten Leistungen erfolgt zum Beispiel anhand eines regelmäßig (monatlich/wöchentlich) erstellten und kommunizierten Qualitäts- und Serviceberichts. Die Reports werden mit Hilfe von bestimmten Filterkriterien und Auswertungsroutinen aus dem bestehenden und dem historischen Pool an gelösten und offenen Incidents erstellt. In den meisten Fällen werden spezifische Anwendungen oder Datenbanksysteme eingesetzt, aus denen relativ leicht die gewünschten Informationen abgeleitet werden können. Diese Reports können Daten zu folgenden Punkten enthalten:

- Anzahl der eingegangenen Calls nach Medienform (Telefon, E-Mail, Fax, etc.)
- Anzahl der eingegangenen Calls nach Kategorie (Lotus Notes, Hardware, Netzwerk, etc.)
- Symptomauswertung (Häufigkeit von Symptomen nach Themengebieten)
- Anzahl der eingegangenen Calls nach Serviceeinstufung (Platin, Gold, Silber, Bronze, etc.)
- Erreichbarkeitsdiagramm (pro Tag), Erreichbarkeitsquote, Callvolumen, Servicelevelerfüllung, wie etwa Anzahl der angenommenen/*nicht* angenommenen Telefonanrufe, Wartezeiten (in Stufen) bis zur Annahme der Calls
- Direktlösungsrate/ Weiterleitungsrate nach Kategorien
- Anzahl der reklamierten und zurückgerouteten Tickets (falsche, unvollständige Informationen)
- Verweildauer (in Stufen) offener Tickets nach Status/Kategorien/Anwendungen
- Anzahl und Dauer von Tickets mit Zeitüberschreitungen und deren Kategorisierung
- Nennung von Problemtickets, die eskaliert wurden oder werden

Wichtig ist dabei natürlich, dass die IT-Mitarbeiter innerhalb dieses Prozesses ihren Einsatz ständig kontrollieren und durch entsprechende Maßnahmen und Regelungen verbessern können. Gerade hier sind der Dienstleistungsgedanke und die Ausrichtung zum Kunden wichtig. So wird unter anderem verhindert, dass Störungen und Service-Requests verloren gehen bzw. falsch registriert werden. Gleichzeitig wird eine kontinuierliche Aktualisierung der CMDB vorangetrieben. So ist es beispielsweise möglich, bei der Aufnahme der Störung in Interaktion mit dem Anwender die in der CMDB vorliegenden Daten abzugleichen. Damit einher geht die kontinuierliche Verbesserung der Kundenzufriedenheit.

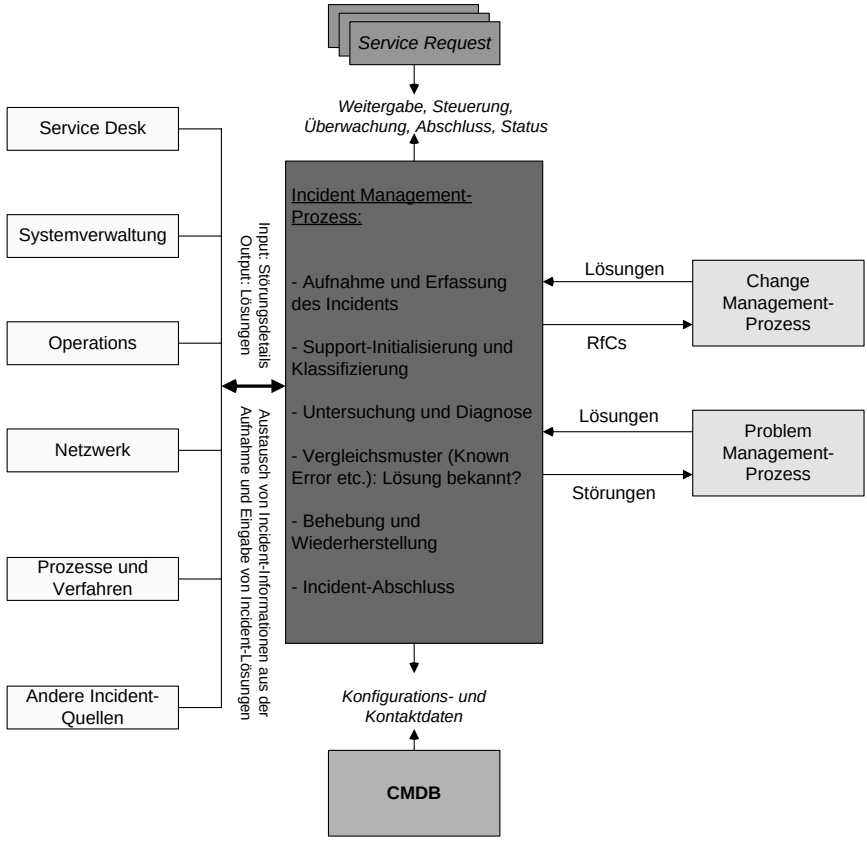


Abbildung 6.5: Incident Management-Prozess im Gesamtzusammenhang

Im Incident Management werden unterschiedliche Aktivitäten durchlaufen (*siehe Abbildung 6.5*):

1. Annahme und Registrierung: Entgegennahme der Störungsmeldung, Erfassung der Daten, Abfragen der Configuration Management Datenbank (CMDB). Ziel ist es, viele der gemeldeten Störungen sofort beseitigen zu können, ohne sonstige Aktivitäten einleiten zu müssen. In allen anderen Fällen werden die vorgesehenen Zuweisungen vorgenommen und die Weiterleitung bzw. Eskalation eingeleitet.
2. Klassifizierung und erste Hilfe: Die erste bzw. korrekte Kategorisierung von Incidents, einerseits zu Beginn und andererseits nach Abschluss der Störung, ist von entscheidender Bedeutung für eine aussagekräftige Management Information. Die Definition der einzelnen Kategorien ist von Unternehmen zu Unternehmen verschieden und könnte sich z. B. an dem vermeintlichen Ursprung der Störung orientieren (Netzwerk usw.).

   Denn Ziel des Incident Management ist es unter anderem, den vereinbarten Service schnellstmöglich wiederherzustellen. Erst im Anschluss daran wird die Priorität des Incidents festgelegt. Die Formel lautet: Priorität = Impact + Dringlichkeit unter Berücksichtigung der vorhandenen Ressourcen.

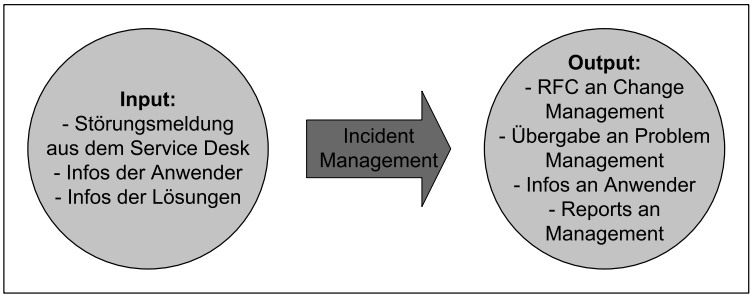


Abbildung 6.6: Prozessverlauf des Incident Management

3. Vergleich (Prüfung Störungsmuster): Hier wird der registrierte und klassifizierte, d.h. kategorisierte und priorisierte Incident mit einem eventuell bereits vorhandenen Incident verglichen. In diesem Zusammenhang wird auch überprüft, ob eine dokumentierte Lösung vorhanden ist. (CMDB und/oder Störungs-/Known Error-Datenbank). Elementare Frage dieses Schritts ist: „Ist das Thema bereits bekannt und ein entsprechender Workaround oder gar eine Lösung vorhanden?"
4. Analyse und Diagnose: Hier stellt sich die entscheidende Frage für das Incident Management: „Ist die Lösung schnellstens an dieser Stelle möglich?" Hier geht es um die Lösungssuche, falls noch keine vorhanden ist.

   Ist die Störung an dieser Stelle nicht zu beheben, so ist der Incident entsprechend weiterzuleiten. Dies kann und muss in der Regel iterativ erfolgen, d.h. mehrere Arbeitsgruppen/Fachbereiche werden durchlaufen. Die Steuerung und Überwachung dieser Untersuchungs- und Diagnosephase ist sorgfältig vorzunehmen und entsprechend zu dokumentieren. Nicht nur nachgelagerte Einheiten sind von der Qualität dieser Information abhängig. Merksatz: Durch die Eskalation eines Incidents wird dieser nicht zum Problem, d.h. es gibt keinen Automatismus!
5. Lösung und Wiederherstellung: Viele Störungen werden direkt aus der Erfassung in die Behebung und Wiederherstellung der geordneten Serviceleistung übergehen. Andere Störungen werden bei der Analyse und Diagnose zusätzliche nachgelagerte Aktivitäten auslösen. Es wird sichergestellt, dass eine Umgehungs- oder Direktlösung einen annehmbaren Service anbietet oder den gestörten/ausgefallenen Service wiederherstellt. Auch hier wird großer Wert auf die Dokumentation des Ablaufes gelegt.
6. Abschluss und Kategorisierung: Diese Phase darf nur vom dazu autorisierten Personal ausgeführt und überwacht werden. Nachdem eine endgültige Überprüfung vorgenommen und die Vollständigkeit der Daten überprüft wurde, kann eine Störungsmeldung abgeschlossen werden. Alle Störungen müssen einer Kategorie zugeordnet sein, damit sichergestellt ist, dass mittels Schlüsselbegriffen und Kennzeichen aussagekräftige Management-Berichte erstellt werden können. Dies ist auch essenziell, um bei erneuten, ähnlichen Störungen die Fehlerlokalisierung zu vereinfachen.

Es müssen alle Störungen, sowohl einfache und banale als auch komplexe und schwer wiegende Incidents, sorgfältig dokumentiert werden (*siehe Abbildung 6.7*).

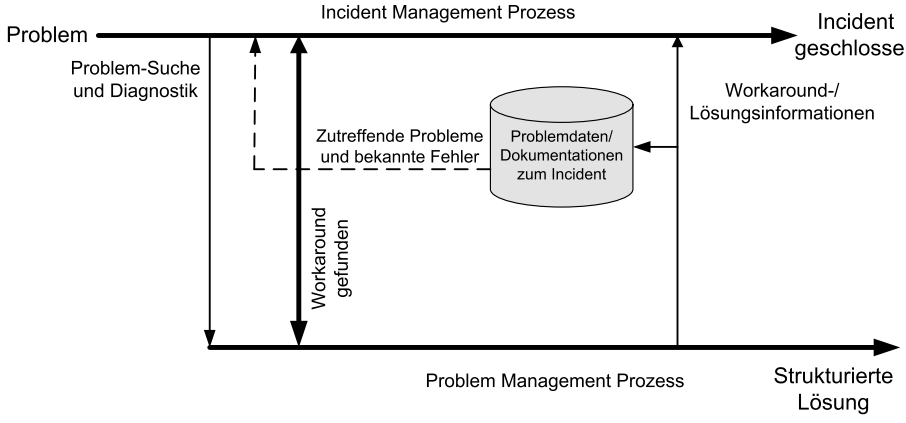


Abbildung 6.7: Incident Management in Bezug auf Workarounds und angrenzende Bereiche

7. Verfolgung und Überwachung: Störungen können komplexe Ausmaße annehmen oder verhältnismäßig einfach und ohne großen Zeitaufwand zu lösen sein. Sie können von einer Person sofort gelöst werden oder komplette Teams stundenlang beschäftigen. Sie können kleinere Unterbrechungen verursachen oder für einen größeren Einbruch der Serviceleistung verantwortlich sein. Es können Minuten oder Tage zwischen Erfassung und Abschluss liegen. Die Anzahl parallel auftretender Störungen kann enorm sein.

   Das Überwachungssystem muss daher in der Lage sein, alle oben genannten Situationen abzudecken und aufzunehmen, um den Status während des ganzen Incident-Lebenszyklus zu verfolgen. Die dabei verwendeten Schlüsselbegriffe für das Personal können zum Beispiel sein: Auswirkung, Benutzerkennung, Störungsnummer, Komponenten-Identifikation etc.

8. Eskalation: Der Mitarbeiter muss darauf vorbereitet sein, scheinbar unlösbare Probleme zu eskalieren, um eine Weiterführung der Aktivitäten und eine zufriedenstellende Lösung zu erzielen. Diese Eskalation muss gemäß definierten und kommunizierten Verfahren ablaufen.

Das Incident Management behält stets die administrative Kontrolle über den Incident-Lebenszyklus (*siehe Abbildung 6.8*). Dies gilt auch für Aktivitäten in nachgelagerten Prozessen wie dem Problem Management (Problem-Lebenszyklus). Der Status eines Incidents spiegelt seine aktuelle Position im Lebenszyklus wider (*neu, angenommen, scheduled, assigned, in Bearbeitung, wartend, beschlossen, geschlossen*). Um einen Incident möglichst reibungslos von einem Zustand in einen anderen zu bewegen, bis er geschlossen wird, ist der Incident Record mit allen notwendigen Details zu pflegen. Dies scheint bei vielen Kolleginnen und Kollegen ein ähnliches Problem darzustellen wie die Erstellung und Pflege von Systemdokumentationen oder das Einbringen von Kommentaren im Source Code. Aber auch hierbei gilt: Es ist absolut

notwendig! Es sollte definiert werden, wer den Record pflegen soll bzw. darf und wann gepflegt wird. Ein solches „Ticket“ kann folgende Inhalte aufweisen:

- Eindeutige Nummer, Anwenderdaten, Datum und Uhrzeit
- Beschreibung (Symptome, Fehlermeldungen)
- Impact, Dringlichkeit, Priorität
- Betroffene Komponenten
- Verwandte Incidents/Probleme/Known Errors
- Ergebnis Klassifizierung und Abschlussklassifizierung
- Status: Aktueller Stand in der Bearbeitung mit allen Aktivitäten (Dokumentation/ Historie)
- Lösung

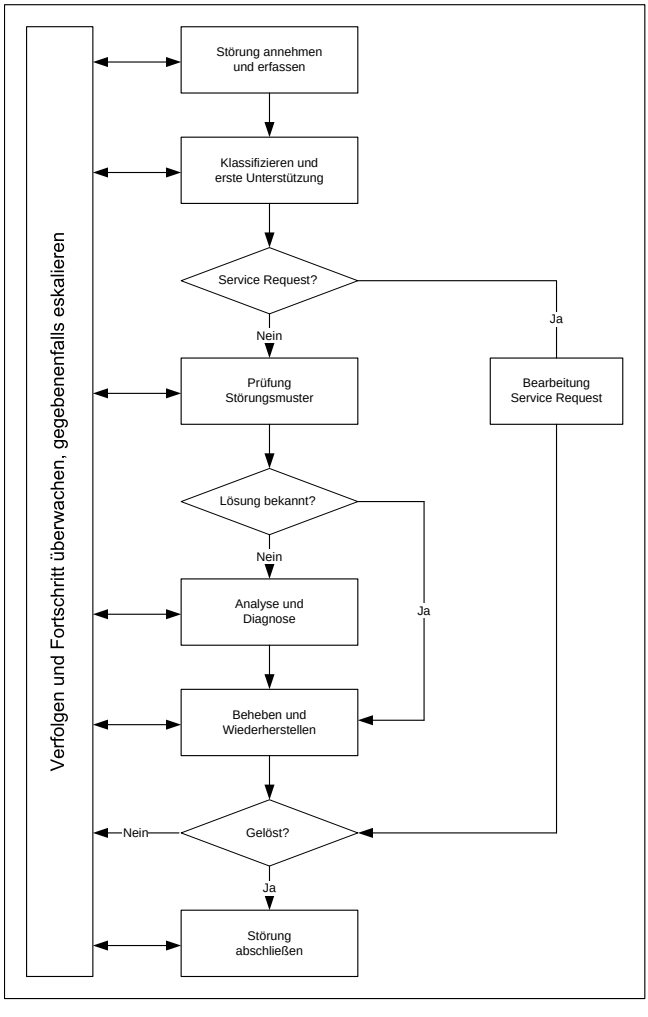


Abbildung 6.8: Aktivitäten im Incident Management

6.3 Das Incident Management im ITIL-Gesamtzusammenhang

Da Probleme, Störungen, Ausfälle oder andere Beeinträchtigungen im System als Incident in unterschiedlichen Bereichen und Ausprägungen auftreten können, stellt das Incident Management zahlreiche Schnittstellen bereit, die auch im Falle einer Eskalation verwendet werden können. Aus dieser Notwendigkeit heraus kann das Incident Management wie eigentlich alle Kapitel aus dem ITIL-Begriff heraus nicht als in sich geschlossenes und abgeschottetes System verstanden werden. So liegt das Incident Management horizontal in der IT-Organisation des Unternehmens und kann durch seine Aktivitäten alle Prozesse berühren. An dieser Stelle wird auch deutlich, dass die Begriffe Incident Management und Service Desk nicht synonym zu verwenden sind. Incident Management als Prozess bleibt nicht auf das Service Desk beschränkt (*siehe Abbildung 6.9*).

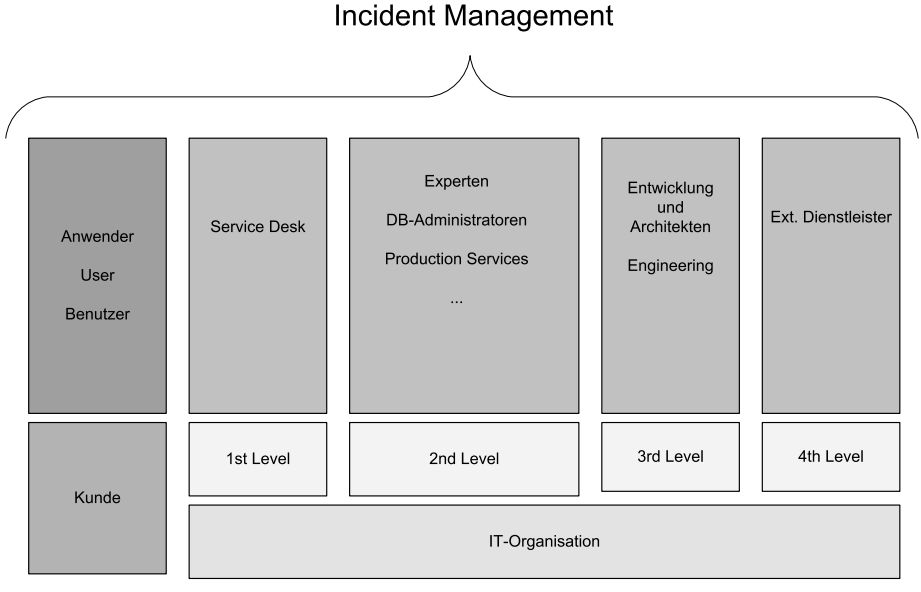


Abbildung 6.9: Incident Management und die Berührungspunkte im Unternehmen

Die Hoheit über den aufgenommenen Incident verbleibt beim Incident Management, um jederzeit adäquat auf Rückfragen reagieren, weitere Informationen aufnehmen oder Eskalationsschritte aufgrund von definierten Vorgaben anstoßen zu können. Hier bewährt sich das Vorhandensein des Single Point of Contact – nicht nur für den Anwender, der seinen defekten Drucker melden möchte. Auch andere Mitarbeiter, die mit einem Incident oder einem Change zu tun haben, wenden sich an das Incident Management, um Informationen zu liefern oder abzugreifen. Dies können ein Eskalationsmanager oder ein Mitarbeiter des Problem Management sein, die weitere Fragen zu einem Incident oder einem Request haben.

Störungen, für die es noch keine Lösung gibt oder die den Kenntnisstand des aktuellen Bearbeiters übersteigen, werden vom Service Desk oder vom jeweiligen Support-Team einem anderen Team mit höherem Kenntnisstand oder den notwendigen technischen Befugnissen zugewiesen. Dieses Support-Team ist für die Behebung der Störung oder für eine nochmalige Weiterleitung zu einem weiteren Support-Team zuständig. Es ist besonders wichtig, dass während des Lösungsvorgangs die verschiedenen Bearbeiter den Status im lncident-Datensatz anpassen („Ticketpflege“) und zudem die Beschreibung der ergriffenen Maßnahmen und die Anpassungen in der Klassifizierung vornehmen (Dokumentation der Historie).

Riskiert man, sich abwendend vom Incident Management, einen Seitenblick auf die Schnittstellen und Berührungspunkte, zeigt sich, dass insbesondere die so genannte Konfigurationsmanagement-Datenbank (Configuration Management Database, CMDB) eine wichtige Rolle spielt, die in der Praxis in mehr oder minder übersichtlichen und nachvollziehbaren Formen auftritt. Ziel dieses Datenspeichers ist es, Bezüge zwischen den Konfigurationselementen (Configuration Items, CIs), Diensten, Anwendern und Kundenanforderungen zu ermöglichen. Über dieses essenzielle Hilfsmittel ist das Incident Management in der Lage, mögliche Störungsursachen oder -zusammenhänge zu finden. Aber auch Ansprechpartner oder Experten zu spezifischen Problemen, wie etwa Produktverantwortliche, potenzielle Ansprechpartner und Eskalationsbeteiligte, können über die CMDB abgerufen werden.

Während der Erfassung einer Störung können Konfigurationsdaten in den Incident-Datensatz der jeweiligen Anwendung im Bereich Incident Management übernommen werden, um ein klareres Bild von der Störung zu erhalten. In der Regel wird der Status der betroffenen Komponenten in der CMDB angeglichen. Auch die Daten des Anwenders können abgefragt und bei Bedarf angepasst werden (*siehe Abbildung 6.10*).

Neben den Tools und Mechanismen zur Arbeit mit Incidents ist eine ausreichend gefüllte CMDB unerlässlich! Daneben gehört auch eine Wissensdatenbank in beliebiger Form als Quelle für bekannte Fehler und für die damit zusammenhängenden Informationen, Lösungen, Details und Ansprechpartner zu den essenziellen Arbeitskomponenten der Mitarbeiter des Incident Management. Das Problem Management unterstützt die Mitarbeiter des Incident Managements, indem es Informationen über Probleme, bekannte Fehler und Workarounds zur Verfügung stellt. Diese Informationen fließen dann in die vorhandene Wissensdatenbank für das Incident Management ein.

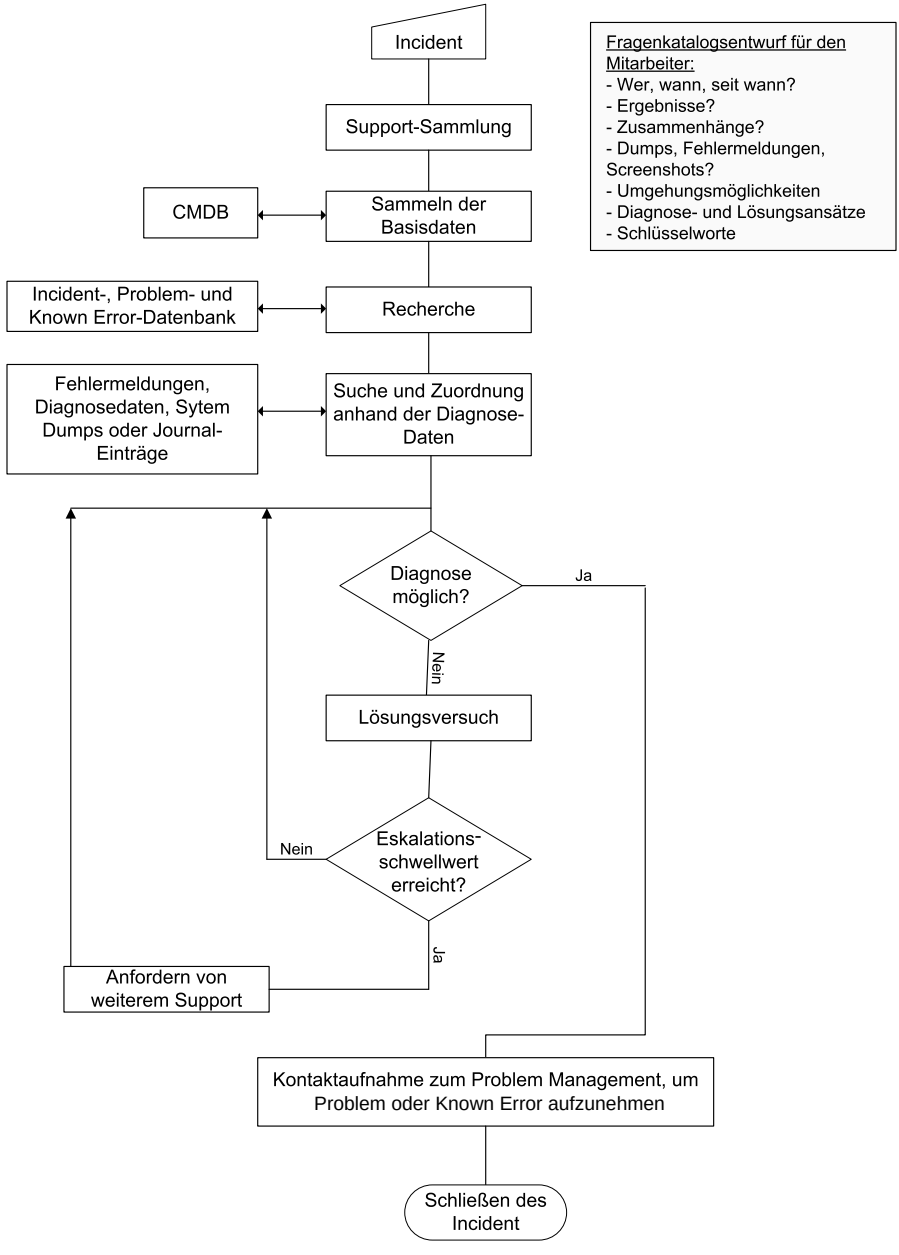


Abbildung 6.10: Suche nach der Fehlerursache

Das nachgelagerte Problem Management (*siehe Abbildung 6.11*) stellt hohe Anforderungen an die Qualität der Störungserfassung, um mögliche Fehler besser aufspüren zu können. Fehlen hier Angaben in der Historie, muss in vielen Fällen der Anwender nochmals kontaktiert werden, es müssen Fragen gestellt und das Problem erneut aufgerollt werden, obwohl der Anwender dies in der Regel bereits bei der Aufnahme des Records getan hat. Dies trägt nicht unbedingt zur Kundenzufriedenheit bei.

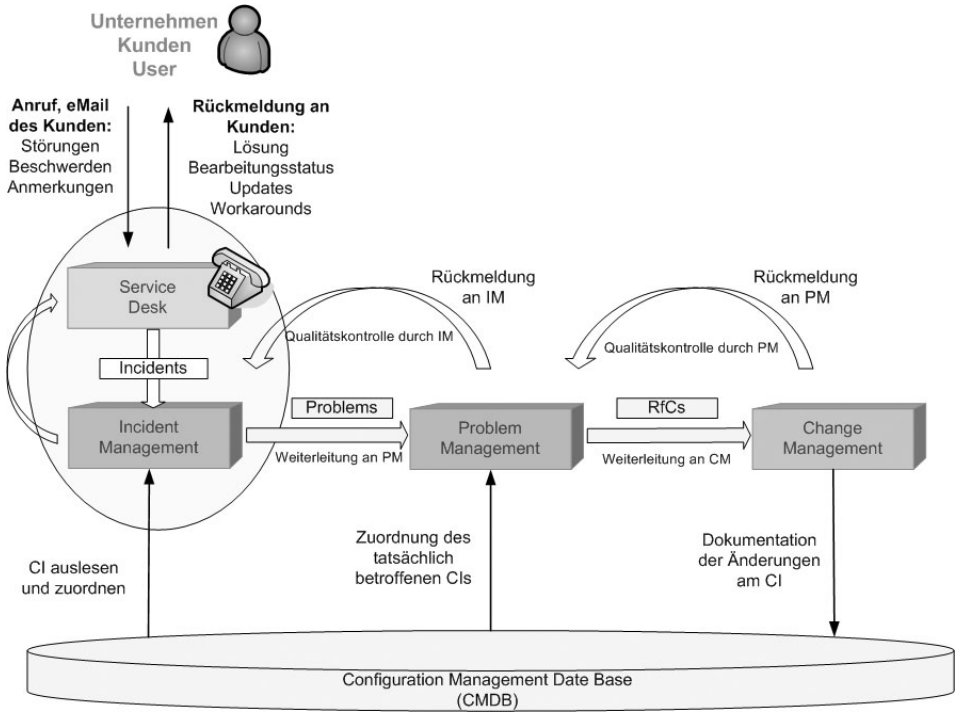


Abbildung 6.11: Der Weg eines Incidents („Incident Lifecycle")

Neben den Incidents werden im Incident Management auch Service Requests entgegengenommen und bearbeitet. Diese werden, wenn sie in die Produktion einfließen, über das Change Management umgesetzt, da es sich in der Regel um Erweiterungen und Änderungen der IT-Infrastruktur handelt. Zusätzlich werden auch Störungen unter der Kontrolle des Change Management behoben, z.B. durch den Austausch oder die Erweiterung von Software-Komponenten, deren Problemverhalten durch ein FixPack oder einen Patch behoben werden. Darüber hinaus liefert das Change Management dem Incident Management Informationen über geplante und den Status von aktuellen Changes. Achtung: 80 % aller Incidents treten aufgrund von nicht-gemeldeten oder nicht-autorisierten Changes auf. Kein Wunder, dass der Bereich Change Management eine wichtige Schnittstelle bei der Behebung von Incidents darstellt. Sollte offensichtlich sein, dass ein Change der Verursacher von Störungen ist, so werden die Informationen über einen fehlerhaften Change an das Change Management zurückgemeldet.

Neben den direkten Schnittstellen aus den ITIL-Disziplinen des Service Support existieren in Bezug auf das Incident Management auch indirekte Schnittstellen zu Disziplinen aus dem Service Delivery-Set:

- Service Level Management: Das Incident Management liefert an das Service Level Management Informationen, anhand derer sich die Qualität des Services beurteilen lässt. Die zwischen den Vertragsparteien vereinbarten Messkriterien der definierten Services bilden die Grundlage für die Bewertung durch den Kunden. Dies wird anhand der Reportings transparent, die das Incident Management zur Verfügung stellt. Das Reporting muss von beiden Vertragspartnern bezüglich der Inhalte, der Berichtszeiträume und der Berichtshäufigkeit abgestimmt sein. Wertvolle Zusatzinformationen, zum Beispiel über eine Änderung der Anzahl oder Art der in der jeweiligen Servicevereinbarung befindlichen Hard- und Software, laufende Hersteller- und Wartungsverträge oder den Umfang der Lizenzverhältnisse, sind die Basis dafür, dass vertragsrechtliche Verpflichtungen nicht auf falschen Grundlagen getroffen werden und die hieraus resultierenden Risiken für die Vertragsparteien minimiert werden.

  Sollten z.B. häufig Störungen bei einem geschäftskritischen Service auftreten und das zugehörige Service Level Agreement damit verletzt sein, müssen über das Service Level Management geeignete Maßnahmen zur Serviceverbesserung in Absprache mit dem Kunden eingeleitet werden. Das Incident Management muss hierzu über die mit dem Kunden vereinbarten Service Level informiert sein.

- Availability Management: Das Availability Management kümmert sich primär um das Messen von Verfügbarkeiten. Um die Verfügbarkeit von Services messen zu können, bedient sich das Availability Management der Daten, die vom Incident Management zur Störungserfassung angelegt werden. Auch die Informationen aus der Statusüberwachung betroffener Configuration-Items (CIs) sind für das Availability Management relevant. Um exakte Werte als Basis für das Availability Management liefern zu können, ist bei Störungen eine präzise Zeiterfassung vom Auftreten bis zur Behebung überaus wichtig. Aus einer unpräzisen Datenbasis können keine realen Auswertungsergebnisse geliefert werden.

- Capacity Management: Das Capacity Management ist an einem optimalen Einsatz der IT-Ressourcen interessiert. Um eine adäquate Planung betreiben zu können, wertet dieser Prozess beispielsweise Störungen aus, um zu überprüfen, ob diese auf einen Mangel an Speicherplatz oder auf zu lange Reaktionszeiten zurückzuführen sind. Vielfach bereitet das Incident Management bereits entsprechende Reports vor, da verwendete Tools häufig entsprechende Sortierungs- oder Stichwortsuchen anbieten. Das Capacity Management stößt daraufhin die erforderlichen Maßnahmen an, um das erneute Auftreten dieser Störung bereits im Vorfeld zu vermeiden.

KPI

KPIs werden über Berichte für unterschiedliche Zielgruppen erstellt. Das Berichtswesen liegt für diesen Prozess in der Verantwortung des Incident-Managers, der auch die Verteilerliste sowie einen Berichtskalender erstellt. Der Service Desk ist der wichtigste Datenlieferant für die Messung des Servicegrads. Aus den historischen Daten werden Trends abgelesen. Beispiele für derartige Messwerte: Gesamtzahl der Störungen, durchschnittliche Lösungszeit, durchschnittliche Lösungszeiten pro Priorität/Durchschnittswerte, die innerhalb des vereinbarten Service Level liegen. Weiterhin können der Prozentsatz der vom First Level Support behobenen Störungen (Lösung in erster Instanz, ohne Weiterleitung), durchschnittliche Supportkosten pro Störung, behobene Störungen pro Workstation oder pro Service Desk-Mitarbeiter, Anzahl der Störungen, die anfänglich falsch klassifiziert wurden oder Anzahl der Störungen, die falsch weitergeleitet wurden, erfasst werden. Dies dient als Basis für eine kontinuierliche Verbesserung sowohl der angrenzenden Servicebereiche als auch des Service Desk an sich. Mehr Informationen zum Thema KPI erhalten Sie in *Kapitel 2.1.7, Key Performance-Indikatoren*.

Das Incident Management wäre ohne die angrenzenden Prozesse nicht in der Lage, erfolgreich zu arbeiten. Grundvoraussetzungen für ein erfolgreiches Incident Management sind neben einer aktuellen und sorgfältig gepflegten CMDB eine enge Beziehung zum Service Level Management und den angrenzenden Bereichen für die richtige Zuweisung von Prioritäten und Lösungszeiträumen.

Im Bereich des Incident Management und in den angrenzenden Supportbereichen kommen Hilfsmittel in unterschiedlichen Ausprägungen zum Einsatz:

- Das so genannte Ticket-System, um Anfragen aufzunehmen, zu protokollieren, kategorisieren und zu priorisieren. Hierüber können beispielsweise auch Records über nachgelagerte Workflowmechanismen zu den angrenzenden Teams geschoben oder Reports gezogen werden.
- Mail In-Datenbanken und andere elektronische Kontaktmöglichkeiten
- Datensammlungen/-banken in Bezug auf Wissendatenbanken, bekannte Fehler und Workarounds. Hierzu zählen auch Datenbanken von Dienstleistern.

Wichtig ist in diesem Zusammenhang nicht nur der Workflowansatz, sondern auch ein entsprechender Komfort, um Reklassifizierungen, Zuordnungen und Lösungen schnell und unkompliziert vornehmen zu können. Neben einer automatischen Erfassung und Protokollierung von Incidents, um Server, Netzwerke, Mainframes und andere Komponenten (möglicherweise über Systems Management-Tools) zu überwachen, bieten sich auch automatische Eskalationsmöglichkeiten an, um zeitnah reagieren zu können.

7 Problem Management

Das Problem Management entstammt dem ITIL-Bereich Service Support. Der Fokus liegt auf dem operativen Bereich und ist von der Intention her proaktiver Natur. Bei Beeinträchtigungen der Services besteht die vorrangige Aufgabe darin, die Wiederaufnahme der Services durch den Anwender schnellstmöglich zu sichern. In dem Moment, wo für einen Fall keine Ursache festgestellt werden kann, wird ein Incident zum Problem. Ein Problem kann durchaus auf mehrere Incidents zurückführbar sein. Das Aufspüren der Gründe für ein Problem ist zumeist aufwändig. Nur selten wird sofort ein direkter Zusammenhang zwischen Ursache und Auswirkung festzustellen sein. Ausnahmen sind Fälle, die in gleicher oder ähnlicher Form schon einmal aufgetaucht sind. Die Schwierigkeit bei Störungen und Unterbrechungen liegt jedenfalls grundsätzlich darin, dass sie wiederholt auftreten können. Wenn das System in einer bestimmten Situation immer mit derselben Meldung reagiert oder die Anrufe der Anwender gleich lauten, kann man klar darauf schließen, dass es noch nicht beseitigte Problemquellen geben muss. Das Problem ist damit aber zumeist eindeutig vorhanden, da reproduzierbar.

Besitzt ein Unternehmen eine gestaffelte Organisation, kommt eine Überleitung vom First Level Support zum Second Level oder Third Level Support zu anderen Personenkreisen zum Tragen. Hier wird das Problem Management aktiviert. Dieses muss die Störungen und Fehler beseitigen, im Vordergrund steht jedoch die Entdeckung der Ursache(n). Hier greifen andere Prozessverläufe als beim Incident Management.

In der IT-Praxis gibt es sicherlich viele bekannte Fälle und Beispiele. Wohl jeder Mitarbeiter, der in IT-Umgebungen arbeitet, weiß darüber zu berichten.

- Datenbankfehler: Anwender aus unterschiedlichen Fachbereichen melden voneinander unabhängig, dass die Daten fehlerhaft seien. Es muss nun festgestellt werden, welche Datenbank falsche Informationen liefert. Gründe hierfür können im DB-Softwaremanagementsystem des Herstellers liegen oder die Datenbank wurde inkonsistent aufgebaut. Man wird die entsprechenden Experten oder Produktverantwortlichen im Unternehmen oder externe Programmierer mit der Problemsuche beauftragen.
- Anwendungsprogrammfehler: Bestimmte Anwendungen bringen dieselbe Fehlermeldung im System. Die Quelle ist hierbei relativ schnell zugeordnet; das Auffinden der Problemursache dauert oft länger. Liegt das Problem in der Anwendung an sich („Bug“), an der Datenbank, einem Bedienfehler oder an etwas anderem? Bei Fremdsoftware muss in manchen Fällen der Support des Herstellers kontaktiert werden.

- Netzwerkfehler: Wenn gemeldet wird, dass bestimmte Ressourcen (Drucker an bestimmten Servern, Datenbanken, etc.), die alle in einem Subnetz liegen, nicht zugreifbar sind, scheint es sich um ein Netzwerkproblem zu handeln. Hier wird die Netzwerkadministration als Erstes eingreifen. Unter Umständen müssen Messgeräte oder Netzanalysatoren eingesetzt werden, um einen Verkabelungs- oder Routerfehler aufzuspüren. Auch die Netzhardware an sich (Switch o.ä.) kann die Fehlerquelle darstellen. Hier sind die Gründe oft nicht einfach oder schnell zu finden.

Die Liste ließe sich beliebig fortsetzen. Vom einfach zu findenden Fehler bis zu extrem komplexen Aktivitäten gibt es hier in der Praxis jede denkbare Abstufung. Die Aufrechterhaltung der SLA-Grundsätze ist dabei oft genug nicht mehr möglich. An der Fehlereinkreisung sind unter Umständen Eskalationsstufen beteiligt, wodurch sich das Ganze natürlich nicht immer einfacher und schneller handhaben lässt. Fehler und Probleme entstammen Störungen. Deshalb arbeiten die Prozessdisziplinen Incident Management und Problem Management in der Regel sehr eng zusammen. Sie halten eine permanente Kommunikation aufrecht und können so adäquat auf Statusanfragen eingehen.

7.1 Problem Management nach ITIL

Das Ziel des Problem Management besteht in der Vermeidung von Störungen. Dieser Prozess bemüht sich, negative Auswirkungen von Fehlern in der IT auf das Geschäft zu minimieren. Um dieses Ziel zu erreichen, führt das Problem Management sowohl proaktive als auch reaktive Aktivitäten aus. Im Rahmen des reaktiven Problem Management wird nach der Ursache für bereits eingetretene Störungen gesucht und Vorschläge zur Umsetzung bzw. Korrektur der Situation initiiert. Proaktives Problem Management versucht, Störungen zu verhindern, bevor sie zum ersten Mal auftreten, indem Schwachstellen in der Infrastruktur identifiziert und Vorschläge zu deren Beseitigung unterbreitet und geprüft werden. Dies umfasst beispielsweise die Überwachung und Auswertung von Protokolldateien, um strukturelle Fehler zu lokalisieren, dokumentieren und verfolgen. Dazu werden Symptome und (vorübergehende) Lösungen von Störungen erfasst. Dazu gehört auch, dass im Bedarfsfall Requests for Change (RfCs) zur Anpassung der Infrastruktur eingereicht werden, um aktuelle Probleme zu beheben oder neue Störungen zu verhindern.

Zunächst gilt es, die Ursache zu untersuchen. Hat man die Ursache herausgefunden, erhält das Problem den Status „Known Error“ (bekannter Fehler), aus dem sich eventuell ein Request for Change für die Behebung der Ursache ergibt. Das Problem Management beschäftigt sich auch danach mit der Verfolgung und der Überwachung von bekannten Fehlern in der Infrastruktur. Zu diesem Zweck werden Daten über alle identifizierten bekannten Fehler, ihre Symptome sowie die verfügbaren Lösungen gepflegt.

Das Problem Management unterstützt das Incident Management, indem es Workarounds und schnelle Lösungen liefert, es ist jedoch nicht selbst für die Behebung der Störung verantwortlich. Während das Incident Management bestrebt ist, die Störung so schnell wie möglich zu beheben, nimmt sich das Problem Management die Zeit, die Ursache zu ergründen und zu beseitigen.

Unterscheidung Incident Management und Problem Management

Das Problem Management beschäftigt sich vorrangig mit der Ursachenforschung, nachfolgender Ursachenbehebung und Präventivmaßnahmen. Manchmal kommen sich Incident und Problem Management dabei in die Quere, liegt doch das primäre Ziel des Incident Management darin, dem Anwender so rasch es geht zu helfen bzw. den Service so schnell wie möglich wieder bereitzustellen (*siehe Abbildung 7.1*). Gelegentlich wird dann eher ein schneller Workaround („quick and dirty") einer permanenten Lösung, die aber eine entsprechende Fehlersuche voraussetzt, vorgezogen.

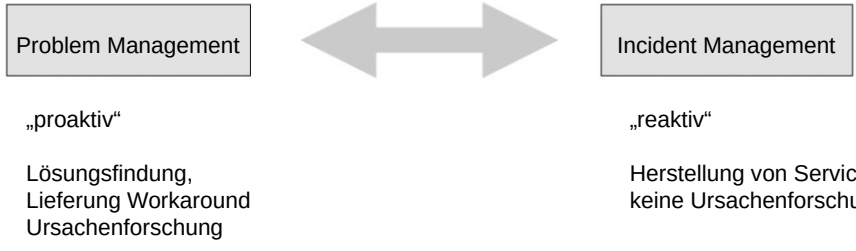


Abbildung 7.1: Unterscheidung Incident und Problem Management

Das Problem Management kann aufgrund einer drastischen Senkung der Anzahl von Störungen und einer Erleichterung des Arbeitsdrucks der IT-Organisation schnell zu einer Qualitätssteigerung der IT Service führen.

Die wichtigsten Zielsetzungen stellen sich folgendermaßen dar:

- optimale und schnelle Ursachenforschung bei allen Störungen, Unterbrechungen oder sonstigen Problemen
- die Elimination der Ursachen
- die Aufrechterhaltung der IT-Dienstleistungen
- die Vermeidung von längerfristigen IT-Systemunterbrechungen
- die Reduzierung der Auswirkungen und Schadensbegrenzung
- das Vermeiden von Problemen durch vorausschauendes Handeln
- das Einleiten von notwendigen Changes in der IT-Infrastruktur

Das laufende Pflegen einer Know-how-Datenbank als Expertensystem hilft, diese Ziele zu erreichen (*siehe Abbildung 7.2*). Andere Prozesse und Fachbereiche sollten hieraus Wissen beziehen können und Zugriff darauf erhalten. Die Prozesse des Problem Management sind erst dann abgeschlossen, wenn die Changes bei einem Problem installiert, konfiguriert und getestet worden sind. Dann erfolgt eine entsprechende Rückmeldung der dort beteiligten weiteren Prozesse. Der spezifische Fehler muss aber eindeutig identifiziert worden sein, damit er nach den Veränderungen nicht mehr auftritt.

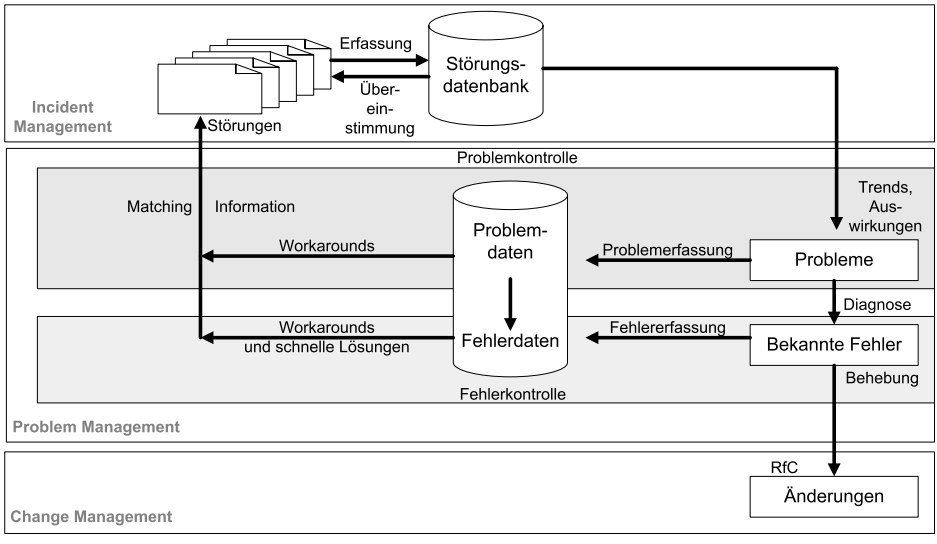


Abbildung 7.2: Prozessabläufe und Werkzeuge nach OGC

7.2 Begriffe des Problem Management

Die IT ist nicht vor Problemen gefeit; sogar die besten Verbesserungen sind nicht im Stande, eine fehlerfreie Produktion zu garantieren. Die Probleme selber können gelöst und ihnen kann vielleicht sogar vorgebeugt werden. Eine der wichtigsten Aufgaben des Problem Management ist es jedoch, dafür zu sorgen, dass Probleme keinen oder einen nur geringen Einfluss auf die Serviceleistungen ausüben und die Anwender davon so wenig wie möglich spüren.

Begriffe im Incident Management und im Problem Management

Die meisten der Begriffe, die für das Problem Management und weitere Prozesse relevant sind, wurden bereits in *Kapitel 6.2, Begriffe des Incident Management*, vorgestellt.

Ein Problem beschreibt dabei eine unerwünschte und ungewollte Situation, die als unbekannte Ursache einer oder mehrerer (aktiver und potenzieller) Störungen auftritt. Ein Problem verursacht mindestens eine Störung. Ist die Ursache des Problems bekannt, wird von einem bekannten Fehler (Known Error) gesprochen (*siehe Abbildung 7.3*). Oft gibt es in einem solchen Fall einen Workaround, um die Beeinträchtigung des Tagesgeschäfts für den Anwender so gering wie möglich zu halten. Zudem wird ein Request for Change (RfC) erstellt und vorgeschlagen, eine Änderung vorzunehmen, die den bekannten Fehler beseitigt.

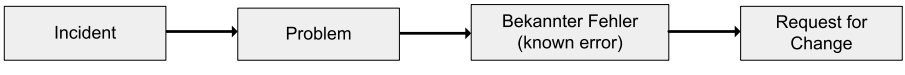


Abbildung 7.3: Zusammenhänge der Begrifflichkeiten

7.3 Aufgaben und Aktivitäten des Problem Management

Im Grunde genommen müsste jede Störung, deren Ursache unbekannt ist, mit einem Problem verknüpft werden. In den meisten Fällen lohnt sich eine solche Verknüpfung jedoch erst, wenn die Störung häufiger auftritt, wenn eine Wiederholung zu erwarten ist, oder wenn es sich um eine einzige schwer wiegende Störung handelt.

Die Daten, die zur Erfassung eines Problems dienen, ähneln den Daten, die zur Erfassung einer Störung herhalten. Es geht beim Problem Management aber verstärkt um die Kenndaten zum Problem. Der Fokus auf den Anwender und seine Daten entfällt. Auch das Problem Management kann ebenso wie jeder anderer ITIL-Prozess eine eigene Datenbank verwenden.

Die Analyse und Ursachenforschung wenden sich den technischen Komponenten (Configuration Items) und den Zusammenhängen, in denen sie zueinander stehen, zu. Dies ist v.a. dann relevant, wenn die Analyse der Infrastruktur bzw. deren Komponenten deutlich macht, dass es Schwachpunkte gibt, die zu dieser und weiteren Störungen führen bzw. führen können. Manche Störungen sind so schwerwiegend, dass ein weiteres Auftreten auf jeden Fall vermieden werden muss. Dies gilt auch für Gefährdungen der vereinbarten Services auf der Basis von SLAs. Ebenso werden neue oder bereits registrierte Störungen, die keinem bereits bekannten Problem oder Known Error zugeordnet werden können, als Problem behandelt.

Die Klassifizierung von Problemen lehnt sich an der Klassifizierung von Incidents an. Die Problemzuordnung erfolgt auf der Basis von Schwerpunkten, die sich nach der untersten Ebene der CIs, die das Problem beeinflussen, richten. Gleichzeitig mit der Klassifizierung erfolgt eine Analyse der Auswirkungen unter Einbeziehung der Dringlichkeit. Wichtig ist in diesem Zusammenhang die Aufnahme und die Aktualisierung des Status. Auch eine Priorität wird zugewiesen.

Die Klassifizierung ist nicht statisch, sondern kann im Laufe des Lebenszyklus eines Problems geändert werden. Wenn zum Beispiel ein Workaround oder eine schnelle Lösung vorhanden sind, kann die Dringlichkeit eines Problems herabgesetzt werden, wohingegen das Auftreten weiterer gleichartiger Störungen die Auswirkungen eines Problems verschlimmern kann.

Die Untersuchung und die Diagnose sind eine iterative Phase (*siehe Abbildung 7.4*), d.h. stetige Wiederholung, während das beabsichtigte Ergebnis mit jedem Mal näher rückt. Oft läuft es darauf hinaus, dass man innerhalb einer Testumgebung unter unterschiedlichen Bedingungen (Labor) immer wieder versucht, die Störung zu reproduzieren. Bei diesen Versuchen können wiederholt mehrere oder andere Fachgebiete einbezogen werden, so dass dann eine andere Lösungsgruppe einen Beitrag zur Analyse und Diagnose des Problems liefert.

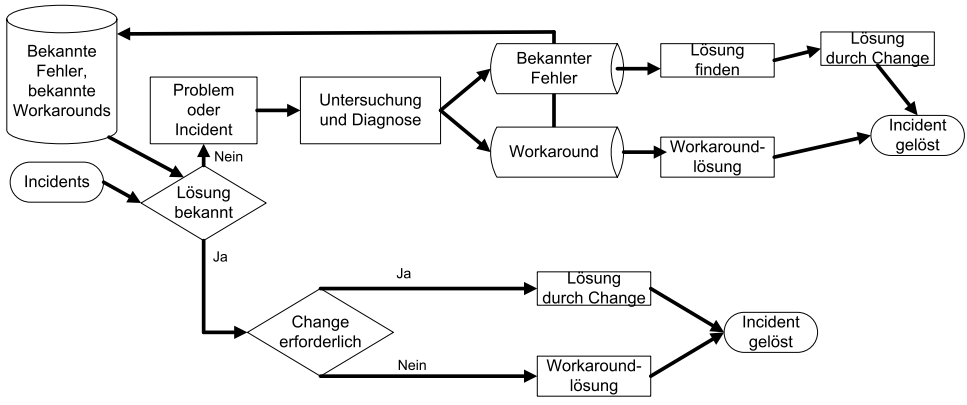


Abbildung 7.4: Probleme erkennen und beheben

Seiteneffekte

Probleme werden nicht nur durch Hard- oder Software verursacht. Es kommt regelmäßig vor, dass das Problem offenbar durch einen Dokumentationsfehler, menschliches Versagen oder einen Verfahrensfehler entstanden ist, z.B. bei der Freigabe einer falschen Software-Version. Aus diesem Grund kann es nützlich sein, auch Verfahrensanweisungen in der CMDB zu registrieren und im Rahmen der Versionsüberwachung zu beobachten.

Fehlerquellen werden oft aus anderen Umgebungen übertragen, aber meist erst in der Produktionsumgebung identifiziert. Jedoch können bereits in den Produkten sowohl von internen Entwicklern als auch Dienstleistern entdeckte bekannte Fehler („Bugs“) existieren.

Wenn die Ursache für ein Problem benannt werden kann, wenn bekannt ist, welches CI (Component Item) oder welche Kombination von CIs dem Problem zu Grunde liegt und wenn ein logischer Zusammenhang zwischen CI und Störung(en) hergestellt werden kann, wird ein bekannter Fehler definiert. Im Anschluss daran führt das Problem Management die Aktivitäten der Fehlerbehebung durch.

Problem Management gliedert sich in drei Subprozesse: Problem Control, Error Control und proaktives Problem Management (*siehe Abbildung 7.5*). Entsprechend dieser Begriffsreihenfolge sieht auch die Abfolge der Prozessaktivitäten aus: Erst kommt Problem Control, dann Error Control. Eine Eselsbrücke für die Reihenfolge ergibt sich aus Erst kommt das *Problem*, das dann zum bekannten *Fehler* (*Error*) wird.

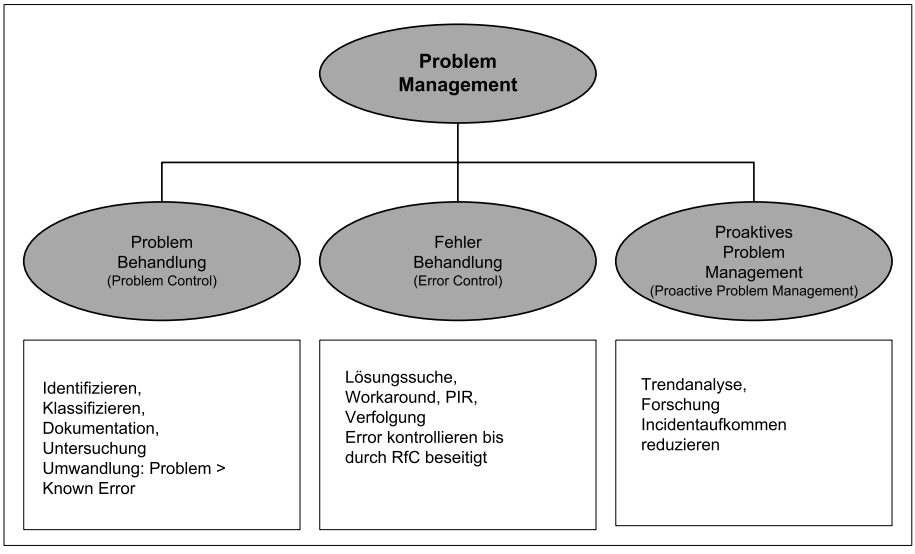


Abbildung 7.5: Subprozesse des Problem Management

- Problem Control, also die Problembehandlung als solche, stellt die erste Phase jeder Aktion des Problem Management dar. Hier liegt der Fokus auf der Umwandlung von Problemen in Known Errors.

  Die genaue Beschreibung des Problems und seine Klassifizierung sowie die Feststellung der Bearbeitungspriorität werden registriert und abgespeichert. Dann erfolgt die detaillierte Untersuchung des Problems und seine Auswirkungen auf die Anwendungen und ganz besonders auf die Services. Es handelt sich hierbei also um Problemklassifizierung (Kategorie, Impact, Dringlichkeit, Priorität). Soweit zu diesem Zeitpunkt möglich, wird Ursachenforschung betrieben. Es gibt Probleme, bei denen gerade die Quellen der Störungen nicht einfach oder schnell aufzufinden sind. Auch aus diesem Grunde ist eine entsprechende Dokumentation unerlässlich. Gegebenenfalls kommt man auch so Fehlerquellen aus anderen Umgebungen auf die Spur.
- Error Control, also die Fehlerbearbeitung/-behandlung: Hier liegt der Fokus auf der Kontrolle von Known Errors, bis diese durch einen Change gelöst oder beseitigt werden. Bekannte Fehler sind solche, die bereits früher schon einmal aufgetaucht sind, ITIL nennt diese Known Errors. Da hier die Ursachen bereits geklärt sind, sind auch die notwendigen Lösungsaktivitäten bekannt (Fehleridentifizierung und -bewertung). Die Lösung des neu ermittelten Problems wird initiiert und an die entsprechende Stelle delegiert. Zugleich können die so genannten RfCs (Requests for Change) an das Change Management weitergeleitet werden, falls das Problem durch Änderungen an der IT-Infrastruktur behoben werden soll. Das Error Control überwacht den Lösungsfortschritt und zeichnet die nachhaltige Lösung auf.

  Bei Known Errors sollte die verursachende Komponente im Problem Management gefunden werden. Solche IT-Komponenten werden als CI (Configuration Item) in der CMDB abgespeichert und können von dort fallweise abgerufen werden. Meistens führen bekannte Fehler zu Änderungsaktivitäten, diese werden als Vorschläge weitergeleitet.

Mitarbeiter des Problem Management geben eine Einschätzung über die zur Behebung eines bekannten Fehlers erforderlichen Maßnahmen ab. Unter Berücksichtigung vorhandener Vereinbarungen hinsichtlich der Service Levels sowie von Kosten und Nutzen wägen sie die verschiedenen Lösungsmöglichkeiten gegeneinander ab. Für den RfC bestimmen sie die Auswirkungen und die Dringlichkeit. Wenn die Beschaffenheit des Fehlers keinen Aufschub duldet (bei sehr schwer wiegenden Störungen), kann gegebenenfalls der Vorgang für eine dringliche Änderung Anwendung finden. Ungeachtet der Art der Entscheidung, die hinsichtlich eines bekannten Fehlers und seiner Lösung getroffen wird, muss diese in jedem Fall dokumentiert werden, damit eine Verwendung durch das Incident Management gewährleistet ist.

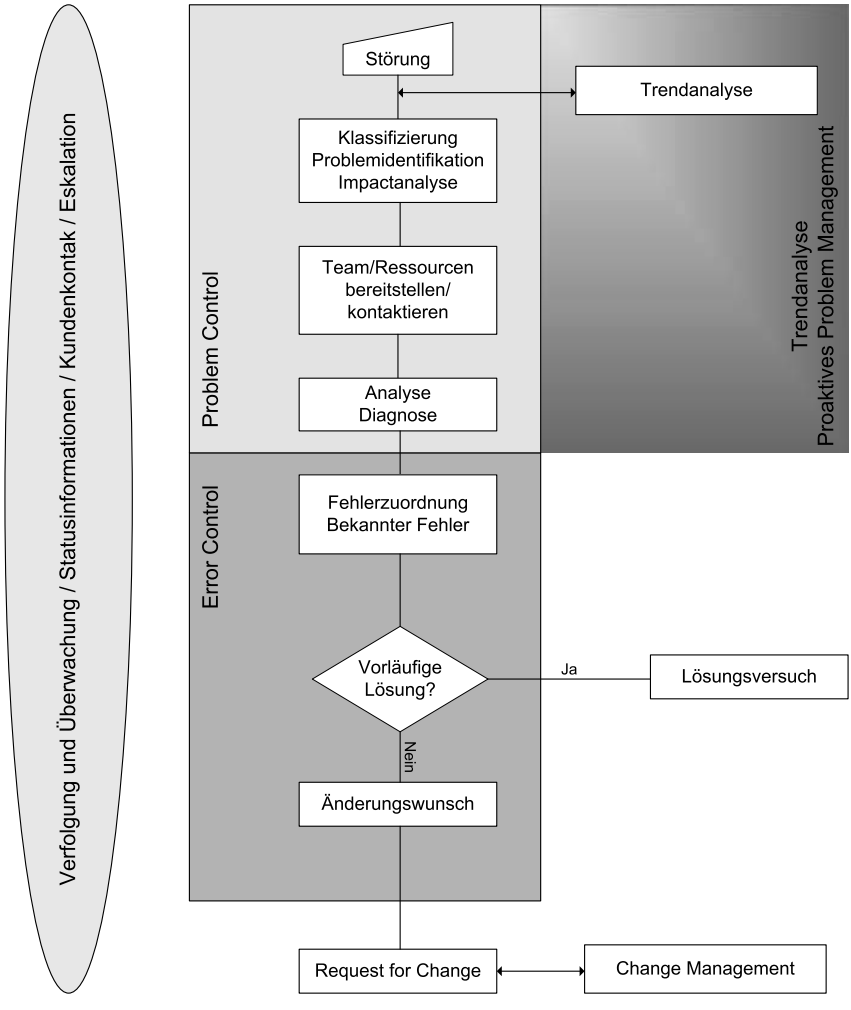


Abbildung 7.6: Problem Management

Bevor ein Problem zum Abschluss gebracht werden kann, muss zunächst die durchgeführte Änderung (Change) evaluiert werden. Zu diesem Zweck bedient man sich eines Post Implementation Review (PIR). Diese Aktivität findet immer im Problem Management statt (häufig Prüfungsfrage), auch wenn die Umsetzung des Changes an sich über das Change Management abläuft (*siehe Abbildung 7.6*)! Ist die Änderung erfolgreich verlaufen, erfolgen eine entsprechende Dokumentation und ein abschließendes Reporting. Es findet Rücksprache mit dem Incident Management statt, um die eventuell mit diesem Problem verbundenen Störungen ebenfalls abzuschließen.

- Proaktives Problem Management (Problemverhütung) hat die Aufgabe, das Incident-Aufkommen langfristig zu reduzieren. Dies zielt auf das Vermeiden von Problemen verschiedener Art ab. Eine wichtige Aufgabe des Problem Management besteht nun darin, Vorkehrungen zu treffen, um ein Problem im Idealfalle gar nicht erst entstehen zu lassen. Hierzu werden die früheren Lösungen analysiert, und aus Trends kann das Entstehen von Problemen schon im Vorfeld erkannt werden. Ein typisches Beispiel hierfür ist das Feststellen von sich abzeichnenden Transfer-Engpässen durch Messungen in Netzwerksegmenten. Ein hohes Datenaufkommen kann darauf hindeuten, dass ein Zusammenbruch eines Teilnetzes bevorsteht.

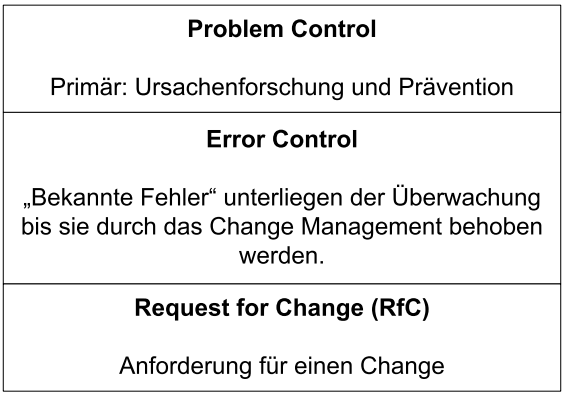


Abbildung 7.7: Bestandteile des Problem Management

Proaktives Problem Management ist insbesondere auf die Trendanalyse und Identifizierung potenzieller Störungen ausgerichtet, bevor diese überhaupt auftreten. Reviews größerer Probleme, Recherche, Protokollanalysen, Ressourcenüberprüfungen und Pflegeaufgaben helfen, mögliche Probleme und Schwachstellen zu identifizieren und proaktiv zu beheben.

Überprüfungen sind allerdings nicht nur für die rein technische Seite des Problem Management anzuraten, sondern auch für die Organisation und deren Verfahren und Werkzeuge (Berichte, Diagnose- und Beseitigungsqualität, Daten und Dokumentation). Je weiter das Problem Management entwickelt ist, umso mehr Zeit kann für proaktive Tätigkeiten verwendet werden.

Problem-Manager: Ein „Hut“ im Problem Management

Der Problem-Manager ist sowohl für alle Aktivitäten innerhalb des Problem Management verantwortlich als auch für die Entwicklung und Pflege der Problem- und Fehlerbehandlung, der Beurteilung der Effizienz und der Effektivität von Problem- und Fehlerbehandlung. Er kümmert sich um das Erstellen und Weitergeben von Managerinformationen an die richtigen Personen, die Beschaffung der für die Aktivitäten erforderlichen Ressourcen sowie die Entwicklung und Verbesserung von Problem- und Fehlerbehandlungssystemen. Die Zuständigkeiten können aufgeteilt werden:

- Reaktive Zuständigkeiten zur Identifizierung und Erfassung von Problemen durch die Analyse von Störungsdaten, die Untersuchung von Problemen nach ihrer Priorität und die Erstellung von RfCs. Diese Personengruppe überwacht den Fortschritt bei der Behebung des bekannten Fehlers und informiert das Incident Management über Workarounds und schnelle Lösungen.
- Proaktive Zuständigkeiten dienen der Identifizierung von Trends, der Datenanalyse, der Erstellung von RfCs und zum Entwerfen von vorbeugenden Konzepten, auch um beispielsweise einer Verbreitung von Probleme über mehrere Systeme entgegenzuwirken.

Die Prozess-Manager können, v.a. im operativen Bereich großer Unternehmen, von Koordinatoren unterstützt werden. Als Inhaber dieser Rolle beschäftigen sich Mitarbeiter vorwiegend mit der Planung oder der Koordinierung im jeweiligen Prozess.

Der Erfolg des Problem Management leitet sich ab aus:

- dem Rückgang der Störungshäufigkeit durch die Lösung von Problemen
- dem Zeitaufwand, der für die Behebung eines Problems nötig ist
- den sonstigen Kosten, die zur Lieferung der Lösung aufgewendet werden müssen

Diese Indikatoren lassen sich messen. Dementsprechende KPIs werden definiert. Die Anzahl der gefundenen und beseitigten Fehlerursachen oder die der eingeleiteten RFCs können Kernparameter darstellen. Im Fokus stehen die Steigerung der Anwenderproduktivität durch eine Reduzierung der Incidents und daraus resultierend eine höhere Kundenzufriedenheit.

7.4 Problem Management im ITIL-Gesamtzusammenhang

Das Problem Management fungiert als Kommunikationspartner gegenüber anderen Prozessgruppen oder ITIL-Funktionen. Besonders eng ist die Zusammenarbeit mit dem Incident Management, wo Störungen als Probleme klassifiziert und an das Problem Management weitergeleitet werden. Das Problem Management stellt hier die nachgelagerte Einheit. Beide Prozesstypen setzen die Existenz eines gut funktionierenden Service Desk voraus, der sich mit dem Problem Management immer

wieder abstimmen muss. Eine qualitativ gute Störungserfassung ist die Voraussetzung für ein einwandfreies Funktionieren des Problem Management, weil die Informationen aus der Störungserfassung die Basis bei der Suche nach strukturellen Fehlern bilden. Aufgrund einer guten und ausführlichen Störungsbeschreibung mit allen relevanten Eckdaten ist es in vielen Fällen dem Problem Management bereits mit diesen Informationen möglich, die Problemursache einzugrenzen.

Das Problem Management unterstützt das Incident Management andersherum ebenso, indem Informationen zu einer Störung aus dem Problem Management in Richtung Incident Management fließen. Solange die Lösung für ein Problem noch nicht bekannt ist, kann vom Problem Management ein Workaround zur Behebung der Störung angeboten werden. Auch Informationen für die Wissensdatenbank des Incident Management bzw. Service Desk werden vom Problem Management bereitgestellt, um selbstständig Lösungen anbieten zu können und genug Material bei der Problemmustersuche vorzufinden, die für die Aktivität des Incident Management relevant ist.

Immer dann, wenn ein Problem durch eine Änderung an Komponenten der IT-Infrastruktur behoben werden soll, kommt das Change Management ins Spiel. Das Change Management ist für die kontrollierte Durchführung von Änderungen, einschließlich der Änderungsanträge, die das Problem Management vorlegt, zuständig, um strukturelle Fehler zu beseitigen. Das Change Management sorgt für die Beurteilung der Auswirkungen und die benötigten Ressourcen sowie für die Planung, die Koordination und die Auswertung der beantragten Änderungen. Es informiert das Problem Management über den Verlauf und den Abschluss von korrigierenden Changes. In Zusammenarbeit mit dem Problem Management werden korrigierende Änderungen evaluiert. Über diese Vorgänge wird im Review nach der Implementierung (Post Implementation Review, PIR) Bericht erstattet (*siehe Abbildung 7.8*). Aktiv wird dieser Schritt stets vom Problem Management durchgeführt. Anschließend können innerhalb der Fehlerbehandlung die bekannten Fehler abgeschlossen werden.

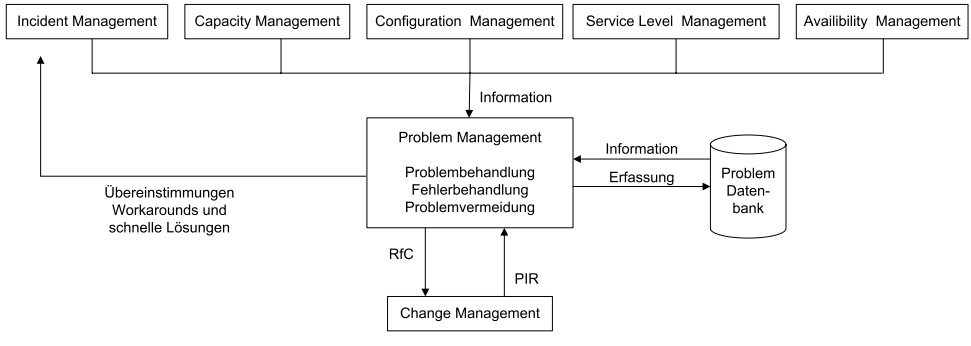


Abbildung 7.8: Schnittstellen zum Problem Management

Das Configuration Management liefert für alle ITIL-Prozesse wichtige Informationen zu den IT-Komponenten jedweder Form und ihre Zusammenhänge. Ohne diese Daten wäre das Aufspüren von Fehlerursachen zusammenhängender Komponenten, deren Fehlerverhalten sich gegenseitig beeinflusst, überaus schwierig. Das Configuration Management liefert so über die CMDB wichtige Informationen über die Komponenten innerhalb der Infrastruktur. Auch Beziehungen zwischen den jeweiligen CIs spielen für die Untersuchungen im Problem Management eine große Rolle.

Das Problem Management liefert dem Availability Management Informationen zu Fehlern bzw. Problemen, so dass es die Ursache für die Nichtverfügbarkeit ermitteln und beheben kann.

Das Capacity Management sorgt für den optimalen Einsatz von IT-Mitteln. Dabei spielen das Management und die Optimierung von Leistungen und Ressourcen eine wichtige Rolle, wobei der Schwerpunkt in der Planung liegt. Finden sich verdächtig oft Ursachen für Probleme in diesem Fokus, ist ein Abgleich zwischen Problem Management und Capacity Management notwendig. Das Problem Management unterstützt das Capacity Management, indem es die Ursache von Problemen hinsichtlich der Kapazität suchen und beheben lässt, um dies dann über das Change Management beheben zu lassen. Achtung: Das PIR wird wie immer über das Problem Management durchgeführt.

Das Service Level Management liefert dem Problem Management wichtige Informationen, auf deren Grundlage Probleme definiert werden können, weil beispielsweise Antwortzeiten außerhalb der in den SLAs vereinbarten Bereichen liegen. Die Verfahren des Problem Management müssen die vereinbarten Qualitätsanforderungen unterstützen. Auch für das Financial Management und das Continuity Management der IT Services spielt das Problem Management diese Rolle. Service Level Agreements sollten im gegenseitigen Interesse der beteiligten Vertragsparteien grundsätzlich so flexibel gestaltet sein, dass eine Anpassung an sich ändernde Rahmenbedingungen, zum Beispiel ausgelöst durch einen Technologiewechsel, im Sinne eines definierten Change Management-Verfahrens in Form von RfCs problemlos durchgeführt werden kann.

8 Configuration Management

Jede IT-Organisation besitzt Informationen über ihre IT-Infrastruktur. Dies gilt insbesondere nach dem Abschluss großer Projekte, in deren Rahmen meist Konzepte und Anwendungssteckbriefe geschrieben, Betriebs- und Systemhandbücher erstellt, abschließend Audits und eine Analyse über die Auswirkungen durchgeführt wurden. Die Kunst liegt jedoch darin, diese Informationen stets auf einem aktuellen und konsistenten Stand zu halten. Liegen zwar Informationen über die Infrastruktur vor, sind diese aber nicht korrekt und aktuell, erscheinen sie mehr oder weniger wertlos. Innerhalb des Configuration Management werden die Daten der Infrastruktur und ihrer Komponenten laufend erfasst und überprüft, um sie aktuell zu halten.

Neben den isolierten technischen Aspekten gibt es hier auch wichtige Informationen über Relationen aller Art wie beispielsweise die jeweiligen Beziehungen zu den angebotenen IT Services und den Komponenten untereinander. Hindergrund ist die folgende Prämisse: Es muss möglich sein, bei einer Veränderung bestimmter Komponenten auch die Auswirkungen auf die entsprechenden Prozesse beziehungsweise auf die verknüpften Dienstleistungen zu erhalten. Macht beispielsweise eine Netzwerkkomponente Probleme, möchte das Unternehmen bzw. die IT-Abteilung vor einem Austausch wissen, wie viele andere Objekte wie Server, Client-Rechner oder andere Komponenten von dieser Komponente abhängig sind. Stehen die Informationen bereit, ist eine Abschätzung der Priorität möglich, d.h. eine Antwort auf die Frage, welche Auswirkungen schlimmstenfalls zu erwarten wären, wenn die Netzwerkkomponente ausfiele.

Configuration Items

Grundsätzlich sind mit Configuration Items (CIs) alle Komponenten gemeint, die für die IT-Dienstleistungen benötigt werden. Sie werden alle in der CMDB eingetragen. Jeder Datenbankeintrag erhält einen identifizierenden Suchschlüssel (Item Key) und Kategorisierungsangaben. Ansonsten sollten dort alle notwendigen Datenfelder vorhanden sein. Wichtig sind vor allem jene Informationen, die die Relationen zu den Diensten ermöglichen. „Welcher IT Service setzt welche Komponenten (CIs) voraus?“ – diese Frage muss das Configuration Management stets aktuell beantworten können. Bei der Datenmodellierung ist äußerste Umsicht geboten, um alle relevanten und später benötigten Informationen aufzunehmen und vorzuhalten.

Die Datensätze in den Datenbanken werden bei ITIL als Configuration Item (CI) bezeichnet. Fragen zur Kompatibilität oder zu möglichen Diskrepanzen sollten schnell beantwortet werden können. Diese enthalten meist auch weitere nichttechnische Daten, welche z.B. die Standorte von Komponenten definieren. Bei

Umzügen innerhalb des Unternehmens müssen diese Angaben geändert werden. Weitere Informationen geben nicht nur Auskunft über den Anschaffungswert, sondern auch den jeweiligen Zeitwert im Rahmen von Abschreibungen. Diese Informationen können dann beispielsweise vom Financial Management oder dem IT Controlling genutzt werden.

8.1 Configuration Management nach ITIL

Ziel des Configuration Management ist es, jederzeit gesicherte und genaue Informationen über die IT-Infrastruktur zur Verfügung zu stellen. Unter der Voraussetzung, dass Systeme und Komponenten sauber installiert und konfiguriert sowie Funktionen und Features korrekt implementiert wurden, sollte das Configuration Management benachbarten ITIL-Gruppen und entsprechend involvierten und verantwortlichen Personen wie dem Management Auskunft geben. Dies bezieht sich auf Finanzdaten und Produktrichtlinien (Policies), Troubleshooting-Informationen sowie die Bestimmung von möglichen Seiteneffekten und Auswirkungen, den IT Service und die damit zusammenhängende Verrechnung. Allgemein gesprochen geht es um die Kontrolle der IT-Infrastruktur und die Unterstützung von anderen (ITIL-) Prozessen durch die Bereitstellung eines möglichst detaillierten Modells der Umgebung als Informations- und Arbeitsgrundlage.

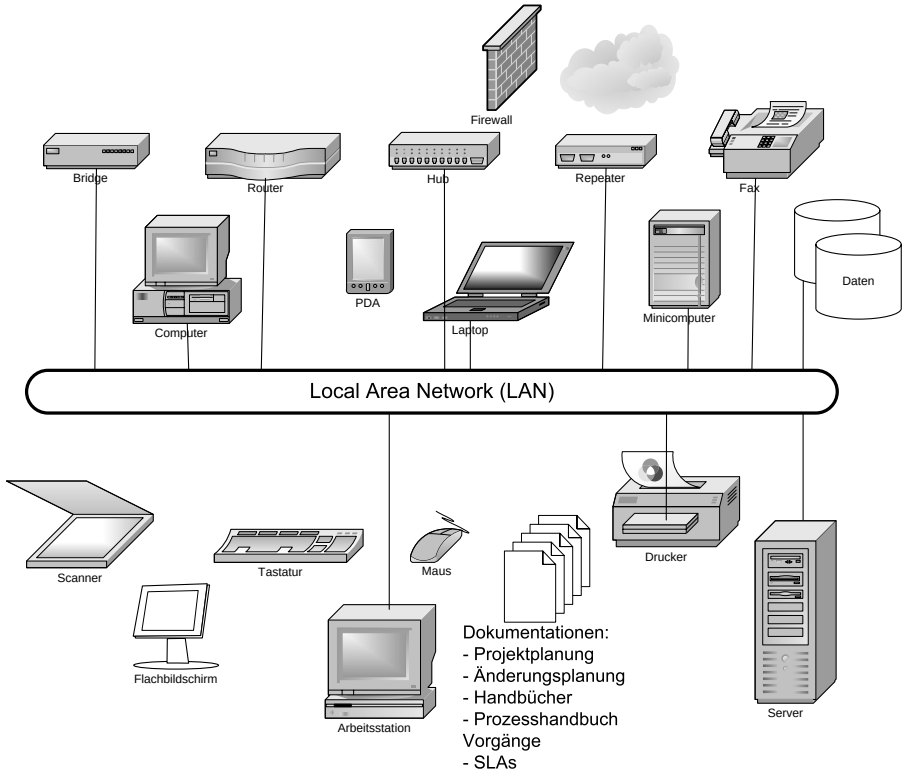


Abbildung 8.1: Configuration Items (CIs)

Das Configuration Management darf nicht mit dem Asset Management verwechselt werden: Das Asset Management ist dem Bereich der Buchhaltung zuzuordnen und überwacht die Abschreibungen für Artikel mit einem Anschaffungswert, der eine zuvor festgelegte Grenze überschreitet.

Asset

Ein Asset gehört zu den Komponenten eines Geschäftsprozesses und kann Menschen, Peripherie, Netzwerkkomponenten, Dokumentationen und Anwendungen umfassen.

Im Rahmen des Asset Management werden Daten über Beschaffungswert, Abschreibung, Geschäftsbereich und Standort gespeichert. Ein gut eingerichtetes Asset Management kann Auftakt für die Einrichtung eines Configuration Management sein. Das Configuration Management geht einen Schritt weiter und verwaltet Informationen über die CIs (Konfigurationen) und setzt sie in Beziehung zueinander. Zudem behält das Configuration Management die Rückmeldung über aktuelle Daten wie den Status von Betriebsmitteln, Angaben über ihren Verbleib und vorgenommene Änderungen im Auge. Der wichtigste Unterschied zwischen einem Asset und einem CI besteht darin, dass CIs Beziehungen besitzen.

8.2 Begriffe des Configuration Management

In der Terminologie des Configuration Management werden die Betriebsmittel und die daraus resultierenden IT Services als Konfigurationselemente (Configuration Items, CIs) bezeichnet. Jedes Betriebsmittel, dessen Existenz und Version erfasst wird, ist ein CI. Dabei kann es sich um PC-Hardware, PC-Software, aktive und passive Netzwerkkomponenten, Server, zentrale Geräte, Dokumentationen, Verfahren, IT Services und alle sonstigen Betriebsmittel handeln, die die IT-Organisation kontrollieren will. Die Beziehungen, in denen CIs zueinander stehen, sind unter anderem für die Störungsdiagnose und für die Vorhersage der Verfügbarkeit der Services nützlich. CIs besitzen Relationen und Attribute, sind eindeutig identifizierbar und müssen verwaltet werden, z.B. bei Changes. Es können vielerlei Beziehungen unterhalten werden, die in logische und physische Beziehungen aufgegliedert werden:

- Physische Beziehungen wie etwa „sind Bestandteil von"/Parent-Child-Beziehung des CI, z.B. ein Diskettenlaufwerk ist Bestandteil eines PC und ein Software-Modul ist Bestandteil eines Programms oder „ist verbunden mit" wie ein PC, der an ein LAN-Segment angeschlossen ist
- Logische Beziehungen wie etwa „ist eine Kopie von", wenn ein Item die Kopie eines Standardmodells, einer Baseline oder eines Programms darstellt

CI Baseline

Dieser Begriff steht für CIs, deren Eigenschaften zu einem bestimmten Zeitpunkt dokumentiert und seitdem nicht verändert wurden, so dass sichergestellt werden kann, dass Informationen in korrekter Form vorliegen. Die daraus hervorgegangene Erhebung dient als Ausgangspunkt für den weiteren Ausbau und die Prüfung neuer Konfigurationen, als Standard für die Auslieferung von Konfigurationen an den Anwender, z.B. Standardarbeitsplatz, als Ausgangspunkt für die Auslieferung neuer Software und als Standard-CI zur Erfassung von Kosteninformationen. Wichtig ist hier eine Dokumentation des Status (Historie) zur Rückverfolgung.

Das Management der CIs erfolgt in der Konfigurations-Management-Datenbank (Configuration Management Database, CMDB). Eine CMDB ist keine Inventarisierungsdatenbank, die lediglich Informationen über momentane aktive Komponenten liefert. Sie geht weit darüber hinaus. Sie ist das Herzstück der ITIL-Prozesse im Unternehmen.

Die CMDB stellt eine große Kartei dar, in der sämtliche IT-Betriebsmittel registriert und in der die verschiedenen Beziehungen zwischen den einzelnen Karten festgehalten werden. In ihrer einfachsten Form basiert die CMDB auf einfachen Formularen oder auf einer Reihe von Spreadsheets. Eine deutlich aussagekräftigere Form der Darstellung ist jedoch wünschenswert. Häufig werden in den Organisationen Dokumentationen der entsprechenden Komponenten bereits zur Verfügung gestellt. Eine CMDB kann aus mehreren Datensystemen bestehen, eine weitestgehende Integration ist anzustreben, um die Verwendung nicht unnötig zu erschweren.

Neben Hard- und Software kann zusätzlich noch die Dokumentation in den Umfang der CMDB aufgenommen werden, z.B. Service Level Agreements (SLAs), Servicekatalog, Verfahren, Handbücher, technische Daten, Organigramme und Projektpläne. In der CMDB sind sie mit Versionsnummer, Veröffentlichungsdatum, Verfasser und sonstigen Daten vermerkt, damit auch die Eigenschaften dieser Dokumente mit Hilfe des Configuration Management und des Change Management gepflegt und vor allem genutzt werden können.

8.2.1 Configuration Management-Datenbank (CMDB)

Wie bei vielen anderen Repository-Systemen muss auch für die Datenbasis des Configuration Management ein Datenmodell entworfen werden. Während des Aufbaus eines solchen Systems werden Entscheidungen hinsichtlich des Umfangs und der Detaillierung der zu erfassenden Informationen getroffen (*siehe Abbildung 8.2*). Für jede Eigenschaft, die erfasst werden soll, müssen zudem ein Verantwortlicher (für die Pflege) und ein Interessent (für die Dokumentation dieser Eigenschaft) identifiziert werden. Je mehr Eigenschaften dokumentiert werden müssen, umso mehr Arbeitsaufwand ist für die ständige Aktualisierung der Informationen erforderlich. Je weniger Ebenen definiert werden, desto geringer ist die Kontrolle und desto weniger Informationen über die IT-Infrastruktur stehen zur Verfügung. Hier ist ein Kompromiss zwischen Anforderungen, Aufwand und Nutzen zu erwägen.

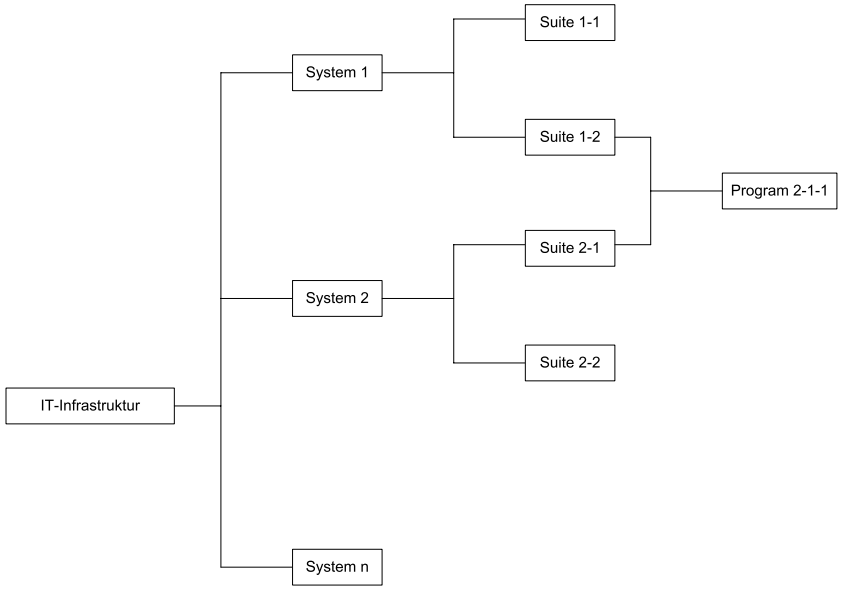


Abbildung 8.2: Detaillierungstiefe

Diese Betrachtungsweise kann in verschiedene Richtungen ausgedehnt werden. Dies gilt sowohl hinsichtlich des Umfangs (Scope) als auch des Detaillierungsgrads der CMDB.

Der CMDB-Scope beschäftigt sich mit der Frage „Wie viele und welche CI-Kategorien/-Typen werden in die Datenbank aufgenommen?“

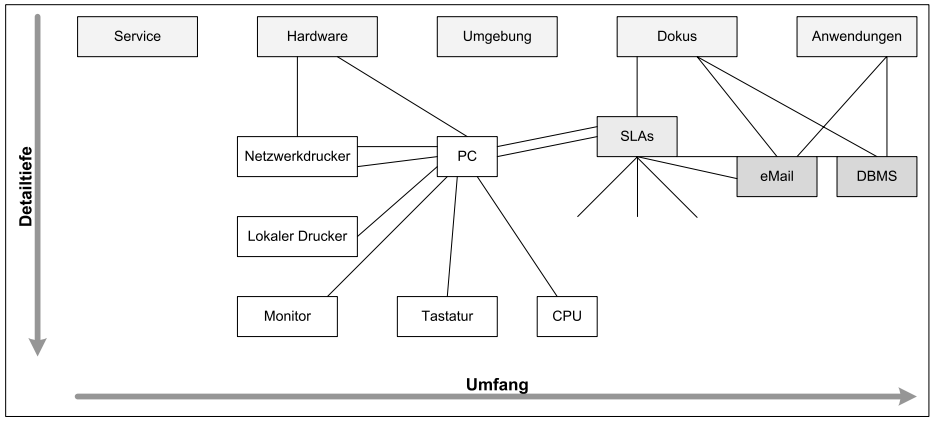


Abbildung 8.3: Größen einer CMDB

Der Detaillierungsgrad kann wiederum in die Anzahl der Ebenen, die zu unterhaltenden Beziehungen, die Namensgebung und die Eigenschaften untergliedert werden (*siehe Abbildung 8.3*). Hier geht es beispielsweise um die Frage „Wie viele Ebenen werden für die einzelnen Kategorien aufgenommen? Ist jede Maus relevant?“ Wichtig ist dabei, dass eine schnelle und umfassende Suche nach bestimm-

ten (verknüpften) Informationen möglich ist. Dabei müssen beispielsweise alle mit einem CI verknüpften Incidents Records, alle mit einem Service verknüpften CIs oder eine CI-Historie gefunden werden können. Auch das Lizenzmanagement lässt sich auf Basis der CMDB vereinfachen.

Im Rahmen einer adäquaten systematischen Namensgebung sollte für ein CI eine eindeutige bzw. einmalige Bezeichnung vergeben werden. Am einfachsten ist eine schlichte Nummerierung, für die eventuell pro Schwerpunkt bestimmte Nummernbereiche reserviert werden. Auf diese Weise können automatisch Nummern generiert werden, wenn ein neues CI angelegt wird. Mit Hilfe der Namensgebung können auch physische CIs mit Bezeichnungen versehen werden, damit diese CIs bei Audits, Wartungsarbeiten und Störungserfassungen eindeutig identifizierbar sind.

Abgesehen von der Einteilung in CI-Ebenen, den Beziehungen und der Namensgebung spielen auch die Eigenschaften bei der Detaillierung der CMDB eine Rolle. Mit Hilfe der Eigenschaften werden Informationen gespeichert, die für das betreffende CI relevant sind. Neben der CMDB werden weitere Libraries zum Speichern von Dokumenten- und SW-CIs benötigt (siehe Release Management).

Die CMDB wird zunächst mit vorhandenen Daten wie etwa aus dem Finanzbereich oder mit anderen bereits verfügbaren Daten zur Infrastruktur geladen und um technische Daten und Dienstleister ergänzt. Hierbei gilt die Einschränkung, dass nur die Daten erfasst werden, für die definitiv Interessenten identifiziert wurden, und dass die IT-Organisation diese Erfassung in Auftrag gegeben hat (Bereitschaft, diese Daten zu pflegen).

8.2.2 Configuration Items (CIs)

Die Lebensdauer einer Komponente lässt sich in verschiedene Zustände untergliedern und jedem Zustand kann ein Statuscode zugewiesen werden (*siehe Abbildung 8.4*). Diese Informationen werden von den Interessen bestimmt, die eine Organisation im Hinblick auf die zu erfassenden Eigenschaften der IT-Inftastruktur geäußert hat. Wenn die Kalenderdaten einer jeden Statusänderung registriert werden, kann sich ein klares Bild über die Lebensdauer eines Produkts ergeben: die Bestelldaten, die Installationsdaten und der Aufwand an Wartung und Support.

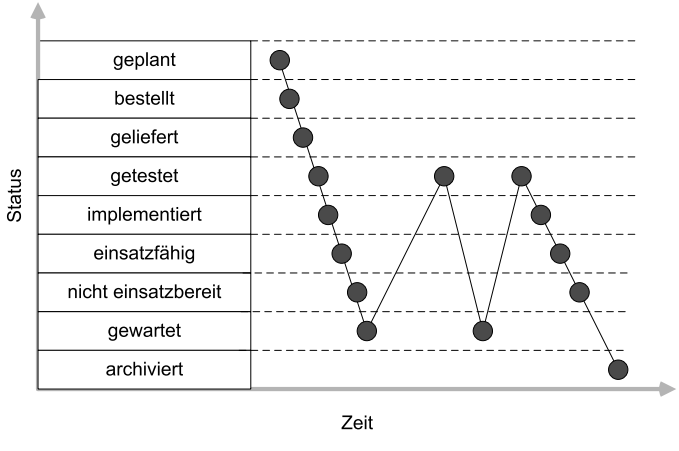


Abbildung 8.4: Status einer CI

Der Status einer Komponente kann auch dafür ausschlaggebend sein, was mit dem jeweiligen CI geschehen darf. Wird zum Beispiel ein Status für Reserven gepflegt (nicht operativ), so dürfen diese Geräte nicht ohne Rücksprache eingesetzt werden (z.B. weil sie Bestandteil eines Continuity-Plans sind). Statusänderungen eines CI können mit einer genehmigten wie auch nicht genehmigten Änderung (Change) oder mit einer Störung in Zusammenhang stehen (*siehe Abbildung 8.5*).

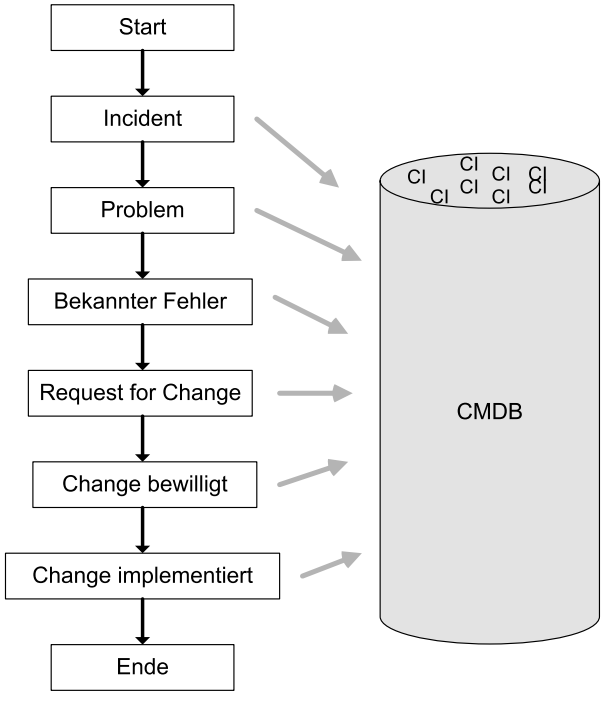


Abbildung 8.5: Input der CMDB

Um die CMDB stets auf dem neuesten Stand halten zu können, müssen die Daten gepflegt werden. Bei sämtlichen Aktivitäten, bei denen die dokumentierten Eigenschaften der CIs oder deren interne Beziehungen geändert werden, sind diese Änderungen in der CMDB festzuhalten.

Zu diesem Zweck kontrolliert und dokumentiert das Configuration Management alle neu hin- zukommenden IT-Betriebsmittel. Für die Hardware können als Erfassungszeitpunkt das Bestell- oder das Auslieferungsdatum herangezogen werden, während es sich für die Software anbietet, sie zum Zeitpunkt ihrer Aufnahme in die Definitive Software Library (DSL) zu registrieren.

Weitere Aufgaben im Rahmen der Kontrolle bestehen darin, die Dokumentation der einzelnen CIs sicherzustellen und sie auf ihre Zulassung zu überprüfen. Das Configuration Management unterhält zu diesem Zweck enge Kontakte zu den Dienstleistern, dem Incident Management, dem Problem Management und dem Change Management.

Wenn innerhalb der IT-Infrastruktur vom Change Management koordinierte Änderungen durchgeführt werden, ist es Aufgabe des Configuration Management,

die diesbezüglichen Informationen in der CMDB zu verarbeiten. Auch wenn andere Prozesse Veränderungen an den CIs anstoßen, behält das Configuration Management die „Herrschaft“ über die CMDB (häufige Prüfungsfrage!). In der Regel gehört in der Praxis die Erfassung von RfCs in den Zuständigkeitsbereich des Change Management. Changes stellen die wichtigste Informationsquelle im Hinblick auf Veränderungen innerhalb der Infrastruktur und somit für die Pflege der CMDB dar. Das Configuration Management stellt also Anforderungen an den Reifegrad anderer Prozesse in der Organisation; in diesem Zusammenhang sind insbesondere das Change Management, der Betrieb sowie der Einkauf zu nennen.

Im Rahmen von Audits lässt sich überprüfen, ob die Daten in der CMDB noch mit der aktuellen Situation übereinstimmen. Audit-Tools können zum Beispiel automatisch die Arbeitsplatz-PCs durchforsten und die aktuelle Situation und den Status dieser IT-Infrastruktur melden. Diese Daten können dann für die Kontrolle und die Aktualisierung der CMDB verwendet werden.

8.3 Ziele und Aktivitäten des Configuration Management

Ziel des Configuration Management ist es, die Überwachung der wirtschaftlichen Bedingungen der IT Services zu unterstützen, indem ein logisches Modell aus IT-Infrastruktur und IT Services gepflegt wird. Andere Betriebsprozesse erhalten Informationen über dieses Modell. Zu diesem Zweck identifiziert, überwacht und kontrolliert das Configuration Management die vorhandenen CIs und ihre Versionen und pflegt diese Informationen.

Dazu gehört auch die Pflege eines gesicherten Datenbestands über Betriebsmittel und IT Services der Organisation sowie die Beschaffung und Bereitstellung genauer Informationen und Dokumentationen über diese Betriebsmittel und IT Services zur Unterstützung aller anderen Service Management-Prozesse.

Der Prozess „Configuration Management“

Ein Prozess ist eine Abfolge von zusammenhängenden Arbeitsschritten mit einem definierten Input und Output sowie einem Ziel.

Als definierter Input für den Configuration Management-Prozess dienen Daten über unterschiedliche Configuration Items. Diese Informationen können aus dem Verlauf und dem Abschluss von Änderungen an der IT-Infrastruktur und aus dem Einkauf stammen. Neben einer gefüllten CMDB, die den wichtigsten Output dieses Prozesses darstellt, gelten auch die verschiedenen Berichte an andere Prozesse und an das IT-Management als Output.

Obwohl das Configuration Management ebenso wie die anderen Prozesse einen logischen Prozessablauf kennt, wird dieser nicht strikt eingehalten. Die Aktivitäten werden mehr oder weniger parallel durchgeführt. Wichtig ist die Organisation des Prozesses vor allem bei der Einführung sowie die Verarbeitung und die Implementierung von neuen Informationserfordernissen.

1. Bei der Planung geht es um die Festlegung von Strategie, Grundsätzen (Policies) und Zielsetzungen für den Prozess, Analyse der bereits vorhandenen Informationen, Auswahl der Werkzeuge und Ressourcen, Einrichtung von Schnittstellen mit anderen Prozessen, Projekten, Dienstleistern usw.
2. Während der Identifizierung wird der Prozess etabliert, der für die Aktualisierung der Datenbank erforderlich ist. Es geht vor allem darum, CI-Kategorien und -Level festzulegen. Die Aktivitäten umfassen die Erstellung eines Datenmodells zur Erfassung aller Komponenten innerhalb der IT-Infrastruktur, deren Beziehungen untereinander, Informationen über Verantwortliche, Status sowie die verfügbaren Dokumentationen. Neben der Erstellung des Datenmodells liegt der Schwerpunkt auf der Realisierung von Verfahren für die Integration neuer CIs und für Veränderungen an den CIs. Aufgrund der sich ständig ändernden Nachfrage nach Informationen werden auch laufend Anpassungen bei der Auswahl der Konfigurationsdaten vorgenommen.

   Bei der Einteilung in Ebenen wird eine Hierarchie von Komponenten und Bestandteilen erstellt. Es werden die Parent CIs sowie die Zahl der Ebenen für die CIs festgelegt (*siehe Abbildung 8.6*). Die höchste Ebene ist die IT-Infrastruktur selbst. Auch die unterste Ebene muss kontrollierbar und pflegbar sein.

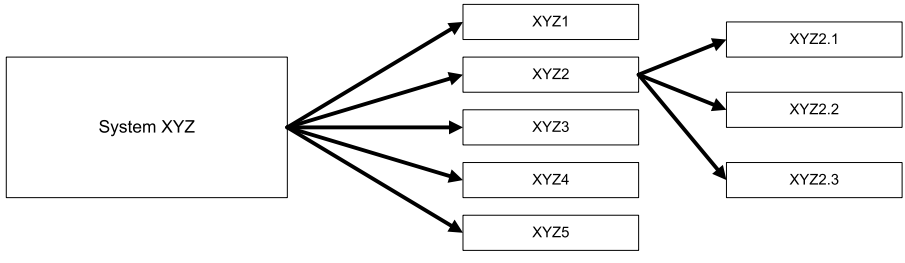


Abbildung 8.6: Parent-Child-Beziehungen

3. Die Kontrolle (Control) stellt sicher, dass der Inhalt der CMDB stets auf dem neuesten Stand ist, indem lediglich zugelassene (autorisierte) und identifizierte CIs akzeptiert und registriert werden. Sie sorgt außerdem dafür, dass kein CI hinzugefügt, angepasst, ersetzt oder entfernt wird, ohne dass diesbezüglich die entsprechende Dokumentation, zum Beispiel in Form eines genehmigten Request for Change (RfC) oder einer angepassten Spezifikation, vorliegt. Alle Veränderungen an der CMDB dürfen nur über das Change Mangement laufen. Voraussetzung ist hier allerdings eine saubere Prozessdefinition und eine entsprechende Rollenverteilung.
4. Die Statusüberwachung beschäftigt sich mit der Speicherung aktueller und historischer Daten über den Status eines CI im Laufe seines Lebenszyklus. Die Statusüberwachung ermöglicht die Verfolgung von Statusänderungen, z.B. „Entwicklung“, „Test“, „Lager“, „im Einsatz“ und „ausgemustert“.
5. Die Verifizierung der Daten in der CMDB erfolgt mit Hilfe von Audits der IT-Infrastruktur. Dabei wird geprüft, ob die erfassten CIs (noch) existieren und ob die eingetragenen Daten korrekt sind. Mit der Hilfe des Berichtswesens werden den anderen Prozessen Informationen zur Verfügung gestellt und Berichte über

Trends und Entwicklungen beim Gebrauch von CIs ausgearbeitet. Dies findet vor allem vor größeren Changes, Release-Wechseln, bei Verdacht auf unautorisierte CIs bzw. stichprobenhaft oder regelmäßig statt. Diese Überprüfung sollte vor größeren Changes oder Release-Wechseln, nach der Implementierung der CMDB oder deren Wiederherstellung, bei Verdacht auf unautorisierte CIs sowie stichprobenhaft oder regelmäßig erfolgen.

Configuration-Manager: Ein „Hut" im Configuration Management

Der Configuration-Manager kann unter anderem die folgenden Aufgaben haben:

- Einbringen von Vorschlägen zum Umfang und zur Detaillierung des Configuration Management
- Kommunikation hinsichtlich seines Prozesses und dessen Bekanntheitsgrad
- Personelle Besetzung und Schulung für seinen Prozess
- Identifizierung und Festlegung der Namenskonventionen
- Aufbau der Schnittstellen zu den anderen Prozessen
- Planung und Aufbau der CMDB und Pflege derselben
- Erstellung von Berichten
- Durchführung von Konfigurationsaudits

8.4 Configuration Management im ITIL-Gesamtzusammenhang

Die CMDB aus dem Configuration Management wird als Mittelpunkt der ITIL-Prozesse angesehen. Hieraus entnehmen die Prozesse ihre Informationen zur IT-Infrastruktur.

Das Incident Management nutzt die CMDB, um Informationen zu IT-Komponenten aus der Infrastruktur zu gewinnen und als Arbeitsgrundlage mit den Incidents zu nutzen. Im Rahmen der Störungserfassung und -klassifizierung nutzt das Incident Management die dokumentierten Zusammenhänge der CIs vor allem zur Störungsdiagnose. Mithilfe dieser Daten kann das Incident Management erfahren, wo sich das CI befindet, wer es administriert, ob ein Problem oder ein bekannter Fehler mit einem Workaround dafür bekannt ist und für welchen Kunden es mit welchem IT Service und welchem SLA verbunden ist.

Das Problem Management ist darüber hinaus an weiter gehenden technischen Details aus der CMDB interessiert. Es muss in der Lage sein, die Infrastruktur zu überblicken, um die CIs im Bedarfsfall in Zusammenhang bringen zu können. Nur so ist es in der Lage, Probleme und bekannte Fehler mit den CIs zu verknüpfen.

Das Change Management muss die Auswirkungen von durchzuführenden Änderungen einschätzen können und autorisiert diese Änderungen (*siehe Abbildung 8.7*). Eine Änderung muss in Beziehung zu den betroffenen CIs gesetzt werden können. Alle über das Change Management durchgeführten Änderungen müssen

in der CMDB dokumentiert werden. So werden Informationen zu den Komponenten konsistent gehalten. Wird die Hardware in einem System verändert, so muss der Zustand des entsprechenden CIs in der CMDB dokumentiert werden. So erhält dieses CI für den Zeitraum der Wartungsmaßnahme den Status „nicht produktiv" oder „in Wartung", bevor es nach Vollendung der Arbeiten wieder auf „aktiv" oder „in Produktion" versetzt werden darf. So unterwirft das Change Management die CIs, ihre Attribute und Stati ständig Veränderungen. Jede Änderung in der IT-Infrastruktur bewirkt unmittelbare Veränderungen an der CMDB und vice versa. Damit liefert das Change Management die wichtigsten Informationen, die erforderlich sind, um die CMDB stets auf dem neuesten Stand zu halten. Andererseits dient die CMDB dem Change Management als Orientierungshilfe.

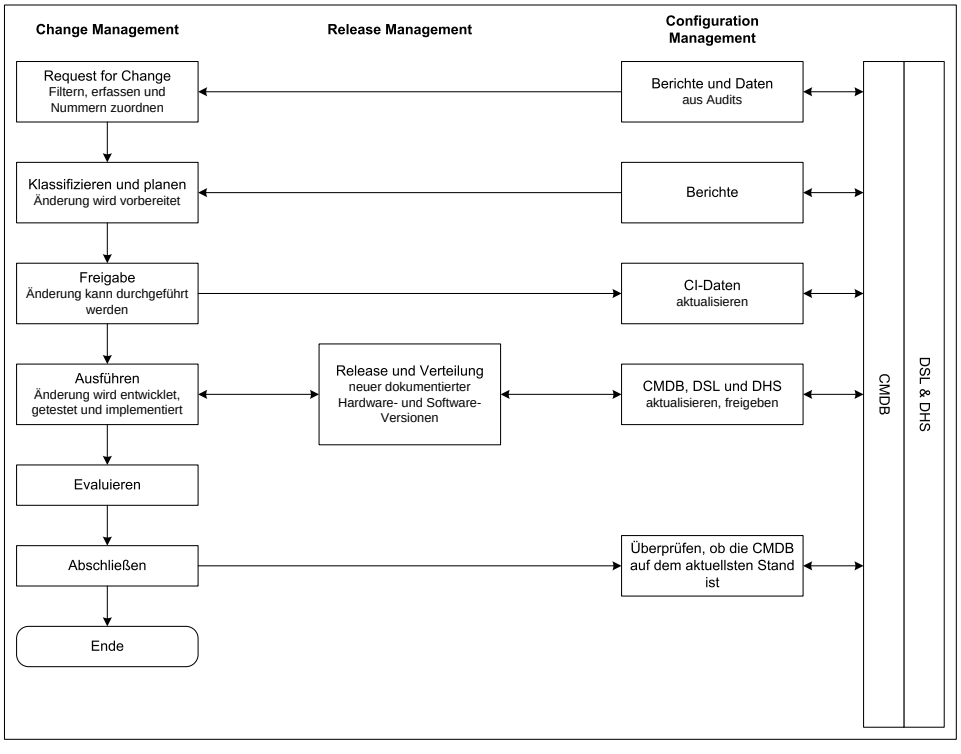


Abbildung 8.7: Schnittstellen des Configuration Management

Das Release Management stellt Informationen zur Planung von Releases und Versionen zur Verfügung. Dies bezieht sich beispielsweise auf die Termine für geplante Release-Umsetzungen, wie etwa Major Releases und Minor Releases. Nach der Durchführung einer Änderung gibt das Release Management eine Rückmeldung. Im Vorfeld fragt das Release Management Informationen über Software-CIs ab, um Daten zu Status, Standort, Quellcode und anderen Details zu erhalten, die in die eigenen Aktivitäten einfließen.

Das Service Level Management benötigt Informationen über die Eigenschaften der IT Services sowie über den Zusammenhang zwischen IT Services und der zu Grunde liegenden Infrastruktur (*siehe Abbildung 8.8*). Daten aus dem Service Level Management wie beispielsweise der Servicekatalog werden als CI in der CMDB abgelegt. So nutzt das Service Level Management die CMDB als Informationsquelle und Informationsablage.

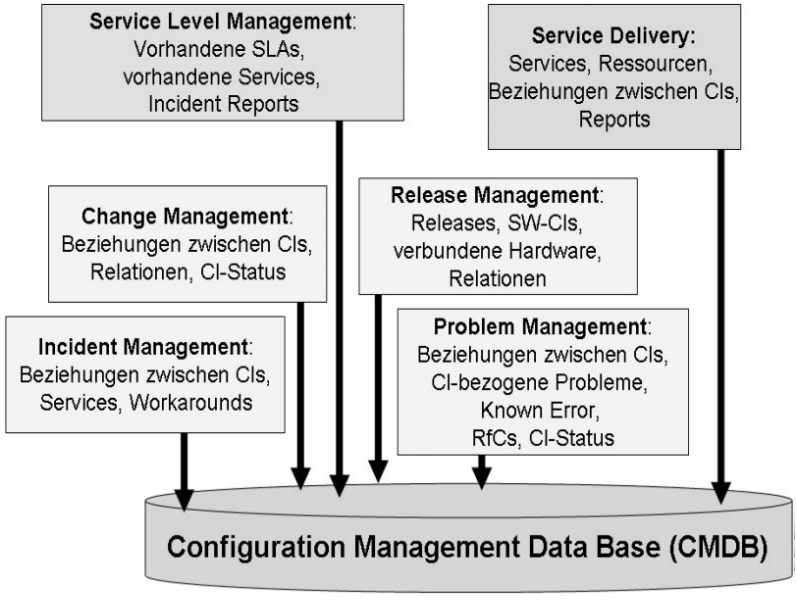


Abbildung 8.8: Informationsfluss zwischen den ITIL-Prozessen und der CMDB

Das Financial Management verwendet ebenfalls Informationen aus der CMDB, um diese als Input für den eigenen Prozess zu nutzen. Dies bezieht sich auf die Nutzung von IT Services, z.B. auf die Angabe, wer eine bestimmte Anwendung benutzt, wer welche Datenbanken bestellt hat, welche Mitarbeiter bestimmte Ressourcenkontingente überschreiten. Die Kosten können so pro Service bzw. Kunde ermittelt werden. So werden Serviceleistungen auf Kunden auf Basis von SLAs und Servicenutzung umgelegt. Zudem werden im Rahmen dieses Prozesses die Betriebsmittel und die Investitionen überwacht (Asset Management).

Das Availability Management soll die in den SLAs geforderte und vereinbarte Verfügbarkeit der Services sicherstellen, indem vorhersehbare Ausfälle reduziert bzw. vermieden werden. Dies bezieht sich auf die in der Infrastruktur verteilten CIs und ihre Beziehungen zueinander. So nutzt das Availability Management die CMDB als Basis für die Analyse und Messung der Verfügbarkeit zu definierender CIs. Dabei geht es auch um die Frage, welche CIs einen Beitrag zu bestimmten IT Services liefern. So werden Schwachstellen ermittelt und die Analyseergebnisse fließen in Verbesserungspläne ein (Component Failure Impact Analysis, CFIA).

Das Continuity Management für IT Services dient der Unterstützung des Business Continuity Managements (BCM), indem sichergestellt wird, dass die IT-Infrastruktur und -Dienste nach einer Katastrophe/Systemausfall innerhalb der vereinbarten Zeit kontrolliert wiederhergestellt werden können. Die Daten aus der CMDB dienen auch diesem Prozess als Informationsquelle. Darüber hinaus dienen die als Baselines in der CMDB abgelegten CI-Daten im Wiederherstellungsfall als definierte und bekannte Basis, auf die zurückgegriffen werden kann. So stehen ausreichend Quellen zur Verfügung, die aber vom Continuity Management laufend überwacht werden müssen. Ändern sich wichtige CIs oder deren Baselines, müssen auch die Pläne des Continuity Management angepasst und erneut getestet werden.

Das Capacity Management beschäftigt sich mit der Ermittlung der benötigten und kostenmäßig vertretbaren Kapazitäten der aktuellen und zukünftigen IT-Ressourcen, um SLAs zeitgerecht zu erfüllen. Dazu ist es zum einen notwendig, die geschäftlichen Anforderungen zu verstehen, um überhaupt zu wissen, welche Bedürfnisse bestehen und über die IT Services abgedeckt werden müssen. Zum anderen sind Kenntnisse über den IT-Betrieb und die Ressourcen notwendig, um zu wissen, welche Komponenten bereits vorhanden sind, in welchem Zustand sie sind und ob diese den Anforderungen genügen. Genau diese Informationen sind über die CIs in der CMDB abrufbar.

9 Change Management

Betriebsunterbrechungen und Serviceausfälle können Auswirkungen unterschiedlicher Reichweite mit sich bringen. Sie betreffen einzelne Anwender, Abteilungsteams oder die gesamte Belegschaft des Unternehmens. Wenn die Workstation eines Anwenders defekt ist und ausgetauscht werden muss, so ist zunächst einmal nur genau dieser Mitarbeiter für eine relativ kurze Zeit betroffen. Fällt ein Switch aus, so sind all jene betroffen, die über diese Netzwerk-Komponente angeschlossen sind. Wird ein neues Betriebssystem eingeführt bzw. auf den PCs installiert, so kann während dieser Zeit kein Mitarbeiter im Unternehmen die IT-Dienste in Anspruch nehmen. Finden Wartungs- und Servicearbeiten dann statt, wenn Mitarbeiter den Service normalerweise nutzen, ist dies Serviceausfällen gleichzusetzen. Damit kommt dem Zeitpunkt bzw. Zeitraum der Wartungsarbeit eine wichtige Rolle zu. Sollen die Anwender möglichst wenig von den angesetzten Wartungsarbeiten spüren, wird der zuständige IT-Manager anordnen, dass die Aktualisierung am Wochnende oder zu einem anderen günstigen Zeitpunkt stattfinden soll, um die Beeinträchtigungen für die Anwender zu minimieren (Wartungsfenster). Dagegen sollte der Tausch eines fehlerhaften PCs relativ schnell erfolgen können. Doch Wartungsarbeiten und andere Eingriffe in die bestehende IT-Infrastruktur finden nicht nur mit dem Ziel einer Problembeseitigung aus dem Incident Management oder Problem Management oder aufgrund von Installationen von Systemkomponenten statt. Auch als Folge von Veränderungen bei Geschäftsprozessen können Änderungen an den IT-Abläufen erforderlich werden. Dies sind dann Reaktionen auf neue Kundenanforderungen und Geschäftsabläufe. Auf Veränderungen in den Business-Rahmenbedingungen erfolgt eine Reaktion in der IT-Infrastruktur. Mögliche Gründe für Änderungen sind Reaktionen auf Kundenbeschwerden, Änderungen in den Geschäftsvorfällen der Kunden, eine veränderte oder neue Gesetzgebung oder die Einführung neuer Produkte bzw. Dienstleistungen.

Die Erfahrung zeigt: Changes führen häufig zu Problemen

In der IT gehören auch aufgrund der steigenden Business-Anforderungen und immer kürzeren Produktentwicklungszyklen Änderungen (Changes) zur Tagesordnung. Die Erfahrungen zeigen jedoch gleichzeitig, dass Störungen in der IT-Infrastruktur häufig auf Änderungen, die zuvor durchgeführt wurden, zurückzuführen sind. Die Ursachen sind mangelnde Sorgfalt, unzureichende Kommunikation und Dokumentation, zu knapp bemessene Ressourcen, unzureichende Vorbereitung oder mangelhafte Analyse der Auswirkungen und Finaltests in der Produktionsumgebung.

Kurz: Probleme verursachen oft Änderungen, Änderungen verursachen in vielen Fällen Probleme.

9.1 Change Management nach ITIL

Generell ist alles austauschbar, was sich in der IT-Landschaft befindet. Die Unterschiede für die Benutzer liegen in der Zeitdauer der Unterbrechung und im Umfang eines Austausches. Der Aufwand von Changes ist sehr unterschiedlich zu bewerten. Dasselbe gilt für Prioritäten und mögliche spätere Auswirkungen beziehungsweise Risiken.

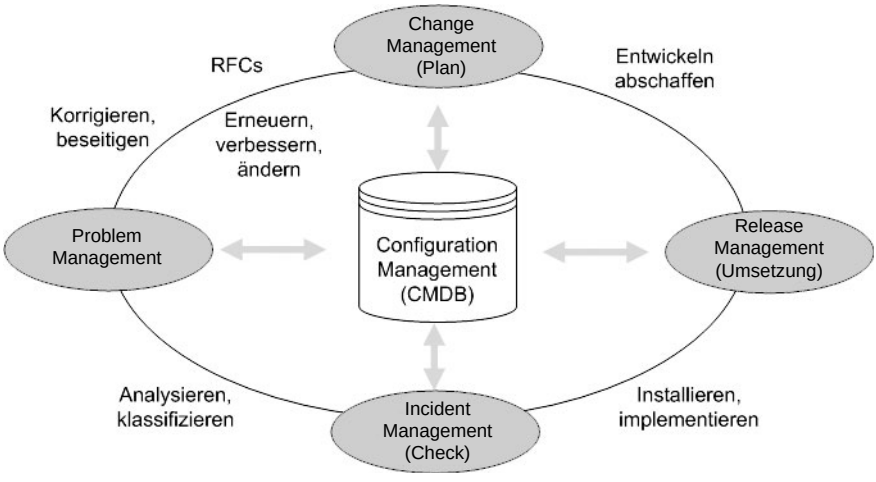


Abbildung 9.1: Dynamisches Change Management

Im Mittelpunkt des Change Management steht das Bestreben, die Anzahl der Änderungen und die durch Änderungen (Changes) verursachten Störungen auf ein Minimum zu reduzieren. Durch standardisierte Methoden und Prozeduren sollen Changes schnell und kontrolliert durchgeführt werden. Die Überwachung ist allerdings nicht technischer Natur, sondern bezieht sich auf den Prozessablauf.

Die große Zahl von Änderungen und die relativ weit reichenden Folgen, welche selbst einfache Eingriffe in die operationelle Infrastruktur haben können, rechtfertigt ihre systematische und kontrollierte Planung und Steuerung. Daher hat sich das Change Management zum Ziel gesetzt, eine effiziente und kostengünstige Implementierung autorisierter Changes mit minimalem Risiko für bestehende und neue IT-Infrastrukturen zu gewährleisten. Der Nutzen ergibt sich aus geringeren Auswirkungen auf die Qualität der Dienstleistungen und die abgeschlossenen SLAs, bessere Kostenschätzungen von geplanten Änderungen, weniger Backout-Fällen (Rollback) und wenn nötig einfacheren und sichereren Backout-Verfahren. Dies schafft bessere Entscheidungsgrundlagen für das Management und eine höhere Produktivität der Benutzer durch größere Verfügbarkeit sowie einen größeren Durchsatz in Bezug auf die Anzahl der Änderungen.

9.2 Begriffe des Change Management

Der Begriff „Change“ steht für das Hinzufügen, Ändern oder Entfernen eines CIs. Ein Incident ist kein Change und nicht jedes Problem führt zu einem Change. Ein Change wird über einen Request for Change (RfC) eingeleitet. Dieser stellt im Grunde genommen einen Antrag auf Durchführung einer Änderung an einem oder mehreren CIs dar. Er ist zentrales Instrument im Change Management. Er ist nicht gleichbedeutend mit einem Service Request, was eher dem Bedarf nach einer Passwort-Zurücksetzung oder dem Wunsch nach einer Änderung von Service-Zeiten gleichkommt.

Request for Change (RfC)

Ein RfC stellt den Antrag für bestimmte Veränderungen von CIs dar, der genehmigt werden muss. RfCs werden vornehmlich durch das Problem Management erstellt, in bestimmten Fällen auch durch das Incident Management oder den Kunden. Die nachfolgenden Genehmigungsverfahren sind je nach Fall unterschiedlich. Es gibt verschiedene Gründe, weshalb ein RfC beantragt werden kann. Unterschiedliche Konfigurations-Einheiten (CIs) können von solchen Änderungen betroffen sein wie etwa Hardware, Software, Telekommunikation, Technik oder Training/Ausbildung, Verfahren/Planung, SLA, Dokumentation.

Ein RfC sollte die folgenden Informationen enthalten:

- Objekt/betroffenes CI, Nummer und ggf. Verweis auf andere Records, Auswirkung, falls Change nicht durchgeführt wird (Benefit)
- Daten zum Antragsteller des Changes (Name, Organisationseinheit)
- Vorgeschlagenes Datum
- Priorität, Impact- und Ressourcenbewertung, Risikobewertung
- CAB-Empfehlung, Autorisierungsdaten (Person, die den Change bewilligt hat, Datum)
- Implementierungs- und Fallback-Plan
- Review-Infos

Alle RfCs müssen registriert und mit einer eindeutigen Change-Nummer versehen werden. Die Berechtigung für Erfassung, Genehmigung, Bearbeitung und Abschluss muss festgelegt werden. Die Verbindung zum Problem Management muss ohne großen Aufwand hergestellt werden können.

Die Verantwortlichkeit für die Durchführung von Änderungen liegt beim Change-Manager, der sämtliche Requests for Change (RfCs) oder Änderungsvorschläge filtert, akzeptiert und klassifiziert. In größeren IT-Organisationen wird er dabei zuweilen von Change-Koordinatoren unterstützt, die ihre Aufgaben als dezentrale Change-Manager innerhalb einzelner Gruppen der Organisation übernehmen. Der Change-Manager ist zudem verantwortlich für die Einholung der notwendigen Autorisierung, für die Planung, Koordinierung und Durchführung der Änderungen.

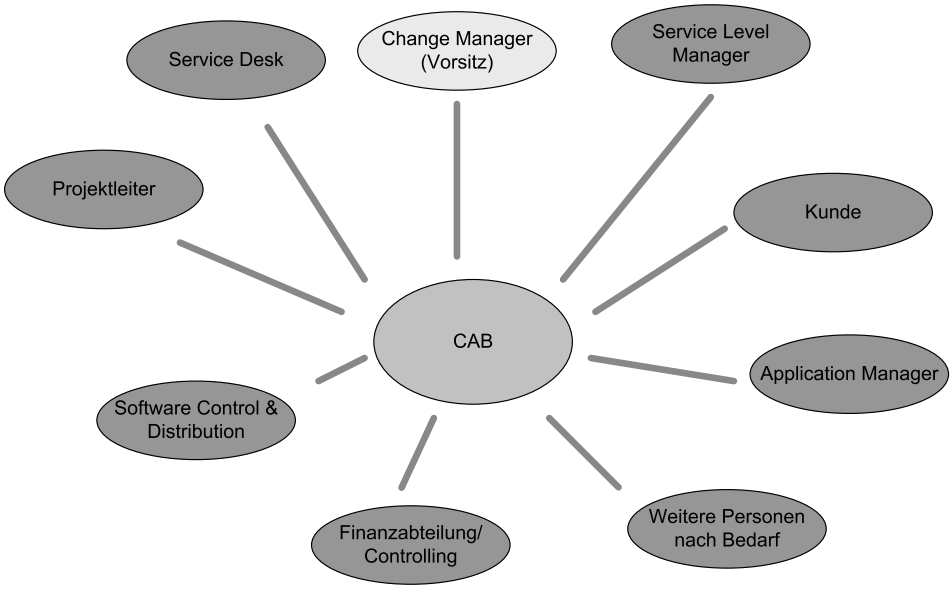


Abbildung 9.2: Change Advisory Board (CAB)

Das Change Advisory Board (CAB, Änderungs-Beirat) wird zu bestimmten Zeiten einberufen, um Änderungen zu beurteilen und zu autorisieren (*siehe Abbildung 9.2*). In der Regel wird dem CAB nur eine Auswahl (schwer wiegender) Änderungen vorgelegt, und es kann zu diesem Zweck unterschiedlich zusammengesetzt sein. Neben dem CAB gibt es für dringende Änderungen ein EC (Emergency Committee), um notwendige Entscheidungen zeitnah treffen zu können. Die typische Zusammensetzung eines CAB besteht z.B. aus Change-Manager (Vorsitzender), Service Level-Manager, Vertretern aus dem Incident Management, Problem Management und Release Management, Vertretern der Anwendungsentwicklung, betroffenen IT-Spezialisten, Bereichsmanagern und Managern der Finanzabteilung sowie Vertretern der betroffenen Kundenumgebung und Vertretern der Dienstleister. CAB und Change-Manager sollten mit einer Kriterienliste arbeiten, um zum einen zu entscheiden, wer bei welchen Change-Themen im CAB/EC vertreten sein sollte. Zum anderen dient die Liste dem CAB zur Bewertung eines Change.

Nach jedem größeren Change ist ein PIR (Post Implementation Review) durchzuführen. Hier sind die Ergebnisse der RfC-Implementierung enthalten. Die Frage ist dabei, ob die Ziele des RfC erreicht wurden und ob es ggf. Seiteneffekte gegeben hat. Primär geht es darum, ob der Change erfolgreich war und ob er zur Problemlösung oder der gewünschten Veränderung geführt hat. Der PIR wird in Abstimmung mit dem Problem Management durchgeführt.

Treten bei der Implementierung eines RfCs Probleme auf, sollte ein Backout- bzw. Rollback-Plan vorhanden sein. Dieser beschreibt, was im Fall des Misslingens passieren soll, um beispielsweise möglichst schnell wieder zum Ausgangspunkt zurückzugelangen. Ein solcher Plan sollte bereits beim Einstellen eines RfCs vorhanden und erfolgreich geprüft worden sein.

9.3 Aufgaben und Aktivitäten des Change Management

Das Change Management ist verantwortlich für unterschiedliche Aktivitäten in Bezug auf Veränderungen, Anpassungen und Verbesserungen der IT-Infrastruktur (*siehe Abbildung 9.3*). Die Mitarbeiter in diesem Bereich verwalten Changes an allen CIs der Produktivumgebung und den Change-Prozess an sich. Dies betrifft auch die täglichen Änderungen im IT-Geschäft. Changes müssen initiiert und dokumentiert werden. Dabei geht es auch darum, Auswirkungen, Kosten, Vorteile und Risiken von Changes einzuschätzen und zu bewerten. Dies geht mit der geschäftsbezogenen Begründung und der Genehmigung von Changes einher. Change-Implementierungen müssen überwacht und abschließende Berichte verfasst werden.

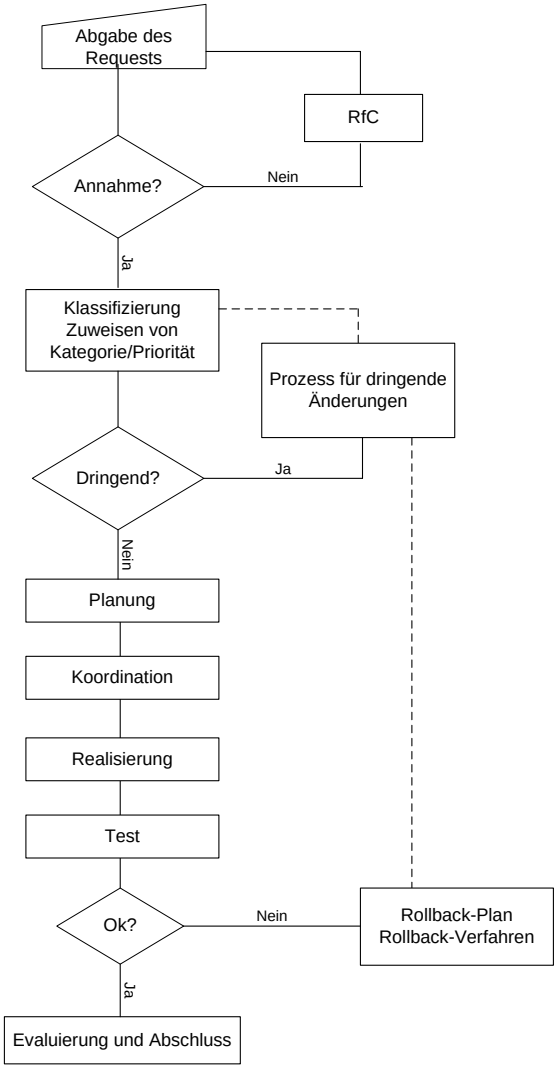


Abbildung 9.3:
Möglicher Change-Ablauf

Das Change Management ist allerdings nicht verantwortlich für Änderungen innerhalb von laufenden Projekten, wie etwa in der Anwendungsentwicklung. Hier sollte es aber eine adäquate Zusammenarbeit mit Abstimmung untereinander geben. Auch CI-Records müssen nicht vom Change Management aktualisiert werden, ebenso wie die Identifizierung von betroffenen CIs. Der Umfang des Change Management-Prozesses wird in Zusammenhang mit dem Configuration Management bestimmt. Das Configuration Management liefert Informationen zur Einschätzung der Auswirkungen von Änderungen und bringt nach Durchführung der Änderungen auch die Konfigurationsmanagement-Datenbank (CMDB) wieder auf den neuesten Stand. Wenn PC-Zubehör in der CMDB aufgeführt wird, so ist z.B. der Austausch einer Tastatur folglich eine Änderung. Auch Kunden und Anwender können Changes beantragen, die allerdings nicht direkt an das Change Management gerichtet, sondern über das Incident Management eingepflegt werden. Daneben können Changes auch aus Projekten stammen oder über Dienstleister kommen, die neue Versionen und Upgrades auf den Markt bringen, die eingespielt werden müssen (*siehe Abbildung 9.4*). Des Weiteren stellt je nach Umgebung auch die Gesetzgebung eine einflussreiche Größe dar, wenn an geschäftliche Aktivitäten neue gesetzliche Anforderungen gestellt werden.

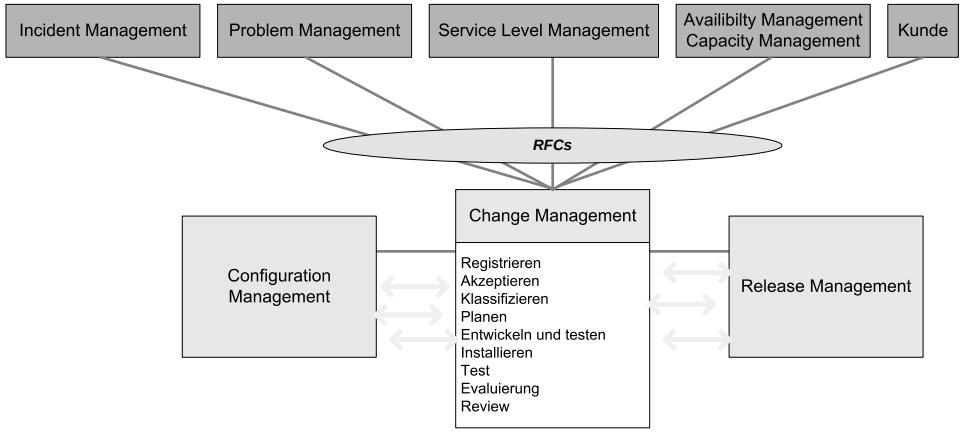


Abbildung 9.4: Requests for Change (RfC) können von jedem Prozess in ITIL und dem Kunden angestoßen werden, hauptsächlich aber über das Problem Management

Folgende Aktivitäten werden bei der Bearbeitung von Änderungen im Change Management-Prozess ausgeführt:

1. Einreichen und Erfassen/Registrieren: Alle RfCs müssen erfasst werden (Reporting). Wenn eine Änderung für die Lösung eines Problems beantragt wurde, sollte gleichzeitig eine Referenz zum bekannten Fehler hergestellt werden.

   Nicht jeder RfC wird innerhalb des Prozesses als Änderung behandelt. Einige routinemäßige Veränderungen, wie etwa Viren DAT-Updates, die klar umschrieben sind, werden standardisiert durchgeführt.

Die Erfassung von RfC macht gleichzeitig eine Organisation der Informationen notwendig. Diese dokumentierten Daten können aus Elementen bestehen wie etwa Identifikationsnummer, Auslöser/Problem mit eventuellem Verweis, Identifizierung der entsprechenden CIs und deren Beschreibung, Begründung für den Change und die benötigten Ressourcen, Datumsangaben, Auswirkungen auf das IT-System und betroffene IT-Abteilungen.

2. Filtern und Akzeptieren (formal): Nach der Erfassung erfolgt eine Prüfung durch das Change Management, die einer Filterung gleichkommt. Requests können im vereinbarten Dialog auch abgelehnt werden. Hier geht es um die generelle Frage, ob ein Change unlogisch, unnötig oder undurchführbar ist. Eine Änderung im System hat aber stets eine Anpassung der Beschreibung in Bezug auf die entsprechenden CIs in der CMDB zur Folge. Es geht auch um die Vollständigkeit der eingereichten Daten: Ist ein Rollback-Plan vorgesehen, sind alle Ansprechpartner und aktiven Mitarbeiter mit Kontaktdaten angegeben, sind alle notwendigen Informationen vorhanden?

   Wenn der RfC akzeptiert wurde, werden die Informationen für die Durchführung der Änderung in einen Change-Datensatz aufgenommen. Gleichartige RfCs sollten zusammengefasst werden, um den Aufwand zu reduzieren.

   Für die ersten Aktivitäten im Change Management existiert eine kleine Eselsbrücke: EVA – Erfassen, Vorab-Bewerten, Akzeptieren.

3. Klassifizieren: Die Einteilung der RfCs erfolgt nach Kategorie und Priorität. Dies beinhaltet das Zuweisen einer Priorität und das Einordnen in eine Kategorie. Die Priorität beschreibt die Wichtigkeit der Änderung und leitet sich von der Dringlichkeit und den Auswirkungen ab. Wenn es sich um die Korrektur eines bekannten Fehlers handelt, wurde die Priorität unter Umständen bereits vom Problem Management übergeben. Der endgültige Code wird jedoch innerhalb des Change Management unter Berücksichtigung der anderen in Bearbeitung befindlichen RfCs festgelegt.

Prioritätsabstufungen

Die Priorität gibt den Impact des Problems und die Dringlichkeit einer Abhilfe schaffenden Aktion wieder. Dies sollte auch im RfC festgehalten werden. Je nach Organisation und Selbstverständnis der Thematik können folgende Prioritätabstufungen existieren:

- Höchste Priorität (dringend): Ein RfC mit dieser Priorität bezieht sich z.B. auf ein Problem, das für den Kunden im Rahmen der Nutzung wichtiger IT-Services erhebliche Schwierigkeiten verursacht. Auch dringend benötigte Anpassungen der IT (z.B. eine Notlösung) werden mit dieser Priorität („Emergency Changes“) umgesetzt. An diesem Punkt werden unmittelbare Reaktionen gefordert, da ansonsten erhebliche Auswirkungen auf das Geschäft drohen. Dringliche Änderungsprozesse weichen von der normalen Vorgehensweise ab, weil in diesem Fall die benötigten Ressourcen sofort zur Verfügung gestellt werden müssen. Eine Dringlichkeitssitzung des CAB/EC oder des IT-Managements kann ebenfalls erforderlich sein. Alle früheren Planungen können Verzögerungen erfahren oder vorerst eingestellt werden.

(Fortsetzung)

- Hohe Priorität: Diese Priorität beschreibt z.B. eine Änderung aufgrund einer schwer wiegenden Störung oder hängt mit anderen dringenden Aktivitäten zusammen. Dieser Änderung wird heute noch oder bei der nächsten Sitzung des CAB oberste Priorität eingeräumt. Potenzieller Schaden ist möglich.
- Normale/mittlere Priorität: Die Änderung hat keine besondere Dringlichkeit oder größere Auswirkung, darf aber nicht auf einen späteren Zeitpunkt verschoben werden. Im CAB erhält diese Änderung bei der Zuteilung von Ressourcen mittlere Priorität. Ein Change mit dieser Priorität behebt lästige Fehler oder fehlende Funktionalität.
- Niedrige Priorität: Eine Änderung ist erwünscht, hat jedoch Zeit, bis sich eine geeignete Gelegenheit ergibt (z.B. eine Folgeversion oder eine geplante Wartung). In diesem Fall existiert keine vertragliche oder technische Notwendigkeit für einen Change.

Es ist möglich und wird in vielen Service Management-Tools praktiziert, die einzelnen Prioritätsstufen mit Nummern zu beschreiben, z.B. 1-2-3-4 oder 4-3-2-1.

Die Kategorie wird vom Change Management auf der Grundlage von Auswirkungen und benötigten Ressourcen in Bezug auf die gesamte IT-Umgebung bestimmt. Diese aus Priorität und Kategorie zusammengesetzte Klassifizierung legt die weitere Bearbeitung des RfC fest und beschreibt somit die Bedeutung der geplanten Änderung. Die einzelnen Kategorien werden vom Change Management zugewiesen; falls nötig in Absprache mit dem CAB, der eine Einschätzung der Auswirkungen der Änderung sowie der Belastung für die Organisation selbst liefert (*siehe Abbildung 9.5*).

- Standard-Change: Routine-Changes sind bereits vollständig beschriebene Änderungen, die zwar jedes Mal erfasst und dokumentiert, aber nicht jedes Mal vom Change Management beurteilt werden müssen. Diese Changes werden nicht dem CAB vorgestellt.
- Geringfügige Folgen: Eine Änderung, die wenig Aufwand erfordert. Der Change-Manager kann diese Art von Änderungen genehmigen, ohne dass er sie dem CAB vorlegen muss.
- Erhebliche Folgen: Änderungen, die einen erheblichen Aufwand erfordern und weit reichende Auswirkungen auf die IT Services zur Folge haben. Solche Änderungen werden im CAB besprochen, um den erforderlichen Aufwand zu definieren und das Risiko zu minimieren. Im Vorfeld und zur Vorbereitung der Sitzung wird zunächst die notwendige Dokumentation an die Mitglieder des CAB sowie gegebenenfalls auch an einige IT-Spezialisten und Entwickler verschickt.
- Weit reichende Folgen: Eine Änderung, für die ein großer Aufwand erforderlich ist. Für eine solche Änderung benötigt der Change-Manager zunächst die Autorisierung durch das IT-Management. Anschließend muss die Änderung dem CAB noch zur Beurteilung und weiteren Planung vorgelegt werden. Es geht um signifikante Auswirkungen auf die IT-Infrastruktur.

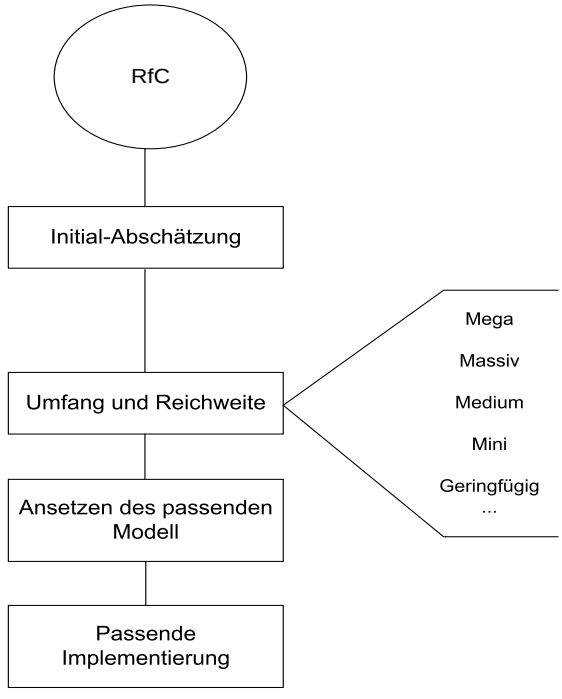


Abbildung 9.5: Change-Einordnung

4. Planen: Gemeinsame Planung anstehender Änderungen und deren Ausführung. Zudem muss die Verfügbarkeit der benötigten Ressourcen nach der Freigabe des Changes geklärt werden. Im Planungszeitraum anfallende Daten müssen in das Change-Dokument einfließen, um es aktuell zu halten. Vielfach ist von einem Change Planning Document (CPD) die Rede. Das Change Management plant alle Änderungen in einem Änderungskalender, dem so genannten Forward Schedule of Change (FSC). Der FSC ist ein Zeitplan für Installationen und Implementierungen. Er enthält Einzelheiten über alle genehmigten Änderungen und deren Planung.

Die Mitglieder des CAB sind bei der Planung größerer Änderungen involviert. Hier geht es um die Verfügbarkeit des Personals, die benötigten IT-Ressourcen, die entstehenden Kosten, die beeinflussten Service-Definitionen und Eigenschaften. Auch der Kunde und seine Planung müssen berücksichtigt werden. Das CAB tritt hierbei als Ratgeber auf. Letztendlich besitzt der Change-Manager eine delegierte Autorität und handelt im Namen des IT-Managements. Bei schwer wiegenden Änderungen kann es erforderlich sein, vor der Besprechung dieser Änderungen im CAB die Übertragung dieser Autorität durch das IT-Management explizit einzuholen. Die Genehmigung einer Änderung, das so genannte Change Approval, kann durch drei Grundprozesse unterstützt werden. Die finanzielle Genehmigung beruft sich auf eine Kosten-Nutzen-Analyse

und Finanzplanung, wobei die technische Genehmigung Auswirkungen, Erforderlichkeit und Realisierbarkeit einander gegenüberstellt. Bei der geschäftlichen Genehmigung erfolgt die Freigabe seitens des Kunden bezüglich Funktionalitätsbedarf und Auswirkungen.

Informationen hinsichtlich der Planung von Änderungen, zum Beispiel in Form eines Forward Schedule of Changes (FSC), sollten mit der erforderlichen Sorgfalt und Konsequenz betrieben werden.

5. Koordinieren: Die Erstellung, der Test und die Implementierung der Änderung werden vom Change Management koordiniert. Das Change Management überwacht, dass die Änderungen wie geplant durchgeführt werden. Es sollte ein klarer Kommunikationsplan vorliegen, in dem festgehalten wird, wer von der Implementierung der Änderung in Kenntnis gesetzt werden soll, z.B. Anwender, Service Desk, betroffene IT-Spezialisten, usw.
   - Nach der Detailklärung und den Vorbereitungen folgt der Test: Bevor die Änderungen realisiert werden können, müssen sie zunächst getestet werden. Im Rahmen der Erstellung, des Tests und der Implementierung kann das Release Management eine wichtige Rolle spielen. Nicht für alle Änderungen ist eine explizite Erstellungsphase notwendig. Aus diesem Grund können standardisierte Änderungen (z.B. der Standortwechsel eines PC) unmittelbar eingeplant und durchgeführt werden. Rollback-Verfahren (Backout) sollten als essenziell akzeptiert werden!

     Sowohl das Backout-Verfahren als auch die Einführungsmethode und das gewünschte Ergebnis der Änderung sollten gründlich überprüft werden. Hierbei sind die Kriterien zu beachten, die bereits vom CAB festgelegt wurden. In den meisten Fällen ist hierfür eine eigene Testumgebung notwendig. Um die erforderliche Objektivität bei der Durchführung der Tests sicherzustellen, empfiehlt es sich, notwendige Tests nicht von den im Rahmen der Erstellung eingesetzten Personen durchführen zu lassen, sondern zum Beispiel von einigen Anwendern oder Support-Mitarbeitern. Außerdem sind klar formulierte Qualitätsvorschriften für die Durchführung und Überwachung der Tests und für die Dokumentation der Testergebnisse erforderlich.
   - Implementieren/Durchführen: Der Change wird auf Basis der Change-Dokumentationen durchgeführt. Diese Aktivität kann als Kernstück im Change Management neben der Genehmigung durch das CAB angesehen werden. Die Implementierung sollte so geplant sein, dass sie den geringsten Einfluss auf die Anwender hat.
   - Evaluieren/Test: Das Change Management überprüft, ob die Änderung erfolgreich durchgeführt wurde, berichtet darüber (Reporting) und zieht Schlussfolgerungen für künftige Projekte (Lerneffekt). Durchgeführte Änderungen werden (eventuell mit Ausnahme von Standardänderungen) nach einer gewissen Zeit evaluiert. Danach wird gegebenenfalls in einer Sitzung des CAB das Ergebnis besprochen und entschieden, ob ein weiterer Review erforderlich ist.

6. Abschließen: Wurde die Änderung erfolgreich durchgeführt, kann der RfC bzw. der Change-Datensatz geschlossen werden. Die Ergebnisse werden in dem so genannten Post Implementation Review (PIR) festgehalten und dienen als Basis für ein entsprechendes Reporting (*siehe Abbildung 9.6*). Der PIR erfolgt prinzipiell direkt nach jedem Change und vor dem Schließen des Records. Ein solcher Change Record kann solange einen Pending-Status bekommen wie etwa „PIR pending".

   Neben dem PIR gibt es noch den Change Review. Je nach Art der Änderung kann ein Review bereits nach einigen Tagen stattfinden, andererseits kann es auch einige Monate dauern. Hier geht es auch um die Frage, ob der Zeit- und Kostenplan eingehalten wurde, der Implementierungsplan korrekt ist und ob der Ressourcenbedarf der Planung entsprochen hat.

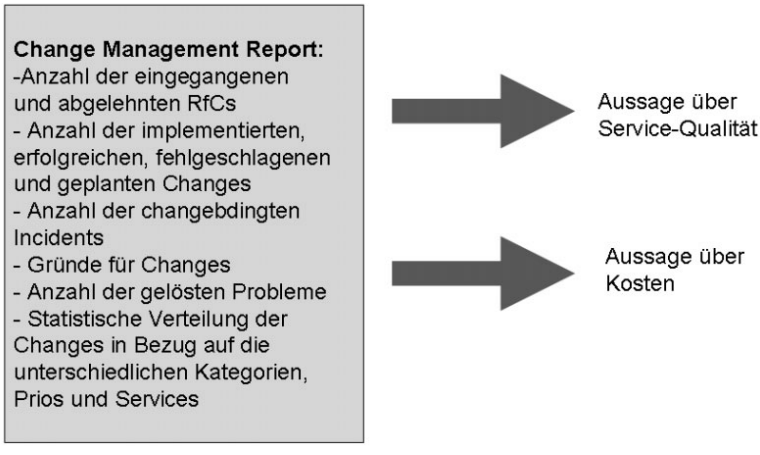


Abbildung 9.6: Change Management-Reports

9.4 Change Management im ITIL-Gesamtzusammenhang

Kein ITIL-Prozess steht isoliert und der Gesamtkontext des IT Service Management ist stets zu berücksichtigen. So existieren in Bezug auf das Change Management unterschiedliche Schnittstellen zu anderen ITIL-Prozessen, aus denen Informationen zum Change Management gelangen oder an die Informationen aus dem Change Management geleitet werden. Dies bezieht sich vor allem auf das Problem Management, Configuration Management und Release Management.

Aus dem Incident Management setzen Service Requests und Incidents den Prozess des Change Management in Gang. Beschwerden über langsame Netzwerkverbindungen können zu Veränderungen führen, wenn Nachforschungen ergeben, dass Antwortzeiten nicht den vereinbarten SLAs entsprechen. Ein Service Request in Bezug auf PC-Peripherie, wie der Austausch einer Hardwarekomponente (Maus, Tastatur, o.ä.), kann einem Standard-Request for Change gleichkommen, der direkt nach einem Genehmigungsverfahren den nachgelagerten Bestellvorgang auslöst, ohne dass das CAB bemüht wird. Es handelt sich um einen Standard-Prozess.

Das Incident Management und das Change Management besitzen aber noch in Bezug auf einen ganz anderen Aspekt Berührungspunkte: Bei der Durchführung von Änderungen können neue Störungen auftreten, die auf eine mangelhafte oder fehlerhafte Implementierung zurückzuführen sind. Auch ein unzureichender Informationsfluss im Vorfeld und während der Vorbereitung trägt nicht zur Kundenzufriedenheit bei. Es ist wichtig, dass die zuständigen Personen im Incident Management vom Implementierungszeitpunkt einer Änderung in Kenntnis gesetzt werden, um damit verbundene Störungen rasch aufspüren und beheben oder als Informationsvermittler bei Nachfragen von Anwenderseite fungieren zu können.

Das Problem Management eröffnet bei häufig auftretenden oder schwer wiegenden Störungen ein Problem, die Ursachen werden gesucht und es wird eine mögliche Lösung in Form eines RfCs an das Change Management weitergeleitet. Die beiden Prozesse arbeiten Hand in Hand. Vielfach werden aus dem Problem Management technisch qualifizierte Requests an das Change Management geleitet. Das Problem Management macht Vorschläge zur Problemlösung und gibt diese zur Annahme und Registrierung weiter. Nach Abschluss der Änderung wird das Problem Management informiert, um den PIR durchzuführen. Nach entsprechender Bestätigung wird das Problem geschlossen.

Das Change Management ist für die Autorisierung von Änderungen in der IT-Infrastruktur verantwortlich und das Configuration Management für die Überwachung des Status von Konfigurationselementen (Configuration Items, CIs). Das Configuration Management zeigt die Beziehungen zwischen den einzelnen CIs auf, so dass die von der Änderung betroffenen Bereiche erkannt werden. Die Erfassung bzw. Dokumentation von Änderungen und der damit verbundenen Informationen in der CMDB sind Aktivitäten, die einen Abgleich zwischen den beiden Prozessen fordern. Routinemäßige Änderungen, die eindeutig beschrieben sind und standardisiert durchgeführt werden können, müssen nicht der Kontrolle und Freigabe des Change Management-Systems unterliegen. Trotzdem hat jede Änderung in der IT-Infrastruktur Auswirkungen auf das entsprechende CI in der CMDB und umgekehrt. Daher stellt die CMDB (nicht nur) für das Change Management eine wichtige Ressource dar (*siehe Abbildung 9.7*). Prämisse ist allerdings eine aktuelle und gut gepflegte Datenbank.

> Die Schnittstellen zum Configuration Management müssen ermöglichen, dass einzelne Items in einem Change aufgenommen werden und ihre Abhängigkeiten kontrolliert werden können.

Das Release Management spielt für das Change Management die ausführende Rolle. Die Durchführung des Changes findet lediglich unter der Kontrolle des Change Management statt.

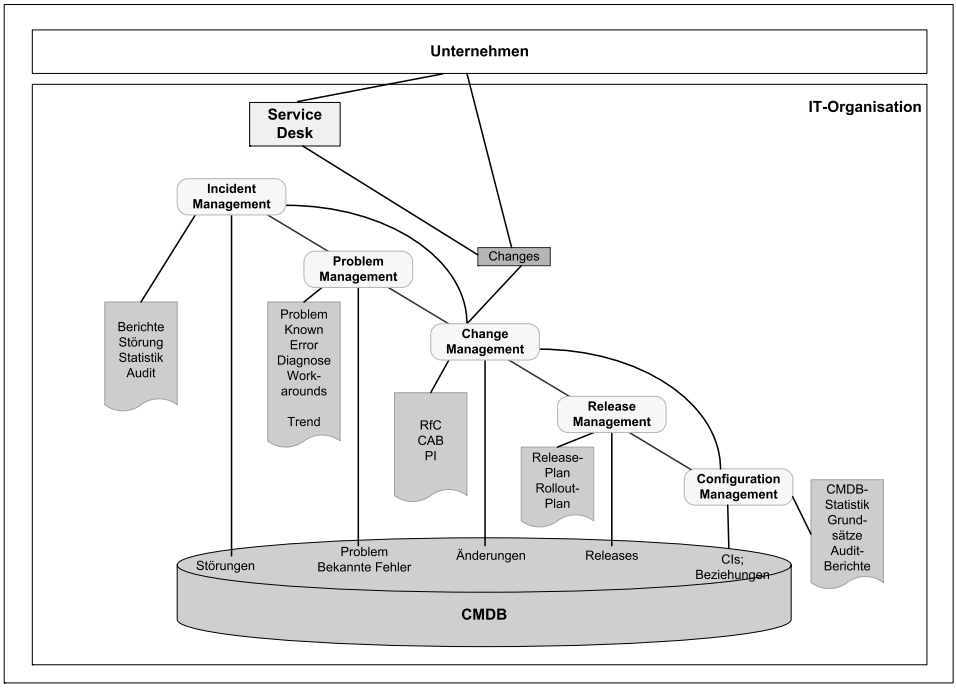


Abbildung 9.7: Change Management und das Zusammenspiel mit der CMDB im Service Support-Set

Die vorbeugenden Maßnahmen und Lösungspläne, welche die Kontinuität der IT Services gewährleisten sollen, müssen ständig überwacht werden. Änderungen in der IT-Infrastruktur können den Continuity-Plan unausführbar machen. Aus diesem Grund arbeitet das Change Management eng mit dem Continuity Management für die IT Services zusammen. So werden größere Änderungen mit dem Continuity Management abgestimmt. In Bezug auf den ITIL-Gesamtzusammenhang hat das Change Management Einfluss auf die Stabilität bzw. Wiederherstellbarkeit der IT-Komponenten und den damit zusammenhängenden IT Service.

In einem Service Level Agreement (SLA) werden alle Dienstleistungen, die als IT Service die Geschäftsbedürfnisse unterstützen sollen, festgeschrieben und mit den entsprechenden KPIs versehen. Bei Änderungen mit weit reichenden Auswirkungen oder hohem Risiko muss in jedem Fall die Umsetzung mit dem Kunden besprochen werden. Das stellt dem Service Level Management einen PSA- (Projected Service Availability-)Bericht zur Verfügung, der eine Übersicht über die Anpassungen für bereits vereinbarte SLAs enthält. Auch die Folgen der zeitlichen Planung für die Verfügbarkeit der IT Services, beschrieben im Forward Schedule of Changes (FSC), sind im PSA-Bericht enthalten.

Zwischen Availability Management und Change Management werden Anforderungen und Informationen in beide Richtungen ausgetauscht. Zum einen stößt das Availability Management Änderungen an, welche die Verfügbarkeit bestimmter IT Services bzw. die damit verbundenen Komponenten (CIs) verbessern sollen. Zum anderen gibt das Availability Management Informationen weiter, die bei der Einschätzung möglicher Auswirkungen von Änderungen helfen. Negative Auswirkungen auf die Verfügbarkeit sollen vermieden werden.

Das Change Management ist auch für Kapazitäts- und Ressourcenveränderungen verantwortlich. Das Capacity Management ist in der Lage, die Auswirkungen von Änderungen bei der Kapazitätsplanung an sich und bei Empfehlungen in Richtung Change Management zu berücksichtigen. So werden vom Capacity Management Anforderungen für Änderungen beantragt, die die Verfügbarkeit verbessern sollen. Die Koordination dieser Änderungen übernimmt das Change Management.

10 Release Management

Der Begriff Release wird im Allgemeinen für neue Versionen von Softwarepaketen benutzt. Betriebssysteme und Applikationssysteme sind bekannte Beispiele hierfür. Im Sinne von ITIL wird jede Art von Configuration Item als Release bezeichnet, welches ein vorhandenes älteres CI ersetzt oder ganz neu hinzukommt. Zu den Releases zählen also auch Hardwarekomponenten aller Art. Mehrere Changes werden zu einem Release zusammengefasst. Die Planung und Steuerung dieser Maßnahmen ist Aufgabe des Release Management.

Releases verändern die produktive IT-Infrastruktur. Die Produktionsumgebung ist derjenige Bereich der IT, in dem sich die Benutzer später bewegen. Sie stellt einen isolierten Bereich dar, welcher nicht ohne weiteres von jedermann verändert werden darf. Programme, Systeme und Geräte unterliegen hierbei einem spezifischen Schutzmechanismus. Es ist eine sehr wichtige Voraussetzung für ein unterbrechungsfreies Arbeiten, dass alle hierfür benutzten Komponenten einwandfrei funktionieren. Der Übergang vom Teststatus zum Produktionsstatus ist bei der Informationstechnologie eine regelmäßig wiederkehrende Funktion. Die Haupttätigkeiten bestehen aus der Implementierung, der Installation und der endgültigen Konfiguration im Sinne der Anwendungen.

Die Umsetzung des Release Management findet oftmals in Form von Projekten statt. Das Release Management nutzt so die Projektmanagement-Methodik, um Veränderungen im Bereich der IT Services zu implementieren. In einem ganzheitlichen Ansatz werden dabei technische und nicht-technische Aspekte der Veränderungen im Projektplan berücksichtigt.

10.1 Release Management nach ITIL

Das Release Management besitzt einen ganzheitlichen Blick auf Änderungen der IT Services und stellt sicher, dass alle Aspekte eines Release (technische und nichttechnische) gemeinsam betrachtet werden. Es hat den Schutz der Produktionsumgebung und die Gewährleistung der Servicequalität durch formelle Verfahren und Kontrollen bei der Implementierung neuer Versionen als Ziel. Im Gegensatz zum Change Management, das auf Kontrolle ausgerichtet ist, konzentriert sich das Release Management auf die Durchführung (*siehe Abbildung 10.1*).

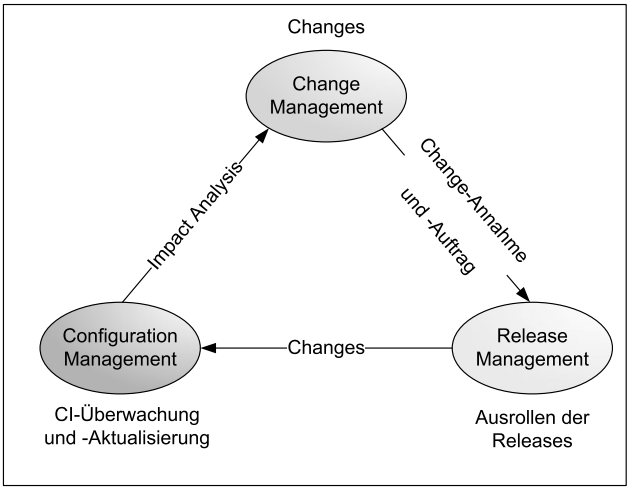


Abbildung 10.1: Release Management

Das Release Management arbeitet eng mit dem Configuration Management und dem Change Management zusammen, um sicherzustellen, die gemeinsame CMDB mit den aktuellen Daten zu versorgen. Der Schwerpunkt beim Release Management liegt auf der Durchführung der geplanten Änderung. Darüber hinaus sorgt das Release Management dafür, dass der Inhalt der Releases in einem Repository, der so genannten DSL (Definitive Software Library, maßgebliche Software-Bibliothek), festgehalten wird. Im DHS (Definitive Hardware Store, maßgebliches Hardware-Lager) werden Hardware-Ersatzteile, insbesondere von standardisierten Grundkonfigurationen, aufbewahrt. Beim Release Management kommen so unterschiedliche Datenspeicher zur Ablage von Informationen, Release-Versionen in Form von Master-Kopien oder Hardwarekomponenten zur Anwendung. Es sollen keine unzulässigen Releases in die Produktiv-Umgebung gelangen. So wird durch eine stabilere Umgebung die Servicequalität und die Kundenzufriedenheit erhöht. In der CMDB werden auch Hardware-Spezifikationen, Installationsanweisungen und Netzwerkkonfigurationen erfasst.

10.2 Begriffe des Release Management

Das Release Management stellt quasi den operativen Teil des Change Management dar. Die Gesamtkontrolle liegt jedoch beim Change Management.

Ein Release beschreibt eine oder mehrere autorisierte Änderungen an einem IT Service oder an Teilen der IT-Infrastruktur. Dieser Begriff bezeichnet darüber hinaus eine Sammlung von neuen/geänderten CIs, die getestet und zusammengeführt in die Produktivumgebung eingeführt werden. Ein Release ist definiert durch die RfCs, die es implementiert. Häufig werden Releases unterteilt in:

- Major Releases: Sie haben Rollout-Character. Sie bezeichnen wichtige Rollouts mit einer zumeist erheblichen Erweiterung der Funktionalität oder beheben eine Reihe von bekannten Fehlern.

- Minor Releases: Sie stellen für die Infrastruktur nur geringfügige Veränderungen dar. Sie enthalten meistens Verbesserungen wie z.B. FixPacks für bekannte Fehler. In manchen Fällen sind sie eher als Notreparaturmaßnahmen anzusehen, die jedoch integral innerhalb eines Release behandelt werden.
- Emergency Fixes: in der Regel als vorübergehende Sofortbehebung für ein Problem oder einen bekannten Fehler gedacht. Der Zeitdruck ist hier ein entscheidender Faktor.

Beispiele für Release-Typen

- Emergency Release: Ein Programmfehler wurde entdeckt und muss umgehend beseitigt werden, da ansonsten die Abläufe und Services behindert werden.
- Major Release: Ein neues Applikationssystem, zum Beispiel eine eBusiness-Anwendung, wird eingeführt. Hier sind Aktionen notwendig, welche sich auf das Gesamtunternehmen auswirken.
- Minor Release: Bei einem einzelnen Anwender muss eine Festplatte ersetzt werden.

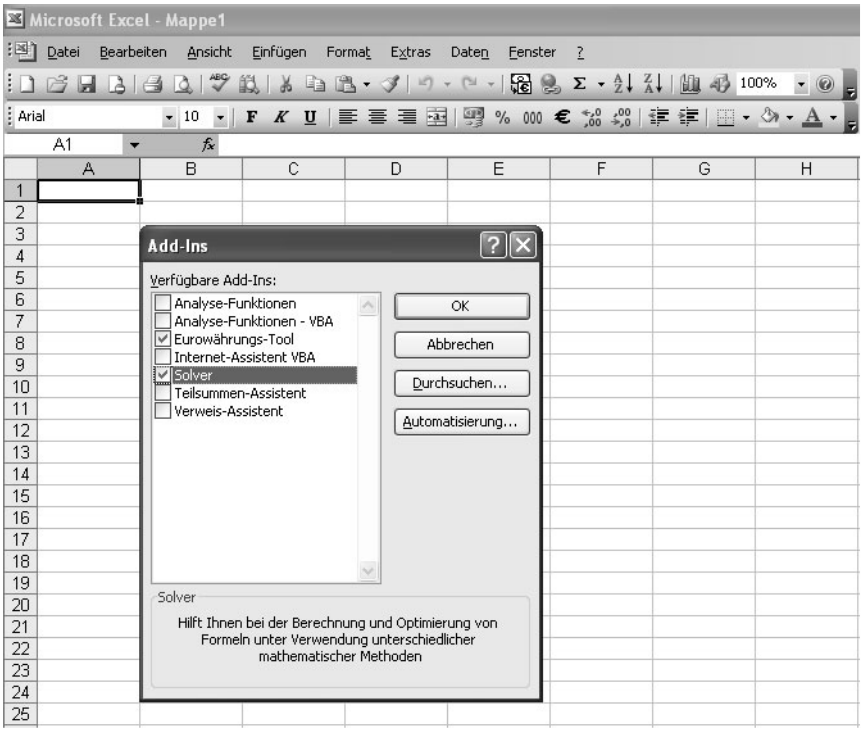


Abbildung 10.2: Add-Ins als Module innerhalb der Anwendung Excel

Neben der Klassifizierung der Releases nach Auswirkungen existiert der Begriff der Release-Einheiten (Release Units). Eine Release-Einheit beschreibt den Anteil an der IT-Infrastruktur, der normalerweise zusammenhängend getestet, freigegeben und ausgerollt wird. Release-Einheiten müssen eindeutig gekennzeichnet sein. Dabei ist zu berücksichtigen, dass Kopien von Software-Produkten über die DSL für unterschiedliche Umgebungen verfügbar gemacht werden können. Dies bezieht sich für Software-Releases auf Bereiche wie eine Suite (Microsoft Office), eine Applikation (Excel oder Access) oder ein Modul (ein Add-In wie Solver unter Excel, *siehe Abbildung 10.2*).

Releases werden in unterschiedlichen Umgebungen verwendet:

- Entwicklungsumgebung: Neue Releases werden in der Regel auf der Basis einer anderen Release-Version erstellt. Das neue Release wird dann zur Kennzeichnung mit der Folgenummer versehen. Die Software darf nur in der Entwicklungsumgebung geändert werden.
- Testumgebung: In einer Testumgebung können die neuen Versionen getestet werden. Hierbei wird oftmals zwischen technischen Tests (durch die Entwickler), funktionalen Tests (durch die Anwender), Implementierungstests durch die Release-„Architekten" und eventuell einem abschließenden Abnahme-Test durch die Anwender und die Dienstleister-Organisation unterschieden.
- Produktionsumgebung: Dies bezeichnet die aktuelle Umgebung, über die den Anwendern Informationssysteme zur Verfügung gestellt werden.
- Archiv: Hier befinden sich nicht mehr aktuelle Originalversionen von Software-Produkten, die in der jeweiligen Version abgelegt werden.

Vokabeln

- Release: Einer oder mehrere autorisierte Changes, beschrieben durch einen RfC
- Release-Grundsätze: Dokument, in dem Rollen und Zuständigkeiten des Release Management beschrieben werden. Hier sind die Angaben zu Release-Einheiten, -Nummerierungsvorgaben und Release-Typen zu finden.
- DSL: Definitive Software Library, in der alle qualitätskontrollierten und freigegebenen Software-CIs gespeichert sind (Master-Kopien)
- DHL/DHS: Definitive Hardware Store: Ersatzkomponenten für entsprechende Hardware-Komponenten der Produktivumgebung, detailliert in der CMDB beschrieben
- Release-Merkmale
  - Umfang des Release, z.B. Full, Delta, Package (Art)
  - Umfang der Freigabe, z.B. Software: Suite, Applikation, Modul (Unit)

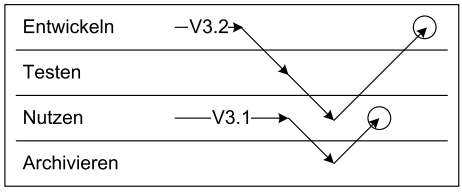


Abbildung 10.3:
Management einer Anwendung mit Rollback

Da durchaus mehrere Releases gleichzeitig möglich sind, erhält jedes Release eine eigene Identifikationsnummer, die auf das betroffene CI verweist und außerdem eine aus einer oder mehreren Ziffern bestehende Versionsnummer enthält (*siehe Abbildung 10.3*):

- Major Releases: Anwendungsname V.1, V.2, V.3 usw.
- Minor Releases: Anwendungsname V.1.1, V.1.2, V.1.3 usw.
- Emergency Fix: Anwendungsname V.1.1.1, V.1.1.2, V.1.1.3 usw.

Emergency Fixes (Bug Fixes) werden häufig auch durch einen angehängten Kleinbuchstaben gekennzeichnet. Selbstverständlich gehören entsprechende Test- und Freigabeverfahren dazu bzw. die jeweils notwendigen Anpassungen oder Rollbacks (Backouts) und die Archivierung.

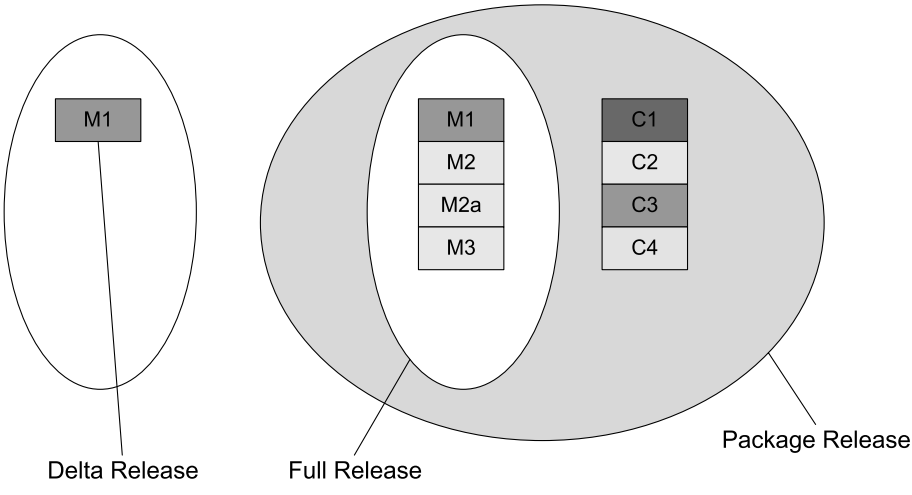


Abbildung 10.4: Unterscheidung der Release-Arten

Das Change Management muss entscheiden, wie viele Changes in ein Release aufgenommen werden können und auf welche Weise das Roll-Out stattfinden soll. Das Ergebnis wird in Release-Arten festgehalten (*siehe Abbildung 10.4*). In diesem Zusammenhang hat das Change Management die Wahl unter den folgenden Release-Arten:

- Full Release: Alle Komponenten der Release-Einheit werden zusammen entwickelt, getestet, verteilt und implementiert.

- Delta Release: Ein Delta Release enthält nur die geänderte Soft- oder Hardware.
- Package Release: Bei Package Releases (gebündelte Releases) handelt es sich um einzelne, voneinander unabhängige Releases.

Die DSL bezeichnet einen Speicherort, an dem alle autorisierten Software-Versionen in Form von Master-Kopien sicher aufbewahrt werden. Von hier aus findet auch die Verteilung aller eingesetzten Software-CIs statt. Hier liegen sowohl die Originalversionen gekaufter Software (inklusive der Lizenzdokumentation) als auch selbst entwickelte Software. Die DSL kann unterschiedliche Versionen derselben Software einschließlich der archivierten Versionen, der Dokumentation und der Quellcodes enthalten. Diese Objekte sollten regelmäßig gesichert werden, da sie neben aktuellen Versionen auch Backout-Versionen enthält. Das Release Management kontrolliert den Lebenszyklus eingesetzter Software, sobald sie in die DSL aufgenommen ist. Das Datenmodell und die Konfiguration der DSL sollten vor dem Einsatzbeginn definiert und dokumentiert werden. Hier liegen in den meisten Fällen nur die Master-Kopien aus der Produktivumgebung, seien es aktuelle oder alte Versionen. Die Libraries der Test- und Entwicklungsumgebung sollten nicht hier abgelegt werden.

Analog zur DSL sollte es einen Bereich geben, um die sichere Speicherung bzw. Lagerung von definitiver Ersatzhardware umzusetzen. Ersatzteile und Hardware-Komponenten werden deshalb im maßgeblichen Hardware-Lager (Definitive Hardware Store, DHS) aufbewahrt. Hierbei handelt es sich um Basiskonfigurationen, die zum Austausch oder zur Reparatur von ähnlichen Konfigurationen in der IT-Infrastruktur dienen. Sie sollten auf demselben Level gewartet werden wie die Hardware der Produktivumgebung. Die Daten über die Zusammensetzung dieser Konfigurationen müssen in die CMDB aufgenommen werden, um die Daten im Bedarfsfall abrufen und die Hardware aus dem DHS verwenden zu können. Auch aufgrund von Compliance-Anforderungem können die Inhalte der DHS bereitgestellt werden. Daten, die zum Teil sechs oder zehn Jahre aus Anwendungsbeständen vorgehalten werden müssen (HGB), finden in der DHS die notwendige Hardware vor, um bei Bedarf über die alten Anwendungen auf die entsprechenden Daten zugreifen zu können. Der DHS kann auch einfach nur als ein allgemeines Ersatzteillager fungieren.

Das Release Management muss die Informationen über die CIs, die in der Konfigurations-Datenbank (CMDB) gespeichert sind, laufend aktualisieren. Mit den Software-Anpassungen in der DSL werden auch die Einträge in der CMDB ergänzt.

10.3 Aufgaben und Aktivitäten des Release Managements

Die IT-Organisation sollte die Planung und den Rollout neuer Release-Versionen kontrolliert durchführen. Andernfalls wird die Organisation häufiger mit Problemen konfrontiert, die auf mangelnde Sorgfalt bei der Durchführung von Releases zurückzuführen sind. Die Kunden sollten die Geduld für eine planmäßige Vorgehensweise aufbringen: Werden Releases unter Zeitdruck durchgeführt, sind unerwünschte Auswirkungen auf das Geschäft die Folge. Das Release Management ist

dementsprechend zuständig für die Kontrolle und die Verteilung von produktiv zu nutzender Software und Hardware. Alle Aktivitäten stehen in Bezug zur CMDB und zur DSL bzw. zum DHS (*siehe Abbildung 10.5*).

1. Release-Grundsätze festlegen: Der Release-Manager erstellt im Vorfeld Release-Grundsätze. In ihnen ist definiert, wie und wann Releases zusammengesetzt und zur Verfügung gestellt werden. Er legt auch die Release-Einheiten fest, die beschreiben, auf welchem Detaillierungsgrad CIs unabhängig voneinander verteilt bzw. eingeführt werden können. Diese Festlegung ist von den möglichen Auswirkungen des Release auf andere Komponenten abhängig. Es muss festgestellt werden, wie hoch der Personal- und Zeitaufwand mehrerer Änderungen im Vergleich zur Durchführung einer individuellen Änderung ist. Auch der Schwierigkeitsgrad einer eventuellen Installation bei den Anwendern spielt eine Rolle.

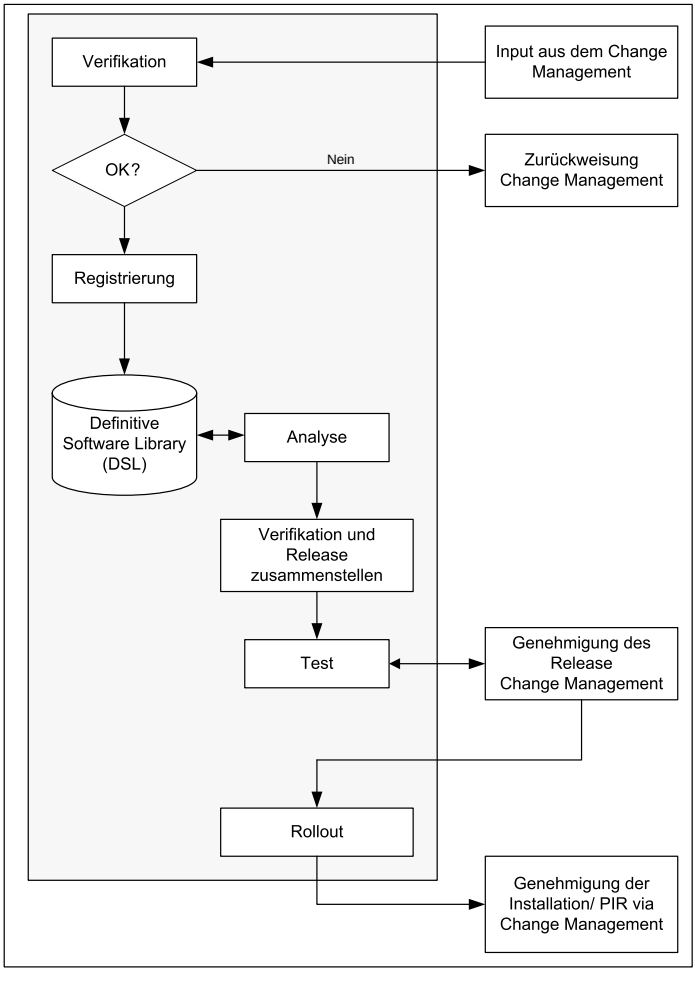


Abbildung 10.5: Prozesse im Release Management

2. Releases planen: Für die Planung eines Release werden Informationen über den Lebenszyklus des Produkts, der zu übergebenden Produkte, eine Beschreibung des jeweiligen IT Services und der Service Levels, Autorisierungen für die betreffenden RfCs usw. benötigt. Der so entstandene Plan enthält Informationen für das Release, Testpläne und die notwendigen Abnahmekriterien.
3. Release-Zusammenstellung und –Konfiguration: Ein Release kann aus einer Reihe von Komponenten (CIs) bestehen, die intern entwickelt und/oder zugekauft worden sind. Installationsverfahren oder Konfigurationsanweisungen sollten ebenfalls als Teil des Release behandelt und als CI vom Change und vom Configuration Management kontrolliert werden. Vor der Verteilung und Produktivschaltung sollte die gesamte Hard- und Software in einer Labor- oder Testumgebung zusammengestellt und getestet werden (*siehe Abbildung 10.6*). Alle Hard- und Software-Komponenten des Release sollten so zusammengestellt sein, dass eine Reproduktion möglich ist. Die Dokumentation aller Verfahren ist überaus wichtig. Ohne diese Informationen kann nicht sichergestellt werden, dass ein Release immer gleich zusammengesetzt wird. In Software-Entwicklungsumgebungen bezeichnet man diese Aktivität als Build Management (Stichwort: Server Build).

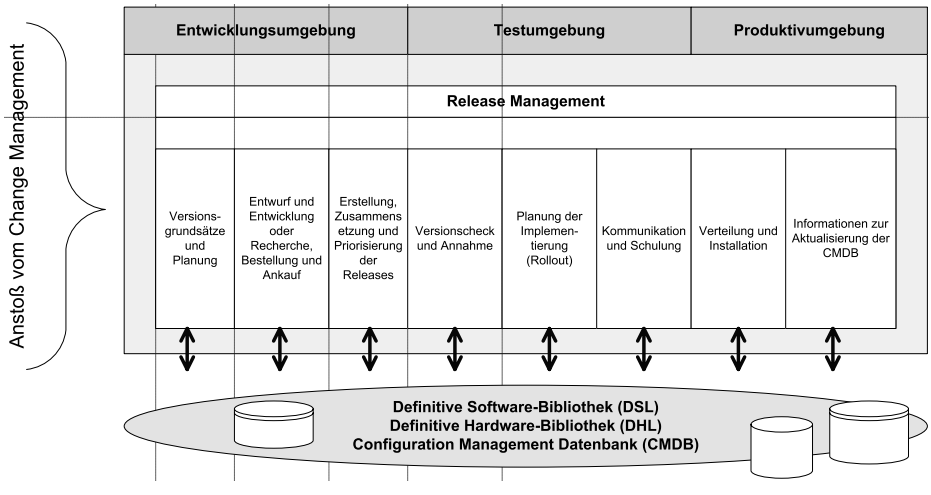


Abbildung 10.6: Aktivitäten und Zusammenhänge

4. Release-Test: Die häufigste Ursache für nicht zufrieden stellende oder nicht erfolgreiche Änderungen sind unzureichende Tests. Um dem entgegenzuwirken, sollte ein Release sowohl funktionale Tests durch Anwender als auch operationale Tests durch Betriebspersonal durchlaufen. Dabei sollten Funktionalitäten, technische und Betriebsaspekte, Leistungsverhalten sowie die Integration in die restliche Infrastruktur berücksichtigt werden. Fallback-Pläne sind zu erstellen und zusammen mit dem Release zu testen. Für das gesamte Release regelt ein Backout-Plan die Maßnahmen zur Wiederherstellung, falls es nicht erfolgreich eingeführt werden konnte. Das Change Management muss sicherstellen, dass ein solcher Plan existiert. Der letzte Schritt ist die Freigabe des Release zur Im-

plementierung. Das Change Management muss für die formale Abnahme durch Anwender und Entwickler Sorge tragen. Die betreffenden Basiskonfigurationen sollten in der CMDB registriert sein. Wird das Release nicht akzeptiert, so wird auf das Change Management zurückverwiesen.

5. Kommunikation und Vorbereitung: Alle betroffenen Mitarbeiter und Prozesse müssen über Pläne und ihre Auswirkungen auf den täglichen Arbeitsablauf informiert werden. Dies kann durch gemeinsame Schulungsmaßnahmen, enge Kooperation oder gemeinsame Release-Abnahmen geschehen. Verantwortlichkeiten sollten kommuniziert und deren Kenntnis in anderen Abteilungen überprüft werden. Falls das Release in Phasen ausgerollt wird, sollten die Anwender über die verschiedenen Phasen und die jeweiligen Inhalte in Kenntnis gesetzt werden. Änderungen an SLAs, internen Vereinbarungen und Absicherungsverträgen sollten im Voraus allen Beteiligten mitgeteilt werden.
6. Verteilung und Installation: Für Software-Verteilung und -Installation sollten, wo möglich, automatisierte Werkzeuge eingesetzt werden. Dies spart Zeit und Ressourcen und erhöht die Qualität. Oftmals kann hierüber auch Erfolg/Misserfolg der Installation verifiziert werden. Des Weiteren empfiehlt es sich, vor der eigentlichen Installation zu überprüfen, ob die Umgebung den Anforderungen des Release z.B. hinsichtlich des Speicherplatzes entspricht.
7. Nach der Installation sollten die Informationen in der CMDB auf den neuesten Stand gebracht bzw. abgestimmt werden, damit auch eventuelle Lizenzvereinbarungen kontrolliert werden können.

10.4 Release Management im ITIL-Gesamtzusammenhang

Das Release Management steht vor allem mit zwei weiteren ITIL-Prozessen in Interaktion: Change Management und Configuration Management. Hierbei ist zu betonen, dass das Release Management ebenso wie das Problem Management als operativer Prozesstyp einzuordnen ist. Das Change Management hat im Vergleich zum Release Management eher Kontroll-Charakter. Das Configuration Management befasst sich in Bezug auf das Release Management vorwiegend mit Kontrolle und Administration.

Release-Manager: Ein Hut im Release Management

Wie bei jedem Prozess sollte auch für das Release Management ein Prozessverantwortlicher benannt werden. Dieser Release-Manager ist für die Einführung, die Einhaltung und die Weiterentwicklung des Release Management-Prozesses verantwortlich. Er unterhält enge Beziehungen zum Configuration-Manager, zum Change-Manager sowie zur Entwicklungs- und Testorganisation. Er gehört in der Regel auch dem Change Advisory Board (CAB) an.

Das Change Management behält stets die Kontrolle über einen durchzuführenden Change. Es übergibt dem Release Management innerhalb seines Prozesses den Auftrag zur Release-Erstellung, um den Change umzusetzen (siehe *Abbildung 10.7*). Auch der Release-Test und die -Abnahme gehören dazu. Das Change Management fragt auch ab, ob das Release ausreichend getestet wurde. Es findet ständige Interaktion zwischen diesen beiden Prozessen statt. Das Release Management überblickt die Details der Change-Implementierung. Das Change Management beschreibt die Verfahren, die sicherstellen sollen, dass die Änderungen autorisiert sind. In Bezug auf den Inhalt und die Zusammensetzung des Release geht es allerdings nicht um technische Feinheiten, sondern um die mögliche Auswirkung. Die Zeitplanung eines Release wird im FSC (Forward Schedule Calendar) des Change Management eingetragen.

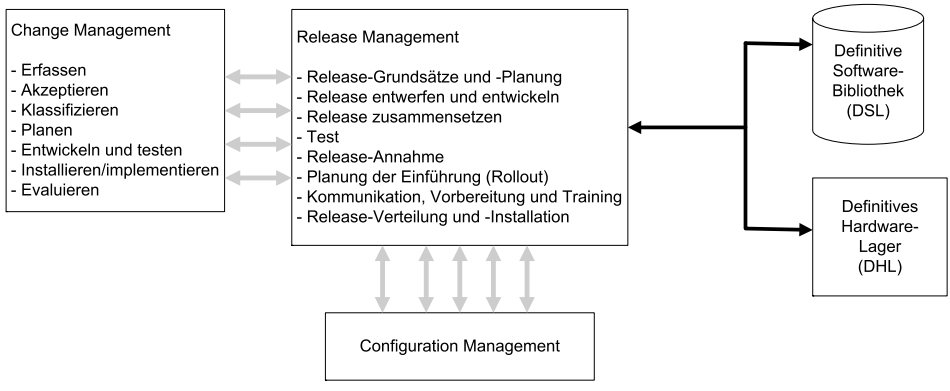


Abbildung 10.7: Schnittstellen des Release Management

Das Configuration Management kümmert sich um die Bereitstellung von Informationen über die IT-Infrastruktur für andere Prozesse, in diesem Fall in Interaktion mit dem Release Management. Es geht dabei um die Kontrolle der IT-Infrastruktur durch Überwachung und die Pflege von Informationen. Neben der CMDB sind auch DSL und DHS daran beteiligt. Alle relevanten Informationen sollten in der notwendigen Detaillierung durch das Configuration Management in der CMDB aktualisiert werden. Die CMDB spiegelt zu jedem Zeitpunkt den aktuellen Status aller autorisierten Hard- und Software wider. So kann sichergestellt werden, dass ein Release nur korrekte Komponenten beinhaltet.

Auch das Problem Management und das Service Desk sollten mit dem Release Management in Kontakt stehen. Dies ist zum einen dann wichtig, wenn die Verteilung erfolgreich abgeschlossen wurde, um eventuelle weitere Kommunikationsschritte aufzunehmen. Zum anderen ist das Service Desk als Kontaktstelle bei auftretenden Problemen in der Produktivumgebung informiert. So kann im Bedarfsfall ein erneuter Kontakt zum Release Management hergestellt werden. Zudem können mit dem erfolgreichen Rollout verbundene Incidents oder Probleme als gelöst betrachtet und entsprechend nachbearbeitet werden.

11 Beispielfragen zum Bereich Service Support

Die Service Support-Prozesse betreffen den Umgang mit dem Anwender/Kunden und die Maßnahmen, mit denen dieser Umgang so gut wie irgend möglich gestaltet wird. Sie stellen sicher, dass alle Fragen, Beschwerden, Anforderungen und Service-Nachfragen optimal bearbeitet werden.

Zu diesem Bereich gehören die Funktion Service Desk als Teil des Incident Managements sowie die folgenden Prozesse:

- Incident Management
- Problem Management
- Change Management
- Release Management
- Configuration Management

Die nachfolgenden Fragen beziehen sich auf den Service Support Set. Wichtig ist für Sie vor allem die Kenntnis über die genaue Aktivitätenabfolge innerhalb der Prozesse. Machen Sie sich klar, welches Ziel welcher Prozess hat und wo welche Verantwortlichkeiten liegen. Noch einmal zusammengefasst für diesen Bereich von ITIL:

- Service Desk: Ansprechpartner, Erfassung, Bearbeitung, Überwachung von Störungen, Unterstützung weiterer Prozesse, Funktion
- Incident Management: Störungen beheben, IT-Service schnellstmöglich wiederherstellen, Störungen werden hier erfasst, angenommen, kategorisiert
- Problem Management: Ursachenforschung zu Problemen, Ursache bekannt: Behebung oder Veränderung (RfC)?
- Configuration Management: Kontrolle der Infrastruktur (Statusüberwachung), Identifizierung von CIs, Dokumentation, Bereitstellung von Informationen
- Change Management: Kontrollierte Durchführung von Änderungen, Reduzierung möglicher negativer Folgen, Beantragungsgenehmigung und Zustimmen der Umsetzung
- Release Management: Nur richtige Versionen in Umlauf gebracht, erfolgreicher Rollout (Durchführung) steht im Vordergrund, „Labor“

IT Service Management nach ITIL besteht aus zwei Prozessgruppen:

- Service Support umfasst die Prozesse zur direkten Unterstützung der Nutzer im täglichen Betrieb (operative Ebene)
- Service Delivery befasst sich mit der mittel- bis langfristigen Planung und Verbesserungen der IT Services (taktische Ebene).

Bei welchem ITIL-Prozess kann eine Einschätzung (Bewertung) nach einer Implementierung (Post Implementation Review) benutzt werden?

A. Application Management

B. Incident Management

C. Problem Management

D. Release Management

Lösung: C. Problem Management: Reviews werden i.d.R. durch das Problem Management realisiert.

Nachdem das Release Management einen kleineren Change zur Integration in die Live-Umgebung komplett getestet hat, kann der Rollout beginnen. Stimmen Sie dieser Aussage zu?

A. Ja, das Release Management ist die adäquate Stelle zur Autorisierung eines Rollout-Starts.

B. Nein, der Change-Manager ist die autorisierte Einheit, um den Change freizugeben. Möglicherweise gibt es einige Umstände, die das Anstoßen des Rollouts verhindern.

C. Wenn die Release-Richtlinien den Release-Manager autorisieren können, kleinere Veränderungsrollouts anzustoßen, kann der Rollout beginnen, ohne dass der Change-Manager dazu direkt kontaktiert werden muss.

Lösung: C. Wenn die Release-Richtlinien den Release-Manager autorisieren können, kleinere Veränderungsrollouts anzustoßen, kann der Rollout beginnen, ohne dass der Change-Manager dazu direkt kontaktiert werden muss: Das Configuration Management, das Change und das Release Management stehen in sehr enger Beziehung zueinander. Wie eng das Verhältnis ist und wodurch Abgrenzungen bestehen, muss durch bestimmte Richtlinien festgelegt werden. Schließlich mutet es als total unsinnig an, für den Austausch einer Maus am Arbeitsplatz eines Durchschnittsanwenders (ohne Bezug zum Vorstand, Produktverantwortlichem o.ä.), den Change-Manager zu kontaktieren und auf sein OK zu warten.

Womit beschäftigt sich die Fehlerkontrolle (Error Control)?

A. zeitliche Lösungen bedenken und ausarbeiten (Workarounds)

B. erkannte Fehler (Known Errors) durch das Prozess Change Management korrigieren

C. Known Errors erkennen und registrieren

D. Known Errors registrieren und verwalten

Lösung: B. erkannte Fehler (Known Errors) durch das Prozess Change Management korrigieren: Hier geht es um die Fehlerbehandlung.

ITIL ist

A. nur eine Ansammlung von Büchern – eine Bibliothek

B. klar definierte Prozesse, die Erfolg garantieren

C. die Art und Weise wie eine IT-Abteilung organisiert sein sollte

D. eine garantierte Geldsparquelle in Verbindung mit einer höheren Kundenzufriedenheit

Lösung: A. nur eine Ansammlung von Büchern – eine Bibliothek

Welche Aktivität muss auf jeden Fall vor der tatsächlichen Durchführung und Aktivierung einer Änderung ausgeführt werden?

A. Kontrolle, ob die Configuration Management Database (CMDB) aktuell ist

B. die Änderung evaluieren

C. den Service Level-Manager informieren

D. die Änderung testen

Lösung: D. die Änderung testen: Keine Änderung im produktiven Umfeld ohne Test. Allein der gesunde Menschenverstand sollte dies schon implizit voraussetzen.

Die Konfigurationselemente (CIs) und die Konfigurations-Management-Datenbank (CMDB) stehen in bestimmten Beziehungen zueinander. Wozu dienen diese Beziehungen?

A. die CMDB verwalten zu können

B. die Cls erfassen zu können

C. Störungen diagnostizieren zu können

D. die Cls auf ihre Richtigkeit kontrollieren zu können

Lösung: B. um die Cls erfassen zu können: Übersichtlichkeit und Kategorisierungsmöglichkeiten helfen bei der richtigen Einordnung und einer guten Dokumentation in der CMDB.

Daten über Elemente werden in der DSL und im DHS gehalten. Wo werden die relevanten Informationen abgelegt?

A. CDB

B. FSC

C. CMDB

D. SLR

Lösung: C. CMDB: Informationen bezüglich der physikalischen Ablage von Soft- und Hardware werden in der Configuration Management Database abgelegt oder es wird darauf referenziert.

Als Change-Manager sind Sie für die Überprüfung (Review) vorgeschlagener Veränderungen (Changes) zuständig, die Ihnen vorgelegt werden. Sie sind sich nicht sicher, ob Sie die Anzahl an Changes, die Sie ablehnen, dokumentieren sollen. Sie haben davon gehört, dass die Dokumentation der abgelehnten Changes es ermöglicht, eine bessere Metrik dieses Prozesses aufzustellen.

A. Ich stimme dieser Aussage zu.

B. Ich stimme dieser Aussage nicht zu.

C. Diese Details müssen vorab mit dem Kunden abgestimmt werden.

Lösung: A. Ich stimme dieser Aussage zu: Es ist wichtig, die Anzahl der abgelehnten Changes und die Ablehnungsgründe festzuhalten. Bei Aufsetzen eines Prozesses ist es wichtig, eine entsprechende Metrik aufzustellen, um sicherzugehen, dass der Prozess verbessert werden kann. Ein Festhalten von Anzahl und Gründen der Ablehnungen kann helfen, den Prozess zu verbessern. Möglicherweise ist das Formblatt zu kompliziert, so dass Changes aufgrund von fehlenden oder falschen Informationen oder einem nicht vorhandenen Rollbackplan abgelehnt werden. Ein Review kann helfen, durch Schulungen und Informationen den Prozess zu verbessern.

Welche der folgenden Personen sollten Mitglieder des Change Advisory Board sein?

1. Problem-Manager
2. Entscheidungsträger aus dem Kundenbereich
3. Change-Manager
4. Senior IT-Berater

A. 2 und 3

B. Alle

C. 1, 2 und 4

D. 1, 3 und 4

Lösung: B. Alle. Jede Person aus dem Stakeholder-Bereich eines relevanten Changes sollte im CAB vertreten sein. Der Problem-Manager muss bei Bedarf mehr Leute in bestimmten Zeiträumen anfordern. Der Kunde bezahlt in der Regel für den Change und erwartet einen geschäftsbezogenen Benefit aus der Umsetzung. Der Change-Manager ist verantwortlich für den Prozess und muss den Change bewilligen. IT-Berater können für andere Bereiche verantwortlich sein, die durch den Change beeinträchtigt werden.

Welche der folgenden Aussagen ist korrekt?

A. Ein Full Release kann mehr als ein Delta Release enthalten.

B. Ein Emergency Release ist immer ein Delta Release.

C. Ein Package Release kann Full Releases und Delta Releases enthalten.

D. Ein Full Release kann Package Releases und Delta Releases enthalten.

Lösung: C. Ein Package Release kann Full Releases und Delta Releases enthalten. Ein Package Release ist eine Sammlung von Releases, als Full Releases oder als Delta Releases. Full Releases können keine Package Releases enthalten. Ein Full Release kann per definitionem keine Delta Releases enthalten. Emergency Releases können jeglichem Releasetyp entsprechen.

12 Service Delivery

Die Prozessorientierung ist das A und O eines dauerhaft erfolgreichen IT-Serviceangebots. Service Delivery steht dabei für die kundengerechte Bereitstellung von IT-Dienstleistungen. ITIL zerlegt das IT-Servicemanagement in elf Disziplinen, die in die Bereiche „Service Support“ und „Service Delivery“ aufgeteilt sind (inklusive Security Management). Für jede dieser Disziplinen liefert die Bibliothek Beschreibungen der Prozesse sowie ihrer Schnittstellen. Diese ermöglichen es dem Anwender, die Prozesse seiner IT-Dienstleistungen zu definieren und zu verbessern.

Mit den Delivery-Prozessen werden die IT Services geplant. Mit Service Delivery etablieren Sie das Bindeglied zwischen Kundenanforderungen, Leistungsprozessen und Technologieeinsatz. Dies ist das wichtigste Instrument für die Ausrichtung der IT Service-Organisation auf die Anforderungen der Kunden und die gezielte Umsetzung der IT-Strategie.

ITIL beschreibt ein systematisches, professionelles Vorgehen für das Management von IT-Dienstleistungen. Die Library stellt nachdrücklich die Bedeutung der wirtschaftlichen Erfüllung der Unternehmensanforderungen in den Mittelpunkt und nicht die rein technische Sicht. Der Bereich Service Delivery als taktische Komponente beschreibt die Kapitel (*siehe Abbildung 12.1*):

- Service Level Management
- Capacity Management
- Availability Management
- IT Service Continuity Management
- Financial Management for IT Services

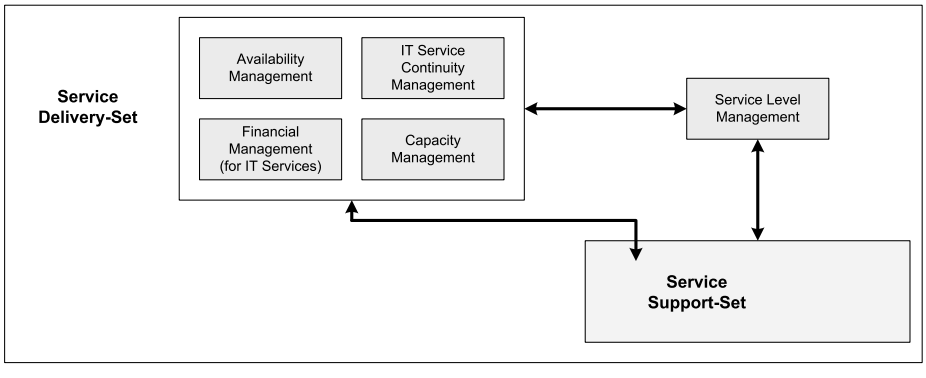


Abbildung 12.1: Abgrenzung der beiden Bereiche Service Support und Service Delivery

Service Delivery unterstützt das IT- und Quality-Management auch dabei, die Ziele der IT-Organisation zu konkretisieren. Es ist zudem ein wesentliches Bindeglied zum Security Management. Das Security Management zählt nicht zum Teilbereich Service Delivery. Ihm ist ein eigenes Buch der Library gewidmet worden. Vielfach wird dieses Thema aber zum Service Delivery gezählt, obwohl es sich über alle Disziplinen erstreckt und auch in der IT-Organisation ein übergreifendes Thema darstellen sollte. IT Security Management hat zum Ziel, die den Informationen zugrunde liegenden Daten und Services gemäß ihrem Wert für das Unternehmen in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit und die definierten SLAs zu schützen.

Service Delivery liefert zentrale IT-Steuerungsprozesse und rückt den Service in den Fokus der Leistungserstellung. Wo die Produkte des Unternehmens selbst einen hohen Anteil an IT-Komponenten besitzen, wird Service Delivery auch zum Instrument für das Kerngeschäft. Maintenance- und Betriebsdienstleistungen für den Kunden sind hier oft auch IT Services.

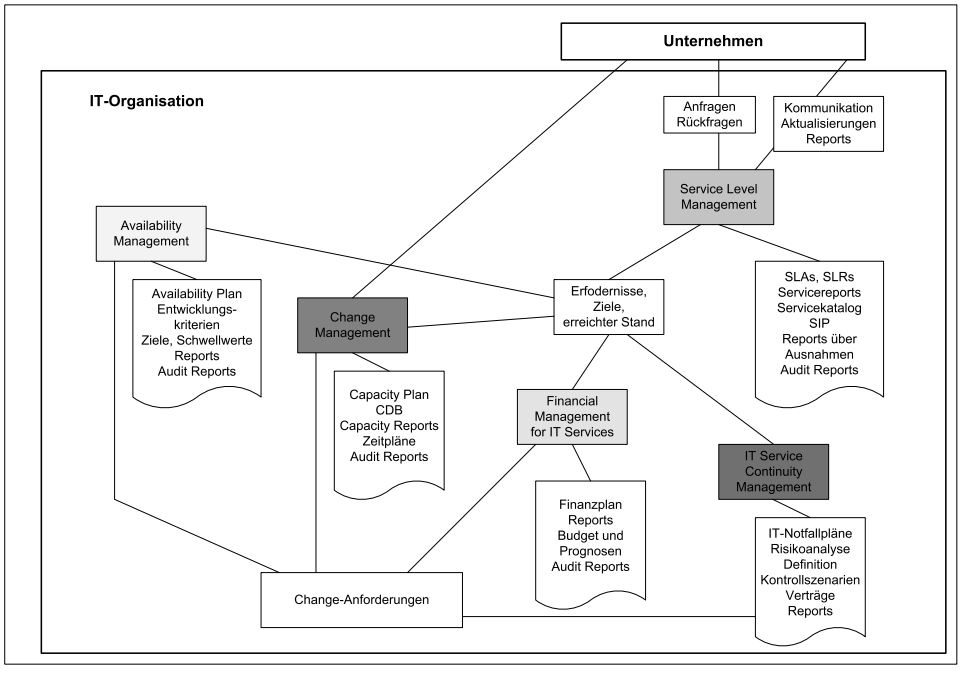


Abbildung 12.2: Bereiche und Verknüpfungen innerhalb des Service Delivery

Dies wird durch folgende Prozesse sichergestellt:

- Dreh- und Angelpunkt der Aktivitäten im ITIL-Bereich ist die Definition sinnvoller, erreichbarer und messbarer SLAs (*siehe Abbildung 12.2 und 12.3*). Diese ermöglichen der Geschäftsführung, den Wert der IT Services aus Business-Sicht zu ermitteln. Das Service Level Management arbeitet an der Erhaltung und allmählichen Verbesserung der auf die geschäftlichen Aktivitäten ausgerichteten IT Servicequalität. Dies geschieht durch einen beständig ablaufenden Zyklus der Abstimmung, der Überwachung, des

Berichtens und des Reviews. Einher damit geht das Messen der IT Services-Leistungen. Bei Bedarf müssen Maßnahmen durchgeführt werden, um unakzeptable Servicequalität auf das gewünschte Maß zu heben. Wichtige Stichworte sind hierbei Anforderungsmanagement, Servicedesign und -planung, Contracting, Monitoring, Reporting und Serviceoptimierung.

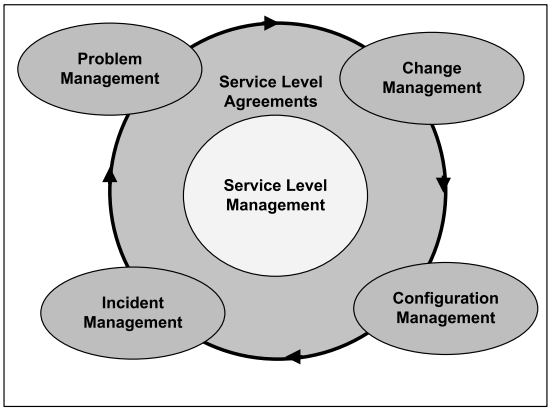


Abbildung 12.3:
Zentrale Rolle des Service Level Managemens – nicht nur für den Bereich Service Delivery

Mit Hilfe von Service Leveln vereinbaren Kunden und Dienstleister (extern oder intern) Qualität und Service-Grad in Bezug auf Art, Umfang, Verfügbarkeit und Kosten. Dabei werden die wechselseitigen Rechte und Pflichten wie Ziele, Kennzahlen, Messverfahren, Maßnahmen und Sanktionen bei Abweichungen definiert und im Service Level Agreement (SLA) festgeschrieben. Kunde und IT-Organisation verbindet so eine klare Vorstellung der beidseitigen Verpflichtungen.

Danach folgen Lieferung, Verwaltung, Überwachung und Reporting der Leistungen gegenüber dem Kunden. Dieser Prozess unterliegt zyklischen Aktionen zur Verbesserung mit dem Ziel, die IT Services auf die tatsächlichen Anforderungen der Geschäftsprozesse des Kunden auszurichten, die Servicequalität zu ermitteln und die Übereinstimmung zwischen der erbrachten und der vereinbarten Leistung dauerhaft sicherzustellen.

- Das Capacity Management dient der Erkenntnis über zukünftige geschäftliche Anforderungen, über die Aktivitäten der Organisation und über die IT-Infrastruktur. Ziel ist die Gewährleistung von anforderungsgerechten Serviceleistungen unter minimalen Kosten. Es stellt sicher, dass die bestehenden Ressourcen optimal eingesetzt und notwendige Anpassungen geplant und realisiert werden. Die Beschaffung von Ressourcen erfolgt geplant und zeitgerecht, d.h. weder zu früh noch zu spät. So wird sichergestellt, dass alle momentanen und zukünftigen Kapazitäts- und Leistungsaspekte, die sich aus den geschäftlichen Anforderungen ableiten, kostenwirksam erbracht werden. Hieraus wird z.B. unter Berücksichtigung der Ergebnisse der Lasttests eine optimale Lastverteilung auf die bestehenden Systeme ermittelt. Das Risiko von Leistungseinbußen infolge fehlender oder mangelhafter Ressourcen wird reduziert. Des Weiteren wird über Prognosen der zukünftigen Geschäftsanforderungen die rechtzeitige Erweiterung der Systeme gesteuert. Die Vorhersagen über den Ressourcenbedarf werden zuverlässiger. Durch Vermeidung von Überkapazitäten kann das Capacity Management einen großen Beitrag zur Kosteneinsparung leisten. Das zentrale Arbeitsmittel ist die Capacity (Management) Database (CDB).

- Das Availability Management optimiert die Leistungsfähigkeit der IT-Infrastruktur und der sie stützenden Organisation, um ein kostenwirksames und nachhaltiges Niveau der Verfügbarkeit zu ermöglichen. Dies schafft die Basis für das Unternehmen, seine eigenen Zielvorgaben einzuhalten. Beim Availability Management wird aus den Geschäftsanforderungen ein allgemeines sowie ein servicespezifisches Verfügbarkeitsniveau definiert, die Umsetzung geplant und die zu definierten Qualitätsparameter (Key Performance Indicators) überwacht.

  Der Kunde erwartet, dass der Service unabhängig von den Umständen, entsprechend der Service Level-Vereinbarung (SLA) erbracht wird. Availability Management hat zum Ziel, die vereinbarte Service-Verfügbarkeit zu gewährleisten, indem es die Anforderungen aus den SLAs in einen Plan zur Erhaltung der Service-Verfügbarkeit umsetzt. Dies wird erreicht, indem man mögliche Ausfälle auf Basis von Analysen vorausberechnet, deren Risiko bewertet und dann entsprechende Service-Architektur-Maßnahmen zur Sicherung der geforderten Verfügbarkeit ergreift.

  Das Aufgabenspektrum berührt dabei die folgenden Themen:

  - Anforderungen in Bezug auf die Verfügbarkeit von Services und Ressourcen feststellen. Basis sind die SLAs.
  - Verfügbarkeitsplan erstellen. Daraus abgeleitet sind die Verfügbarkeitsprognosen zu erstellen und die entsprechenden Maßnahmen zu planen.
  - tatsächliche Verfügbarkeit ermitteln. Durch die Messbarkeit der Verfügbarkeitsziele kann die interne und die externe Leistung überwacht und gesteuert werden.
  - Verfügbarkeit ständig verbessern (Qualitätskreis von Deming)

- Das Continuity Management for IT Services unterstützt den allgemeinen Prozess des Continuity Management des Unternehmens, indem es sicherstellt, dass die benötigten IT-Technik- und Service-Ressourcen innerhalb der aus Sicht des Unternehmens erforderlichen und vereinbarten Zeiträume wiederhergestellt werden können.

  Primäres Ziel ist es dabei aber, die relevanten Service-Leistungen auch in Ausnahme- und Notfällen sicherzustellen. Ein Notfall ist ein Ereignis gegen das sich ein Unternehmen nicht schützen kann. So kann beispielsweise ein ganzes Rechenzentrum durch ein Erdbeben zerstört werden. Die Aufgabe für das Continuity Management besteht darin, basierend auf einer Risikoanalyse, schützenswerte IT Services zu identifizieren und Maßnahmen zu ergreifen. Wie diese Vorsichtsmaßnahmen aussehen und welchen Umfang sie haben, liegt im Ermessen des Unternehmens. Nicht immer geht aus einer solchen Analyse konkreter Handlungsbedarf in Sachen Notfallplanung hervor. Für ein Logistikzentrum mit angeschlossenem Rechenzentrum wird das Management Maßnahmen ergreifen, um den Gebäudekomplex zu schützen, falls einer der Fahrer die Kontrolle über einen der täglich über das Gelände fahrenden LKWs verlieren sollte. Hier besteht ein konkretes Risiko, da täglich Hunderte von LKW im Gebäudebereich rangieren. Auch in Bezug auf Erdbeben oder Überschwemmungen werden Maßnahmen ergriffen, falls das Gebiet diesem Risiko unterliegt. Ein Flugzeugabsturz stellt ebenfalls ein Risiko für das Areal dar. Die Wahrscheinlichkeit für eine solche Katastrophe kann aber so gering sein, dass diesbezüglich keinerlei Maßnahmen ergriffen werden.

Um das Verhältnis der zu erwartenden Kosten den quantifizierten Verbesserungen gegenüberstellen zu können, ist eine Risikoanalyse notwendig. Das IT Service Continuity Management definiert und plant alle Maßnahmen und Prozesse für unvorhergesehene Katastrophenfälle. Ein IT Service Continuity-Plan stellt sicher, dass bei Eintritt eines Notfalls kontrolliert und ohne Zeitverzug gehandelt werden kann, um Folgeschäden minimal zu halten.

Dabei ist das IT Service Continuity Management in den übergeordneten Prozess Business Continuity Management eingebettet. Es ist ständig in die Aktivitäten des Change Management involviert und arbeitet eng mit den anderen Bereitstellungsprozessen (Service Delivery) zusammen.

- Das Financial Management bietet eine kostenwirksame Verwaltung der IT-Komponenten und der finanziellen Ressourcen, die für die Erbringung von IT Services eingesetzt werden. Es ist ein integraler Bestandteil des Service Management und stellt die essenziellen Management-Informationen zur Verfügung, die für die Gewährleistung einer effizienten Erbringung des Service benötigt werden. Kurz: Der finanzwirtschaftliche Aspekt des IT Service Management wird über das Financial Management for IT Services abgewickelt.

  Dieser Bereich lässt sich dabei in Bezug auf seine Ausrichtung und die damit zusammenhängenden Aktivitäten in drei Unterbereiche aufteilen:

  - Budgetierung: Budget planen, Standardkosten kalkulieren, Budget überwachen, Kosten und Erlöse kontrollieren
  - Kostenrechnung: Ist-Kosten ermitteln (Kostenarten/Kostenstellen), Service-Kosten errechnen, Aufwendungen nach Kostenstellen überwachen, Zahlungseingang/-ausgang überwachen
  - Leistungsverrechnung: Verrechnungsmodalitäten festlegen, Preisliste erstellen und pflegen, Rechnungen erstellen

Aufgabe des Service Delivery ist die Durchführung der planerischen und steuernden Prozesse zur professionellen Durchführung der IT-Dienstleistungen auf taktischer Ebene.

Das IT Management nach ITIL unterteilt die zu unterstützenden Prozesse in drei Ebenen:

- Strategische Ebene: Management von IT-Dienstleistungen; dazu zählen unter anderem Qualitätsmanagement und IT Service-Organisation
- Taktische Ebene: ITIL widmet der Planung und Steuerung von IT-Dienstleistungen ein eigenes Buch, das als Service Delivery bezeichnet wird. Dazu zählen Service Level Management, Financial Management for IT Services, Capacity Management, IT Services for Continuity Management und Availability Management
- Operative Ebene: Die Unterstützung von IT-Dienstleistungen wird dem ITIL-Subset Service Support zugerechnet. Dazu zählen Service Desk, Incident Management, Problem Management, Configuration Management, Change Management und Release Management

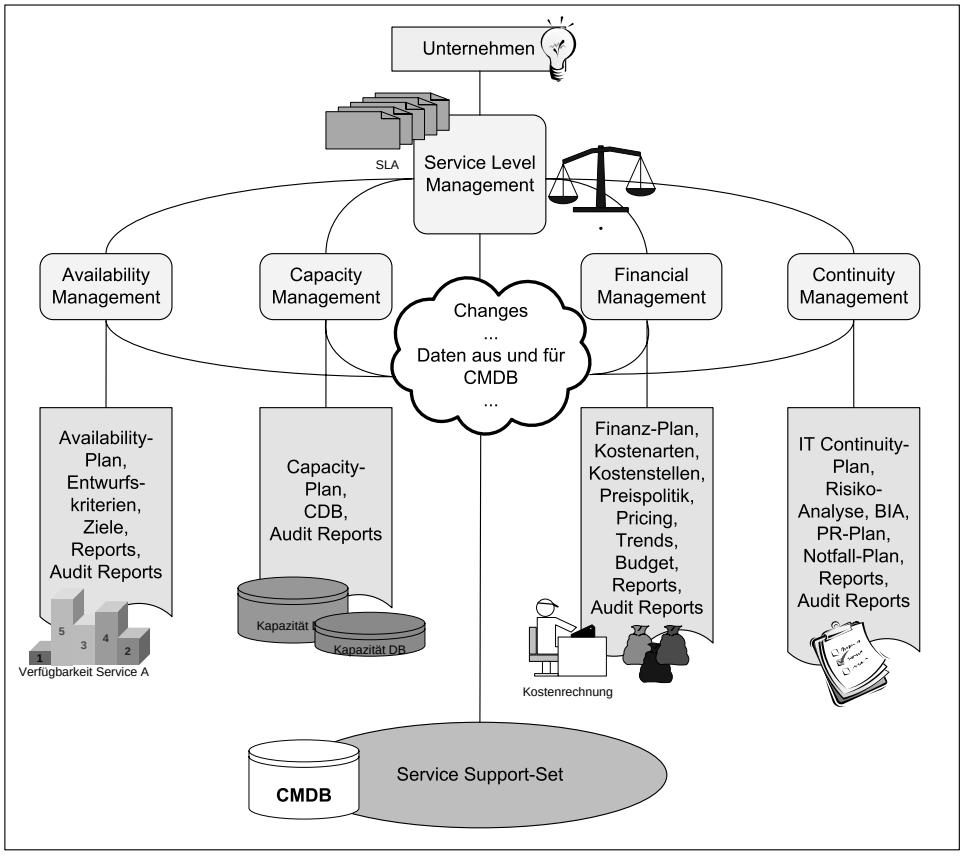


Abbildung 12.4: Zusammenhänge im Service Delivery-Bereich

Durch den zentralen Einsatz von SLAs (*siehe Abbildung 12.4 und 12.5*) wird der Nutzenbeitrag der IT Services transparent. Die Anforderungen der Kunden fließen kontinuierlich in die Servicegestaltung ein. Service Levels werden aktiv geplant, unerfüllbare Zusagen vermieden. Die Vereinbarungen mit Kunden und Dienstleistern sind festgeschrieben, einsehbar und somit bekannt. Die Service Level-Anforderungen sind so konkret, dass sie mess- und steuerbar sind. Dies ist vor allem in Hinsicht auf den globalen ITIL-Gedanken relevant: Nur das, was messbar ist, kann verbessert werden.

Für die IT-Infrastruktur und deren Verwaltung bedeutet dies einen transparenten Überblick darüber, welche Leistungen und IT-Komponenten einen Beitrag für konkrete Services liefern. Die Erlös- und Aufwandsstruktur jedes Services ist bekannt und der IT-Dienstleister, sei es extern oder intern, kann seinen Deckungsbeitrag steuern und gegenüber dem Kunden festlegen. Wie zuverlässig der Service geliefert wird, kann über Reportingfunktionen, die in jedem Prozess implementiert werden müssen, ermittelt werden. Dem Kunden können so standardisierte wie auch individuelle Service Level-Reports auf effektive Weise zur Verfügung gestellt werden. Preis, Leistung und Qualität der Serviceerstellung sind für die Kunden

jederzeit transparent. Die Kundenseite ist in der Lage, ihre IT-Kosten über die eigenen Serviceanforderungen selbst zu beeinflussen. So wird aus der defensiven Kostendiskussion eine zukunftsgerichtete Nutzendiskussion und aus dem Kostenfaktor IT ein strategisches Instrument zur Erreichung der Ziele ihrer Anwender. ITIL hilft dabei, dies zu erreichen.

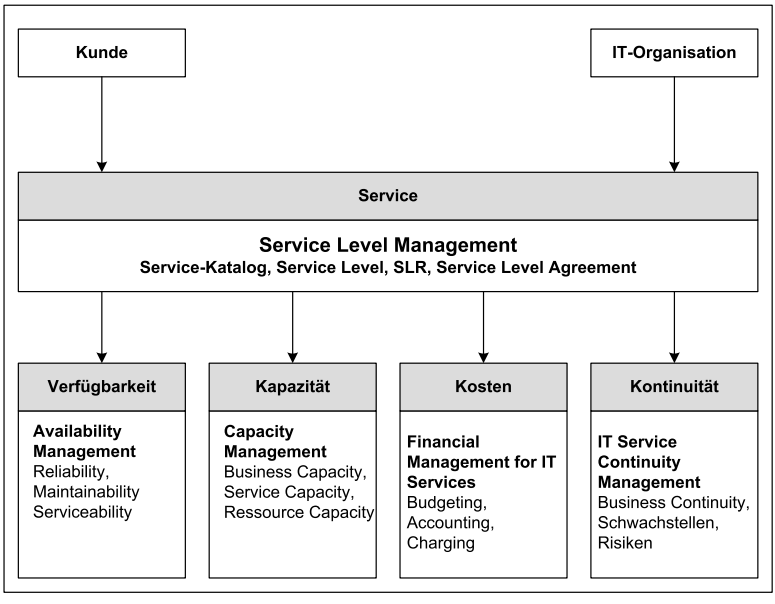


Abbildung 12.5: Aspekte des Service Delivery

Viele IT-Abteilungen sind von diesem Ziel noch weit entfernt. Oft versperrt eine dominierende Technologiesicht den Blick auf kundengerechte Servicegestaltung. Unklare Serviceanforderungen und Standards nehmen dem IT-Management die notwendige Transparenz, um Qualität und Wirtschaftlichkeit der IT-Leistungen gezielt zu steuern. Dieser Misstand zeigt sich dementsprechend in allen Hierarchieebenen. Wie soll der Netzwerkspezialist im Problem Management oder die Datenbankadministratorin über die Anforderungen zwischen IT und Kunde Bescheid wissen, wenn diese einige Ebenen höher nicht klar sind? Mangels Standardisierung sind Leistungs- und Infrastrukturinhalt der Services in vielen Bereichen unzureichend bekannt, die zuverlässige Erbringung von Services schlecht steuerbar, Vereinbarungen mit Kunden und Dienstleistern schwer auf ihre Einhaltung kontrollierbar und deshalb oft unverbindlich. Monitoring und Reporting erfordern oft hohen Aufwand. Den IT-Mitarbeitern fehlt häufig der Bezug zu den von ihnen unterstützten Services. Die Auswirkungen ihres Handelns auf Servicequalität und Kundenzufriedenheit können sie nur bedingt einschätzen. Hier kommt wieder der Faktor der inneren Einstellung und Serviceausrichtung hin zum Kunden zum Tragen. Jeder Mitarbeiter beeinflusst durch sein Verhalten das Bild, das die IT-Abteilung beim Kunden hinterlässt.

Fehlen zudem Informationen über die Zusammenhänge zwischen IT Services und Leistungserstellung im Betrieb, kommt auch der finanzielle Faktor wieder ins Spiel. In einem solchen Fall sind die Deckungsbeiträge der Services nicht ermittelbar. Die Kunden fordern transparente Preismodelle. Um dieses Ziel zu erreichen, müssen komplizierte Umlageverfahren etabliert werden, die oft wenig mit der wirklichen Aufwandsstruktur zu tun haben. Mangels Leistungstransparenz kommt es häufig zu einer einseitigen Kostendiskussion, die kaum objektiv geführt werden kann. Hier werden dann meist Äpfel mit Birnen verglichen und das IT-Management fühlt sich nicht selten in der Defensive.

Um diesem allgemeinen Misstand abzuhelfen, der sich ohne Gesamtausrichtung auf ein IT Service Management durch zahlreiche Bereiche zieht, wendet sich ein IT-Dienstleister dem Thema ITIL zu. Ziel der planerischen und steuernden Prozesse im Service Delivery ist es dabei, dass die Anforderungen des Kunden an den IT-Bereich bestmöglich geplant, umgesetzt und überwacht werden können. Dazu gehört eine bessere Kundenorientierung.

Mit der Etablierung von ITIL als De-facto-Standard über die letzten Jahre sind jedoch auch die Erfahrungen mit einer erfolgreichen Einführung von ITIL gewachsen. Es lassen sich sechs kritische Erfolgsfaktoren identifizieren:

- Die Beziehung der IT-Abteilungen zum Business ist so transparent wie möglich implementiert. Die Erwartungen des Business sind klar festgehalten.
- IT-Services werden in der Quantität und Qualität mittels SLAs vereinbart, wie diese vom Kunden erwartet/benötigt werden.
- IT-Abteilungen vereinbaren ihre Unterstützung zur Service-Erbringung. Die Ziele der IT-Abteilungen sind auf die Service-Erbringung ausgerichtet.
- IT-Dienstleister kommunizieren mit derselben „Prozess-Sprache".
- Die Detaillierung der ITIL-Prozesse erlaubt den IT-Abteilungen, ihre Aufgaben bei der Erbringung eines IT-Services zu erfüllen. Die Prozessimplementation wird realistisch geplant.
- Organisatorische Veränderungen sind integraler Bestandteil der Planung und des Projektes.

13 Service Level Management

In der Vergangenheit wurden der Umfang und die Qualität der Dienstleistungen hauptsächlich durch die IT-Abteilungen bestimmt, die sich dabei redlich bemühten, den Anwendern die richtige Servicequalität anzubieten. Mittlerweile unterliegt die Abhängigkeit des Geschäftserfolges immer stärker der eingesetzten IT und den entsprechenden IT Services, die von den Kunden genutzt werden. Dementsprechend sind Dynamik und Komplexität heutiger Geschäftsprozesse nicht von der IT zu vernachlässigen. Hier stellt sich die Frage, wie das Gleichgewicht zwischen den Anforderungen von der Kundenseite (Servicenehmer, -nachfrager) und den Möglichkeiten der IT-Abteilungen (Servicegeber, -anbieter) aussehen kann. Wichtig ist, sich auf einer gemeinsamen Ebene zu treffen und die beiderseitigen Erwartungen unter einen Hut zu bringen. So wird eine beiderseitige Verantwortlichkeit für den Service gewährleistet, welcher in gegenseitigem Einvernehmen entschieden und fortlaufend überarbeitet wird (*siehe Abbildung 13.1*). Service Level Management (SLM) ermöglicht die Umsetzung des Szenarios als IT Service Management-Disziplin. Hier werden Verträge zwischen Kunden und Betreibern von IT-Dienstleistungen verhandelt, vereinbart, überwacht und ausgewertet. Auf diese Weise ist gewährleistet, dass Anspruch und Wirklichkeit, Kosten und Qualität in ein ausgewogenes Miteinander überführt werden.

Service Level Management richtet die IT-Einrichtungen und Service-Leistungen an den tatsächlichen betrieblichen Anforderungen und den durch die Anwender formulierten Bedürfnissen aus. Die Kunden betrachten das Service Level Management mit anderen Augen als einen einzelnen Serviceanbieter. Das Service Level Management sieht sich als Schnittstelle, an der die unterschiedlichen Sichtweisen und Anforderungen vereint werden.

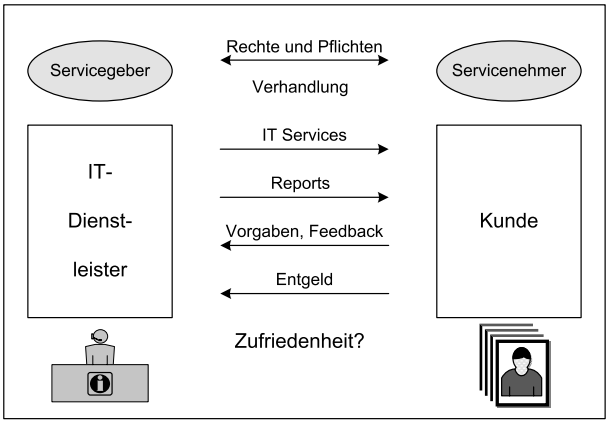


Abbildung 13.1:
Service Level Management als Schnittstelle

Dies bedeutet, dass das Service Level Management die betriebswirtschaftlichen und juristischen Anforderungen im Auge behalten muss. Hinzu kommen die vorhandenen organisatorischen und technischen Maßgaben. Der wesentliche Erfolgsfaktor für Service Level Management ist die Standardisierung. Die unterschiedlichen Serviceanforderungen von Anwender- oder Kundenseite stoßen auf breit gestreute und vielfach unbekannte Leistungen der IT-Organisation. Um Licht in das Dunkel zu bringen, brauchen beide Seiten Transparenz. Dies kann mit Hilfe flexibel zusammenstellbarer Services als standardisierte Bausteine realisiert werden, deren Leistungsinhalt, Qualitätseigenschaften und Deckungsbeiträge für das IT-Management und den Kunden transparent sind. Dies wiederum führt ebenfalls zu einer Stärkung des Bewusstseins der IT-Mitarbeiter für Service Level-Ziele und Kundenwünsche und schafft größeres Vertrauen der Anwender in die IT-Systeme und das Service Management. Das Ergebnis eines solchen Abstimmungsprozesses muss vertraglich geregelt werden, Services müssen in Anlehnung an den IT Service Management-Gedanken plan- und steuerbar, zu kalkulieren, zu messen und zu verrechnen sein. Da sich das Serviceportfolio einer IT-Abteilung bzw. eines IT-Unternehmens direkt aus der ganzheitlichen Strategie ableiten sollte, erscheint Service Level Management nicht nur als Schnittstelle zwischen Kunden und den IT-Prozessen bzw. den damit zusammenhängenden Technologien, sondern auch als Bindeglied zwischen Management- und Leistungsprozessen in der IT.

13.1 Service Level Management nach ITIL

Service Level Management ist für die Standardisierung und Überwachung der IT Services verantwortlich. Hier werden die Kundenanforderungen in Dienstleistungsprodukte der IT-Organisation umgesetzt, die Services geplant und vertraglich vereinbart. Der Prozess stellt auch die laufende Überwachung der zugesagten Service Levels und das Service-Reporting sicher. Auch die Absicherungsverträge mit Dienstleistern sowie Operational Level Agreements zur Sicherstellung interner Leistungen unterliegen dem Service Level Management. Dies ist einer der zentralen Service Management-Prozesse mit weit reichender Bedeutung für die Kundenzufriedenheit und die professionelle Steuerung der IT-Organisation und dient gleichzeitig zur Steuerung der IT-Servicequalität. Ziel dieses Prozesses ist es, die Geschäftsprozesse des Kunden optimal zu unterstützen. So werden in diesem Prozess die Qualität und Quantität der IT Services zu vertretbaren Kosten verhandelt, definiert, gemessen und kontinuierlich verbessert.

13.2 Begriffe des Service Level Management

Ein IT Service geht im ITIL-Verständnis über die Konfrontation eines Anwenders mit einem technischen System hinaus. Um auf den Nutzen für den Kunden fokussieren zu können, muss die Definition der IT Services auf die Unterstützung des Geschäftsprozesses abzielen. Es ist häufig von „der Bereitstellung eines oder mehrerer technischer Systeme in einer Form, die zur Ermöglichung oder Unterstützung eines Geschäftsprozesse dient“ die Rede. Allerdings muss sich ein IT-Unternehmen oder eine IT-Abteilung nach unterschiedlichen Kriterien zu einem Service-Provider

entwickeln. Wichtig ist dabei die Unterstützung durch das Management und eine entsprechende Servicekultur im Unternehmen (*siehe Abbildung 13.2*). Das Ziel sollte auch stets die Etablierung einer Servicekultur mit entsprechenden Service-Prozessen sein und nicht das reine Vertragswerk.

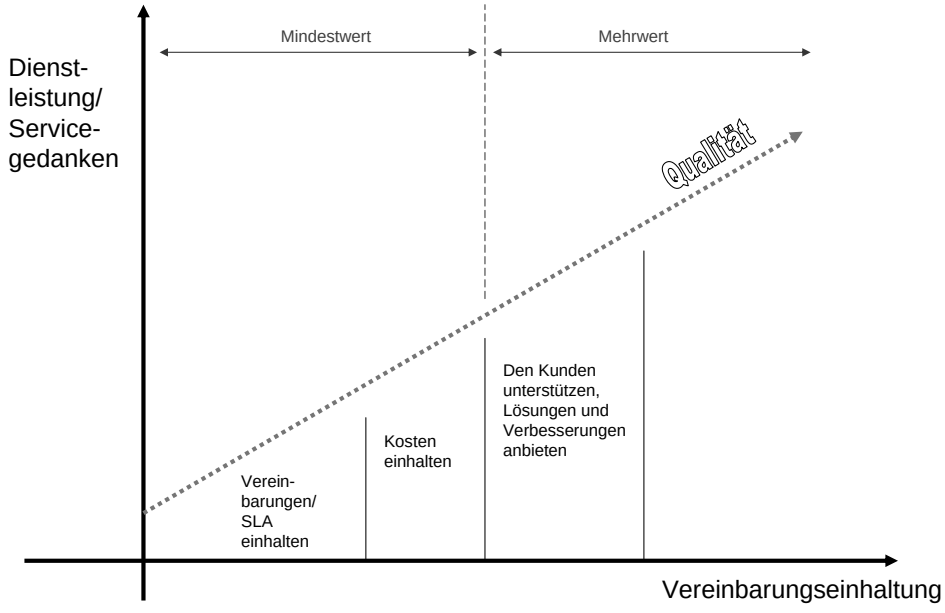


Abbildung 13.2: Kundenzufriedenheit und Business-Unterstützung sind oberstes Gebot

Jeder externe oder interne Abnehmer von IT Services wird als Kunde betrachtet. Der Dienstleister ist in der Regel die IT-Organisation. Da auch innerhalb der IT-Organisation oft IT Services in Anspruch genommen werden und die IT-Organisation dadurch selbst zum Kunden wird, entstehen bisweilen komplexe Beziehungen. Daher ist es in der Praxis wichtig, die Rollenverteilung innerhalb des Prozesses bezüglich der konkreten Maßnahmen zu beachten.

Das Service Level Management besitzt eine Art Vermittlerrolle zwischen Kunde und IT Service (*siehe Abbildung 13.3*), wobei interne und externe Vereinbarungen aufeinander abgestimmt sein müssen. Die Fixierung dieser Beschlüsse hinsichtlich der zu leistenden IT Services erfolgt in den Service Level Agreements (SLAs). Weitere Hilfsmittel in Form von unterschiedlichen Dokumenten und Schriftstücken sind Bestandteile des Prozesses. Vorrangiges Werkzeug ist das Service Level Agreement, das eine Menge von zwischen einem Servicegeber und einem Servicenehmer fest definierten und messbaren Service- und Leistungsvereinbarungen darstellt. So werden Rechte und Pflichten zwischen dem Servicegeber und dem Servicenehmer verbindlich festgelegt. Service Level Agreements sind kennzahlenbasierte Vereinbarungen, d.h. die zu gewährleistenden Servicequalität eines Dienstleistungsanbieters mit seinem Kunden wird messbar.

Der Kunde ist der Vertreter einer Organisation oder einer Organisationseinheit, der befugt ist im Namen der Organisation(seinheit) Vereinbarungen über die Inanspruchnahme von Services zu treffen. Es handelt sich also in der Regel nicht um den (End-)Anwender dieser IT Services. Der Dienstleister ist der Vertreter einer Organisation, der befugt ist, im Namen der Organisation Vereinbarungen über die Erbringung von IT Services zu treffen.

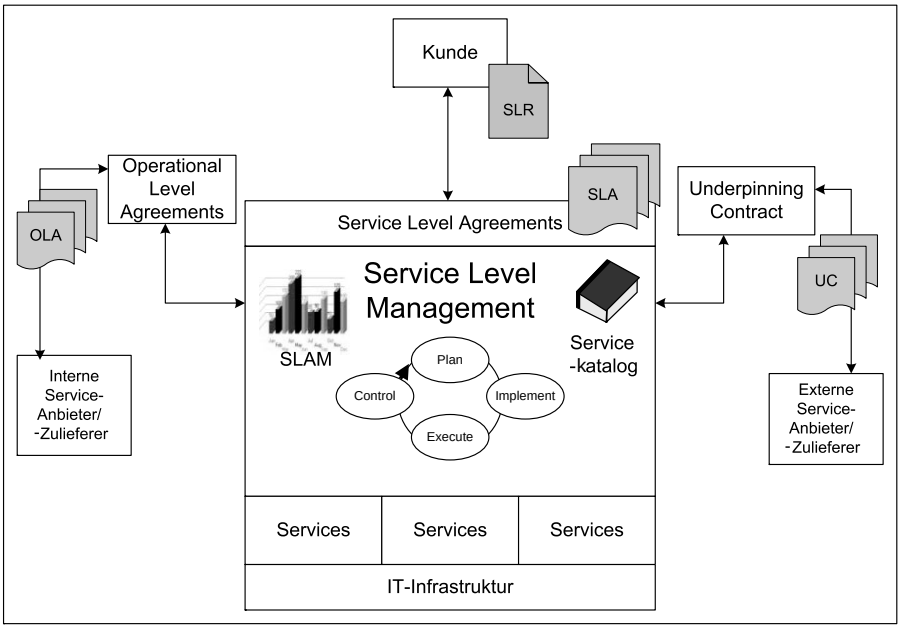


Abbildung 13.3: Bestandteile des Service Level Management

Die Serviceanforderungen (Service Level Requirements, SLRs) stellen die Anforderungen des Kunden an den IT Service dar. Sie bilden die Grundlage für die Erstellung und die Anpassung der IT Services. Die manchmal abstrakten Wünsche der Kundenseite sollen in präzise Beschreibungen modelliert werden, um diese dann in die SLAs, die Vereinbarung als Ergebnis, einzubringen.

In seiner verbindenden Funktion führt das Service Level Management Gespräche mit dem Kunden über dessen geschäftliche Anforderungen, ohne sich dabei in technischen Details zu verlieren. Das SLA beschreibt die IT Services in nicht-technischen Begriffen. Für die Dauer der Vereinbarung gilt das SLA als Vertrag in Bezug auf die Leistungserbringung und Steuerung der IT Services. SLAs lassen sich nach unterschiedlichen Gesichtspunkten aufsetzen. Zum einen existiert eine Servicebasierte Sicht, bei der ein SLA für einen relevanten Service definiert wird. Zum anderen besteht die Möglichkeit, SLAs Kunden-basiert zu definieren. Hier wird ein SLA für alle Services eines Kunden aufgesetzt. Ein weiterer möglicher Ansatz ist eine Mischform, die so genannte Multi-Level-Struktur, in der z.B. alle für die ganze

Organisation eines Kunden relevanten Vereinbarungen in einem allgemeingültigen Bereich zusammengefasst werden (Corporate Level), und in anderen Bereichen Service-basierte bzw. Kunden-basierte Vereinbarungen Anwendung finden.

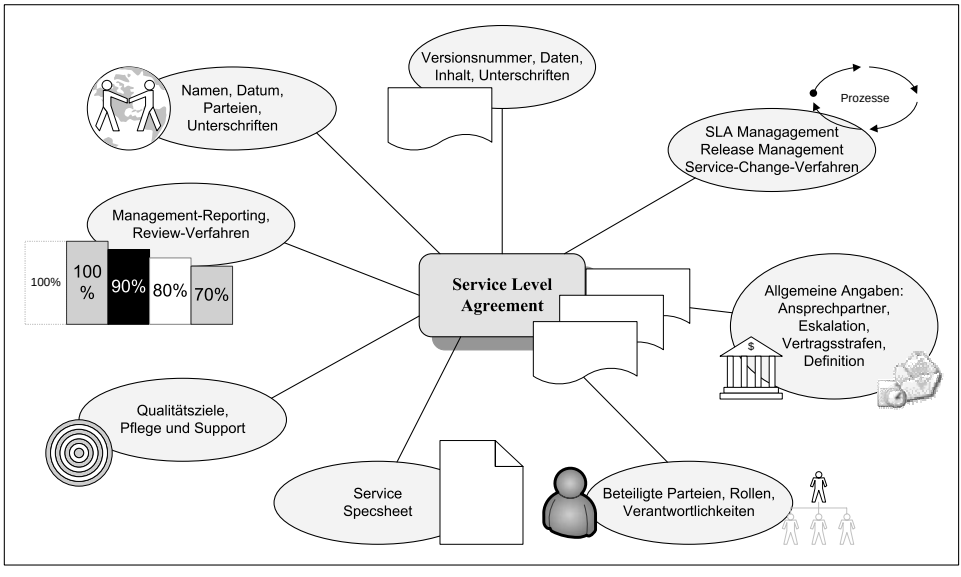


Abbildung 13.4: Bestandteile eines SLA

Egal welcher Ansatz gewählt wird: Fest steht, dass ein SLA in wenigen nicht-technischen Worten folgende Aspekte regelt (*siehe Abbildung 13.4*):

- Service-Beschreibung: Überblick über vereinbarte Leistungen
- Service-Definition: Ergebnis einer Leistung oder Teilleistung, gegebenenfalls die zur Leistungserbringung erforderliche Mitwirkungs- und Beistellpflicht des Kunden
- Service Levels: Qualitätsausprägung der in der zugehörigen Service-Definition beschriebenen Leistung oder Teilleistung
- Service-Messgröße: Erfüllungsgrad des zugehörigen Service Level. Die Anzahl der gemäß dem Service Level erbrachten Leistungen wird in Relation zu den insgesamt zu erbringenden Leistungen gesetzt und durch spezifische Messvereinbarungen ergänzt, wie beispielsweise Betrachtungszeitraum, Messpunkte und Systeme, aus denen die Messpunkte generiert werden (Serviceparameter, Kennzahlen und Zielwerte).
- die Veränderungsverfahren (Change-Prozeduren)
- Definition des Gültigkeitszeitraums etc.

Ein SLA regelt so Grenzwerte, Messverfahren, Rahmenbedingungen, Kommunikations- und Eskalationsparameter und die Anforderungen an das Reporting.

Risiken

Nicht immer sind SLAs durchgängig und messbar, vor allem wenn diese mit „unpassenden" Kennzahlen überladen werden. Abhilfe ist möglich, wenn SLAs Teil einer Balanced Score Card sind (*siehe Abbildung 13.5*). BSC ist eine Managementmethode, mit der ein Unternehmen mittels strategischer Kennzahlen gesteuert werden kann. Sie stellt ein Führungssystem dar, mit dessen Hilfe strategische Ziele in den betrieblichen Alltag übertragen werden.

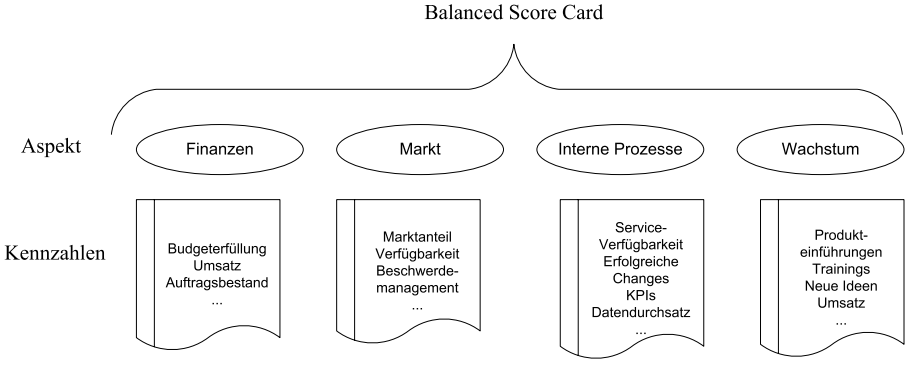


Abbildung 13.5: Beispiel zu BSC

Diese Methode basiert im Wesentlichen auf der Formulierung von Zielen, deren Erfüllung mittels einer geeigneten Kennzahl kontrolliert werden kann. Dabei werden Ziele in Teilziele heruntergebrochen und an Teilzielverantwortliche übergeben. Aufgrund möglicher Abweichungen von Soll-Werten der Kennzahlen kann auf jeder Ebene eine Nicht-Erfüllung der Ziele nachgewiesen werden und entsprechend gegengesteuert werden.

Der Service Quality Plan (SQP) stellt einen dokumentierten Plan und die Spezifizierung interner Ziele zur Gewährleistung der vereinbarten Service Level dar und versteht sich eher als internes Dokument. Die Bezugsgrößen dieser Ziele werden auch Leistungsindikatoren (Key Performance Indicators) genannt. Für jeden Prozess werden solche Ziele festgelegt. Die Leistungsindikatoren werden aus den Service Level Requirements abgeleitet und in den so genannten Specsheets dokumentiert.

In den Specsheets wird der Inhalt der Service Level Requirements (externe Spezifikationen) in eine technische Form gebracht, die für die Realisierung der IT Services erforderlich ist (interne Spezifikationen). Hier geht es um die technischen Maßnahmen auf der Seite des Serviceanbieters, die erforderlich sind, um die Service Levels einzuhalten. Es geht um die Konsequenzen für den Dienstleister, z.B. erforderliche Ressourcen. Das Specsheet ist ein Provider-internes, d.h. nicht durch den Kunden einsehbares Dokument. Dem Dienstanbieter bleiben in Bezug auf die Details der technischen Umsetzung Freiheiten, solange er die vereinbarten SLAs erfüllt. In den Specsheets können beispielsweise geeignete Berechnungsmethoden enthalten sein, um Komponenten- und Dienstparameter abbilden zu können.

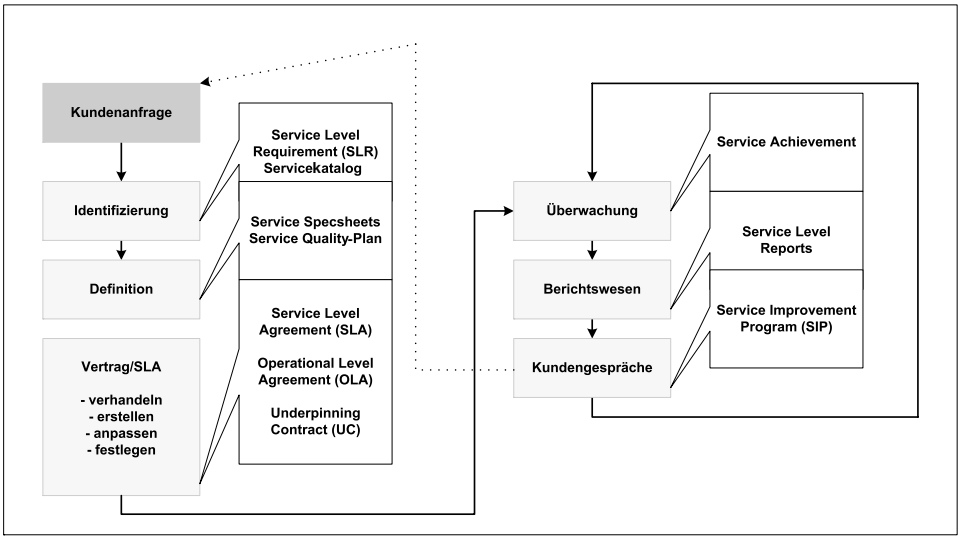


Abbildung 13.6: Der Prozess und die damit zusammenhängenden Dokumente und Begriffe

Viele Experten vertreten die Meinung, dass die Erstellung eines Kataloges aller IT-Services (Service Catalog) einer der ersten und wichtigsten Schritte bei der Einführung von ITIL ist (*siehe Abbildung 13.6*). Der Servicekatalog (Service Catalog) der IT-Organisation beschreibt das gesamte Portfolio an IT Services und die damit verbundenen möglichen Service Level. Dabei geht es um die Servicebeschreibung an sich, Funktionen und Leistungen, Reaktionszeiten, Service-Erbringer und andere Details. Der Servicekatalog bietet so eine detaillierte Übersicht aller IT Services plus die Optionen, den IT Service anzupassen. Als Vorbereitung zu den SLA-Verhandlungen dient dieser Katalog als Angebots- und Verhandlungsgrundlage.

Das Service Level Management bietet einen guten Ansatz für ein Service-Optimierungs-Programm (Service Improvement Program, SIP), dessen Umsetzung in vielen Fällen in Form eines Projekts und über jährliche Reviews in Zusammenarbeit mit dem Problem Management und dem Availablity Management initiiert wird. Hier werden Aktionen, Phasen und Meilensteine dokumentiert, die zur Verbesserung eines IT Service in einem Bereich oder Prozess beitragen.

Im Service Review Meeting (SRM) wird abgefragt, ob die Service Levels und die damit verbundenen Ziele für die IT-Abteilung(en) erreicht wurden. Die Frage nach dem Erfüllungsgrad steht im Mittelpunkt. Im Bedarfsfall können Anforderungen von Kundenseite entstehen, die Aktionen im Change Management anstoßen, um eine Verbesserung zu initiieren.

Um sicherzugehen, dass der Service-Anbieter die gewünschten Services in vereinbarter Qualität auch leisten kann, sichert sich dieser wiederum ab. Dabei wird zwischen externen und internen Lieferanten unterschieden, die den eigentlichen Serviceanbieter unterstützen (*siehe Abbildung 13.7*).

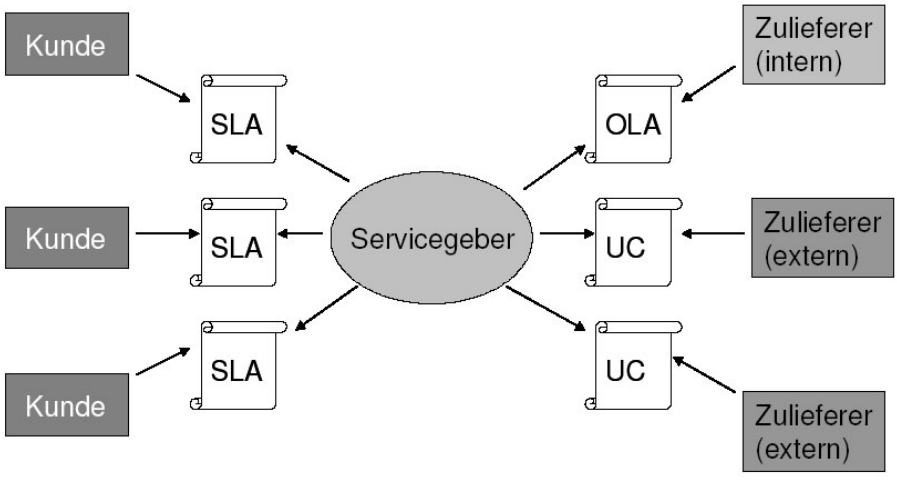


Abbildung 13.7: Vereinbarungen in unterschiedliche Richtungen

Ein Operation Level Agreement (OLA) stellt eine Vereinbarung mit einem internen IT-Bereich als Zulieferer dar. Es enthält Absprachen über einen (Teil-)Service in einem Bereich, z.B. über die Verfügbarkeit des Netzwerks, die für die Erbringung des Gesamtservices in Richtung des Kunden relevant ist. Ein Servicegeber an sich kann somit gleichzeitig als Serviceanbieter und als Servicenutzer fungieren. Ein OLA dient somit zur Unterstützung der IT-Organisation, die den gesamten IT Service leistet, und ist ein Vertrag im juristischen Sinne.

Dagegen stellt der Absicherungsvertrag (Underpinning Contract, UC) einen Vertrag mit einem externen Dienstleister dar, der die Vereinbarungen über die Abwicklung bestimmter Bereiche eines Services enthält. Vergleichbar ist ein solcher Vertrag mit der externen Ausführung eines OLAs. Sollte Anpassungsbedarf bestehen, sollten wenn möglich OLA oder UC an die SLAs angepasst werden und nicht umgekehrt.

Der erreichte Service Level (Service Achievement) beschreibt die tatsächlich erbrachten Services über erreichte Service Levels innerhalb der definierten vereinbarten Zeitspanne. Kurz: Die Übereinstimmung der vereinbarten Qualität mit der erzielten Qualität.

Juristische Aspekte

SLAs können verbindliche Abreden zwischen den Vertragsparteien, vertragliche oder vertragsergänzende Regelungen und selbstständige vertragliche Regelungen oder Einbindungen in einen bestehenden Vertrag darstellen.

Steht auf beiden Seiten derartiger Vereinbarungen dasselbe Unternehmen, handelt es sich nicht um einen Vertrag im eigentlichen Sinne. Es geht eher um eine Absprache innerhalb des Unternehmens. Mithilfe dieser Vereinbarung verpflichten sich beide Seiten einerseits zu Service-Leistungen einer definierten Qualität und andererseits zu entsprechenden Mitwirkungsaktionen.

13.3 Aufgaben und Aktivitäten des Service Level Management

Ausgehend von den Anforderungen des Servicenutzers lässt sich das Service Level Management als ein beständiger Kreislauf des Verhandelns, Überwachens, Berichtens und Überprüfens ansehen, der bei Bedarf Aktivitäten auslöst, um unzureichende Servicequalität und -quantität zu verbessern. Für den Kunden bedeutet dies auch, dass die Leistung der IT-Organisation messbar ist, somit besser überwacht werden kann und dokumentiert wird.

Service Level-Manager: Ein Hut im Service Level Management

Die Verantwortung für das Service Level Management obliegt dem Prozess-Manager, der die effektive Durchführung des Prozesses sowie die Erreichung der damit verbundenen Vorteile sicherstellt. Die Funktion des Prozess-Managers muss nicht an eine einzige Person gebunden sein. Die Aufgaben des Service Level-Managers sind beispielsweise die Erstellung und Pflege des Servicekatalogs sowie die Formulierung und Pflege eines effektiven Service Level Management für die IT-Organisation.

In der *Abbildung 13.8* ist der Prozessverlauf des Service Level Management grob skizziert. Dieser enthält zwei Unterprozesse, die parallel ausgeführt werden können. Die in der ersten (oberen) Hälfte beschriebenen Tätigkeiten beschäftigen sich damit, Vereinbarungen zu treffen, während sich die Aktionen in der zweiten (unteren) Hälfte auf die Gewährleistung dieser Vereinbarungen konzentrieren.

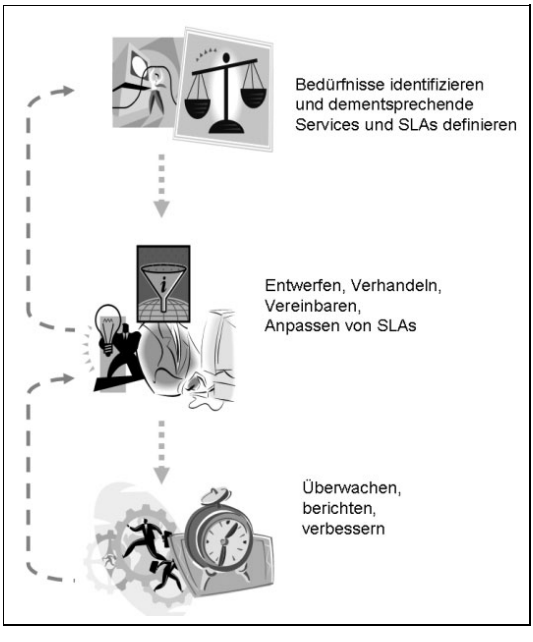


Abbildung 13.8:
Das Leben mit SLAs ist nicht statisch

Zu den Aktivitäten des Service Level Management zählen insgesamt:

1. Identifizierung: Zuallererst geht es darum, die Kundenbedürfnisse zu erkennen und festzulegen. Dabei geht es darum, die Business-Anforderungen aus der Organisation heraus und die daraus resultierenden Serviceanforderungen (SLR) zu ermitteln. Hier ist eine entsprechende Pflege der Kundenbeziehung unumgänglich. Diese Aktion erfordert sowohl Kenntnisse aus dem Bereich der Geschäftsanforderungen als auch aus der IT, um die entsprechenden Möglichkeiten darlegen zu können. Erfahrungsgemäß kennen die Kunden ihre eigenen Anforderungen und Erwartungen nicht vollständig, weil sie bei bestimmten Aspekten eines Services davon ausgehen, dass sie entsprechend erbracht werden, ohne dass Vereinbarungen erforderlich sind. Dies unterstreicht nochmals die Notwendigkeit, dass Service Level-Manager ihre Kunden gut kennen müssen und in der Lage sein müssen, ihren Kunden zu helfen, zu klären, welche Services und Service Levels sie wirklich benötigen und zu welchen Kosten sie diese erhalten.

   Hierbei handelt es sich jedoch nicht um eine einmalige Aktivität, sondern vielmehr um eine Tätigkeit, die aufgrund von Berichten und Prüfungen, auf Verlangen des Kunden oder auf eigene Initiative der IT-Organisation sowohl hinsichtlich bereits existierender als auch hinsichtlich neu zu erbringender Services immer wieder ausgeführt werden muss.

2. Definition: IT Services und die dazugehörige SLA-Struktur müssen erstellt werden. Dies wird über externe und interne Basisdokumente realisiert wie etwa das Service Specsheet und den Service Quality-Plan. Die Ziele werden auf die Wünsche und Bedürfnisse des Kunden ausgerichtet und in den Service Level Requirements und Servicespezifikationen festgelegt. Die Kundenerwartungen werden formal in den Serviceanforderungen (Service Level Requirements, SLRs) hintergelegt (*siehe Abbildung 13.8*).

   Für die Festlegung der Service Level Requirements sind unterschiedliche Angaben erforderlich. Dazu gehören beispielsweise eine allgemeine Beschreibung der Funktionen, die der Kunde von dem Service erwartet, Uhrzeiten und Tage, an denen der Service verfügbar sein soll (Servicezeit), Anforderungen an die Service-Verfügbarkeit und die für die Erbringung des Service notwendigen IT-Funktionen. Damit in Zusammenhang stehen Verweise auf aktuelle Betriebsmethoden oder die Qualitätsstandards, die beim Entwurf des Services berücksichtigt werden, und gegebenenfalls Verweise auf SLAs, die angepasst oder ersetzt werden müssen.

   Der Definitionsprozess kann in mehreren Phasen von der Detaillierung der Kundenwünsche bis hin zur Ausarbeitung technischer Voraussetzungen für die Erbringung des Services ablaufen. Dies spiegelt sich dann in den Specsheets (zur Servicespezifikation) wider, die im Einzelnen die Erwartungen und Anforderungen des Kunden (extern) und die Konsequenzen für die IT-Organisation (intern) dokumentieren. Der Servicekatalog als Verzeichnis aller Dienstleistungen, die die IT erbringt, kann aus den Servicespezifikationen resultieren. So werden Änderungen an den Service Levels in den Specsheets und im Servicekatalog verarbeitet, um die SLAs aus den geänderten Specsheets neu zu generieren.

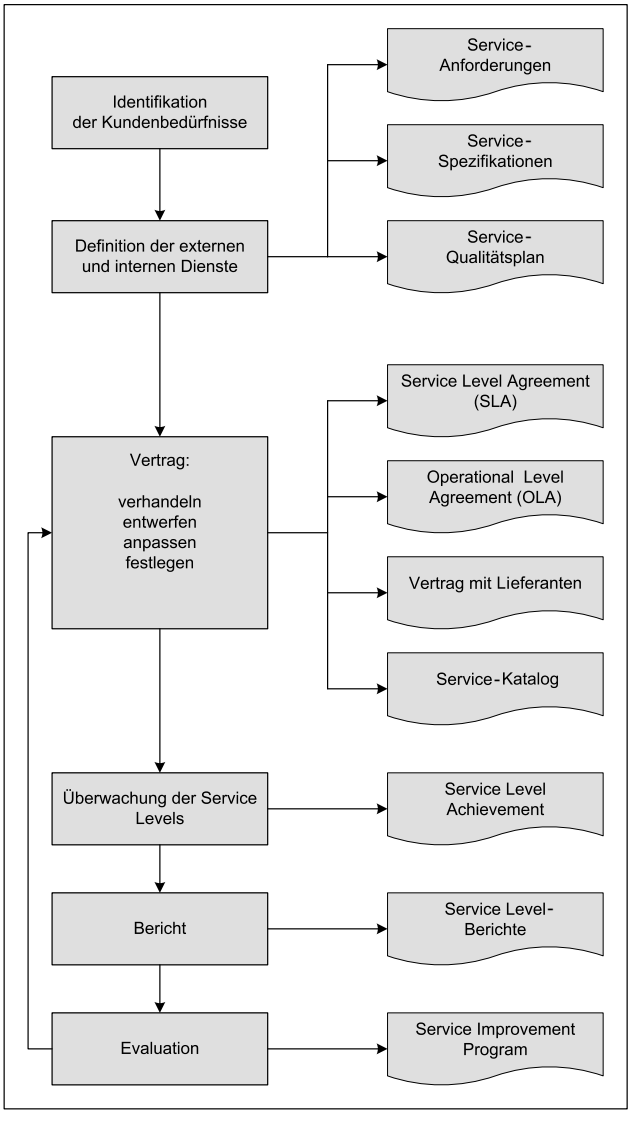


Abbildung 13.9: Service Level Management-Prozess

3. Service Level Agreement Monitoring (SLAM): Vereinbarte SLAs und die definierten Service Levels müssen natürlich auch eingehalten werden. Die Überwachung der Servicequalität ist eine notwendige Aktivität, für die Leistungsindikatoren (KPIs) herangezogen und verglichen werden. Die tatsächlich realisierten Service Levels werden in Service Achievements dokumentiert. Sie stellen den aktuell an den Kunden gelieferten Service Level dar.

Die Überwachung sollte nicht nur von der technischen Seite geprägt sein, sondern auch Verfahrensweisen beinhalten, wie etwa die Abwicklung von Incidents und Requests hinsichtlich der Kundeninteraktion.

4. Berichtswesen/-erstattung: Erstellung von Service Level-Reports an Kunden und IT-Manager, die gewünschte und definierte Informationen enthalten wie etwa die Service Achievements eines bestimmten Zeitraums (*siehe Abbildung 13.10*). Dem Kunden und der IT-Organisation werden so regelmäßig Berichte über die realisierten Service Levels vorgelegt. Auf diese Weise werden die Ist- und Soll-Stände miteinander verglichen, um die vertraglich vereinbarten Service Levels zu kontrollieren und ggf. zu verbessern. Auf Basis dieser Dokumente können eine Überprüfung der Vereinbarungen und gegebenenfalls eine Anpassung stattfinden.

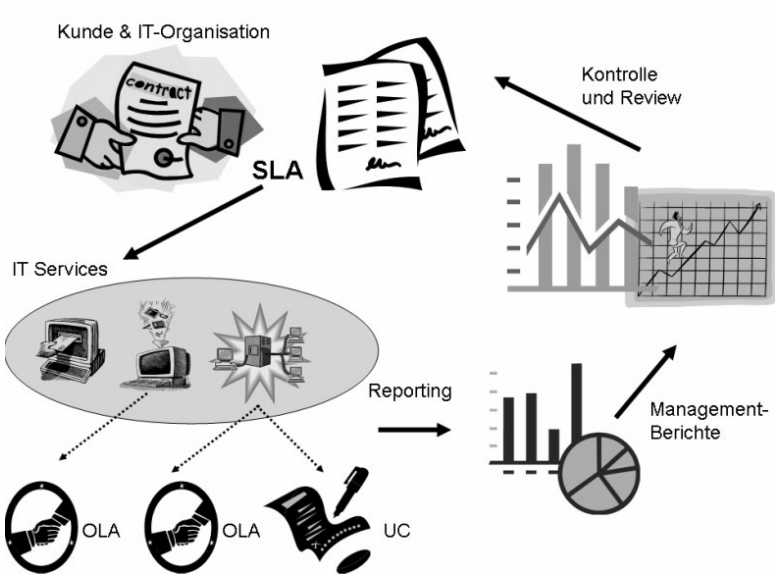


Abbildung 13.10: Reports als wichtiger Prozessbestandteil

5. Auswertung (mit dem Kunden) und Review: Hier geht es um mögliche Probleme in Verbindung mit Dienstleistungen, der Identifizierung von Trends und entsprechenden Verbesserungsvorschlägen (SIPs). Der Service wird evaluiert, um herauszufinden, ob er verbessert werden muss. Gegebenenfalls wird ein Service-Optimierungs-Programm initiiert. Darüber hinaus werden regelmäßig Erfahrungen, Anregungen und Veränderungswünsche des Kunden zu den geleisteten IT Services abgefragt, welche unter Umständen in neue oder erweiterte SLAs einfließen können. Dies hätte Change-Anforderungen (RfCs) für die SLAs zur Folge.

13.4 Service Level Management im ITIL-Gesamtprozess

Dem Service Level Management kommt eine zentrale Rolle im IT-Management zu, da alle Aktivitäten in der IT Auswirkungen auf die Service-Erbringung haben. Service Level Agreements (SLAs) sind inzwischen innerhalb von IT-Organisationen und vor allem im Verhältnis zwischen IT Service-Provider und dem Kunden bzw. Abnehmer von IT Service-Leistungen weit verbreitet. Gemeint ist damit eine transparente Beschreibung einer Kunden-Lieferanten-Beziehung, mittels derer qualitätsoptimierend auf die Erbringung von IT Service-Leistungen und die Sicherstellung von Zielen durch Vereinbarung von Service Level-Einfluss genommen werden kann. Vor allem im Bereich IT Outsourcing ist eine Leistungserbringung ohne vereinbarte SLA nicht vorstellbar. Aber auch für interne IT-Abteilungen sind SLAs ein wichtiges Kriterium.

Das Service Level Management spielt eine Schlüsselrolle innerhalb der IT Service Management-Prozesse und pflegt engen Kontakt zu den sonstigen Support- und Delivery-Prozessen. Alle Prozesse und Funktionen des Service Management zielen letztlich auf die Erbringung qualitativ hochwertiger IT Services für die Kunden ab.

Service Level Management ist für interne und externe Dienstleistungen anwendbar. Dies gilt insbesondere für das Service Desk, egal ob dieser intern oder extern betrieben wird. Anfragen und Beschwerden an das Service Desk werden aufgenommen und über Reportings als Information dem Service Level Management zur Verfügung gestellt.

Problem Management umfasst alle Funktionen und Abläufe zur Behebung von Störungen und Fehlern im Betriebsablauf. Incident Management umfasst alle Abläufe zur schnellstmöglichen Wiederherstellung der vereinbarten Services. Hier fallen Abweichungen vom gewohnten bzw. vereinbarten Service Level als erstes auf, wenn sich die Incident-Menge zu einem bestimmten Service oder einer Komponente der IT deutlich erhöht. Für das Service Level Management sind die Informationen, wann welche Services wie häufig ausgefallen sind, wichtig, um die Qualität des Service zielgerichtet im Rahmen des Service Quality-Plans zu verbessern.

In der CMDB aus dem Configuration Management-Prozess wird die IT-Infrastruktur als Modell abgebildet. Dazu gehören auch Dokumente wie die SLAs oder der Servicekatalog. Durch die Relationen der CIs in der CMDB können die entsprechenden Vereinbarungen und Dokumente zu einem betroffenen CI rasch gefunden und die Informationen daraus abgeleitet werden. Und da das Configuration Management für alle angrenzenden Prozesse in Form der CMDB ein wichtiges Repository zur Verfügung stellt, das sich auch auf die SLAs bezieht, haben alle anderen Bereiche Zugriff auf die Daten aus dem Service Level Management.

Zielsetzung des Change Management ist eine effiziente und kostengünstige Implementierung autorisierter Änderungen mit minimalem Risiko für bestehende und neue IT-Anwendungssysteme und Infrastrukturen. Aufgabe und Herausforderung des Change Management ist dabei, sicherzustellen, dass die notwendigen Änderungen gut vorbereitet und kontrolliert ohne negative Auswirkungen auf das Business ablaufen. In den SLAs kann definiert werden, welche Änderungen die Kundenorganisation unter welchen Bedingungen wie einreichen kann. Schließlich ist ein SLA auch ein CI, dessen Veränderung stets unter der Kontrolle des Change Management abzulaufen hat. Dies bezieht sich auch auf die Kosten, die ein solcher Change verur-

sacht. Etwaige Änderungen eines Service und der entsprechenden SLAs werden über das Change Management abgewickelt. Die Schnittstellen zwischen Service Level Management und Change Management werden von allem bei Neuverhandlung von SLAs beansprucht. Gründe für eine Veränderung können in unterschiedlicher Ausprägung Änderungsanforderungen und die Neuverhandlung von Preisen aufgrund von Änderungen des Leistungsumfangs beziehungsweise der Leistungsqualität sein. Auch veränderte Marktbedingungen, Neuverhandlung von Vertragselementen etwa aufgrund von Veränderungen im Leistungsumfang oder Restrukturierungsmaßnahmen bei einem der Vertragspartner sind mögliche Ursachen.

Über das Availability Management soll die in den SLAs geforderte und vereinbarte Verfügbarkeit der Services sichergestellt werden, indem vorhersehbare Ausfälle reduziert bzw. vermieden werden. Dies bezieht sich neben der Gewährleistung eines kosteneffektiven und definierten Verfügbarkeitsniveaus auch auf die Prognose, die Planung und das Management der Service-Verfügbarkeit. Die Verfügbarkeit ist einer der am häufigsten verwendeten Service Levels, wobei die Realisierung und Optimierung der Verfügbarkeit der Services generell im Vordergrund stehen.

Capacity Management umfasst alle Funktionen und Abläufe mit den dahinterliegenden Kosten- und Leistungsaspekten zur Umsetzung und Sicherstellung der zukünftigen und momentanen Kundenanforderungen. Diese spiegeln sich in den SLAs wieder. Zu diesem Zweck wird ein Capacity-Plan erstellt, der Informationen über die aktuelle Zusammensetzung der Infrastruktur sowie Planungen für die Zukunft enthält. Das Service Level Management liefert dem Capacity Management Informationen über die aktuellen und künftigen Services. Diese Informationen sind für eine genaue Kapazitätsplanung essenziell.

Das Continuity Management gewährleistet die Fähigkeit einer Organisation, im Anschluss an die Unterbrechung des Geschäftsbetriebs weiterhin das zuvor festgelegte und vereinbarte Niveau von IT Services zur Unterstützung der geschäftlichen Mindestanforderungen zu erbringen. Entsprechende Maßnahmen werden auch in den SLAs inklusive der korrespondierenden Kosten festgeschrieben.

Auch das Security Management tauscht Informationen mit dem Service Level Management aus. Vertraulichkeit und Integrität gehören zu einem Service. Diesbezügliche Informationen fließen auch in die SLAs ein. Das Security Management kümmert sich um die Umsetzung der Maßnahmen und überwacht diese Sicherheitsvereinbarungen.

Ein Ziel des Service Level Management lässt sich als ausgewogenes Verhältnis zwischen Kundenanforderungen und Kosten der Services beschreiben. Für den Serviceanbieter geht es darum, die Kosten der Eigenleistung und der eingekauften Fremdleistung pro Service bzw. CI zu kalkulieren. Dabei müssen unterschiedliche Szenarien in puncto Kapazitätsauslastung berücksichtigt werden. Voraussetzung für eine effektive Kalkulation sind Angaben über den Ressourcen-Verbrauch und die Kostenquellen. Kunden können das Preismodell beeinflussen, wie etwa durch die Wahl des Service Level und dessen Ausprägung. Der Kostenfaktor spielt bei der Verhandlung der SLAs eine entscheidende Rolle.

14 Availability Management

Availability Management hat zum Ziel, die in den SLAs definierte Verfügbarkeit eines Services sicherzustellen. Um dies zu erreichen, werden mögliche Ausfälle auf Basis von Analysen vorausberechnet, das entsprechende Risiko bewertet und dann nach Bedarf Service-Architektur-Maßnahmen zur Sicherung der geforderten Verfügbarkeit ergriffen. Hier geht es um die Summe der Maßnahmen, die dafür sorgen, dass die IT Services und die damit verbundenen Komponenten der IT-Infrastruktur zur Verfügung gestellt werden. Availability Management hilft, die Leistung der IT Services zu verbessern und so ein effizientes Niveau der Verfügbarkeit zu sichern, das sich an den SLA-Vorgaben orientiert.

Neben der Messung und Planung der Verfügbarkeit (Availability) spielen weitere Aspekte eine wichtige Rolle in diesem Bereich, die die Gesamtverfügbarkeit und die entsprechenden Kennzahlen beeinflussen, etwa die Steuerung der Reliability (Zuverlässigkeit). Hier geht es um die Vermeidung von Service-Ausfällen. Ist diese eindeutig bestimmbar oder existiert ein Risiko, was die Kontinuität eines Services angeht? Dies geht Hand in Hand mit dem Aspekt der Wartbarkeit von IT Services bzw. den entsprechenden Komponenten (Maintainability). Wie aufwändig gestalten sich Wartungen und welche Kosten sind damit verbunden, v.a. wenn dies in regelmäßigen Intervallen durchgeführt werden soll? Einfluss auf die Gesamtverfügbarkeit nimmt auch die Servicefähigkeit (Serviceability), bei der es um die Frage geht, welcher Service überhaupt mit einer Komponente in Zusammenhang steht und wie der Service daraus abzuleiten ist. Das Verfügbarkeits-Management spielt eine in starkem Maße präventive Rolle und beeinflusst damit die Servicequalität und Kundenzufriedenheit.

Warum sind diese Faktoren so wichtig? Die Verbindung der Geschäftsabläufe und der Informationstechnologie sowie der damit verbundenen Services hat sich in den letzten Jahren zu einer echten Abhängigkeit entwickelt. Kein Unternehmen kann sich dagegen wehren und zu Karteikarten und einer reinen Papierwelt ohne EDV zurückkehren. Diese Möglichkeit ist uns mittlerweile aufgrund der Entwicklung in den letzten Jahren verwehrt. Neben den gesellschaftlichen Konsequenzen betrifft dies in hohem Maße den geschäftlichen Erfolg eines Unternehmens. Eine funktionierende und verfügbare IT-Infrastruktur, auf die jederzeit zugegriffen werden kann und die genau den Service liefert, der via SLAs vereinbart wurde, ist essenziell. Ausfälle von mehreren Stunden oder gar Tagen können das Unternehmen so viel Geld kosten, dass verheerende Konsequenzen für den Bestand und das Image des Unternehmens auftreten. Die ITIL-Prozesse sollen genau dem entgegenwirken. Denn zahlreiche Studien haben gezeigt, dass viele Unternehmen kaum in der Lage sind, einen Ausfall der wichtigsten IT Services mehr als ein paar Stunden zu überleben.

14.1 Availability Management nach ITIL

Für den Großteil der Unternehmen ist die dauernde Verfügbarkeit der IT-Dienstleistungen von immenser Bedeutung. Availability Management misst, plant und steuert die Verfügbarkeit von IT Services und der entsprechenden Komponenten.

Das Thema Verfügbarkeit steht im Fokus der geschäftlichen Anforderungen und der Benutzerzufriedenheit. Zur Verbesserung der Verfügbarkeit ist ein Verständnis des Zusammenhangs zwischen Technologie und Geschäft wichtig. Das Messen und Planen der Service- und CI-Verfügbarkeit stehen im Mittelpunkt des Availability Management. Dazu gehören auch die Prognose, die Planung und das Management der Service-Verfügbarkeit und die Gewährleistung eines kosteneffektiven und festgelegten Verfügbarkeitsniveaus, das durch aktives Betreiben eines Risiko-Managements unterstützt wird. Dem Kunden gegenüber wird dies durch entsprechende Berichte, die aus den Messverfahren und Statistiken stammen, nachgewiesen. Der Erfolg dieses Prozesses wird mittels Kennzahlen (KPIs) gemessen, die den SLAs entstammen.

Wichtig ist aber vor allem, dass ein Verständnis dafür entwickelt wird, was die geschäftlichen Anforderungen ausmachen und welche Anforderungen die Benutzer stellen, die sich in den SLAs widerspiegeln werden. Natürlich sollte das Bemühen im Vordergrund stehen, das Verfügbarkeitsniveau der IT-Infrastruktur und der Services ständig zu verbessern. Dies ist ein Gedanke, der mit dem so wichtigen Begriff der Servicekultur in Verbindung steht.

Die Verfügbarkeit der IT Services wird beeinflusst durch die Komplexität der IT-Infrastruktur, der Definition des Services an sich und der IT-Organisation, die damit in Zusammenhang steht, beispielsweise durch das Wissen und die Erfahrung der Mitarbeiter, die in ausreichender Anzahl zur Verfügung stehen müssen. Selbst, wenn irgendetwas schief geht, kann die IT-Organisation durch ihr Verhalten und ihre Reaktion ein entsprechendes Echo bei Benutzern und Kunden hervorrufen. Es ist zum Beispiel immer besser, wenn die IT-Abteilung vor dem Kunden merkt, dass es ein Problem gibt und dies entsprechend kommuniziert und Lösungsstrategien oder Workarounds anbietet. Die Sicht der Anwender ist äußerst wichtig.

Ähnlich wie beim Configuration Management in Bezug auf die Ausprägung der CMDB stellt sich auch beim Availability Management die Frage nach dem eingesetzten Umfang im Unternehmen. Da sich das Availability Management nicht nur mit dem Messen und Verwalten in Bezug auf das Thema Gesamtverfügbarkeit beschäftigt, sondern auch mit der entsprechenden Planung und Implementierung, muss der Prozess sicherstellen, dass die kundenseitigen Anforderungen konsistent umgesetzt werden. Das Availability Management sollte alle bereits existierenden und alle neuen Services einbeziehen, die für den Kunden relevant sind. Die diesbezüglichen Anforderungen werden in SLAs und SLRs auf Kundenseite definiert. Auf geschäftskritische Komponenten sollte besonderes Augenmerk gelegt werden.

So bilden die Verfügbarkeitsanforderungen aus den Service Level Agreements Verhandlungsgrundlagen für die Verhandlungen mit internen und externen Dienstleistern, die die entsprechende IT-Abteilung gegenüber dem Kunden unterstützen sollen. Mit deren Hilfe werden die internen Anforderungen nach außen gespiegelt, um an jeder Stelle die in den SLAs definierten Vorgaben erfüllen zu können. Geringere Anforderungen an externe Lieferanten im Vergleich zu denen der IT-Abteilungen zum Kunden stellen das schwächste Glied in der Kette dar und führen zu Problemen.

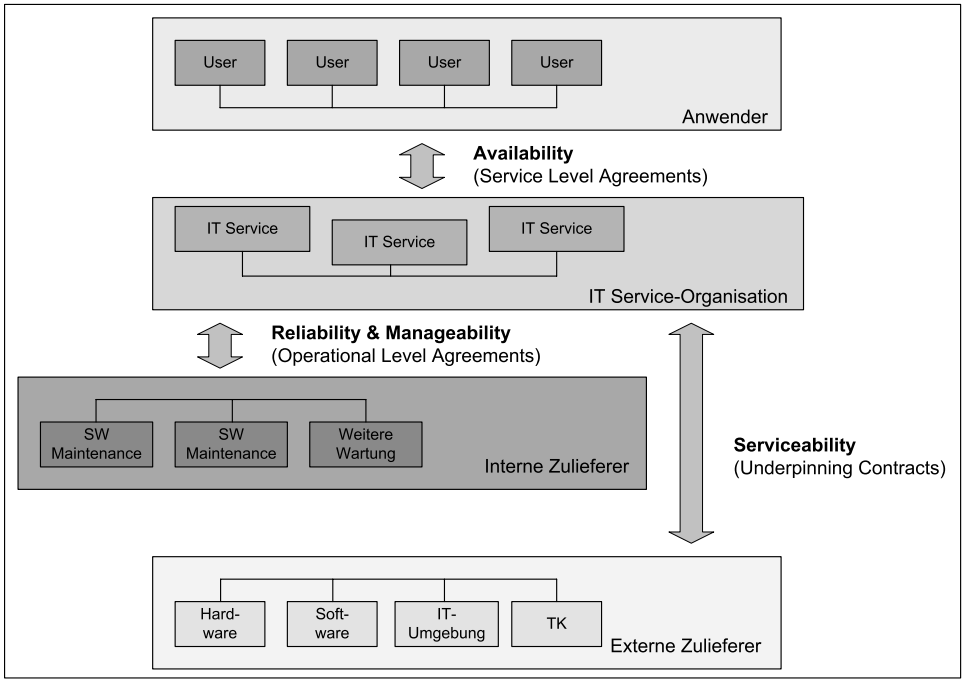


Abbildung 14.1: Verwendung der Begriffe aus dem Availability Management

Es ist jedoch wichtig, dass trotz der engen Zusammenhänge von Availability Management, Security Management und Continuity Management das Availability Management nicht für die Continuity-Planung zuständig ist und keine Aufgaben übernimmt, die mit den Geschäftsanforderungen in Bezug auf Aktionen nach einem Desasterfall in Verbindung stehen.

14.2 Begriffe des Availability Managements

Da unter ITIL Messbarkeit ein wichtiger Faktor ist, stellt sich in Bezug auf das Availability Management die Frage, wofür die Verfügbarkeit steht und wie sie gemessen werden kann.

Verfügbarkeit ist die Fähigkeit einer Komponente oder eines Services, seine geforderte Funktionalität zu einem bestimmten Zeitpunkt oder während einer bestimmten Zeitdauer zu erfüllen. Ein IT Service, der durchgängig verfügbar im Sinne der SLA-Anforderungen ist, besitzt geringe Ausfallzeiten und eine schnelle Wiederherstellungsrate im Falle eines Incidents. Die Verfügbarkeit an sich ist allerdings nicht statisch, sondern befindet sich in einem Spannungsfeld unterschiedlicher Einflüsse wie der eigenen Komplexität, der Zuverlässigkeit der Komponenten in Bezug auf einen Service, der IT-Organisation, der Ansprüche und deren Abstufungen sowie der Merkmale der externen Zulieferer. Hier ist zu betonen, dass das Availability Management zwei Ansätze im Hinterkopf behalten muss: Zum einen die Verfügbarkeit aus der Sicht des IT Service und zum anderen diejenige aus der Sicht der IT-Komponente.

Verfügbarkeit ist eine Bewertung, die sich aus Messwerten ableiten lässt. Das Maß für diese Anforderung wird in der Regel als Verhältniszahl bzw. in Grad/Prozent bezogen auf die SLAs ausgedrückt. Allerdings ist nicht die Verfügbarkeit der in den SLAS geforderten Verfügbarkeit maßgeblich, sondern die absolute Verfügbarkeit (*siehe Abbildung 14.2*). Zu wissen, dass 99 % der in den 99,8 % geforderten Verfügbarkeit erfüllt wurden, ist nebensächlich im Anbetracht dessen, dass die an sich geforderte Verfügbarkeit nicht gewährleistet werden konnte.

$$\%\ Verfügbarkeit = \frac{Erreichte\ verfügbare\ Zeit}{Vereinbarte\ verfügbare\ Zeit} \times 100\%$$

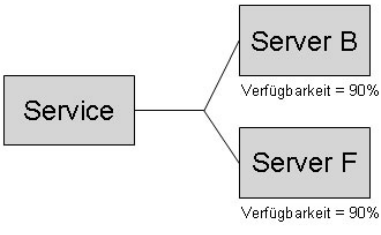
Ein hohes Maß an Verfügbarkeit (Availability) bedeutet, dass der Anwender jederzeit bzw. im vereinbarten Rahmen über den IT Service verfügen kann. Ausfälle sind selten und im Bedarfsfall kann eine schnelle Behebung des Problems gewährleistet werden.

Seriell:

Serielle Verfügbarkeit:

$A_{Service} = A_{Server\ B} \times A_{Server\ F} = 0{,}81 = 81\ \%$

Parallel:



Parallele Verfügbarkeit:

$A_{Service} = 1 - [(1 - A_{Server\ B}) \times (1 - A_{Server\ F})] = 0{,}99 = 99\ \%$

Abbildung 14.2: Grundsätzlich ist die Verfügbarkeit paralleler Komponentensysteme höher als bei seriellen Objekten. Die Zuverlässigkeit eines Service nimmt zu, wenn Ausfälle verhindert werden können.

Zuverlässigkeit (Reliability) bedeutet, dass der Service für die Dauer eines vereinbarten Zeitraums störungsfrei zur Verfügung steht, d.h. die Abwesenheit operativer Fehler. Wichtig ist aber vor allem die Frage: Was versteht der Kunde unter Verfügbarkeit?

Der Zuverlässigkeit eines IT Service ist zum einen abhängig von jeder Komponente der IT-Umgebung, die mit dem entsprechenden Service zusammenhängt, also beispielsweise die Wahrscheinlichkeit, dass eine Komponente ausfallen wird. Zum anderen spielt die Fehlertoleranz (Resilience) eine Rolle. Dies bezeichnet die Fähigkeit einer Komponente oder eines Services, betriebsfähig zu bleiben, wenn eine oder mehrere andere Komponenten ausgefallen sind. Dieser Aspekt wird entsprechend modelliert und implementiert. Die Verfügbarkeit nimmt zu, wenn Ausfälle verhindert werden, z.B. durch Fehlertoleranz (Resilience) von Komponenten.

Wartbarkeit (Maintainability) bezieht sich auf die Fähigkeit einer Infrastruktur-Komponente, im Fehlerfall den Betrieb eines Service aufrecht zu erhalten oder diesen Service bei einem Ausfall wiederherzustellen. Hierzu gehören auch präventive Wartungsarbeiten. Die Wartbarkeit einer Komponente kann in folgende sieben Stufen strukturiert werden:

- Vorwegnahme eines Fehlers (Anticipation)
- Fehlersuche (Detection)
- Diagnose (einschließlich der Selbstdiagnose einer Komponente)
- Fehlerbehebung (Resolve)
- Wiederherstellung nach einem Fehler (Recovery)
- Wiederaufnahme des Services und der Daten (Restoration)
- proaktive Maßnahmen zur Fehlervorbeugung (Preventive Maintenance)

Daneben spielt auch die Sicherheit eine große Rolle in Sachen Verfügbarkeit. Die beiden entsprechenden Prozesse stehen in engem Bezug zueinander (*siehe Abbildung 14.3*). Beim Security Management geht es um die Implementierung von Schutzmaßnahmen zur Sicherstellung kontinuierlicher Services unter Voraussetzung von Vertraulichkeit, Integrität und Verfügbarkeit.

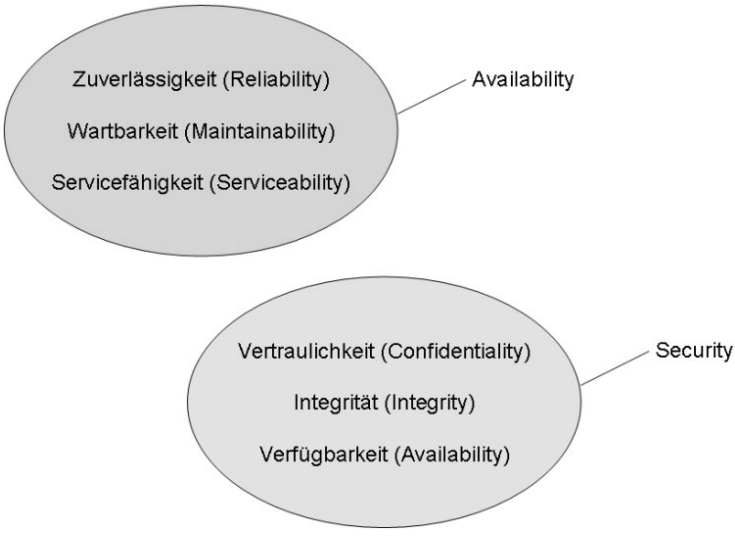


Abbildung 14.3: Availability und Security

Servicefähigkeit (Serviceability) beschreibt die vertraglichen Pflichten der externen Dienstleister (Third Parties), die z.B. in Form von Underpinnig Contracts definiert wurden. In den Verträgen ist die Art des Supports für einen externen Service festgelegt. Da es sich hierbei also um die Komponente eines IT Service handelt, bezieht sich die Wartbarkeit nur auf die jeweilige Komponente und nicht auf die gesamte Verfügbarkeit des Services. Ist ein Dienstleister für den gesamten IT Service verantwortlich, kommen Servicefähigkeit und Verfügbarkeit die gleiche Bedeutung zu. Servicefähigkeit kann an sich nicht gemessen werden, es ist keine metrische Größe. Nur die Verfügbarkeit, Zuverlässigkeit und Wartbarkeit eines Services und der Komponenten können unter diesem Aspekt gemessen werden.

Terminologie

- Zuverlässigkeit: Service steht für die Dauer eines vereinbarten Zeitraums störungsfrei zur Verfügung
- Wartbarkeit: Aufwand, der erforderlich ist, um den Betrieb eines Service aufrecht zu erhalten oder diesen Service bei einem Ausfall wieder herzustellen
- Servicefähigkeit: Vertragliche Pflichten der externen Dienstleister
- Resilience: Strapazierfähigkeit, Fehlertoleranz: Fähigkeit einer Komponente oder eines Services, betriebsfähig zu bleiben, wenn eine oder mehrere Komponenten ausgefallen sind

Der Ausdruck „vitale Geschäftsfunktionen“ wird verwendet, um die für den Geschäftsbetrieb kritischen Elemente zu kennzeichnen.

Wie alle ITIL-Disziplinen kommt dem Thema „Messen und Kontrollieren“ eine besondere Bedeutung zu, denn:

Was man nicht messen kann ... kann man nicht kontrollieren (Tom DeMarco).

Daraus können andere Sätze abgeleitet werden wie zum Beispiel:

„Wenn Du etwas nicht messen kannst, kannst Du es nicht managen.“

„Wenn Du etwas nicht messen kannst, kannst Du es nicht verbessern.“

„Wenn Du etwas nicht messen kannst, kann es nicht sehr wichtig sein.“

„Wenn Du etwas nicht beeinflussen kannst, dann miss es nicht.“

Für den Prozess Availability Management gilt dies nicht. Hier geht es primär um das Messen von Verfügbarkeiten. Dies ist neben dem Reporting ein wichtiger Output dieses Prozesses. Schließlich treten immer und überall Fehler auf. Nicht immer steht ein Service in vereinbarter Qualität zur Verfügung. Dabei sind die folgenden Begriffe für einen Service relevant:

- Durchschnittliche Ausfallzeit (Mean Time to Repair, MTTR): die durchschnittliche Zeitdauer zwischen dem Auftreten einer Störung und der Wiederherstellung des Service, auch Downtime genannt. Diese Zeitspanne ergibt sich aus der Summe aus Erkennungszeit und Bearbeitungszeit. Der auf diese Weise ermittelte Wert bezieht sich auf die Wiederherstellbarkeit und die Servicefähigkeit eines Service.

- Durchschnittliche produktive Zeit bis zum Auftreten einer Störung (Mean Time Between Failures, MTBF): die durchschnittliche Zeitdauer zwischen der Behebung einer Störung und dem Auftreten der nächsten Störung, auch Uptime genannt. Dieser Wert gibt Auskunft über die Zuverlässigkeit eines Service.
- Durchschnittlicher Zeitraum zwischen dem Auftreten von Störungen (Mean Time Between System Incidents, MTBSI): die durchschnittliche Zeit zwischen dem Auftreten zweier nacheinander auftretender Störungen, also die Summe aus MTTR und MTBF.

Aus der Beziehung, die zwischen MTBF und MTBSI besteht, ist ersichtlich, ob es sich um viele kleine Störungen oder einige wenige große Störungen handelt.

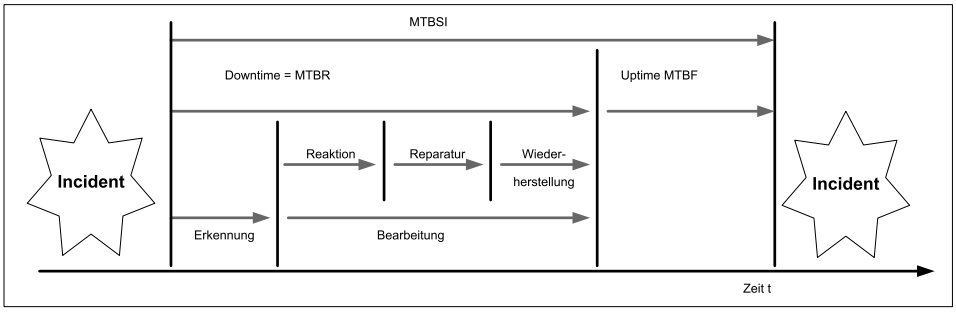


Abbildung 14.4: Kenngrößen aus dem Availability Management/Incident-Lebenszyklus

Diese Begriffe stehen in Verbindung mit dem so genannten Incident-Lebenszyklus (Incident Life Cycle). Mit dem Auftreten einer Störung beginnt dieser Zyklus (*siehe Abbildung 14.4*). Jeder Incident durchläuft dabei unterschiedliche Stati, wobei die Dauer variieren kann, abhängig von den Reaktionen der Dienstleister, sei es extern oder intern, die sich um den Incident kümmern müssen:

1. Störung tritt auf: Hier ist der Einstiegspunkt des Zyklus; er bezeichnet den Zeitpunkt, an dem der Incident auftritt. Entweder merkt der Anwender, dass ein Service ausgefallen ist oder nicht in gewohnter Weise verwendet werden kann, oder die Störung wird auf andere Weise (technisch, physisch, logisch) festgestellt.
2. Erkennung: Der Dienstleister wird über den Incident informiert. Die Zeit, die zwischen den ersten beiden Schritten verstreicht, wird Erkennungszeit genannt.
3. Diagnose: Der Dienstleister diagnostiziert die Incident-Ursache und stößt die Lösung an, um die Störung zu beheben. Dies korrespondiert mit den Aktionen im Incident Management und Problem Management. Die aufgewendete Zeit wird Reaktionszeit (Response Time) genannt.
4. Reparatur: Der Dienstleister schafft das Problem aus der Welt.
5. Wiederherstellung: In dieser Phase wird der Service wieder zur Verfügung gestellt.
6. Verwendung des Service: Die Zeit, in der der Service in vereinbarter Weise zur Verfügung gestellt wird.

Da die Ausfallzeit zum Teil von der Reaktionsgeschwindigkeit der IT-Organisation abhängt und beeinflussbare Aspekte darstellt, die deutliche Auswirkungen auf den Service und die Kundenzufriedenheit haben, sollten diesbezügliche Vereinbarungen in die SLAs aufgenommen werden. Es gibt immer geplante Zeiten der Nicht-Verfügbarkeit.

IT-Komponenten ohne Backupfähigkeit werden als „Single Point of Failure" bezeichnet und können Impacts verursachen. Diese Schwachstellen im System müssen identifiziert werden. Dazu können unterschiedliche Methoden eingesetzt werden.

Eine Möglichkeit besteht in der Component Failure Impact Analysis (CFIA). Diese Methode beruht auf einer Verfügbarkeitsmatrix, in der die für jeden Service strategisch wichtigen Komponenten festgehalten werden. Daneben existieren weitere mögliche Methoden, um Planungs-, Verbesserungs-, und/oder Reportingaktivitäten zu unterstützen. Bei der Fault Tree Analysis (FTA) kann die Kette von Ereignissen bestimmt werden, die zu einer Störung führen kann (*siehe Abbildung 14.5*). Die entsprechende Schemaerstellung beruht auf Boolescher Algebra. Weitere Techniken sind CRAMM (CCTA Risiko-Analyse und Management-Methode), SOA (System Outage Analysis) zur Ermittlung der Störungsursachen, Effektivitätsberechnung, Prozessuntersuchung zur Unterbreitung von Verbesserungsvorschlägen sowie TOP (Technical Observation Post), wobei hier die Konzentration auf einen Teilaspekt der Verfügbarkeit durch ein spezielles Team realisiert wird.

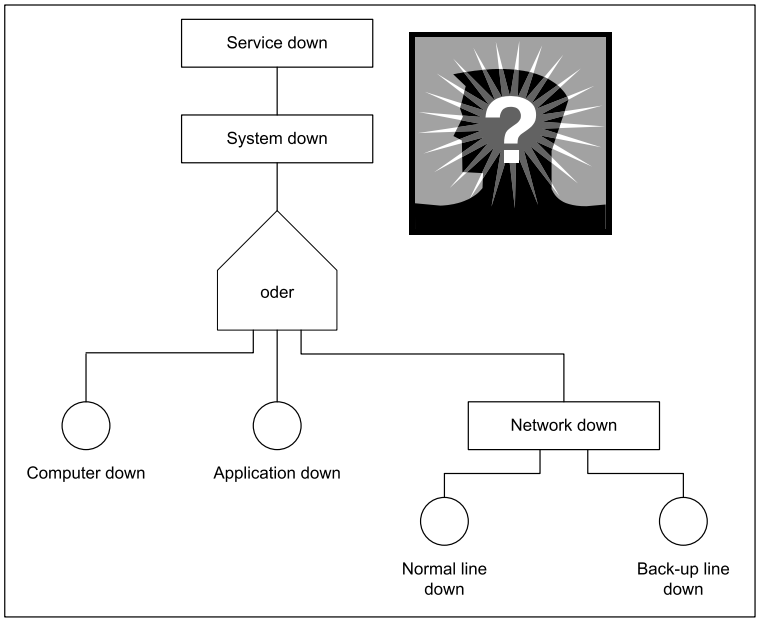


Abbildung 14.5: Suchen in einer Kette von Ereignissen, die einen Fehler verursacht haben können: FTA

Daneben können unterschiedliche Methoden zur kontinuierlichen Verbesserung eingesetzt werden. Um den hohen Anforderungen der Verfügbarkeit zu genügen, werden viele Komponenten von größter Wichtigkeit ausfallsicher implementiert. Diese werden z.T. redundant zur Verfügung gestellt und mit Fehlererkennungs- und Fehlerkorrekturmechanismen versehen, um möglichst schnell reagieren und das Problem beheben zu können. Häufig sind zusätzlich organisatorische Maßnahmen notwendig. All diese Anforderungen werden über die Einrichtung des Availability Management gewährleistet.

Der Verfügbarkeitsplan stellt ein Schlüsseldokument für das Availability Management dar. Er sollte die aktuellen Verfügbarkeitslevel gegenüber den geforderten Levels darstellen und die Aktivitäten benennen, die durchgeführt werden, um das angeforderte Verfügbarkeitsniveau zu erreichen und zu halten. Der Plan kann als eine Art Wachstumsdokument gesehen werden. Außerdem können die Planungen für neue Services und Richtlinien für die Wartungsaktivitäten aufgenommen werden. Auch möglichen technischen Entwicklungen sollte an dieser Stelle Rechnung getragen werden. Wenn es um fragliche Entscheidungen geht, sollte ein Kosten-Nutzen-Vergleich für alle Optionen stattfinden und einfließen, in denen Risiken und Benefits aufgezeigt werden. Geht es um Änderungen der Verfügbarkeit bestehender Services, sollten die Details zum Änderungsverfahren im Verfügbarkeitsplan zu finden sein.

14.3 Aufgaben und Aktivitäten des Availability Management

Das Availability Management umfasst das Design, die Implementierung, das Messen und die Verwaltung der Verfügbarkeit innerhalb der IT-Infrastruktur. Das Availability Management setzt ein, sobald die Anforderungen für einen IT Service festgeschrieben sind. Wie viele Prozesse aus dem ITIL-Umfeld ist dies ein fortschreitender Prozess, der im Grunde genommen erst endet, wenn dieser IT Service nicht mehr aktiv verlangt wird. Die Anforderungen spiegeln das entsprechende kosteneffektive und festgelegte Verfügbarkeitsniveau für die IT Services wider, mit dessen Hilfe das Unternehmen in der Lage ist, seine Ziele zu verwirklichen.

Damit die IT den Geschäftsbetrieb überhaupt unterstützen kann, müssen die Anforderungen des Unternehmens mit den Möglichkeiten, die die IT-Infrastruktur und die IT-Organisation bieten, umgesetzt werden können. Ist dem nicht so und die Anforderungen und Möglichkeiten driften auseinander, setzt das Availability Management an und schlägt seinerseits Lösungen vor. Um diesen Zustand unter Kontrolle zu halten, muss das aktuelle Verfügbarkeitsniveau gemessen und nötigenfalls verbessert werden. Der Prozess umfasst demnach sowohl proaktiv als auch reaktiv ausgerichtete Aktivitäten. Dies spiegeln auch die Eingangsdaten und Ergebnisse dieses Prozesses wieder (*siehe Abbildung 14.6*).

Abbildung 14.6: Der Prozess des Availability Management

Availability-Manager: Ein Hut im Availability Management

Für die Einrichtung und Steuerung des Prozesses muss die Rolle des Availability-Managers innerhalb der Organisation festgelegt werden. Seine Aufgaben bestehen zum Beispiel darin:

- den Availability Management-Prozess in der Organisation zu definieren und zu entwickeln,
- zu veranlassen, dass die IT Services so entworfen werden, dass die realisierten Service Levels (bezüglich Verfügbarkeit, Zuverlässigkeit, Servicefähigkeit, Wartbarkeit und Wiederherstellbarkeit) mit den vereinbarten Service Levels übereinstimmen,
- Berichte zu erstellen,
- die Verfügbarkeit der IT-Infrastruktur so zu optimieren, dass eine kosteneffektive Verbesserung der Services für das Unternehmen entsteht.

Die Aktivitäten drehen sich um Planung und Kontrolle der Verfügbarkeit:

1. Ermittlung der Verfügbarkeitsanforderungen von der Geschäftsseite für neu zu implementierende oder bereits bestehende Services (*siehe Abbildung 14.7*). Die Anforderungen müssen für die mit diesem Service zusammenhängenden Komponenten formuliert werden. Dies geht Hand in Hand mit den Wiederherstellungsoptionen und der Verfügbarkeit, wie etwa Wartungszeiträume, Downtime-Optionen oder mögliche Auswirkungen auf den Geschäftsbetrieb.

2. Risikoanalyse und Planung der Verfügbarkeit in Zusammenarbeit mit anderen Prozessen, wie beispielsweise mit dem Continuity Management. Die entworfenen Designkriterien hinsichtlich Verfügbarkeit, Zuverlässigkeit und Wartbarkeit werden einem kritischen Review unterworfen, um mögliche Schwächen möglichst früh zu erkennen und auszugleichen. Dadurch werden u.a. zu hohe Entwicklungskosten, unvorhergesehene Ausgaben, Single Points of Failure (SPOF), zusätzliche Kosten der Dienstleister und Lieferverzögerungen vermieden.

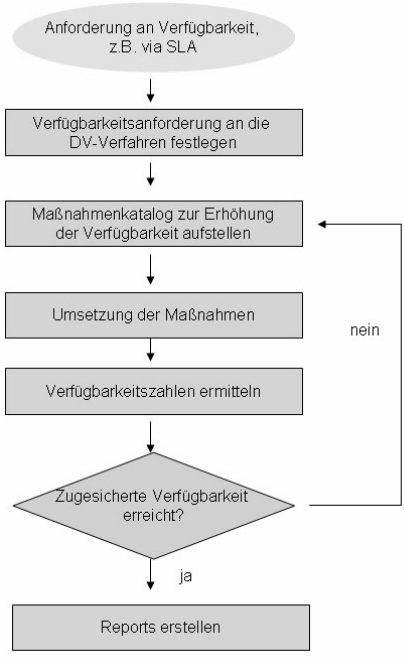


Abbildung 14.7:
Schematischer Prozessverlauf

Da eine hundertprozentige Verfügbarkeit kaum sicherzustellen ist, sollten Zeiten der Nicht-Verfügbarkeit berücksichtigt werden. Im Falle einer Störung des IT Service ist es wichtig, dass die Störung schnell erkannt und angemessen behoben wird, um die vereinbarten Verfügbarkeitsnormen zu gewährleisten. Daher müssen die entsprechenden Anforderungen in die Vereinbarungen in Form von SLAs und OLAs einfließen.

3. Monitoring: Aufstellung der Kriterien für Messung und Berichtswesen der Verfügbarkeit, Zuverlässigkeit und Wartbarkeit, das die Sichtweise von Business, Anwendern und der IT-Organisation widerspiegelt. Die geforderten Informationen bilden die Grundlage für die Kontrolle von SLAs, die Behebung von Problemsituationen und die Formulierung von Verbesserungsvorschlägen. Bei der Frage, was wie häufig gemessen werden soll, leistet das so genannte IT Availability Metrik-Modell (ITAMM) rudimentäre Unterstützung (*siehe Abbildung 14.8*). Zu bedenken ist allerdings nicht nur die Frage, was gemessen werden soll, sondern auch, wie es in Reportings kommuniziert wird. Je nach Zielprozess sind unterschiedliche Gewichtungen möglich. In Richtung Capacity Management können

beispielsweise Verfügbarkeitstrends dargestellt werden, die Sachverhalte zur Kapazität oder Antwortzeiten aufzeigen. In Richtung Sevice Level Management geht es um Informationen zu SLA- oder OLA-Aktivitäten.

4. Fehleranalyse: Nach Vorlage der Daten prüfen die Beteiligten die Ursachen und Verweise, die die geforderte Verfügbarkeit beeinträchtigt haben. Der Grund für ein unakzeptables Verfügbarkeitsniveau muss gefunden und beseitigt werden.
5. Availability-Prognose und Risikobewertung: Die Trend-Analyse spielt eine wichtige Rolle. Auf proaktiver Ebene sollen typische Ausfälle vorherzusehen und ein diesbezügliches Risiko zu bewerten sein. Das reine Messen der Verfügbarkeit reicht nicht aus.
6. Erstellung eines Verfügbarkeitsplans als wichtiges Ergebnis des Availability Management-Prozesses, das ständigen Reviews und Änderungen unterliegt

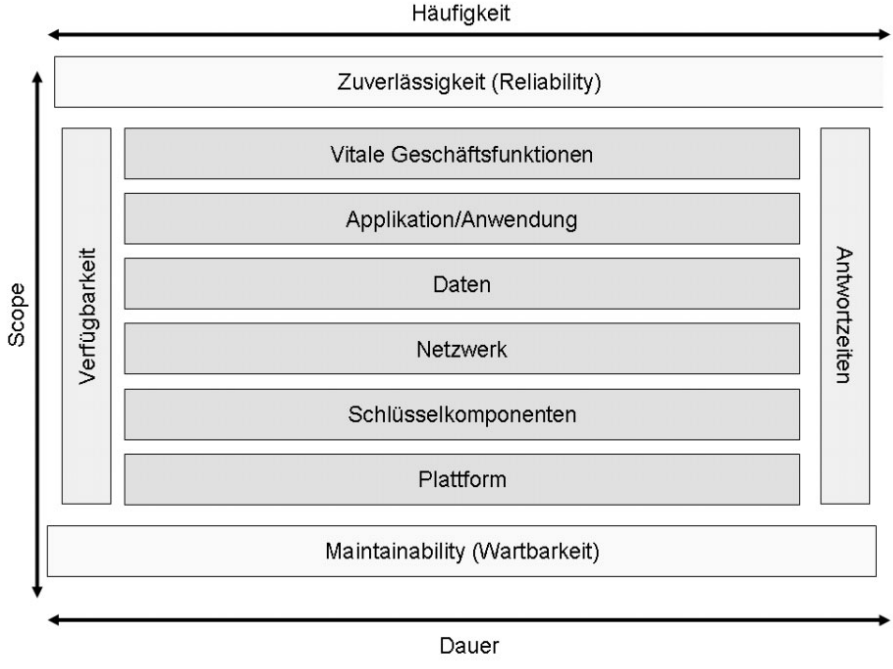


Abbildung 14.8: IT Availability-Metrik-Modell

7. Weitergabe von Reports: Diesbezüglich existieren drei Sichtweisen, die sich auf den IT-Support (Fokus auf Komponenten), den Anwender (Fokus auf Services) und/oder den Kunden (Fokus auf das Business) beziehen können.

14.4 Availability Management im ITIL-Gesamtzusammenhang

Viele Unternehmen können heute ohne ihre IT-Infrastuktur mit Anwendungen und Informationssystemen zur Unterstützung ihrer internen und externen Geschäftsprozesse (kurz: ohne ihre IT Services) nicht mehr existieren. Sie können es sich nicht einmal mehr leisten, auch nur für wenige Stunden auf die wichtigsten ihrer IT Services zu verzichten. Dies gilt beispielsweise für Zulieferer der Automobilindustrie. Wichtig für die Realisierung einer guten Servicekultur, die den ITIL-Gedanken unterstützt, sind einerseits Kenntnisse in Bezug auf den Kunden, den geschäftlichen Hintergrund und die IT-Infrastruktur. Andererseits spielen die ständige Optimierung der Verfügbarkeit und der Kundenzufriedenheit im Rahmen der Möglichkeiten eine wichtige Rolle. Fachwissen und Fähigkeiten des Personals, die Management-Prozesse und die ITIL-Verfahren unterstützen diesen Vorgang.

Wirksame Überwachungs-, Analyse- und Bericht-Systeme sollten für die Arbeit des Availability Management bereitgestellt werden. Dabei werden Berührungspunkte zum Configuration Management, dem Change Management und dem Problem Management berücksichtigt.

Behalten Sie stets im Hinterkopf, dass alle anderen ITIL-Prozesse die Verfügbarkeit beeinflussen. Dies kann in bi- oder in uni-direktionaler Richtung erfolgen, je nach Möglichkeiten und Anforderungen innerhalb der Organisation (*siehe Abbildung 14.9*).

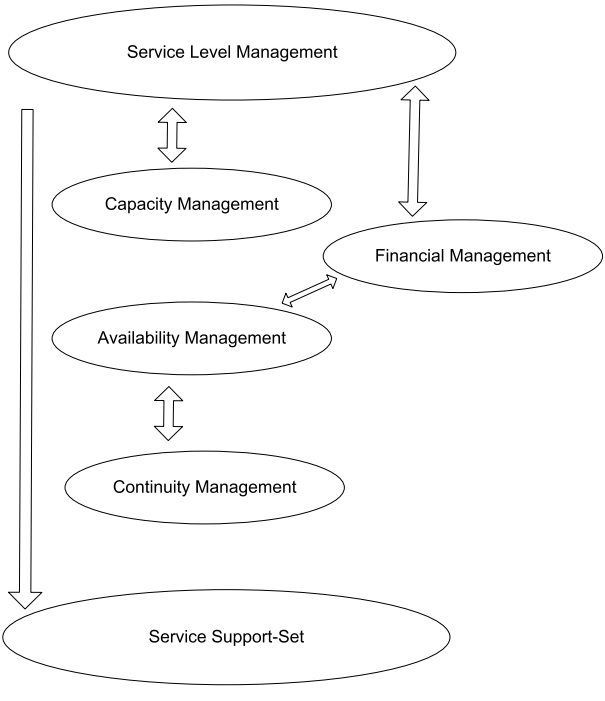


Abbildung 14.9: Zusammenwirken von Availability Management und weiteren ITIL-Prozessen

Das Configuration Management verfügt durch die CMDB über Informationen zur IT-Infrastruktur und deren Konfiguration. Sie stellt dem Availability Management so essenzielle Daten zur Verfügung. Hier dienen vor allem Auszüge aus der Datenbank für das Availability Management als Input, die bei der Vorhersage von Verfügbarkeiten, Filtern von Single Points of Failures (SPoF) oder Ausfindigmachen von Ansprechpartnern für bestimmte Komponenten helfen. Daneben stellt die CMDB eine wichtige Quelle für Informationen in Bezug auf Incidents, Probleme und Changes dar, die sich auf die Infrastruktur, einen Service oder einzelne Komponenten beziehen können.

Das Problem Management hängt unmittelbar am Incident-Lebenszyklus, da es für das Auffinden von Problemursachen zuständig ist und eine Behebung des Problems anstoßen muss. Auch das Incident Management ist in diese Tätigkeiten involviert, da Störungen zur Verfügbarkeit hier kommuniziert werden. Außerdem liefert der Prozess Berichte, die Daten über die Häufigkeit von bestimmten Fehlerklassen, Wiederherstellungszeiträume und die Reparaturdauer enthalten. Bei der Planung der Wartbarkeit spielt u.a. ein einwandfrei funktionierender Incident Management-Prozess mit den richtigen Eskalations-, Kommunikations-, Backup- und Wiederherstellungsverfahren eine wichtige Rolle. Aufgaben, Zuständigkeiten und Befugnisse sollten absolut klar sein.

Müssen Änderungen an den Verfügbarkeitsanforderungen zu einer Komponente oder einem Service und den damit zusammenhängenden technischen Maßnahmen umgesetzt werden, kommt das Change Management ins Spiel. Unter der Verantwortung dieses Prozesses werden die Änderungen realisiert, die im Rahmen der Verfügbarkeitsmaßnahmen notwendig sind. Andersherum informiert das Change Management das Availability Management über geplante Änderungen, die im FSC festgeschrieben werden.

Die Capacity Management Database (CDB) stellt Informationen zur Kapazitätsverwaltung der IT-Infrastruktur bereit. Diese Daten können das Availability Management unterstützen, indem Informationen zu geplanten Updates von Hard- und Software, Netzwerkkomponenten, Auslastung, Kapazität und Performance bereitgestellt werden. Kapazitätsanpassungen können die Verfügbarkeit eines Service beeinflussen. Andersherum wirken sich Verfügbarkeitsanpassungen auf die Kapazität aus. Beispielsweise liefert das Capacity Management in Bezug auf die Component Failure Impact Analysis (CFIA) relevante Daten, so dass das Availability Management weiß, wo gegebenenfalls Aktionen in Richtung Erhöhung der Fehlertoleranz notwendig sind.

Das Service Level Management nutzt die Reporting-Daten aus dem Availability Management, um dies in die Verhandlung bestehender SLAs einfließen zu lassen. Die Verfügbarkeit ist dabei eines der wichtigsten Themen. Andersherum liefert das Service Level Management Informationen zu den Anforderungen hinsichtlich der Verfügbarkeit einer Komponente oder eines Service.

Das Financial Management liefert Informationen zu den Kosten, die mit dem Upgrade eines Services oder einer IT-Komponente in Verbindung stehen, die einen höheren Grad an Verfügbarkeit bieten soll. Informationen für das Financial Management werden in Form von Kostendaten bereitgestellt bei der Frage, was die Nicht-Verfügbarkeit einer Komponente oder eines Services für das Unternehmen finanziell bedeutet. Dies dient u.a. der Rechtfertigung bei Budgetverhandlungen.

Als Input vom Continuity Management für das Availability Management dient die Bewertung der Auswirkungen auf das Business bezüglich der vitalen Geschäftsfunktionen in Abhängigkeit von der Verfügbarkeit (kritische Unternehmensprozesse). Dem Continuity Management werden Informationen zur Verfügbarkeit bereitgestellt.

Ein wichtiger Erfolgsfaktor für das Availability Management ist die Integration mit den IT Security-Prozessen. Sicherheit und Verfügbarkeit haben umfassende Wechselwirkung in der IT, Sicherheit und Zuverlässigkeit sind eng miteinander verknüpft. Ein schlechtes Konzept für die Informationssicherheit kann sich unmittelbar auf die Verfügbarkeit der Services auswirken. Ohne einen hohen Grad an Informationssicherheit lässt sich keine hohe Verfügbarkeit erreichen.

15 Continuity Management

Notfälle, Naturkatastrophen, unvorhersehbare Ereignisse wie der 11. September, also in Form eines Terrorangriffs, die Strom-Blackouts, mangelnde Vorkehrungen gegen Hackerangriffe und Virenattacken oder die Flutkatastrophen in Deutschland treffen Unternehmen oft und äußerst empfindlich. Sie verursachen neben weiteren Bereichen auch Schäden in der IT eines Unternehmens, ohne deren normale Nutzungsmöglichkeit fast allen Unternehmen der geschäftliche Exitus droht. Dem wirkt das Continuity Management für IT Services entgegen. Es hilft dem Geschäftsbetrieb, Risiken abzuschätzen und zu benennen, und ist dafür verantwortlich Vorsorge- und Notfallmaßnahmen zu organisieren. Erst wenn bekannt ist, worin das Risiko für das gesamte Unternehmen und nicht nur für die IT selbst besteht, kann in Vorsorgemaßnahmen und Maßnahmen im Zusammenhang mit einer möglichen Katastrophe investiert werden. Das Continuity Management trägt im Notfall entscheidend zum Überleben eines Unternehmens bei. Leider hat sich diese Ansicht noch nicht in allen Unternehmen durchgesetzt – genau so wenig wie die Investitionsbereitschaft in ähnliche Maßnahmen, die Risiko Management und Security tangieren. Hier gilt anscheinend der Leitsatz „Solange uns nichts passiert, müssen wir auch nicht aktiv werden." Die entsprechende Einsicht kommt leider oft zu spät. Ist erst einmal ein Notfall, eine Katastrophe oder ein ähnlich gelagertes, unvorhergesehenes Ereignis eingetreten, ist es fast immer zu spät. Dabei geht es nicht nur um die Gefahr eines möglichen Datenverlusts oder des Verlusts der IT-Infrastruktur in Teilen oder als Ganzes als finanziellem Verlust, sondern um den Verlust der Reputation. Das ist ein Grund, warum es so wenig Erfahrungswerte zu diesem Thema gibt. Niemand möchte zugeben, dass dem Unternehmen ein so eklatanter Verlust aufgrund von fehlender Planung bzw. Managementverschulden unterlaufen ist.

Doch mittlerweile scheint sich die Erkenntnis durchzusetzen, dass proaktive Vorsorge ein besseres Mittel ist als hilflose Nachsorge, um sich auf diese Geschehnisse so gut es geht vorzubereiten. Viele Unternehmen erkennen, dass Continuity Management kein Luxus, sondern zwingende Notwendigkeit ist – auch aufgrund der bestehenden gesetzlichen Anforderungen wie Basel II oder KontraG. Effiziente Geschäftsprozesse sind in der Regel ohne unterstützende IT Services nicht mehr denkbar. Aufgrund dessen hat sich der Aufgabenbereich Continuity Management von der IT bis in den Geschäftsbereich verlagert.

Das primäre Ziel besteht in der Sicherstellung von relevanten Service-Leistungen auch in Ausnahme- und Notfällen. Ein Notfall oder eine Katastrophe stellt ein unvorhersehbares Ereignis dar, gegen das sich die Betroffenen nicht schützen können. Beispiele sind Naturkatastrophen wie Schäden durch Blitz, Brand und Überschwemmungen. Entsprechend einer Risikoanalyse sind Szenarios zu entwerfen, schützenswerte IT Services zu identifizieren und im Bedarfsfall Maßnahmen zu ergreifen. Das Aufstellen eines IT Service Continuity-Plans soll gewährleisten, dass

bei Eintritt eines Notfalls kontrolliert und ohne Zeitverzug gehandelt werden kann, um Folgeschäden minimal zu halten und den Service innerhalb eines vereinbarten Zeitraums wiederherzustellen. Der Plan enthält ebenfalls eine klare Aussage darüber, wie und wann die darin aufgeführten Maßnahmen zum Einsatz gelangen.

15.1 Continuity Management nach ITIL

Für viele Manager ist das Continuity Management for IT Services (Kontinuitäts-Management, mancherorts auch als Contingency Management bezeichnet) immer noch ein Luxus. Es existieren jedoch Statistiken, aus denen deutlich hervorgeht, dass sich auch in Deutschland regelmäßig Katastrophen verschiedenster Ausprägung ereignen. Obwohl das Risiko eines totalen Verlustes klein ist, so besteht es doch, und nach einem solchen Ereignis ist es kein Trost zu wissen, dass die Wahrscheinlichkeit für dessen Eintreten eigentlich nur eins zu einer Million gewesen wäre.

Eine Katastrophe ist viel schwerwiegender als eine Störung. Ursachen für Katastrophen sind zum Beispiel Sabotage, Feuer, Blitzeinschlag, Wasserschaden, Einbruch, Vandalismus und Gewalt sowie weit reichende Stromstörungen und Gerätedefekte. Zudem sorgt das Internet bisweilen für Katastrophen, man denke nur an Denial of Service (DoS), die Erfolg haben und den eBusiness-Betrieb lahm legen. Die Überlegungen und Umsetzungen hinsichtlich einer Kontinuitätsplanung und deren Erstellung könnte vielen Unternehmen eine Menge Ärger ersparen. Wichtig ist, dass die IT und mögliche Katastrophen nicht isoliert betrachtet werden. Continuity Management muss auf verschiedenen Ebenen greifen: Business, Services, Ressourcen.

Da die IT Services und die damit verbundenen Prozesse den Geschäftsbetrieb unterstützen sollen, liegt der Fokus des Continuity Management auf der Unterstützung des übergeordneten Business Continuity Management (BCM). Dies geht Hand in Hand mit einem entsprechenden Risiko-Management und der Frage, wo die Risiken denn überhaupt liegen? Denn hier geht es um unvorhersehbare Ausfälle, die selten bis nie vorkommen. Daher existieren auch wenige Erfahrungen oder Messwerte zu der Risikoeinschätzung. Dies unterscheidet das Continuity Management vom Availability Management (*siehe Abbildung 15.1*).

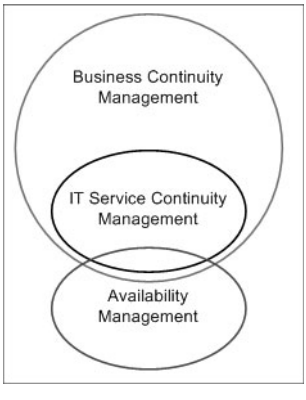


Abbildung 15.1:
Zusammenhang zwischen Business Continuity Management, IT Service Continuity Management und Availability Management

Business Continuity Management beinhaltet nicht nur rein organisatorische oder fachliche Aspekte. Nur wenn technische und nicht-technische Seiten betrachtet werden, können die Möglichkeiten des Continuity Management effektiv umgesetzt werden.

Der Risikoeinschätzung kommt hier eine entscheidende Rolle zu. Dies fängt allerdings nicht erst in der IT-Abteilung an, sondern setzt bereits im operativen Geschäft des Unternehmens an. Die beiden Bereiche Business Continuity Management (BCM) und Continuity Management für IT Services (ITSCM) arbeiten Hand in Hand, weil sich das Unternehmen der Abhängigkeit zwischen IT und Geschäftsprozessen bewusst ist.

- Das Business Continuity Management (BCM) beschäftigt sich mit der Analyse und dem Management der Risiken, damit die Organisation jederzeit die erforderliche Mindestproduktionskapazität und/oder den Mindestservice gewährleisten kann (*siehe Abbildung 15.2*). Hier geht es um Verhandlungen mit Geldgebern wie Banken, Verhandlungen zu Ausweichproduktionsstätten, Evakuierungsplänen, um das Festlegen von Verantwortlichkeiten und Rollen. Dieser Prozess ist bemüht, die Risiken auf ein akzeptables Maß festzulegen. Im Anschluss daran sind Maßnahmen und Pläne für die Wiederherstellung der geschäftlichen Aktivitäten aufzustellen, falls eine Unterbrechung der Geschäftsaktivität infolge einer Katastrophe entsteht. Das Business Continuity Management steht über dem IT Continuity Management und gibt die geschäftskritischen Anforderungen für die IT vor. Dabei geht es zuerst um die Ermittlung der geschäftskritischen Prozesse und die Schäden bei einer geschäftsrelevanten Service-Unterbrechung, die nicht ad hoc zu beheben ist (Business Impact-Szenario). Welche weiteren Faktoren existieren neben den IT Services wie Geschäftsunterlagen, Energieversorgung, Facilities oder Personal? Daneben ist auch zu ermitteln, welche zeitlichen Wiederherstellungsvorgaben für die Kernaktivitäten und eine Komplett-Wiederherstellung bestehen.

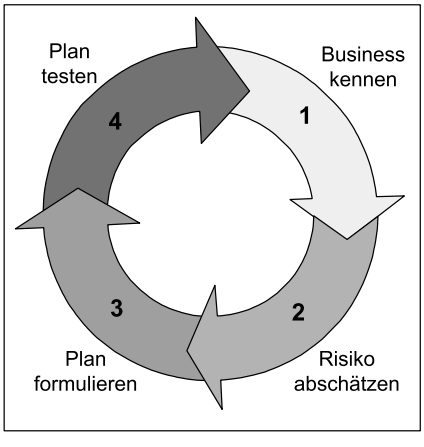


Abbildung 15.2:
Business Continuity Management

- Das Continuity Management für IT Services (ITSCM) ist der Prozess, der auf der IT-Seite Maßnahmen trifft, damit das Unternehmen seinen Betrieb fortsetzen kann. Die Maßnahmen dieses Prozesses leiten sich aus den Vorgaben des Business Continuity Management ab. Der Maßnahmenkatalog lässt sich in zwei Bereiche aufgliedern.

Zum einen geht es um die Beschränkung von Risiken, z. B. durch die Installation zuverlässiger Systeme mit einer hohen Fehlertoleranz, zum anderen um die Einrichtung von Wiederherstellungsmöglichkeiten, z.B. Backup-Systeme und redundante Systeme, deren aktiver Einsatz erst nach dem Eintreten eines Notfalls notwendig wird.

15.2 Aufgaben und Aktivitäten des Continuity Management

Die Aufgabe des Continuity Management besteht darin, die Wiederherstellbarkeit von IT Services nach einer Katastrophe (einem unvorhersehbaren Ereignis) bzw. einem großen Systemausfall innerhalb der vereinbarten Zeit kontrolliert sicherstellen zu können. Diese Anforderungen einschließlich der Notfalldefinition und die Ergebnisse einer entsprechenden Analyse und nachfolgenden Planung fließen in die SLAs ein. Dazu gehört auch das Durchführen von vorbeugenden Maßnahmen, um Ausfälle zu vermeiden bzw. Maßnahmen zur Wiederherstellung der Dienstleistungen nach dem Katastrophenfall zu definieren. Dazu werden zunächst die Risiken ermittelt und dann ein Continuity-Plan erstellt, der dem Change-Management unterstellt und regelmäßig getestet werden muss.

Das Continuity Management für IT Services lässt sich nach folgenden Aspekten unterteilen:

- Definition des Umfangs: Grundsätze, Schwerpunkte, Ressourcen, Projektierung
- Erfordernisse und Strategie: Business Impact-Analyse, Schwachstellenuntersuchung (*siehe Abbildung 15.3*), Bedrohungs- und Risikoanalyse (CRAMM), Mapping von Geschäftsprozessen auf Services und Komponenten, IT Service Continuity-Strategie („Kontinuitätsoptionen“)

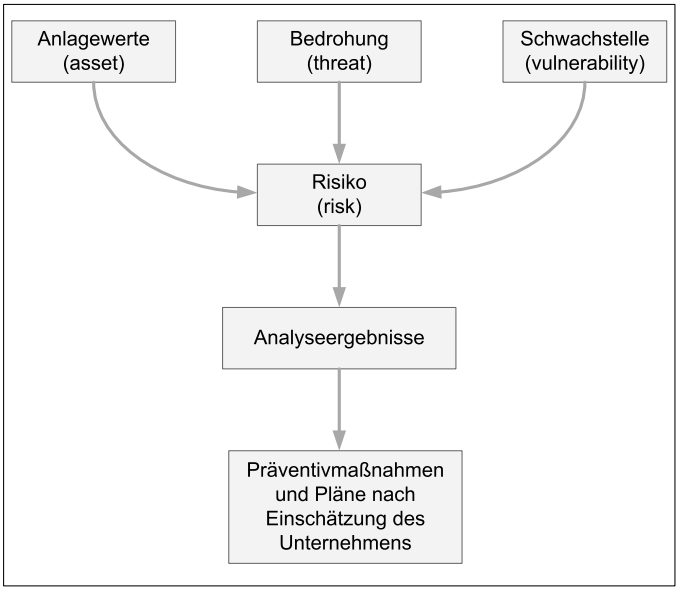


Abbildung 15.3: Begriffe des Continuity Management

- Implementierung: Planung (Organisation und Implementierung), Risikominimierung (Maßnahmen, Einrichtungen), Recovery-Pläne, Test (Prozesse und Pläne)
- Operatives Management: Training/Bewusstsein, Review und Audit, Test, Change Management, Qualitätskontrolle des Prozesses

Die Aktivitäten des Continuity Management lassen sich in folgende Schritte unterteilen:

1. Bei der Initiierung des ITSCM geht es darum, Rahmen und Umfang des ITSCM zu definieren, Verantwortlichkeiten und Ressourcen zuzuweisen und eine adäquate Projektplanung zur Implementierung des Prozesses festzulegen. Zu Beginn des ITSCM wird die gesamte Organisation einer genauen Prüfung unterzogen.

   Es ist erforderlich, möglichst frühzeitig Grundsätze auszuarbeiten und diese in der gesamten Organisation bekannt zu machen, damit alle betroffenen Personen und Instanzen die Notwendigkeit eines ITSCM erkennen und verstehen. Auf der Grundlage der Bedingungen, die eventuell durch eine Versicherung, durch die gültigen Qualitätsnormen (ISO 9000) und die Normen für das Security Management (BS 7799), die übergeordneten Unternehmensgrundsätze u.ä. vorgegeben werden, wird das Vorgehen festgelegt und die anzuwendenden Methoden für die Risiko-Analyse und die „Business Impact Analysis" ausgewählt. Die Einrichtung einer ITSCM-Umgebung erfordert eine erhebliche Investition an Arbeitskräften und Anlagen.

2. Definition von Anforderungen und Strategien mittels Expertenbeurteilungsverfahren oder empirischen Befragungsmethoden: Eine Hauptaufgabe des Continuity Management besteht darin, eine Bedrohungsanalyse für die Geschäftsprozesse durchzuführen (Business Impact-Analyse, BIA). Auf diese Weise wird herausgefunden, welche der geschäftskritischen Services einem Risiko unterliegen oder eine Schwachstelle darstellen und welche CIs mit den kritischen Geschäftsprozessen zusammenhängen. Mögliche Auswirkungen werden pro Geschäftsprozess untersucht, um festzustellen, welche den größten Einfluss auf den Geschäftsbetrieb und das Fortbestehen des Unternehmens haben. Darüber hinaus ist es wichtig, vorab zu klären, wieviel und was die Organisation bei einer schwer wiegenden Unterbrechung des Service zu verlieren hat. In der Praxis müssen die Unternehmen oft einen Kompromiss zwischen Kosten und Wünschen eingehen, was die Auswahl kritischer Services betrifft. Auch die Frage nach einer entsprechenden Versicherung wäre zu klären. Die Business Impact-Analyse identifiziert in der Regel nur das Minimum der kritischen Anforderungen zur Unterstützung des Geschäftsbetriebes.

   Auch die spezifisch angebotenen Services werden untersucht (Service-Analyse). Eine Anpassung der Service Levels an eine Ausweichsituation kann nur nach Rücksprache mit dem Kunden beschlossen werden. Für kritische Services gilt wiederum die Überlegung, ob Präventivmaßnahmen erforderlich sind oder ob nach Wiederherstellungslösungen gesucht werden soll. Dieselben Überlegungen gelten auch für die IT-Infrastruktur. Hier werden die Abhängigkeiten zwischen Services und IT-Komponenten näher untersucht. Zu diesem Zweck wird mit Hilfe der Daten aus dem Availability Management eine Analyse durchge-

führt, welchen der IT Services eine kritische Funktion zukommt (*siehe Abbildung 15.4*). Das Capacity Management liefert Informationen zu den benötigten Kapazitäten. Diese Informationen werden später für die Festlegung der Kontinuitätsoptionen pro Service herangezogen.

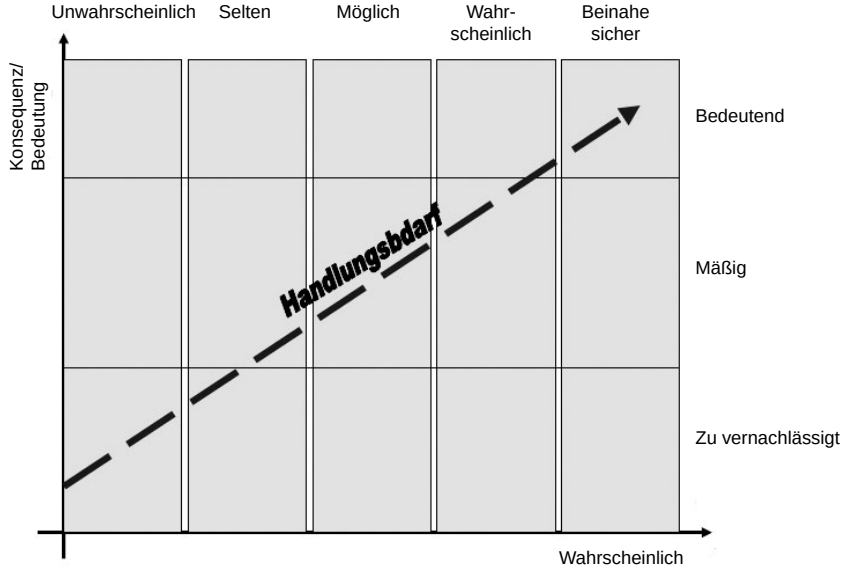


Abbildung 15.4: Schwachstellen-Analyse

Um insgesamt zu eruieren, welchen Risiken ein Unternehmen ausgesetzt ist, empfiehlt es sich, eine Risiko-Analyse vorzunehmen. Hier geht es darum, herauszufinden, mit welcher Wahrscheinlichkeit ein bestimmter Katastrophenfall eintreten kann und wie die Bedrohungen für das Unternehmen aussehen. Neben der Frage nach den Risiken an sich geht es auch um die Einstufung von Schwachstellen. Das Ziel ist die Aufstellung eines Kontinuitätsplans und daraus resultierend die Definition von Gegenmaßnahmen. Nach der Identifizierung der Betriebsmittel erfolgt eine Analyse der Bedrohungen und Abhängigkeiten sowie die Berechnung der Wahrscheinlichkeit (hoch, mittel, gering) für das Eintreten einer Katastrophe. Danach werden die Schwachstellen genauer untersucht. Auch ihnen wird ein Wert zugeordnet (hoch, mittel, gering); Schließlich werden die Schwachstellen und Bedrohungen für den IT-Bereich gegeneinander abgewogen. Hieraus ergibt sich die Einschätzung der Risiken.

Die Risikobewertung, die Analyse der IT-Komponenten und deren Stellenwert sowie die Wahl der Kontinuitätsoptionen können mit Hilfe der CCTA-Risiko-Analyse-Management-Methode (CRAMM) vorgenommen werden, die auch im Availability Management Verwendung findet.

3. Für die Implementierung muss zwischen Risikobegrenzung, Wiederherstellung geschäftlicher Aktivitäten und IT-Wiederherstellungsoptionen unterschieden werden. Dabei geht es auch um die Abgrenzung von Risikobegrenzung (Prävention) und Wiederherstellungsplanung (Kontinuitätsoptionen). Auf Grundlage

der Risikoübersicht können unter Berücksichtigung der Kosten und Risiken Präventivmaßnahmen ergriffen werden. Ziel dieser Maßnahmen kann es ein, sowohl die Wahrscheinlichkeit als auch die Auswirkungen von Katastrophen zu verringern und damit den Umfang eines Kontinuitätsplans zu begrenzen. Hier fließen als Faktoren die finanzielle Bewertung der möglichen Maßnahmen, die Vor- und Nachteile der Optionen und der Umfang der nötigen Ressourcen zur Umsetzung der Planung ein (*siehe Abbildung 15.5*).

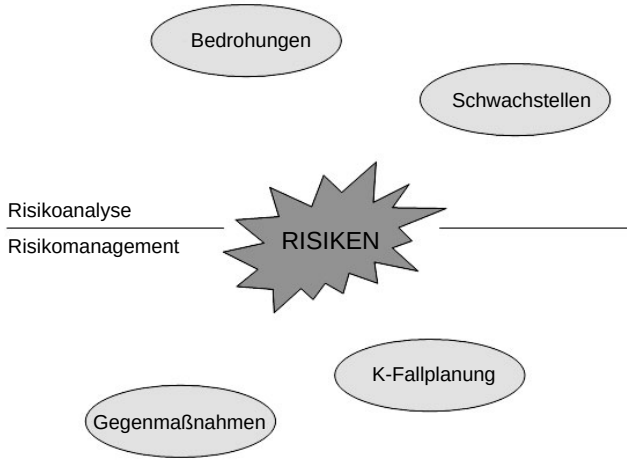


Abbildung 15.5: Risikoanalyse und -bewertung

Die Möglichkeiten reichen von der höchsten Form der Prävention als „Fortress Approach", die sich als Vorgehen darstellt, um nahezu sämtliche Schwachstellen zu beseitigen (unterirdisches Rechenzentrum mit eigener Strom- und Wasserversorgung), bis hin zu lediglich rudimentären Ansätzen.

Da niemals alle Risiken durch Präventivmaßnahmen abgedeckt werden können, sollte eine Kontinuitätsplanung erfolgen. Um das Fortbestehen des Unternehmens im Katastrophenfall gewährleisten zu können, muss für einige Bereiche eine Ausweichmöglichkeit gefunden werden (Menschen, Ausstattung, Facility-Dienste wie Strom, Wasser und Archivmaterial). Für eine rasche Wiederherstellung des IT Service stehen einige Optionen zur Auswahl. Diese werden auch Kontinuitätsoptionen genannt:

- Nichts tun: Wer diese Option wählt, sollte sicher sein, dass er auch ohne EDV seinen Betrieb weiterführen kann. Diese Option wird nur selten angewandt, weil nur wenige geschäftliche Prozesse ohne IT funktionieren. Hier gilt: Daumen drücken, beten oder sich einfach in sein Schicksal ergeben.
- Manueller Rückgriff: … zurück zu Karteikasten und Rechenschieber: Diese Möglichkeit ist für die geschäftskritischen Services meist nicht mehr durchführbar, weil es heutzutage nicht mehr genügend Mitarbeiter gibt, die über die notwendige Erfahrung verfügen, um auf manuelle Systeme zurückgreifen zu können (ohne IT). Zudem sind die in der Vergangenheit üblichen Systeme oftmals nicht mehr vorhanden. Für einige kleinere, weniger wichtige Services ist ein Ausweichmanöver vielleicht möglich.

- Wechselseitiges Abkommen (Reciprocal Agreement): Diese Option kommt zum Einsatz, wenn zwei Organisationen eine ähnliche IT-Landschaft besitzen und über eine Kooperation gemeinsam beschließen, sich im Notfall gegenseitig mit Kapazitäten auszuhelfen (eher für dezentrale Datenlagerung möglich). Mögliche Änderungen der IT-Infrastruktur müssen stets aufeinander abgestimmt werden.
- Allmähliche Wiederherstellung (Gradual Recovery, Cold Standby): Diese Option eignet sich für Unternehmen, die über einen längeren Zeitraum (z.B. 72 Stunden) ohne IT Service funktionsfähig sind und einen langsamen Wiederaufbau planen. Die Option besteht aus einer leeren Computerumgebung (mit Energieversorgung, Anschlüssen, Kabeln, Facitlity) ohne IT-Equipment. Der Standort muss in ständiger Verfügbarkeit bereitstehen. Diese Kontinuitätsoption existiert als lokal, portabel, mobil oder fest installiert (mit Dienstleisterunterstützung).
- Zügige Wiederherstellung (Intermediate Recovery, Warm Standby): Diese Option bezieht sich auf den Zugang zu einer vergleichbaren operativen Umgebung, in der nach einer Anlaufzeit (24 bis 72 Stunden) die Services wie vereinbart wieder aufgenommen werden können. Dies kann beispielsweise durch den Schwenk auf eine Referenz- oder Testumgebung realisiert werden, die aber meist nur reduzierte Kapazität und Leistung aufweist. Mutual Fallback bezeichnet das Umschalten auf diese internen Ausweichmöglichkeiten. Daneben sind für diese Option die Varianten intern/extern und mobil möglich. Diese Variante kann über eine feste Lokation oder eine mobile Option (Aufleger) genutzt werden.
- Sofortige Wiederherstellung (Immediate Recovery, Hot Standby): Ziel dieser Option ist eine unmittelbare bzw. sehr schnelle Wiederherstellung (weniger als 24 Stunden) des Service mit Hilfe einer duplizierten Produktionsumgebung sowie der Spiegelung von Daten. Diese Form wird in vielen Firmen über ein Ausfallrechenzentrum bereitgestellt.

Die allgemeine Planung (Notfall-, K-Plan, Krisenmanagement), Präventivmaßnahmen (USV, RAID), Standby-Absprachen, Schulung und Informationen lassen sich hier integrieren bzw. laufen parallel.

4. Implementierung: Dieser Schritt beinhaltet die Umsetzung der Planung und die Einrichtung des Continuity Management-Prozesses. Dazu zählen auch organisatorische Maßnahmen wie etwa das Einrichten eines Teams und weiterer Ansprechpartner unter der Führung des Managements (Krisenmanager). Auf der obersten Ebene sollte ein Gesamtplan mit Katastrophenplan, Schadensbeurteilungsplan, Wiederherstellungsplan, Vital Records Plan (für die kritischen Geschäftsprozesse) sowie Krisenmanagement und PR-Plan (Public Relations) genehmigt werden. Zusammen mit dem Availability Management werden Präventivmaßnahmen und Wiederherstellungsoptionen getroffen. Die Einbeziehung und die Unterstützung durch das oberste Management sind wichtig für das allgemeine Problembewusstsein und die Sensibilisierung im Unternehmen.

Die Pläne sollten detailliert ausgearbeitet sein und einen formalen Charakter besitzen. Des Weiteren sollte beachtet werden, dass ein Kontinuitätsplan laufender Pflege unterliegen muss. Notwendige Änderungen müssen von den betroffenen Personen und Instanzen genehmigt und kommuniziert werden. Hier ist streng darauf zu achten, dass die IT Continuity-Maßnahmen mit den Business Continuity-Maßgaben abgestimmt werden.

Im Mittelpunkt steht das Ausarbeiten, Prüfen und Pflegen eines Kontinuitätsplans, der genügend Einzelheiten enthält, um eine Katastrophe zu überleben und den normalen Service (termingerecht) wiederherstellen zu können (*siehe Abbildung 15.6*). Dieser Plan beinhaltet Verantwortlichkeiten und die Auflistung des Notfall-Teams, eine Checkliste bzw. Anweisungen zum vereinbarten Verfahren, allgemeine Anweisungen und Dokumente (Fluchtpläne, Sammelpunkte, etc.) und die Recovery-Strategie für die Kontinuitätsoption.

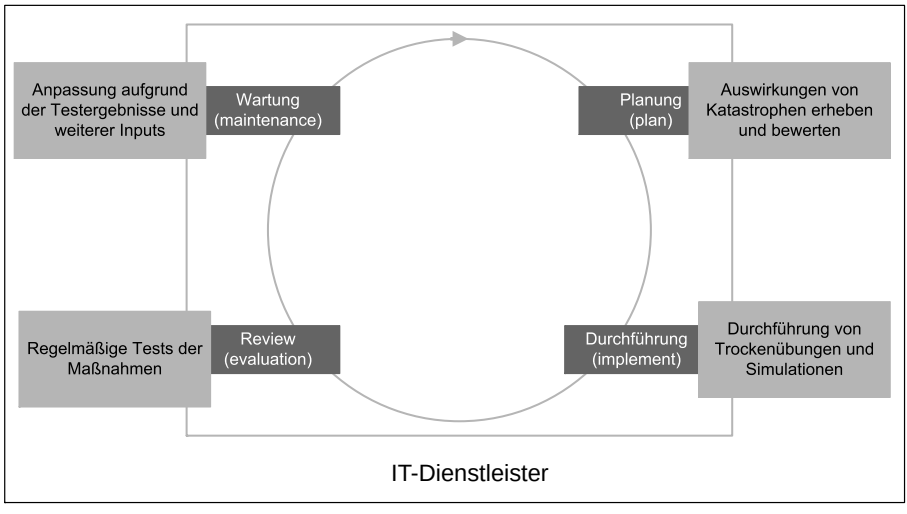


Abbildung 15.6: Aktvitäten-Einteilung im Continuity Management

5. Betrieb und Prozesssteuerung: Ein wirksamer Continuity-Plan sollte umfassend entwickelt und getestet sein. Er muss den Bedürfnissen entsprechen sowie die Zustimmung und Akzeptanz der Mitarbeiter aufweisen. Schulungen sollten sicherstellen, dass alle Mitarbeiter über den Prozess informiert werden. Alle Mitarbeiter müssen über ausreichende Kenntnisse verfügen, um an einer Wiederherstellung unterstützend mitwirken zu können, bzw. wissen, wie sie sich in einem Katastrophenfall zu verhalten haben. Darüber hinaus sind Übungen und Schulungen im Hinblick auf eine Kontinuitätssituation ebenfalls anzuraten.

   Die Pläne sollten regelmäßig auf ihre Aktualität hin überprüft und getestet werden (*siehe Abbildung 15.7*). Tests können auch bereits während der Entwurfsphase stattfinden. Für die IT ist ein solches Audit bei jeder wichtigen Änderung innerhalb der IT-Infrastruktur erforderlich. Nachdem eine Änderung der Strategie der IT oder des Unternehmens beschlossen wurde, sollte ebenfalls ein Audit durchgeführt werden. Wenn die Pläne und die Strategie angeglichen werden, fällt die Durchführung dieser Anpassung wieder unter die Regie des Change Management. Die Empfehlung lautet, dass bei der Erstellung, jährlich und nach jedem signifikanten Change eine Überprüfung unter realistischen Bedingungen stattfinden sollte.

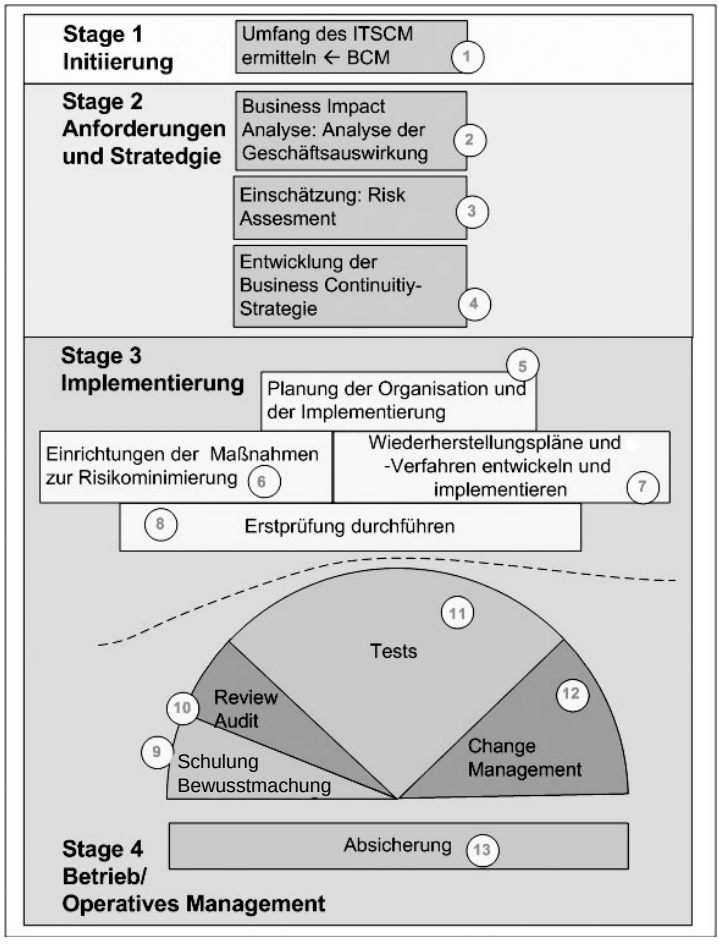


Abbildung 15.7: Schritte im Continuity Management-Prozess

Im Rahmen der Kontrolle wird bestimmt, ob die Qualität des Prozesses (Verfahren und Dokumente) den Anforderungen der geschäftlichen Seite des Unternehmens genügt. Hierfür sollten vorher Erfolgskriterien und Kennzahlen festgelegt werden.

Für eine optimale Prozesssteuerung sind Berichte des Managements, kritische Erfolgsfaktoren und Leistungsindikatoren wichtig. Wenn sich eine Katastrophe ereignet hat, wird selbstverständlich ein Bericht über die Ursache und die Folgen sowie über das reaktive Vorgehen bzw. dessen Erfolg erstellt. Dies gilt auch für Simulationen in einer Testsituation. Mängel, die sich in der Vorgehensweise gezeigt haben, führen dann zu Verbesserungsplänen für die übrigen Einrichtungen. Das Managementberichtswesen dieses Prozesses besteht darüber hinaus u.a. aus Auswertungsberichten über die Tests, die hinsichtlich des Recovery-Plans ausgeführt werden.

Der Mehrwert des Continuity Management sollte offensichtlich sein. Neben dem geschäftlichen Überleben einer Katastrophe durch Risikobeherrschung haben auch die Punkte der Kostenersparnis, die Erfüllung gesetzlicher Bedingungen (wie etwa Basel II und KonTraG) oder das Kunden- und Partnervertrauen ihre Berechtigung innerhalb der Überlegungen zur Implementierung dieses Prozesses.

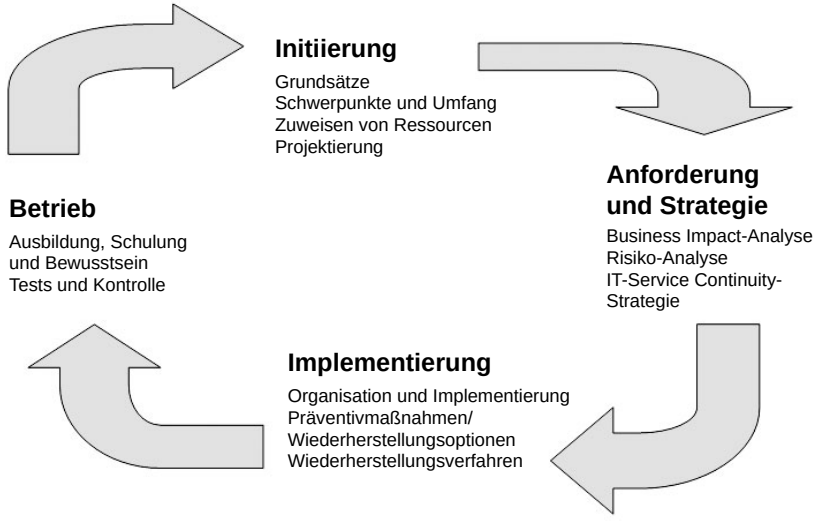


Abbildung 15.8: Kreislauf des Continuity Management

Ohne Einführung und Akzeptanz von Configuration Management und Change Management neben dem Continuity Management lassen sich die Anforderungen zur Implementierung, um eine kontrollierte und definierte Wiederherstellung zu realisieren, nicht umsetzen. Auch das Bewusstsein und die Schulungsmaßnahmen innerhalb des Unternehmens in Bezug auf dieses Thema spielen eine wichtige Rolle, ebenso wie das Testen der Pläne.

15.3 Continuity Management im ITIL-Gesamtzusammenhang

Neben der Verbindung zum Management des Unternehmens besitzt das IT Continuity Management Schnittstellen zu den anderen ITIL-Prozessen.

Das Service Level Management betont die Verpflichtungen, die bezüglich eines IT Service eingegangen wurden. Dies bezieht sich auch auf das Thema Wiederherstellung von Komponenten. Die Anforderungen bezüglich der Wiederherstellung der IT Services im Katastrophen- oder Notfall werden in den SLAs definiert.

Das Availability Management unterstützt das ITSCM, indem es Präventivmaßnahmen entwickelt und implementiert. Die beiden Prozesse arbeiten eng zusammen und tauschen ihre Informationen zu den jeweiligen Komponenten und IT Services aus.

Das Configuration Management verfügt durch die CMDB über ein modellhaftes Abbild der Infrastruktur, seiner Komponenten und Services. Das Continuity Management erhält hier Daten über die CIs und ihre Beziehungen als Soll-Situation nach einer Katastrophe. Die CMDB dient so in ihrer Gesamtheit als Baseline der gesamten Infrastruktur, auch wenn sich das Continuity Management nur auf die in den SLAs definierten Anforderungen stützt. Für die Katastrophe muss die CMDB verfügbar sein.

Das Capacity Management sorgt dafür, dass die Business-Anforderungen durch vorhandene IT-Ressourcen umgesetzt werden können. In Bezug auf das Continuity Management gilt dies vor allem für die Beschaffung und den Einsatz von Präventivmaßnahmen.

Das Change Management trägt dafür Sorge, dass die Continuity-Pläne stets auf dem neuesten Stand sind, indem es das Continuity Management in Bezug auf alle Änderungen einbezieht, die sich auf die Präventivmaßnahmen oder die Kontinuitätspläne auswirken können. Nach entsprechenden Changes müssen die Notfallpläne erneut einer Prüfung und einem Test unterzogen werden, um sicherzustellen, dass die Veränderungen entsprechend verarbeitet wurden. Für jede Änderung sollte untersucht werden, in welchem Maße sie sich auf die Recovery-Pläne auswirkt.

16 Capacity Management

Das Capacity Management kümmert sich darum, dass notwendige Kapazitäten bezüglich der IT Services zum richtigen Zeitpunkt zur Verfügung stehen. Dieser Prozess des Service Delivery-Bereiches zielt darauf ab, die benötigten IT-Ressourcen optimal zu nutzen und innerhalb des gegebenen und optimalen Finanzrahmens die Geschäftsziele zu erreichen. Aus diesem Grund muss das Capacity Management sicherstellen, dass die für die IT Services vorgehaltenen Kapazitäten den SLAs gerecht werden. Das Capacity Management richtet seine besondere Aufmerksamkeit auf heutige und zukünftige IT-Kapazitätsanforderungen und stellt diese plattformübergreifend sicher. Wichtig ist, dass rasch auf Veränderungen reagiert werden kann, um Kapazitätsprobleme im vorhinein zu vermeiden. Dabei spielt die Zuverlässigkeit der Prognosen in Bezug auf die aktuelle und zukünftige Nutzung der IT Services eine wichtige Rolle. Kenntnisse über die Zusammenhänge in der Infrastruktur und deren Kostenverhalten helfen bei der Einschätzung. Außerdem müssen die Zusammenhänge zwischen Störungen, Problemen und Kapazitätsmerkmalen von Komponenten verstanden werden. Nur dann ist eine adäquate technische Ausrichtung des Unternehmens möglich. Den aktuellen und zukünftigen Anforderungen entsprechend müssen die jeweiligen Betriebsmittel zur Verfügung stehen. Dabei spielen unterschiedliche Faktoren eine Rolle: Die benötigten Ressourcen müssen in ausreichender Menge/Volumen bereitstehen und zudem am richtigen Ort, zum richtigen Zeitpunkt und zum optimalen Preis bezogen werden können. Hier ist neben der Ausrichtung auf die momentane Situation das Erkennen von Trends und Zyklen der Ressourcenauslastung überaus wichtig. Die Systeme müssen immer wieder den aktuellen Entwicklungen angepasst werden.

Kapazitätsprobleme dürfen nicht erst in Angriff genommen werden, wenn Performanceprobleme auftreten. Neben den technischen Anforderungen ist auch der Blick auf die betriebswirtschaftliche Seite essenziell. Das Kapazitätsmanagement muss in der Lage sein, wirtschaftliche Entscheidungen zu treffen und Anforderungen zu formulieren, die eine Optimierung der benötigten IT-Ressourcen ermöglichen. Dieser Prozess liefert Vorschläge und Anmerkungen für kapazitätskritische Änderungen. Es ist Aufgabe des Capacity Management, Tipps und Kennwerte zu liefern, um korrekte Zusatzinformationen für die Erweiterung der Infrastruktur bereitzustellen.

Da die Analysen kontinuierlich zu erbringen sind und Entscheidungen im Rahmen von Änderungsprozessen oft schnell getroffen werden, muss sich das Capacity Management eigener Instrumente und Verfahren bedienen, um diesen Anforderungen gerecht zu werden. Dazu wird i.d.R. auch der Aufbau einer Capacity-Datenbank (CDB) gehören, die eng mit dem Configuration Management verknüpft ist. Dies betrifft aber auch Automatismen für Messungen und Trendanalysen. Dies ist besonders für ein proaktives Capacity Management wichtig.

16.1 Capacity Management nach ITIL

Dieser Prozess kümmert sich um die Gewährleistung der Kundenanforderungen bezüglich der Infrastruktur-Ressourcen und IT Services durch rechtzeitige und kostengünstige Bereitstellung der erforderlichen Betriebsmittel. Treibende Kraft sind stets der Kunde und seine Bedürfnisse, wobei der Kunde allerdings keine spezifischen Kapazitätsanforderungen in Bezug auf Hardware oder Software stellt, sondern Services benötigt, um seine geschäftlichen Bedürfnisse umzusetzen und den Erfolg des Unternehmens voranzutreiben.

Das Capacity Management erstellt aus den Geschäftsanforderungen den Kapazitätsplan und überwacht dessen Einhaltung. Dabei wird in Business, Service und Ressource Capacity Management unterschieden. Weitere Aufgaben sind Application Sizing, Tuning, Service-Modellierung und Bedarfsmanagement (Demand Management), die in unterschiedlicher Ausprägung in den drei Subprozessen zum Einsatz kommen.

Die IT Services, die mit den Kunden in Service Level Agreements (SLAs) festgelegt sind, müssen jederzeit gewährleistet sein. Dazu wird eine Management-Funktion benötigt, die sich direkt mit den heutigen und zukünftigen Anforderungen an die Menge und Leistungsfähigkeit der Ressourcen auseinandersetzt. Sie stellt sicher, dass die Dienstleistungen rechtzeitig und mit minimalen Kosten erstellt und ausgeliefert werden. Die Aktivitäten im Capacity Management ermöglichen dem Unternehmen, die bestehenden Kapazitäten wirtschaftlich und effektiv einzusetzen. Es liefert zudem wertvolle Entscheidungsunterlagen zur Planung der IT-Infrastruktur.

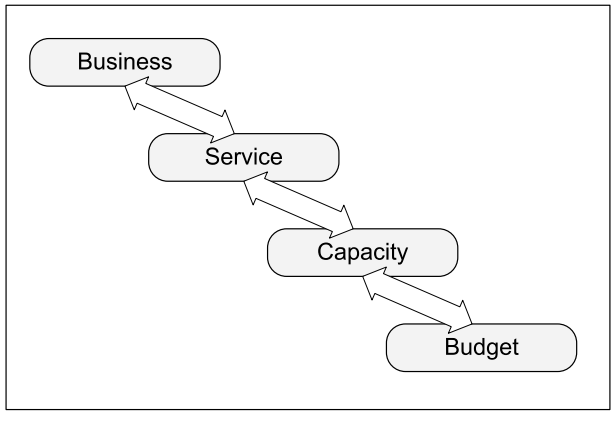


Abbildung 16.1: Zusammenspiel zwischen Business und IT

Das Capacity Management stellt im Grunde genommen eine Art Vermittlerrolle dar. Durch sie soll eine Balance zwischen Kosten und Kapazität sowie Angebot und Nachfrage in Bezug auf die Unternehmens-IT geschaffen werden (*siehe Abbildung 16.1*). Das Hauptziel des Capacity Management ist das Erreichen einer anforderungsgerechten Serviceleistung mit minimalen Kosten. Das Optimum heißt in diesem Zusammenhang nicht zu früh, nicht zu spät, nicht zu wenig, nicht zu viel, an den richtigen Stellen. Es dürfen weder zu hohe Kosten entstehen noch Ressourcen ausfallen oder Services beeinträchtigt werden. Daraus ergibt sich ein ständiger

Balanceakt. Aus diesem Grund ist es unvermeidbar, in einem gewissen Rahmen Überkapazitäten zur Verfügung zu stellen, um im Bedarfsfall rasch auf das Überschreiten eines Ressourcenverbrauchs reagieren zu können. Die Kosten, die durch Beeinträchtigung oder gar Ausfall eines Services entstehen, sind in der Regel um ein Vielfaches höher als die eingesparten Kosten.

Das Capacity Management versucht deshalb, unüberlegte Käufe und Überraschungen zu verhindern, indem verfügbare Mittel besser genutzt, rechtzeitig erweitert oder an das Nutzungsverhalten angeglichen werden. Zudem kann es dazu beitragen, dass die Kapazitäten der unterschiedlichen Bereiche eines Service gut aufeinander abgestimmt sind, damit teure Investitionen in bestimmte Komponenten auch adäquat genutzt werden. Dabei ist zu berücksichtigen, dass die Kosten nicht alleine von der direkten Investition abhängen, sondern auch stark von dem entsprechend damit zusammenhängenden Verwaltungsaufwand und den Servicekosten.

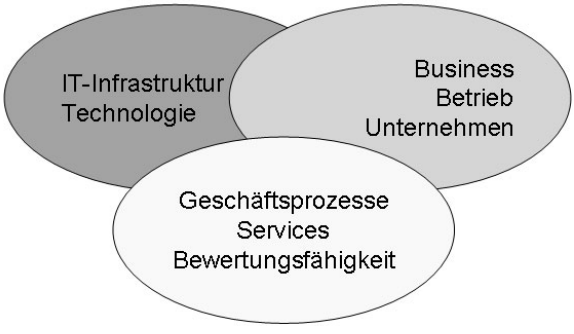


Abbildung 16.2: Unterschiedliche Anforderungen an das Capacity Management

Mit der Einrichtung eines Capacity Management kann die IT-Organisation jedoch zu hohen Investitionen, Überkapazitäten sowie Adhoc-Anpassungen der Kapazität vorbeugen, denn insbesondere Letzteres wirkt sich ungünstig auf die Qualität des IT Service aus. So hat zum Beispiel ein Wildwuchs von Speicherkapazität Folgen für die Erstellung von Sicherungskopien auf Bändern und für die Geschwindigkeit der Suche (Browsing) nach Dateien, die im Netzwerk gespeichert sind. Daraus ergibt sich die Notwendigkeit, dass das Capacity Management teils als reaktiv (Unterstützung bei kapazitätsbedingten Incidents und Problemen), teils als proaktiv (Vermeidung zukünftiger Kapazitätsengpässe) anzusehen ist. Dabei gilt: Je erfolgreicher die proaktiven Tätigkeiten im Capacity Management verlaufen, desto weniger Bedarf entsteht überhaupt an reaktiven Aktionen.

16.2 Begriffe des Capacity Managements

Um die mit den Kunden vereinbarten Service Level dauerhaft zu erfüllen, erscheint eine konsistente und nachhaltige Kapazitätsplanung als essenziell. Dabei geht es aber nicht nur um eine rein technische Sicht auf die technischen Bedürfnisses des Unternehmens, sondern auch um die Sicht auf die zugrunde liegenden Geschäftsprozesse, denen die Anforderungen entstammen. Diese bestimmen die Rolle und

Effektivität des Capacity Management. Für das Capacity Management sind Informationen über die Business-Strategie und den damit verbundenen Business-Plan und die IT-Strategie von wesentlicher Bedeutung. Daraus ergibt sich eine Dreiteilung des Capacity Managementsprozesses (*siehe Abbildung 16.3*).

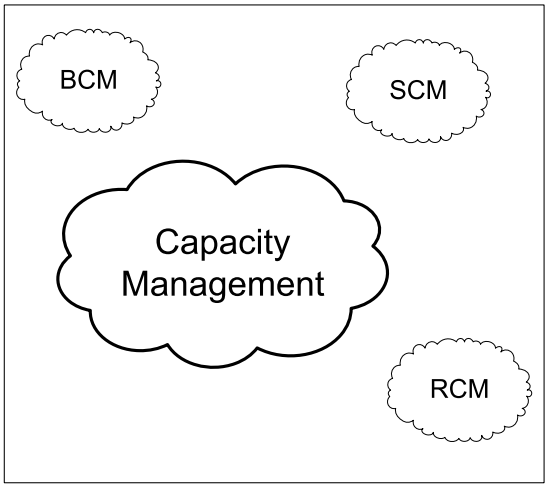


Abbildung 16.3: Die drei Unterprozesse des Capacity Management

- Business Capacity Management (BCM): Hier liegt die Verantwortung dafür, dass zukünftige geschäftliche Anforderungen rechtzeitig erkannt, durchdacht, geplant und umgesetzt werden. Über diesen proaktiven Subprozess müssen Anforderungen und Trends aus dem Geschäftsbereich identifiziert, in die entsprechenden Serviceanforderungen übersetzt und im Kapazitätsplan berücksichtigt werden. Er dokumentiert die aktuelle Situation (falls möglich mit Hilfe durchgespielter Szenarien) inklusive Spitzenwerte und Engpässen und einer Prognose zum künftigen Gebrauch und die Mittel, die benötigt werden, um der voraussichtlichen Nachfrage nach IT Services entsprechen zu können. Somit dient er auch als Abschätzung über die zukünftig notwendigen Haushaltsmittel (Investitionsplan) und hilft bei der Einführung (Zeitrahmen der Planung, Methoden) neuer Themen. Basis der Kapazitätsplanung sind Geschäftspläne, Geschäftsbewertungen und -szenarien, Geschäftsprognosen und eine Ist-Analyse. Durch die ebenfalls enthaltenen Empfehlungen und Aussichten inklusive der Berücksichtigung von aufgetretenen Problemen und Skalierungsoptionen bildet er eine wichtige Entscheidungsgrundlage. Der Kapazitätsplan enthält außerdem Daten über die aktuellen und geplanten Services, eine Ressourcenübersicht und entsprechende Verbesserungsvorschläge und Empfehlungen (erwartete Vorteile, Auswirkungen, Kosten). Ein solcher Plan sollte jährlich erstellt werden, wobei pro Quartal die Aktualität zu überprüfen ist.

  Der Fokus des Business Capacity Managements liegt darauf, das Business zu unterstützen, wobei sich die Business Requirements aus den Unternehmungsplanungen ergeben, die die erforderlichen neuen Services und die damit verbundenen Änderungen deutlich machen. Es besteht auch eine enge Verbindung zum Service Level Management. Zur Anpassung der IT an die Gegebenheiten des Unternehmens werden Techniken wie Application Sizing und Modelling eingesetzt.

- Service Capacity Management (SCM): Über diesen Unterprozess soll sichergestellt werden, dass die Servicekapazitäten in Verbindung mit den dahinter liegenden Ressourcen und IT-Verfahren so definiert sind, dass die in SLAs begründeten Serviceanforderungen erfüllt werden. Der Fokus liegt hier auf der Service-Performance und der SLA-Einhaltung. Dazu sind Kenntnisse über die IT Services notwendig. Um eventuelle Kapazitätsprobleme sichtbar zu machen, muss die Service-Nutzung überwacht (Monitoring) und analysiert werden. Die Messung der SLAs und das damit zusammenhängende Reporting spiegelt sich in den bereits aus dem Service Level Management bekannten Service Achievements wider.
- Ressource Capacity Management (RCM): Dieser Unterprozess liefert Details zur vorhandenen und geplanten Ressourcennutzung als Entscheidungsgrundlage für die Ergänzung von Komponenten, wann Upgrades oder Zukäufe notwendig sind und was diese Umsetzung kostet. Dazu ist es notwendig, die Komponenten und Ressourcen der IT-Umgebung zu kennen, die Ressourcennutzung zu überwachen und zu analysieren und die gemessene Performance entsprechend zu tunen. Darüber hinaus muss der Bereich stets über neue Entwicklungen und Technologie im Bilde sein. An dieser Stelle findet auch die bereits erwähnte CFIA (Component Failure Impact Analysis) statt, die zusammen mit dem Availability Management durchzuführen ist. Hier findet also das eigentliche Ressourcen-Management statt, das sich mit der Frage beschäftigt, ob auch zu Peekzeiten genügend Kapazitäten vorhanden sind. Dem gegenüber wird das Tuning bzw. Performance Management eingesetzt (*siehe Abbildung 16.4*).

Unterscheidung und Zusammenspiel der Subprozesse

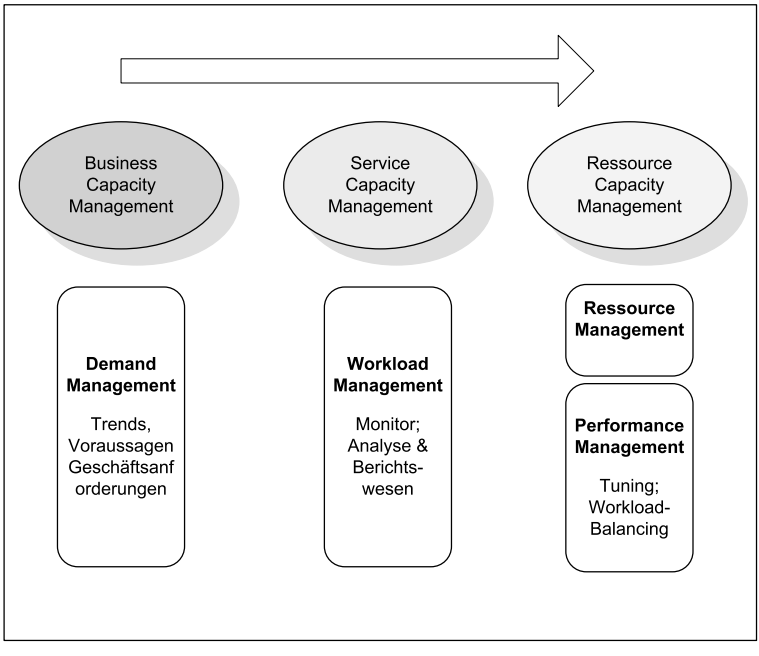


Abbildung 16.4: Stichworte zur Dreiteilung des Capacity Management

(Fortsetzung)

Das BCM stellt sicher, dass zukünftige Geschäftsanforderungen rechtzeitig bekannt und berücksichtigt werden, um diese in der IT-Organisation zu planen und zu implementieren. Dies kann erreicht werden, indem bestehende Daten der Ressourcennutzung zur Ermittlung zukünftiger Anforderungen hochgerechnet werden.

Das SCM kontrolliert die Leistung der aktuellen, operativen IT-Dienstleistungen, die bereits in Anspruch genommen werden. Es ist dafür verantwortlich, dass die Leistungsparameter aller IT-Dienstleistungen gemäß der in den SLAs vereinbarten Größen gemessen und überwacht werden. Die Ergebnis-Daten müssen gespeichert, ausgewertet und in Form von Berichten weitergegeben werden. Wenn es notwendig ist, werden Maßnahmen ergriffen, damit die IT Services in ausreichendem Maße den Geschäftsanforderungen entsprechen. Dabei ist oft die Unterstützung durch das RCM nötig.

Das RCM kontrolliert die einzelnen Komponenten aus der IT-Infrastruktur. Die Messdaten werden ausgewertet und weitergegeben. Bei Bedarf müssen die Ressourcen angepasst werden.

Die Capacity Management-Datenbank (Capacity Management Database, CDB) besitzt eine zentrale Rolle beim Capacity Management. Der Aufbau der Kapazitätsdatenbank umfasst das Sammeln und die Pflege technischer, geschäftlicher und sonstiger Daten, die für das Capacity Management wichtig sind (*siehe Abbildung 16.5*).

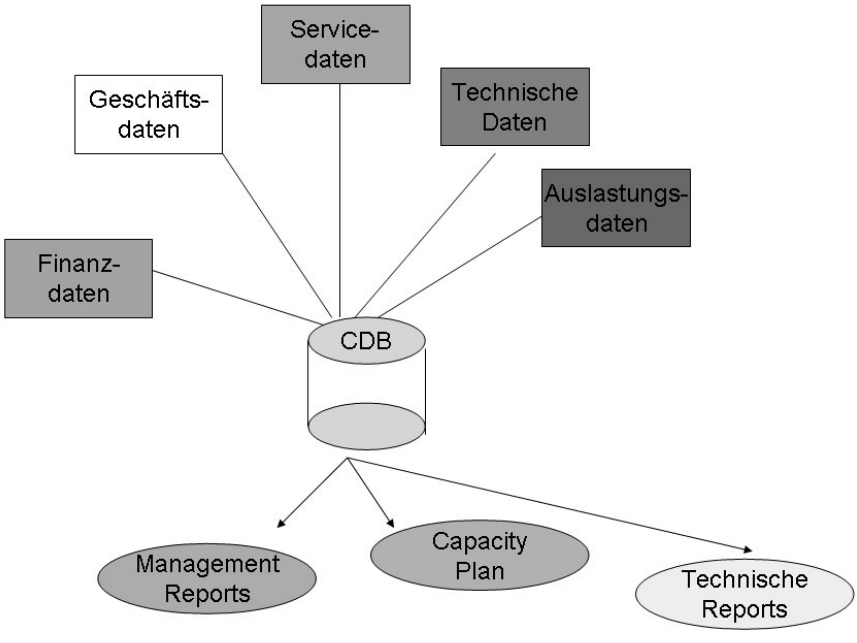


Abbildung 16.5: Capacity Management-Datenbank (CDB)

Hier sind alle wesentlichen Daten und Informationen enthalten, auf denen die Arbeit dieses Prozesses basiert. Dieses Repository enthält Daten zum Thema Business, Service, Technik, Finanzen und Nutzung in Form von Schwellenwerten der einzelnen zu überwachenden Kapazitäten. Dazu gehören auch Hard- und Softwaredaten, Finanz- und Kostendaten mit entsprechenden Kapazitäts- und Leistungsangaben, Empfehlungen zur Optimierung, Prognosedaten und einige mehr. Häufig existiert nicht nur eine einzige Datenquelle, sondern es werden eine Reihe von unterschiedlicher Repositories für die Ablage der Informationen über die Kapazität verwendet.

16.3 Aktivitäten und Aufgaben des Capacity Management

Das Capacity Management hat die Aufgabe, die benötigten, kostenmäßig vertretbaren Kapazitäten der aktuellen und zukünftigen IT-Ressourcen zu ermitteln, um die Vorgaben aus den SLAs zeitgerecht erfüllen zu können. Dies ist allerdings nur möglich, wenn zum einen die geschäftlichen Anforderungen der Kundenseite verstanden werden und zum anderen der IT-Betrieb und die dazugehörigen IT-Ressourcen bekannt sind (*siehe Abbildung 16.6*). Nur so ist eine Abstimmung der beiden Seiten möglich. Dabei geht es primär darum, Kapazitätsengpässe und Überraschungen zu vermeiden. Wichtig sind sowohl Kenntnisse über die strategischen Entwicklungen beim Kunden als auch über technologische Entwicklungen. Die Umsetzung der Aufgaben im Capacity Management erfolgt z.T. reaktiv (Unterstützung bei kapazitätsbedingten Incidents, Messen, Verbessern), z.T. proaktiv (zukünftige Engpässe vermeiden, Analyse, Prognose).

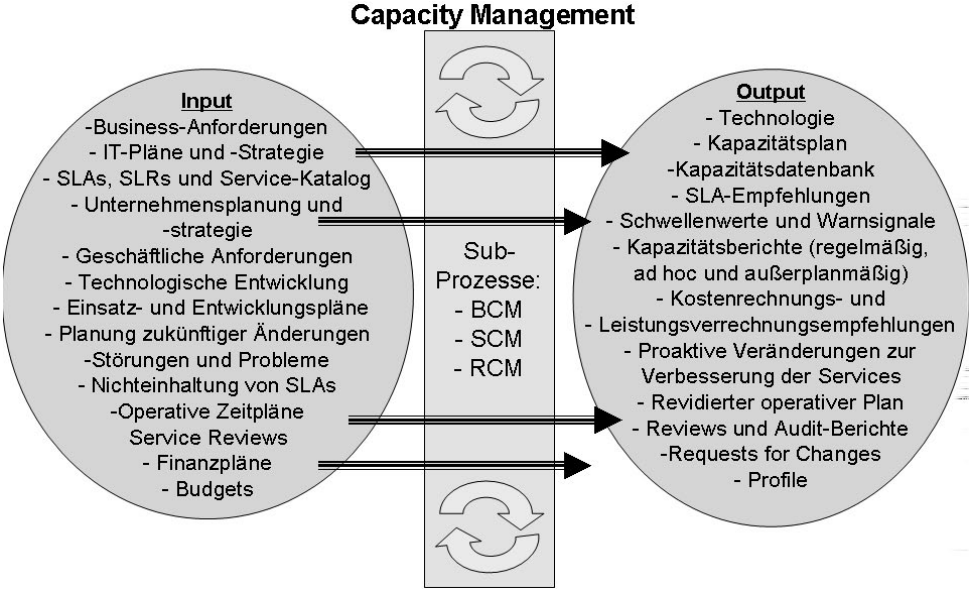


Abbildung 16.6: Der Prozess Capacity Management

Dadurch dass das Capacity Management in ständigem Dialog mit dem Kunden steht, beispielsweise durch den Datenabgleich zu Anforderungen und Möglichkeiten, ist auch eine höhere Kundenzufriedenheit möglich. Der Kapazitätsplan ist dementsprechend in regelmäßigen Abständen zu aktualisieren. Der Planungshorizont wird durch das Capacity Management erweitert, externe Dienstleister der IT-Organisation werden rechtzeitig über Anforderungen informiert, Panikkäufe und plötzliche Anforderungen, die scheinbar aus dem Nichts auftauchen, vermieden. Es geht allerdings nicht nur darum, dass existierende Anforderungen durch die IT effektiv, effizient und rechtzeitig umgesetzt werden, sondern auch um die Optimierung der Verteilung der IT-Kapazitäten und Services innerhalb der Organisation.

Im Gegensatz zu vielen anderen Prozessen der ITIL-Bereiche laufen die Aktivitäten nicht so stringent ab wie beispielsweise beim Incident Management oder Change Management (*siehe Abbildung 16.7*).

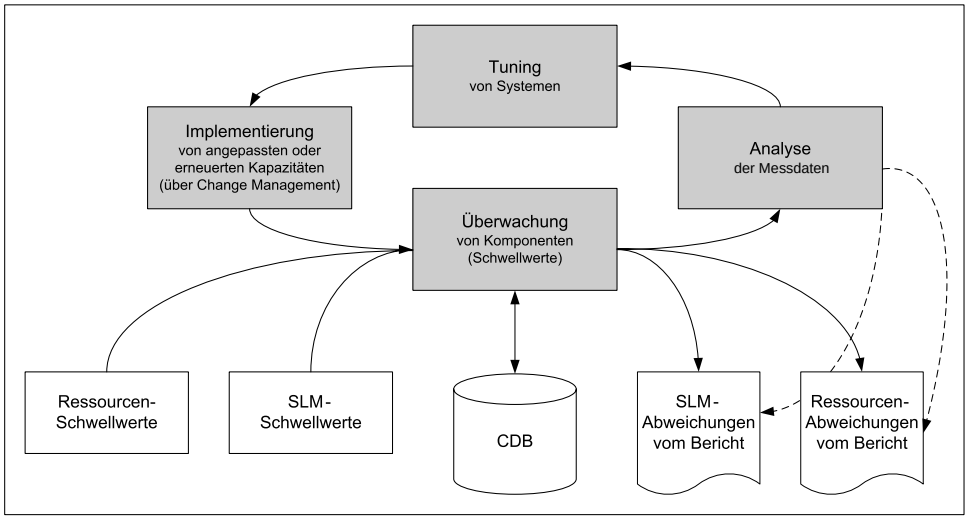


Abbildung 16.7: Aktivitäten im Capacity Management nach OGC

Für das Capacity Management wird zwischen fortlaufenden und Ad-hoc-Aufgaben unterschieden (*siehe Abbildung 16.8*). Fortlaufende Tätigkeiten sind iterative Tätigkeiten (Monitoring, Analyse, Tuning, Implementierung), Bedarfsmanagement und Speicherung der Daten in der CDB. Jeder der drei Teilprozesse BCM, SCM und RCM besitzt diese iterativen Tätigkeiten mit unterschiedlichem Fokus und verschiedenen Anforderungen hinsichtlich Monitoring und Reporting.

Das Application Sizing dient der Bestimmung von Kapazitäten (z.B. Hardware oder Netzwerk), die erforderlich sind, um neue (oder veränderte) Anwendungen zu unterstützen. Diese Aktivität ist endlich in Bezug auf die jeweilige Anwendung. Sie wird in der Regel über Projektarbeit umgesetzt oder wenn ein größerer Change einer bestehenden Anwendung ansteht. Die Aktivität gilt als abgeschlossen, sobald die Anwendung in die Produktion übernommen wurde. Innerhalb des Application Sizing geht es darum, die benötigten Ressourcen für eine Anwendung abzuschätzen, so dass die geforderten Service Levels umgesetzt werden. Um dies umsetzen zu können, muss das Thema Application Sizing integraler Bestandteil des Lebens-

zyklus jeder Anwendung im Unternehmen sein (Project Life Cycle). Dieses Thema steht in Interaktion mit weiteren Bereichen und Tätigkeiten, wie etwa Fehlertoleranz, Service Level-Spezifizierungen, Qualitätssicherungen oder Support.

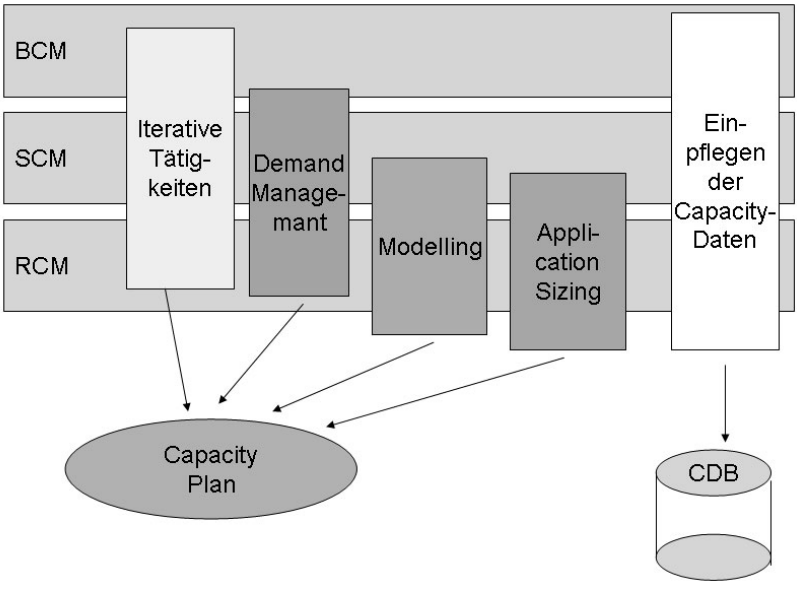


Abbildung 16.8: Tätigkeiten des Capacity Management

Modellierung (Modelling) steht für das Vorgehen, bei dem anhand von Rechenmodellen die Folgen verschiedener Alternativen für den Einsatz von verfügbarer oder gegebenenfalls anzuschaffender Kapazität zu bestimmen sind. Dabei werden zum Beispiel unterschiedliche Szenarien für die Zunahme der Nachfrage nach IT Services berücksichtigt. Ziel ist, das Verhalten eines IT Service in einem bestimmten Umfang und mit einer Auswahl von bestimmten Aufgaben und Tasks vorherzusagen. Dabei bedient sich das Capacity Management unterschiedlicher Techniken und Vorgehensweisen. Dies reicht von Annahmen aufgrund von Erfahrungswerten eines Experten, Hochrechnungen aufgrund der momentanen Situation, Pilotstudien und Prototypen bis hin zu ausgefeilten Benchmark-Tests. Unterschiede liegen bei diesen Modellen vor allem in Bezug auf den Preis vor.

Das Demand Management (Bedarfsmanagement) unterstützt als Werkzeug die Nachfragesteuerung des Kunden. Es dient der Beeinflussung des Anwenderverhaltens im Hinblick auf dessen Ressourcennachfrage und die entsprechende Ressourcennutzung. Das Bedarfsmanagement liefert somit einen wichtigen Beitrag für die Erstellung, die Überwachung und die eventuelle Anpassung sowohl des Kapazitätsplans als auch der SLAs. Demand Management verlangt sowohl nach einem Verständnis für die IT Services als auch nach der Kenntnis des Nutzerverhaltens auf Kundenseite. Dies bezieht sich auf die Frage, ob und welche Peekzeiten auftreten oder ob bestimmte zeitabhängige Aktivitäten bei den Benutzern existieren. Eine Beeinflussung des Services kann in physikalischer (z.B. Stoppen bestimmter Services, Zugriffslimitierung auf eine bestimmte Anzahl) oder finanzieller Hinsicht (z.B. Reduzierung von Kosten für den Service zu bestimmten Zeiten, Bepreisung für

Speicherplatz ab einem bestimmten Schwellenwert) erfolgen. Der Kostenrechnung aus dem Financial Management kommt so in diesem Zusammenhang eine wichtige Rolle dabei zu, das Anwenderverhalten zu beeinflussen. Das Demand Management wird generell in zwei Arten unterschieden:

- Short-term Demand Management (kurzfristig) muss dann eingreifen, wenn kurzfristig ein Kapazitätsmangel entsteht, z.B. wenn sich Probleme ankündigen oder der Service bereits beeinträchtigt ist. In diesem Fall können eventuell nicht alle, aber doch ein Teil der Services weitergeführt werden. Das Capacitiy Management muss dann unter Berücksichtigung der Geschäftsprioritäten für das Unternehmen die noch durchführbaren Services zuordnen.
- Long-term Demand Management (langfristig) kommt zum Einsatz, wenn es aus Kostengründen nur schwer vertretbar ist, zusätzliche Investitionen vorzunehmen. Insbesondere dann, wenn der Kapazitätsmangel nur zu bestimmten Zeiten auftritt, ist die Kostenargumentation oft schwierig. Das Capacity Management muss dann ermitteln, ob eine Kapazitätserweiterung wirklich notwendig ist oder das Problem auch durch eine Verteilung bzw. Verlagerung der Last zu lösen ist. So können eventuelle Spitzen mit erhöhtem Kapazitätsbedarf vermieden werden.

Das Monitoring im Capacity Management kümmert sich darum, dass die Verwendung jeder Ressource und jedes Services fortlaufend überwacht wird. Dabei ist eine Spezifizierung notwendig. Die Überwachung muss beispielsweise für die jeweilige Plattform umgesetzt werden. Die Daten müssen in Bezug auf die Themen Kapazität und Performance gesammelt und anschließend sowohl dem Ressource Capacity Management als auch dem Service Capacity Management zur Verfügung gestellt werden. Dabei sind unterschiedliche Ausprägungen und Abstufungen möglich. Teil der Überwachung sollte auch die Definition von Schwellenwerten und Baselines für Profile für das normale (störungsfreie) operative Geschäft sein. Das Monitoring ist nicht nur auf Teilausschnitte der IT-Infrastruktur beschränkt, sondern muss in der Lage sein, ein Gesamtbild der Umgebung dazulegen.

Die Analyse bedient sich der Daten aus dem Monitoring. Trends werden identifiziert, Baselines können definiert und verwendet werden. Aufgrund von Vergleichswerten sind Aussagen möglich, die auch die SLAs und deren Einhaltung betreffen. Auch Abweichungen von bereits erfolgten Trendaussagen können über das Analysieren aufgedeckt werden und zu einer Revidierung führen.

Tuning in Bezug auf das Performance Management bezieht sich auf Messung, Überwachung und Angleichung („Tuning“) der Leistungen der Komponenten innerhalb der IT-Infrastruktur. Ziel ist die optimale Einstellung für ein System.

Das Ziel der Implementierung liegt darin, Kapazitätsveränderungen via Changes in die Produktivumgebung einzubringen, die über die Überwachung, Analyse und das Tuning angestoßen wurden. Diese Aktivität geht Hand in Hand mit dem Change Management. Veränderungen dieser Art können erhebliche Auswirkungen auf das System verursachen. Es ist überaus wichtig, dass diese Veränderungen ebenfalls in das Monitoring einbezogen werden.

Auch das Erstellen und Füllen der Capacity Management-Datenbank (CDB) ist Teil der Aktivität innerhalb des Capacity Management. Daten aus der CDB werden von allen Subprozessen verwendet. Der Kapazitätsplan stellt neben dem Kapazitätsplan ein Output des Capacity Managements dar. Primäres Ziel ist ein Plan, der den aktuellen Level der Ressourcennutzung und Service-Leistungen (Performance)

widerspiegelt. Aufgrund von weiteren Angaben aus dem Unternehmensbereich werden Vorhersagen über zukünftige Entwicklungen festgeschrieben.

Das Berichtswesen dokumentiert Abweichungen der umgesetzten Verwendung der Kapazitäten im Vergleich zur geplanten Kapazitätsbeanspruchung, Trends innerhalb dieser Abweichungen und den diesbezüglichen Einfluss auf die Service Levels. Andere ITIL-Prozesse und das Management werden über das Wachstum bzw. die Abnahme der Kapazitätsbeanspruchung auf lange wie auf kurze Sicht informiert und die Kapazitätsschwellwerte, die bei Erreichen zur Beschaffung weiterer Kapazität führen, werden kommuniziert. Die Berichte liefern so die Steuerungsdaten der Prozesse.

Der Einführung des Capacity Management-Prozesses sollte eine entsprechende Planung vorangehen. Einige der notwendigen Aktivitäten wie das Monitoring und das Tuning existieren vielleicht schon innerhalb der IT-Organisation. Dies ist für das Capacity Management aber in der Regel auszuweiten, um alle der betreffenden CIs bzw. Ressourcen zu erfassen. Im Zuge der Einführung geht es auch um das Design der CDB. Erfolgsfaktoren für das Capacity Management liegen in den genauen Vorhersagen und Prognosen für das Geschäfts- und den Anwendungsbereich, in der Kenntnis der IT-Strategie und -Planung sowie deren Genauigkeit. Notwendig ist neben Kenntnissen der Entwicklungen im Technologiebereich auch die Zusammenarbeit mit anderen Prozessen.

16.4 Capacity Management im ITIL-Gesammtzusammenhang

Das Capacity Management besitzt wie alle Prozesse aus dem Service Delivery-Set eine große Nähe zum Management des Unternehmens. In diesem Fall geht es vor allem um die Planung und die Finanzierung von Investitionen im IT-Bereich. Andere ITIL-Prozesse stehen in engem Zusammenhang zum Capacity Management, um ihre Arbeit effektiv durchführen zu können. Dies gilt auch für die operativen Prozesse aus dem Service Support-Set.

Das Capacity Management erhält aus dem Incident Management Informationen zu Störungen, die sich aufgrund von Kapazitätsproblemen ergeben. Die Störungsursachenzuordnung kann in vielen Fällen erst dann stattfinden, wenn so viele Störungen zu einem Thema aufschlagen, dass offensichtlich wird, dass Kapazitätsprobleme dahinterstecken. Gegebenenfalls stellt das Capacity Management dem lncident Management Diagnose-Werkzeuge zur Verfügung, um Kapazitätsprobleme zu erkennen (Diagnose) oder zu beheben (Lösung). In vielen Fällen sind Monitoring-Tools in der Lage, automatisiert Informationen über Kapazitätsengpässe an das Incident Management zu übermitteln. Innerhalb der Zusammenarbeit mit dem Incident und Problem Management hält das Capacity Management die beiden Prozesse in Bezug auf potenzielle Kapazitäts- oder Performance-Probleme auf dem Laufenden. Automatische Benachrichtigungsfunktionen oder die Aufzeichnung von Known Errors helfen dabei. Das Capacity Management unterstützt das Problem Management darüber hinaus durch Werkzeuge und Informationen. Des weiteren können Sachkenntnis und Fähigkeiten aus dem Capacity Management-Prozess der Unterstützung des Problem Management in den unterschiedlichen Bereichen dienen. Dabei werden Kapazitätsprobleme identifiziert, diagnostiziert und gelöst. Das Problem Management nimmt auch Informationen zu Kapazitätsproblemen in seine Known Error-Datenbank für das

Incident Management auf. Ergebnisse aus der Analyse von Performance- und Kapazitätsproblemen werden dem proaktiven Teilbereich des Problem Management zur Verfügung gestellt.

Das Capacity Management sollte im CAB vertreten sein, um Informationen über den Kapazitätsbedarf sowie über die Auswirkungen, die eine Änderung auf den IT Service haben können, zur Verfügung zu stellen. Veränderungen in Bezug auf die Kapazität können erhebliche Auswirkungen auf die IT-Infrastruktur haben. Die Informationen über Änderungen stellen wiederum einen wichtigen Beitrag für die Kapazitätsplanung dar. Veränderungen, die das Capacity Management anstößt, müssen wie alle anderen RfCs über das Change Management laufen. Dies bezieht sich auch auf die Aspekte Tuning, Upgrades und Erweiterung des Monitorings.

In Bezug auf das Configuration Management ist die enge Beziehung zwischen CDB und CMDB hervorzuheben. Eigentlich bildet die CDB einen Unterbereich der CMDB ab. Ohne die korrekten und aktuellen Informationen aus der CMDB kann die CDB nicht als Basis des Capacity Management dienen.

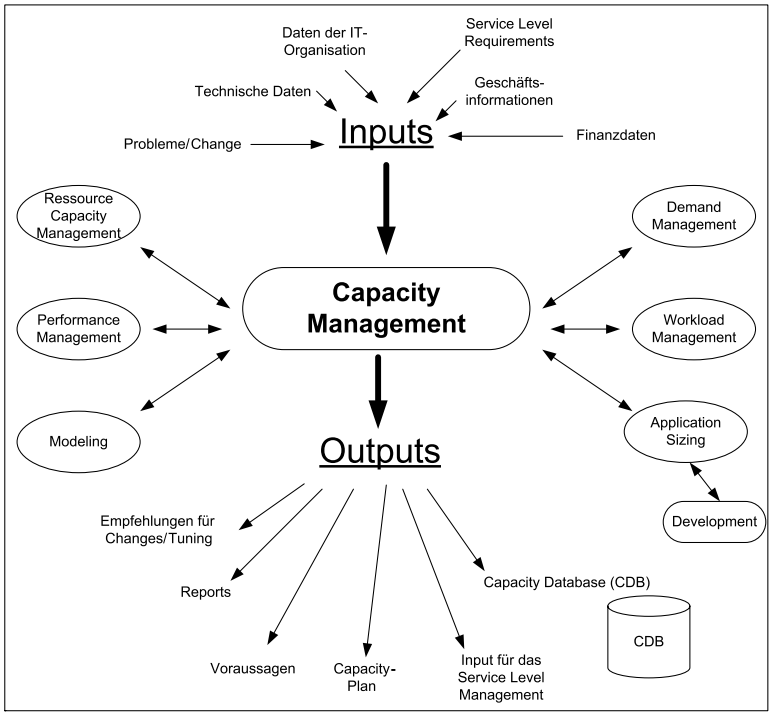


Abbildung 16.9: Aktivitäten im Capacity Management und direkte Schnittstellen zu weiteren ITIL-Prozessen

Dem Release Management bietet das Capacity Management Unterstützung in Sachen Verteilungsstrategie der Ressourcen der IT-Infrastruktur, beispielsweise bei der Verteilung von Software über das Netzwerk. Das Capacity Management kann die unterschiedlichsten Informationen zu wichtigen Faktoren der Aktivitäten im Release Management beisteuern. Dies bezieht sich sowohl auf Einzelaktionen als auch auf die fortlaufende Strategie des Release Management. Das Release Manage-

ment sollte bei geplanten Aktionen stets abklopfen, ob der Kapazitätsaspekt ausreichende Beachtung gefunden hat.

Das Capacity Management unterstützt das Service Level Management bezüglich der Performance- und Kapazitätsziele für neue oder veränderte Anforderungen. Das Capacity Management misst und überwacht die Performances und liefert wertvolle Informationen für die Kontrolle und einen eventuellen Abgleich der vereinbarten Service Levels und die diesbezüglichen Berichte.

Das Capacity Management und das Availability Management arbeiten Hand in Hand. Performance- und Kapazitätsprobleme können Auswirkungen auf die Verfügbarkeit eines Services haben. Sinkt die Verfügbarkeit eines Services unter einen in den SLAs definierten Schwellenwert oder weicht diese von der gewohnten Verfügbarkeit ab, schlägt dies negativ auf der Kundenseite auf und wird durch die Überwachung des Capacity Management in den entsprechenden Berichten erfasst und kommuniziert. Beide Prozesse bedienen sich vielfach derselben Werkzeuge und wenden dieselben Techniken an, wie beispielsweise die Component Failure Impact Analysis (CFIA) und die Fault Tree Analysis (FTA), um Schwachstellen aufzudecken.

Das Capacity Management benötigt als Input auch Daten aus dem Financial Management. Andersherum stellt das Capacity Management dem Financial Management seine Unterstützung bei der Erstellung von Investitionsfinanzplänen, für Kosten-Nutzen-Überlegungen und im Rahmen von Entscheidungen über Investitionen zur Verfügung. Über die Zusammenarbeit der beiden ITIL-Prozesse wird der ökonomischen Seite der IT Services Beachtung geschenkt. Zudem steuert das Capacity Management notwendige Informationen für die Verrechnung von Services, die im Zusammenhang mit der Kapazität stehen (zum Beispiel die Verteilung von Netzwerkkapazität), bei.

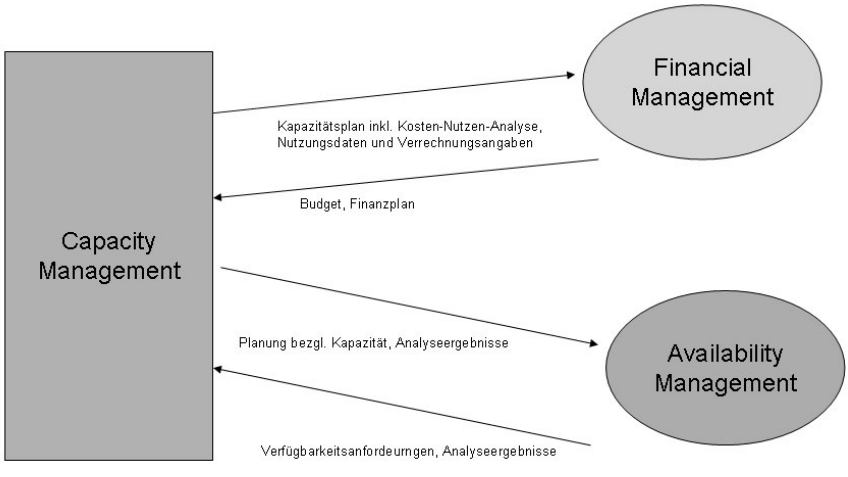


Abbildung 16.10: Schnittstellen und Interaktion zwischen den Prozessen

Das Capacity Management definiert die Mindestkapazität für die Kontinuitäts- und Recovery-Optionen, die erforderlich sind, damit der Service im Falle von Störungen aufrecht erhalten werden kann. Dieser Kapazitäts- und Performancebedarf ist auf den jeweils aktuellen Grundbedarf abzustimmen. Der Kapazitätsplan muss den Anforderungen aus dem Continuity Management für IT Services gerecht werden.

17 Financial Management for IT Services

Das Financial Management beschäftigt sich mit den durch die Erbringung der Dienstleistungen entstehenden Kosten und mit der Weiterverrechnung dieser Kosten mit dem Kunden. Zunächst ist es notwendig, eine Kostentransparenz im IT-Bereich zu erreichen, um auf dieser Basis ein Weiterverrechnungsmodell aufzubauen und umzusetzen. Die Preistransparenz ist für den Kunden entscheidend und hilft ihm, seine IT-Kosten zu steuern. Möglich ist dies nur über die Schaffung der Prozess- und Leistungstransparenz aus Sicht der IT Services und die Kenntnis der Infrastrukturzusammenhänge. Die tatsächlichen Kosten für die IT Services werden häufig jedoch nicht ausreichend berücksichtigt. Neben den für die Verfahren und die einzelnen CIs anfallenden Kosten werden häufig die Ressourcen für Kommunikation, Interaktion und Aktion der betroffenen Personen vernachlässigt.

Der Nutzungsgrad der Services und ihrer Komponenten muss verbrauchsspezifisch ermittelt und kostenspezifisch auf die Nutzer verteilt werden, damit die IT-Organisation kostendeckend arbeiten kann. Neben den eigentlichen Bedürfnissen und dem Nutzungsverhalten des Kunden spielen, wie auch beim Capacity Management, die zukünftigen technologischen Entwicklungen eine Rolle. Diese müssen, ebenso wie Aussagen über die Nutzungs- bzw. Verbrauchsentwicklung des Kunden, in die finanziellen Überlegungen für die Organisation eingebunden werden. Kundenverhalten, das sich nicht immer an seine eigenen strategischen Vorgaben hält, sofern diese überhaupt vorhanden sind, und kurze Produktzyklen insbesondere im Softwarebereich, machen Aussagen über die Zukunft und dementsprechende Planungen schwierig.

Das Financial Management sieht seine Aufgaben in einem effizienten Einsatz der IT Services und seiner Ressourcen sowie analog dazu in den benötigten finanziellen Mitteln. Zudem kontrolliert dieser Prozess die Leistungserbringung durch den IT-Bereich unter betriebswirtschaftlichen Aspekten (*siehe Abbildung 17.1*). Dazu gehören auch Kosten-Nutzen-Rechnungen. Financial Management gibt darüber hinaus finanzielle Informationen zur Entscheidungsfindung an das Management weiter. Die Verfahren des Financial Management stellen zudem das Kostencontrolling und die Serviceverrechnung sicher. Beachten Sie: Der Preis eines Services hat Auswirkungen auf den Absatz, d.h. auf das Nutzungsverhalten des Kunden. Tauchen in der IT-Organisation Probleme aufgrund des Anwenderverhaltens auf, kann das entsprechende Verhalten bzw. der „Service-Konsum“ über den Preis gesteuert werden. Dies kann sich z.B. auf Maildatenbanken, die die elektronische Post der letzten vier Jahre enthält, SAN- oder Plattenplatz auf Servern, die als Gimmick- oder MP3-Ablage missbraucht werden, beziehen. Auch längst fällige Konsolidierungsmaßnahmen sind so umzusetzen. Eine ähnliche Empfehlung stammt auch aus dem Capacity Management.

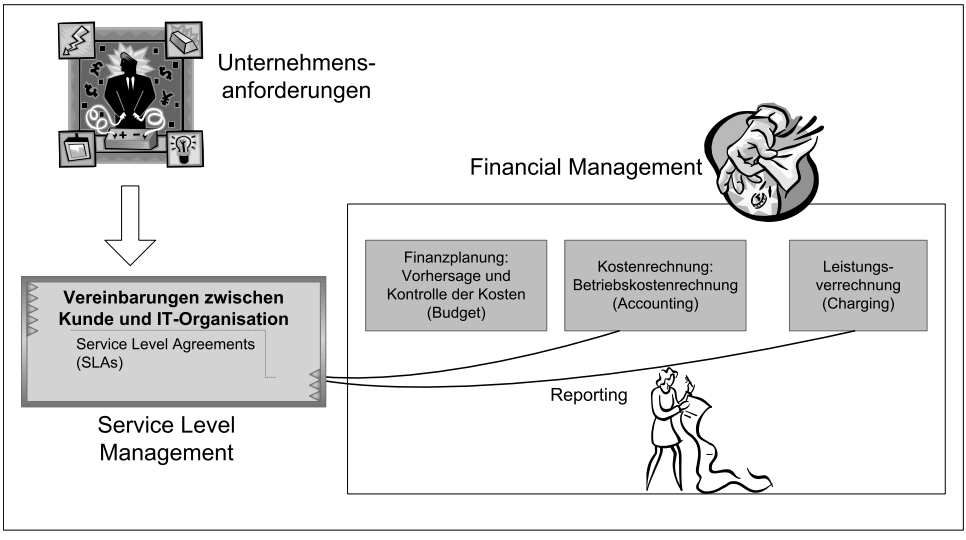


Abbildung 17.1: Die Kenntnis der Serviceanforderungen ist essenziell

Viele Unternehmensbereiche und damit IT Service-Nutzer empfinden die IT-Kosten als zu hoch. Oft erscheinen die Zahlen entweder allzu pauschal verteilt oder in einer Form abgerechnet, die der Kunde nicht versteht. So kann das Gefühl entstehen, dass die ihm zugeordneten IT-Kosten nicht beeinflussbar oder steuerbar sind. An dieser Stelle setzt das Financial Management ein. Die erbrachten Leistungen müssen so definiert werden, dass der Kunde sie erkennt und versteht. Die abgenommenen Leistungsmengen müssen dokumentiert werden und die verrechneten Kosten mit der Leistungsmenge nachvollziehbar übereinstimmen. Wer IT-Leistungen innerhalb der Geschäftsprozesse in hohem Maße benötigt, wird auch hohe IT-Kosten akzeptieren. Wer den Preis von IT-Leistungen kennt, wird die Ressourcen wirtschaftlicher einsetzen.

17.1 Financial Management nach ITIL

IT Services unterstützen den Geschäftsbetrieb. Die beiden Bereiche eines Unternehmens sind mittlerweile eng miteinander verzahnt. Die meisten Unternehmen können gar nicht mehr ohne ihre IT Services leben. Die tatsächlichen Kosten für das unentbehrliche Hilfsmittel IT werden in vielen Fällen jedoch nicht ausreichend berücksichtigt. Das kann auch daran liegen, dass sich die Verrechnung von IT-Leistungen recht komplex gestaltet. So werden nur selten die tatsächlichen Kosten pro Kunde adäquat aufgedeckt. Genau diesem Umstand arbeitet das Financial Management entgegen. Denn die Kosten in der IT müssen genauestens ermittelt, verwaltet und transparent aufgezeigt werden. Ohne diese Aufschlüsselung existiert keine fundierte Entscheidungsgrundlage, weder für die IT-Organisation noch für das Unternehmen. Aus diesem Grund ist das Financial Management verantwortlich für die Rechenschaft über Ausgaben der IT Services und die dementsprechende Zuordnung der Kosten zu den einzelnen Services bzw. CIs. Auf dieser Basis können Entscheidun-

gen für oder gegen Investitionen im IT-Bereich erfolgen. Dazu gehören auch die Kontrolle und Verwaltung des IT-Budgets sowie die Weiterverrechnung an den Kunden, falls es sich um ein externes Dienstleistungsverhältnis oder den Betrieb eines Profitcenters handelt. Financial Management ist daher als ein integraler Bestandteil des Service Management anzusehen. Es stellt die essenziellen Management-Informationen zur Verfügung, die für die Gewährleistung einer effizienten, wirtschaftlichen und kostenwirksamen Erbringung des Services benötigt werden. Kurz: Es geht um die Finanzmittelplanung, Identifizierung, Überwachung und Weiterberechnung der Kosten im IT-Bereich.

17.2 Begriffe und Definitionen des Financial Management

Ein effizientes Financial Management-System ermöglicht der Organisation, vollständig über die Ausgaben der IT Services Rechenschaft abzulegen und diese Kosten den Services zuzuordnen, die für die Kunden der Organisation erbracht wurden. Nur so ist es möglich, eine realistische Methode der Kostenrechnung für diese Services anzuwenden. Diese Vorgehensweise macht den Kostenaufwand für die Kunden transparenter. Um kosteneffiziente IT Services anzubieten, müssen die drei Aspekte Qualität, Kosten und Kundenwünsche berücksichtigt werden. Wichtig ist dabei, zuallererst die Anforderungen und Bedürfnisse des Kunden zu ermitteln. Auf der anderen Seite des Tisches sitzt dem Kunden die IT-Organisation gegenüber. Diese kann gegenüber dem Kunden unterschiedlich positioniert sein.

Als Accounting Center ist sie dafür verantwortlich, mindestens die entstandenen Kosten zu ermitteln. Als Recovery Center muss sie die entstandenen Kosten ermitteln und den Kunden- bzw. Organisationseinheiten zuweisen können. Am eigenständigsten und mit den meisten Aufgaben gegenüber dem Kunden steht das Profitcenter als Dienstleister. Es ist eine eigenständige Geschäfts- oder Gesellschaftseinheit, die je nach Vorgabe gewinnorientiert, kostendeckend oder subventioniert arbeiten muss.

Ganz wichtig ist neben den unterschiedlichen Sichtweisen der aufgeschlüsselten Aufgaben basierend auf der Geschäftsform die Aufgabenteilung des Finance Management in die drei Subprozesse Budgeting, Accounting und Charging. Wichtig: Das Billing als expliziter Subprozess gehört nicht in diesen Prozess (für ITIL)!

Das Financial Management for IT Services sieht sein Aufgabenfeld in der Verwaltung der Kosten zur Erbringung der zugesicherten Services (Kostenrechnung) und in der Weiterverrechnung der Leistungen an den Kunden (Leistungsverrechnung). Das Financial Management bietet eine kostenwirksame Verwaltung der IT-Komponenten und der finanziellen Ressourcen, die für die Erbringung von IT Services eingesetzt werden.

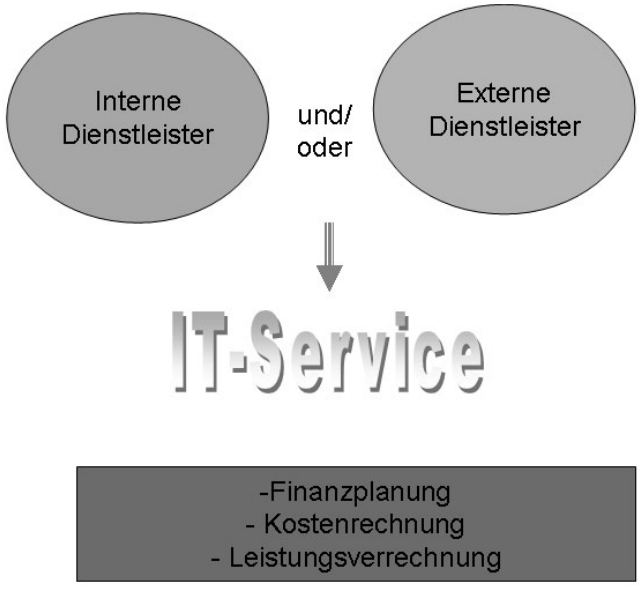


Abbildung 17.2: Geschäftsperspektiven auf das Finance Management

Die Finanzplanung (Budgeting) beschäftigt sich mit der Kostenvorhersage (Prognose) und dem Ausgabenmanagement (Budgetplanung). Dies stützt sich auf die Prognose des Nachfrageverhaltens des Unternehmens zur Vorhersage der Servicekosten. Historische Daten helfen bei der Vorhersage, die anhand der Beurteilung und Sachkenntnis der verantwortlichen Personen(en) ausgearbeitet werden. Budgetüberschreitungen sollen vermieden und die Kostendeckung gewährleistet werden.

Bei der Kostenrechnung (Accounting) geht es um die Feststellung der tatsächlich angefallenen Kosten. Diese werden mit Hilfe einer exakten Kostenermittlung pro Kunde, pro Service, pro Aktivität usw. aufgeschlüsselt. Da aber der IT Service für den Kunden im Mittelpunkt steht und dieser auch nur von der Kundenseite gesehen und angefordert wird, müssen die einzelnen Kosten, die mit den Services verbunden sind, genau ermittelt werden. Dies ist auch die Basis für eine Kosten-Nutzen-Analyse. Die Kostenrechnung richtet sich an den internen Empfänger im Unternehmen. Es geht stets um die Gegenüberstellung der beiden Größen Kosten und Leistungen. Es gibt keinerlei gesetzliche Vorgabe, wie die Kostenrechnung zu gestalten ist. Kosten sollten stets sorgfältig untersucht werden, damit sie auch beeinflusst werden können. Hier hilft die Kostenrechnung weiter. Sie ist ein wichtiges Hilfsmittel zur erfolgreichen Unternehmenssteuerung.

Die Kostenrechnung muss den Werteverzehr zur Leistungserstellung mengenmäßig und wertmäßig erfassen, gliedern, analysieren und Aussagen machen über

- den betrieblichen Werteverzehr (die Kosten)
- den betrieblichen Wertezuwachs (die Leistungen bzw. den Ertrag)

Dazu dienen vor allem die Ermittlung des Betriebsergebnisses, die Aufstellung einer periodischen, kurzfristigen Erfolgsrechnung (monatlich/vierteljährlich) und die Ermittlung der Herstell- und Selbstkosten je Leistungseinheit. Letzteres dient sowohl als Grundlage für die Preispolitik als auch, in größerem Rahmen gedacht, als Wertansatz für die Bilanz.

Eine nicht zu unterschätzende Aufgabe der Kostenrechnung liegt in der Bereitstellung von Informationen für die Preispolitik. Dazu gehören nicht nur die Daten für die Kalkulation. Mit Hilfe der Kostenrechnung können Sie auch prüfen, ob Ihre Selbstkosten unter oder über den am Markt erzielbaren Preisen liegen. Sollen neue Produkte eingeführt werden, liefert Ihnen die Kostenrechnung die Grundlage für die Preisbildung überhaupt.

Preispolitik

Unter Preispolitik werden alle marktbezogenen Maßnahmen und Entscheidungen des Unternehmens verstanden, mit denen die Preise beeinflusst und durchgesetzt werden können. Ein Ziel ist es, den wirtschaftlichen Erfolg eines Produktes sicherzustellen. Meist wird jedoch eine Kombination von Zielen verfolgt, wie Gewinnmaximierung und Marktanteilssteigerung. Die Preispolitik umfasst die Analyse, Planung, Umsetzung und Kontrolle von Aktivitäten bezüglich des Preises als Marketing-Instrument, z.B. Preisgestaltung oder Rabattpolitik.

Zusammenfassend ist zu sagen, dass die Kostenrechnung eine

- Planungsrechnung ist, indem sie Informationen zu Prognosen und Entscheidungen zur Verfügung stellt;
- Kontrollrechnung in dispositiver Hinsicht und zur Ausführungskontrolle ist;
- Dokumentationsaufgabe hat, die hauptsächlich freiwillig durchgeführt wird, in wenigen Punkten aber auch eine gesetzliche Vorgabe hat (z.B. Aufbewahrungspflichten von Kalkulationen).

Folgende Maßnahmen fördern die Kostentransparenz gegenüber dem Unternehmen:

- gut strukturierte Berichte, die mit dem Empfänger der Berichte erarbeitet und auf seine Bedürfnisse abgestimmt worden sind
- realitätsnahe, einheitliche und gleichzeitig einfache Verrechnungsmodelle
- standardisierte Erstellungs- und Verteilungsprozesse für das Berichtswesen
- kein zu hoher Detaillierungsgrad bei der Kundenverrechnung, da ansonsten der Vorwurf der Scheingenauigkeit entstehen kann
- die Verwendung von kundenorientierten Kostenträgern

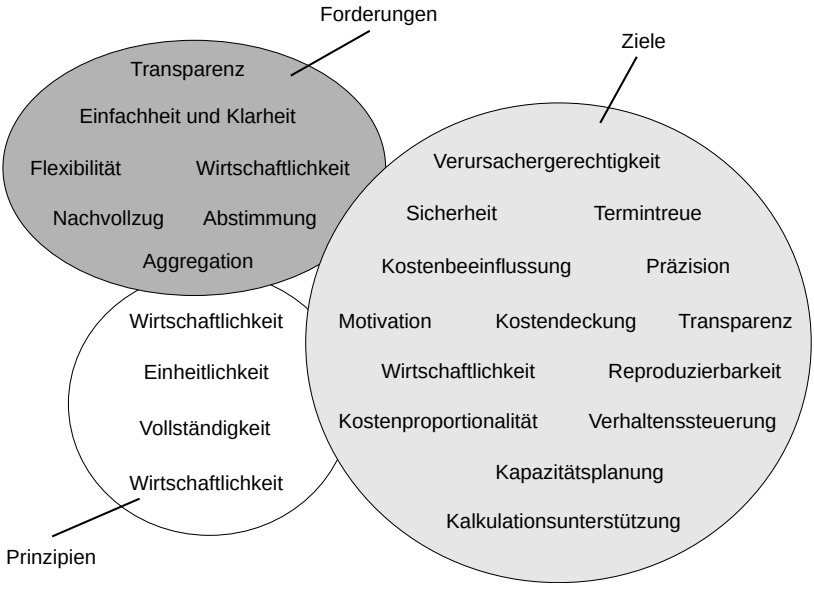


Abbildung 17.3: Faktoren für die IT-Kostenrechnung

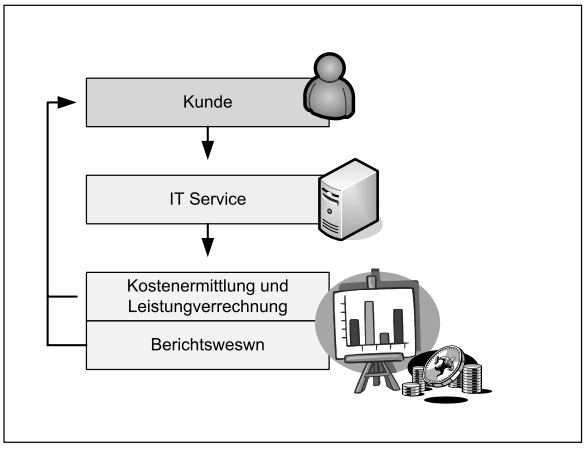


Abbildung 17.4: Aktivitäten im Financial Management

Bei der Leistungsverrechnung (Charging) als drittem Subprozess werden die Serviceleistungen auf den Kunden umgelegt (*siehe Abbildung 17.4*). Dies basiert auf den SLAs und der Servicenutzung. Hierunter fallen alle Aktivitäten, die erforderlich sind, um einem Kunden die Services, die für ihn geleistet wurden, in Rechnung zu stellen. Nur so ist eine Beeinflussung des Nutzer- und Kundenverhaltens über den Preis möglich. Vorab muss jedoch festgelegt werden, wie das Pricing erfolgen soll (z.B. Kosten, Kosten plus Aufschlag, Marktpreis oder Festpreis). Dies wird über die Preisgestaltung gelöst. Durch Leistungsverrechnung sinken die IT-Kosten nicht zwangsläufig. Aber die Fachseite als Kunde kann bewusst entscheiden, ob sie mehr oder weniger IT einsetzt. Sie

übernimmt damit die Verantwortung für ihre Kosten. Darüber hinaus ist eine angemessene Leistungsverrechnung eine der besten Möglichkeiten für den IT-Leiter, die Leistung aktiv zu kommunizieren und aus dem reinen Kostenfokus zu lösen.

Financial-Manager: Ein „Hut" im Financial Management for IT Services

Das Finance Management braucht wie jeder andere ITIL-Prozess einen Verantwortlichen. Der für den Prozess verantwortliche IT-Finanzmanager sollte mit dem Management der übrigen Prozesse sowie der Finanzabteilung auf einer Ebene arbeiten, um die Richtlinien für Finanzplanungs-, Kostenrechnungs- und Verrechnungssysteme festlegen zu können. Der Finanzmanager einer IT-Organisation tauscht sich mit dem Service Level-Manager darüber aus, welche Kosten zur Erfüllung vorhandener und neuer geschäftlicher Anforderungen anfallen, wie sich die Verrechnungsgrundsätze der Organisation auf die Kunden auswirken. aber auch, welchen Einfluss diese Maßnahmen auf das Kundenverhalten haben.

17.3 Kosten, Kosten, Kosten …

Jede Preiskalkulation sollte zunächst berücksichtigen: Welche Kosten verursacht es im Unternehmen, ein Produkt herzustellen und zu verkaufen bzw. eine Dienstleistung zu erbringen? In aller Regel gilt: Der Verkaufspreis sollte alle dazugehörigen Kosten plus einen Gewinn abdecken. Dabei sind Kosten nicht gleich Kosten, sondern sie lassen sich in unterschiedliche Kostenarten und -kategorien gliedern (*siehe Abbildung 17.5*). Eine Einteilung und Verteilung der Kosten wird als essenziell angesehen, um die Kosten überhaupt adäquat umlegen zu können.

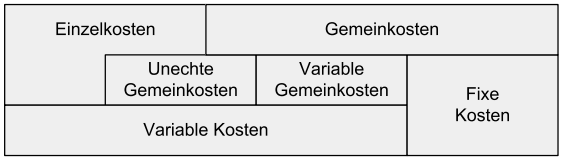


Abbildung 17.5: Kosteneinteilung nach Zurechen- und Veränderbarkeit

- Einzelkosten und Gemeinkosten: Je nachdem, wie Kosten bestimmten Kostenträgern zugeordnet werden können, ist die Rede von Einzel- oder Gemeinkosten. Einzelkosten lassen sich einem Kostenträger direkt zurechnen. Dies bezieht sich zum Beispiel auf das Material, das für ein Produkt verwendet wird oder mit einem Service einhergeht. Gemeinkosten lassen sich dem einzelnen Kostenträger nicht mehr direkt zuordnen. Sie können nur über Zuschlagssätze auf die verschiedenen Kostenträger aufgeteilt werden. Die Verwaltungskosten können z.B. nicht mehr einzelnen IT Services direkt zugeordnet werden.

Im allgemeinen ITIL-Sprachgebrauch wird dabei von direkten (= Einzelkosten) und indirekten Kosten (= Gemeinkosten) gesprochen, was aber in der deutschen betriebswirtschaftlichen Terminologie nicht korrekt ist. Die Bedeutung ist aber gleich: Indirekte Kosten sind Kosten, die nicht spezifisch und exklusiv einem IT Service zugeordnet werden können, z.B. Gebäude (Büro), unterstützende Services (wie die Nutzung des Netzwerks) und Verwaltungskosten (Stunden). Diese müssen dann anteilig berechnet werden. Das Kriterium für die Kategorisierung lautet Zurechenbarkeit.

Für einen klaren Kostenüberblick sollte nach Kosten unterschieden werden, die regelmäßig in derselben Höhe anfallen, und nach Kosten, die nutzungsabhängig sind oder aus anderen Gründen Schwankungen unterliegen. Das Kriterium für die Kategorisierung lautet Veränderbarkeit.

- Variable Kosten sind Kosten, die sich der veränderten Marktlage anpassen (Angebot und Nachfrage). Diese werden auch proportionale Kosten genannt. Die Materialkosten nehmen beispielsweise mit steigender Produktionsmenge insgesamt proportional zu. Sie verringern sich z.B. im gleichen Verhältnis, wie die Produktion zurückgeht. Die auf ein Stück umgerechneten Materialkosten bleiben bei schwankender Beschäftigung konstant. Variable Kosten erscheinen deshalb als verhältnismäßig unproblematisch. Zu dieser Kostenart gehören beispielsweise die Kosten für externe Mitarbeiter sowie für Druckertoner, Papier, Heizung und Strom. Diese Kosten entstehen in Abhängigkeit von den erbrachten Services.
- Fixe Kosten stellen Kosten dar, die von der Beschäftigung und Marktlage nur sehr unwesentlich abhängen. Sie können auch als Kosten der Betriebsbereitschaft bezeichnet werden. Die fixen Kosten verändern sich mit steigender oder sinkender Produktion nicht. Sie treten in jeder Abrechnungsperiode unverändert auf. Sie laufen auch dann weiter, wenn sich die Produktion (d.h. der Service) verringert oder gänzlich eingestellt wird.

Eine Cost Unit (Leistungseinheit) ist die kleinste verrechenbare Einheit pro Ressource. In Bezug auf den Aspekt Personal ist eine Cost Unit identisch mit einer Arbeitsstunde.

Eine dritte Unterscheidung der Kosten erfolgt auf der Grundlage von Kapital- und Betriebskosten:

- Kapitalkosten: Diese Kosten stehen im Zusammenhang mit der Anschaffung von Vermögenswerten, die in der Regel langfristig verwendet werden. Der Aufwand für die Anschaffungskosten wird über mehrere Jahre hinweg abgeschrieben, wobei jedoch lediglich der Abschreibungsbetrag den Kosten zugerechnet wird. Die Finanzierung erfolgt über Fremd- und/oder Eigenkapitel.
- Betriebskosten: Hierbei handelt es sich um regelmäßig auftretende Kosten, denen keine materiellen Betriebsmittel gegenüber stehen, z. B. Wartungsverträge für Hard- oder Software, Lizenzkosten, Versicherungsprämien usw.

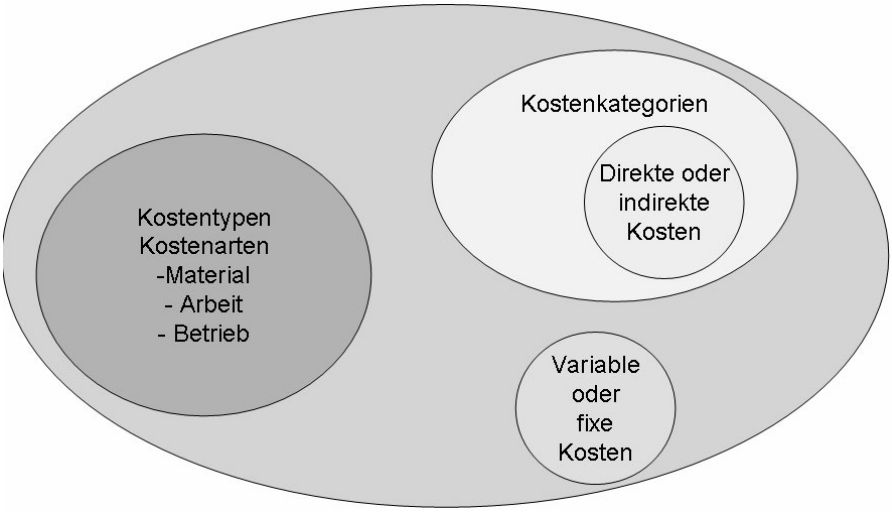


Abbildung 17.6: Unterschiedliche Aspekte des Kostenmodells

Daneben existieren weitere Einteilungsmöglichkeiten (*siehe Abbildung 17.6*):

- Funktionen in der IT-Organisation: Bei einer Einteilung nach betrieblichen Funktionen lassen sich die Kostenstellen abbilden, indem beispielsweise Betriebs-, Support- und Verwaltungskosten erfasst werden.
- Herkunft der Kostenfaktoren: Primäre und sekundäre Kosten unterscheiden die Herkunft der Kosten. Die primären Kosten setzen sich aus Kosten zusammen, die direkt entstehen. Dazu gehören Personal- und Hardwarekosten. Sekundäre Kosten entstehen bei der innerbetrieblichen Leistungserbringung und setzen sich aus Primärkosten sowie den zusätzlich investierten Mehrkosten zusammen, die zur Leistungserbringung geführt haben. Sie werden deshalb auch gemischte, zusammengesetzte oder abgeleitete Kosten genannt.

ITIL schlägt zwei Kostenmodelle mit unterschiedlichen Kostenträgern vor. Beim ersten Modell werden alle Kosten auf die Kunden bzw. die entsprechenden Abteilungen im Unternehmen (*siehe Abbildung 17.7*), beim zweiten auf die IT-Dienstleistungen umgelegt.

Nachdem die Grundlage für die Überwachung der Kosten feststeht (zum Beispiel pro Abteilung, pro Service oder pro Kunde), werden die Kostenarten erstellt, unter denen die Kosten verbucht werden können.

Beide Kostenmodelle nutzen die gleichen Kostenarten als Basis. Als Kostenarten werden die Kategorien für die Kosten des Personals sowie der Hardware, der Software, der Miete, des Transfers und der externen Leistungen vorgeschlagen. Die Kategorie für die Transferkosten umfasst alle Kosten der internen Leistungskonsumation. Die Kategorie der externen Leistungen dient der Zuteilung von extern bezogenen Leistungen, die man keiner der anderen Kategorien zuteilen kann. Die Kostenarten können je nach gewünschtem Detaillierungsgrad verfeinert werden.

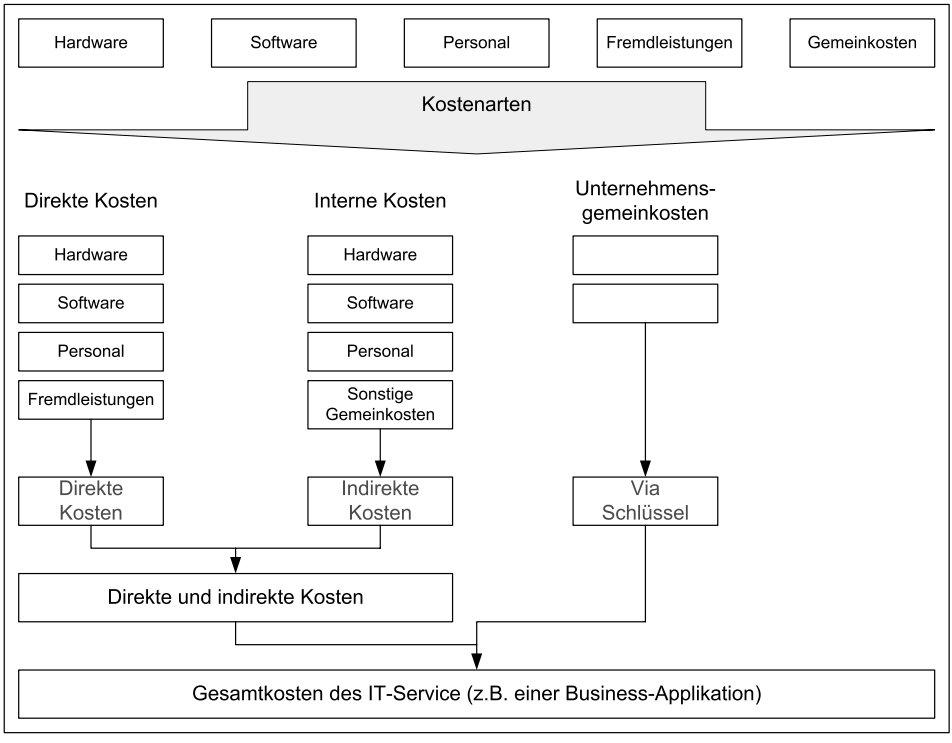


Abbildung 17.7: Kosteneinteilung pro Kunde bzw. Abteilung

Die Hardware lässt sich zum Beispiel in Unix und Windows Server, PCs etc. oder strategische Hersteller aufteilen. Je nach Größe der Organisation kann die Zahl der Kostenarten variieren. Im Anschluss an die Einrichtung der Kostenarten kann ihre Kategorisierung erfolgen. Es gibt insgesamt sechs Hauptkostenarten, die sowohl direkte als auch indirekte Kosten enthalten:

- Ausrüstungskosten/Equipment Cost Unit (ECU): Alle IT-Hardware-Komponenten wie Server, Speicherplatz, Kommunikation und Netzwerk oder Drucker
- Softwarekosten/Software Cost Unit (SCU): Sowohl direkte als auch indirekte Kosten, die für den Betrieb der Anlage erforderlich sind, z.B. System-Software, Datenbankmanagementsysteme, Anwendungsentwicklungssysteme oder Anwendungen
- Organisationskosten/Organisation Cost Unit (OCU): Direkte und indirekte Personalkosten, die sowohl fest als auch variabel sein können, wie Gehälter, Schulungen oder Reisekosten
- Mietkosten/Accommodation Cost Unit (ACU): Alle direkten und indirekten Unterbringungskosten wie etwa Computerräume, Büros oder übrige Einrichtungen wie Testräume, Schulungsräume, Klimaanlage usw.

- Übertragbare Kosten/Transfer Cost Unit (TCU): Eine Kostenart, die in Zusammenhang mit Gütern und Services steht, die von einer anderen Abteilung ausgeführt werden. Hierbei handelt es sich um die interne Verrechnung zwischen unterschiedlichen Abteilungen innerhalb einer Organisation.
- Managementkosten/Cost Accounting (CA): Kosten, die in Verbindung mit dem eigentlichen Finanzmanagement und der entsprechenden Verwaltung entstehen

Später kann gegebenenfalls je nach Kategorie noch die Art der Verrechnung festgelegt werden. Geht es darum, IT-Dienstleistungen als Kostenträger zu veranschlagen, werden die direkten Kosten den IT-Produkten bzw. -Ressourcen zugeordnet. Die Umlage der PCs, Server, Mainframeleistung und Infrastruktur verhält sich ähnlich.

Beispielüberlegung: Kunden als Kostenträger

Bei der Verwendung des IT-Kunden als Kostenträger wird ausgehend von den Kostenarten eine Aufspaltung der Kosten vorgenommen. Die direkten Kosten wie dedizierte Server und Software werden direkt den Abteilungen zugeordnet. Die indirekten Kosten werden weiter in zurechenbare und nicht zurechenbare Kosten unterteilt. Die zurechenbaren indirekten Kosten, welche sich den Abteilungen verursachergerecht zuteilen lassen, werden zu den direkten Kosten der jeweiligen Abteilung addiert. Dazu werden Mengenschlüssel wie PCs und Lizenzen als Grundlage für die Aufteilung der Kosten herangezogen. Die PC- und Betriebssystem-Kosten werden dann entsprechend ihrer Anzahl pro Abteilung verteilt. Weitere Software wie Office-Pakete oder Notes-Installationen werden nach Lizenzanzahl aufgeteilt. Für nicht dedizierte Server und die Mainframeleistung kann beispielsweise die durchschnittliche CPU-Leistung als Bezugsgröße herangezogen werden. Komponenten wie Kabel, Router und Software werden zu einem indirekten Kostenblock (z.B. Kostenstelle Infrastruktur) zusammengefasst. Anstatt den genauen Verbrauch eines jeden Benutzers zu berechnen, werden diese gesammelten Kosten nach der PC-Anzahl verteilt. Die verbleibenden nicht zurechenbaren indirekten Kosten („Overhead-Kosten"), müssen mehr oder weniger willkürlich auf die Abteilungen verteilt werden. Vorgeschlagen werden zum einen die gleichmäßige Aufteilung der Overhead-Kosten zu je einem Drittel auf die drei Abteilungen und zum anderen eine Aufteilung im Verhältnis der bereits direkt und indirekt zugewiesenen Kosten. Werden diese Kosten auf die bereits zugeteilten addiert, steht als Ergebnis der Gesamtkostenblock pro IT-Kunde respektive pro Abteilung, fest.

Wer sich überhaupt nicht für die betriebswirtschaftliche Seite der IT interessiert, dem sei gesagt: Es geht einfach nur um die Frage, wie die für einen Service oder einen Kunden erbrachten Leistungen finanziell umgelegt werden können. Und: Im Test macht der ITIL-Prozess Financial Management den kleinsten Fragenanteil aus.

17.4 Aufgaben und Aktivitäten des Financial Management

Eine kosteneffektive Betriebsführung erfordert genaue Vereinbarungen über die zu erbringenden Services sowie über die Kosten, die in diesem Zusammenhang verursacht werden. Ohne Kenntnisse über anfallende Kosten und die verwendeten Ressourcen zu den genutzten IT Services ist zukunftsgerechte Planung nicht nur für das Unternehmen schwierig. Die drei Subprozesse Finanzplanung, Kostenrechnung und Leistungsverrechnung des Financial Management helfen bei der Schaffung einer transparenten Kostenstruktur und -ermittlung.

1. Der Planungsaspekt des Financial Management schafft klare und definierte, konsistente Strukturen bezüglich der strategischen Unternehmensziele, der Geschäftsprozesse und der anfallenden Kosten. Werden im Rahmen der Unternehmens- und Strategieplanung die langfristigen Zielsetzungen eines Unternehmens ausgearbeitet, so werden für die jeweiligen Ziele eines Zeitraums Finanzpläne definiert. Die Finanzplanungsmethode ist abhängig von der Finanzpolitik, die in einem Unternehmen verfolgt wird:
   - Incremental Budgeting: Planung auf Basis der Vorjahreszahlen und der historischen Entwicklung.
   - Zero-Based Budgeting: Bei dieser Methode werden keine historischen Daten als Basis verwendet. Die Begründung der Ressourcen im Finanzplan erfolgt in Form von Kosten.

   Die Budgetierung stellt sicher, dass ausreichend liquide Mittel zum Betreiben der IT vorhanden sind, und erlaubt eine Kontrolle der Wirtschaftlichkeit. Um das Finanzplanvolumen festlegen zu können, müssen zunächst die Schlüsselfaktoren für die Wachstumsgrenzen eines Unternehmens bekannt sein. Dabei werden die folgenden Unterfinanzpläne erstellt:
   - Verkaufs- und Marketingfinanzpläne
   - Produktionsfinanzpläne
   - Managementfinanzpläne
   - Kosten- und Investitionsfinanzpläne

   Als Finanzplanungszeitraum wird in den meisten Fällen das Geschäftsjahr verwendet. Um bessere Kontrollen erwirken zu können, bieten sich kürzere Zeiträume an. Oft werden aus strategischen Gründen auch größere Zeitrahmen wie etwa drei oder fünf Jahre bei der Planung zugrundegelegt.
2. Bei der Kostenrechnung geht es um die Verteilung entstandener Kosten auf unterschiedliche Kostenposten (Kostenträger, -stellen). Im Mittelpunkt stehen die Frage, was die Kosten verursacht, und die anschließende Verrechnung anhand bestimmter Kriterien. Die Kostenartenrechnung beantwortet die Frage, welche Kosten während einer bestimmten Periode entstanden sind. Dabei werden alle Kosten nach Kostenarten (z.B. Materialkosten, Personalkosten, Raumkosten, Hardware-Kosten, Software-Kosten) gesammelt und gegenüber dem finanziellen Aufwand abgegrenzt. Die Kostenstellenrechnung gibt eine Antwort auf die Frage, an welcher Stelle der Unternehmung die Kosten entstanden sind. Deshalb werden Kostenstellen gebildet, d.h. die Unternehmung wird in Teilbereiche gegliedert,

welche einheitliche und kalkulierbare Leistungen erbringen. In der Kostenstellenrechnung werden die Gemeinkosten grundsätzlich nach dem Verursachungsprinzip diesen Kostenstellen zugerechnet. In der Kostenträgerrechnung werden die Einzelkosten und Gemeinkosten einer bestimmten Zeitperiode auf die einzelnen Kostenträger verteilt. Kostenträger sind Kalkulationsobjekte wie IT Services, welche im Servicekatalog aufgeführt sind.

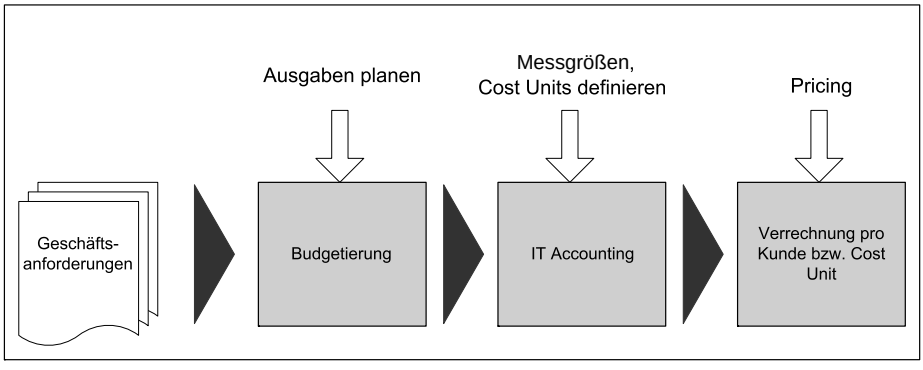


Abbildung 17.8: Prozessabfolge des Financial Management

3. Die Verrechnung von intern verursachten Kosten bzw. die Leistungsverrechnung (Charging) basiert auf dem Wunsch der IT-Organisation, sich sämtliche verursachten Kosten wieder hereinzuholen. Dies gilt als Re-Finanzierung der entstandenen IT-Kosten. Eine Verrechnung der Kosten für die erbrachten Services funktioniert allerdings nur, wenn die tatsächlich verursachten Nutzungskosten für die IT Services bekannt sind.

Bevor ein Preis festgesetzt wird, werden die Verrechnungsgrundsätze (Charging Policies) definiert. Es sind unterschiedliche Methoden für die Einführung der Leistungsverrechnung, z.B. von einer Stufenform bis hin zur realen Verrechnung, denkbar:

- Kommunikation der Informationen (Communication of Information, No Charging), um die Kunden für die Kosten zu sensibilisieren, die durch die Nutzung der IT-Leistungen durch ihre Abteilungen entstehen
- Pricing Flexibility: Preise werden pro Jahr ermittelt und verrechnet.
- Notational Charging: Die Leistungen werden zwar fiktiv in Rechnung gestellt, müssen jedoch noch nicht bezahlt werden. Diese Methode gibt der IT-Organisation die Möglichkeit, Erfahrungen zu sammeln und eventuelle Fehler zu korrigieren.

Die Ermittlung des Preises für einen bestimmten Service (Preisbildung) gestaltet sich häufig als sehr komplexes Unterfangen, das sich aus den folgenden Schritten zusammensetzt:

- Ermittlung der direkten und der indirekten Kosten
- Feststellung von Preisniveaus auf dem Markt
- Bedarfsanalyse des Services auf dem Markt
- genaue Analyse der Kundenzahl und der Konkurrenz

Neben der Re-Finanzierung der Kosten beeinflusst der Preis auch die Nachfrage nach dem Produkt bzw. Service. Dies dient als Instrument zur Nachfragesteuerung beim Kunden. So können auch neue Services mit relativ niedrigen Preisen eingeführt werden, die über andere etablierte Services unterstützt werden.

Es gibt unterschiedliche Preisstrategien, wie zum Beispiel:

- Cost Plus (Kosten plus Aufschlag): Enthält mehrere Berechnungsmodelle, die alle auf die Verrechnung verursachter Kosten plus Gewinnprozentsatz (Cost + % Aufschlag) hinauslaufen. Die Kosten und die Gewinnspanne können auf unterschiedliche Weise definiert werden:
  - Gesamtkosten einschließlich Gewinnmarge.
  - Nebenkosten plus Gewinnspanne (zur Deckung der durchschnittlichen Festkosten, Kosten pro Posten und Kapitalerträge ausreichend)
  - Eine der beiden oben genannten Möglichkeiten, jedoch mit einer Gewinnspanne von 0 %
- Going Rate (Geltender Preis): Betrifft Services, für die bereits Preisvereinbarungen existieren
- Target Return (Festpreis): Bezieht sich auf Services, für die bereits im Vorfeld die erforderlichen Erträge festgelegt wurden
- What the Market will bear (Marktpreis) im Sinne marktüblicher Preise
- Negotiated Contact Price (vereinbarter Preis): Der Preis wird mit dem Kunden ausgehandelt.

4. Berichtswesen für das IT Service Management: Je nach Verrechnungsgrundsätzen wird die festgestellte Nutzung an IT Services dem Kunden in Rechnung gestellt oder mitgeteilt. Als entsprechende Vereinbarungen können in Bezug auf den letzten Punkt beispielsweise monatliche Zusammenfassungen der Kosten und Einnahmen kommuniziert werden.

5. Berichtswesen für den Kunden: Normalerweise setzt das Unternehmen das Format fest, in das die Finanzdaten einfließen sollen. Detailinformationen können sich auf den IT-Verbrauch des letzten Jahres beziehen. Dazu gehört die Angabe, ob die tatsächlich aufgelaufenen Kosten den vorausgesagten Kostenprofilen entsprechen. Auch Angaben über die aktuellen Verrechnungsgrundsätze und die Kostenstellungsmethoden sowie Angaben, ob die IT Investitionen in bestimmten Bereichen vornimmt, sind möglich.

Hilfreich für die zukünftige Ausrichtung sind Informationen darüber, ob es irgendwelche Änderungen oder Abweichungen gibt, wodurch sie verursacht wurden und welche Gegenmaßnahmen einzuläuten sind.

17.5 Financial Management im ITIL-Gesamtzusammenhang

Das Financial Management für IT Services ist ein wichtiger Bestandteil für erfolgreiches IT Service Management. Es verschafft dem Unternehmen, bei richtiger Anwendung, wesentliche Management-Informationen darüber, ob die IT Services leistungsorientiert, wirtschaftlich und kostengünstig betrieben werden.

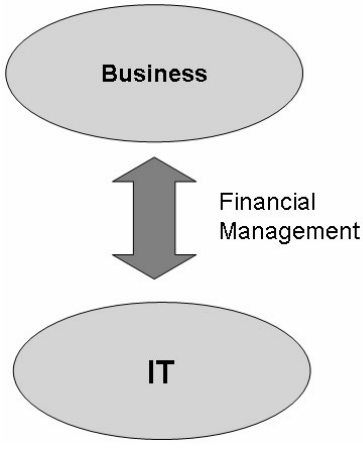


Abbildung 17.9: Enge Verbindung von IT-Organisation und Unternehmen

Ziel einer IT-Kostenrechnung muss es sein, die stark mit technischen, Input-orientierten Bezugsgrößen gemessenen IT-Leistungen in geeigneter Art und Weise für den Kunden aufzubereiten. Sie sind umzuformen und zu bündeln. So können output-orientierte IT-Kundenprodukte entstehen, die über Bezugsgrößen gemessen werden, die dem Kunden verständlich sind. Für den Kunden entsteht eine größere Transparenz, während gleichzeitig die Bereitstellung von Steuerungsinformationen für das IT-Management beibehalten werden kann. Die Transparenz für die Kundenseite kann noch weiter erhöht werden, indem ein Produkt- bzw. Servicekatalog erstellt wird, aus dem klar hervorgeht, welche IT-Leistungen zu welchen Konditionen verrechnet werden.

Aus dem Inhalt eines solchen Katalogs sollte hervorgehen, was welche IT Services und Produkte leisten. Daneben können weiteren Informationen wie etwa der Preis pro Bezugseinheit und die Bezugsgröße, bestimmte Bedingungen sowie Service Level Agreements aufgeführt werden. Service Level Agreements sind ein geeignetes Mittel, um dem Kunden die Kosten für eine IT-Dienstleistung differenziert auszuweisen. So wird betont, dass der Kunde nicht nur für die reine „Benutzungserlaubnis“ und den Betrieb einer Anwendung zahlt, sondern auch für weitere Merkmale wie Verfügbarkeit, Antwortzeiten und Zuverlässigkeit des Service. Der Kunde und die unterschiedlichen Abteilungen oder Fachbereiche verlangen nach Flexibilität. Je mehr Möglichkeiten ein SLA dem jeweiligen Kunden einräumt, die Service Levels zu variieren und auf seine eigenen Bedürfnisse abzustimmen, umso größer sind die Bedeutung und der potenzielle Vorteil der Leistungsverrechnung.

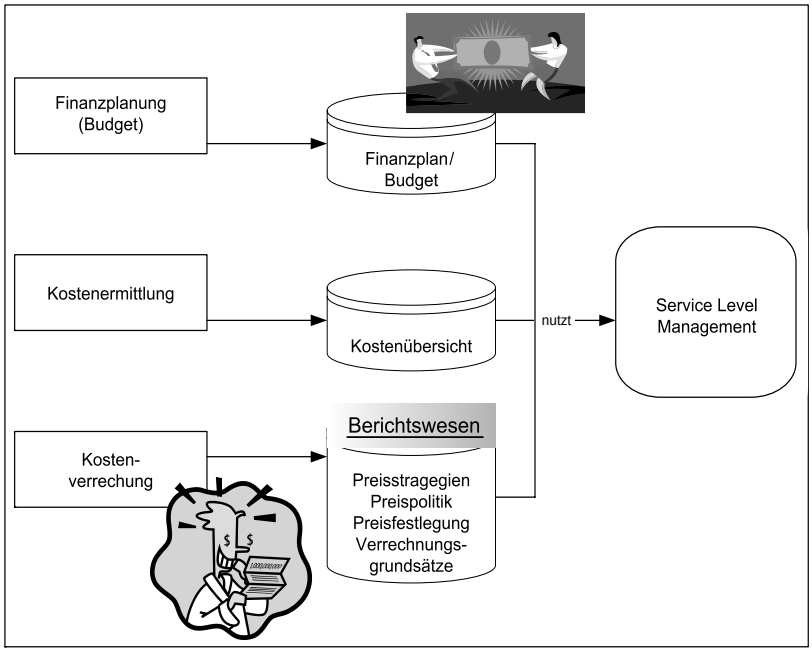


Abbildung 17.10: Zusammenarbeit Service Level Management und Financial Management

Kosten und Kapazität sind eng miteinander verknüpft. Das Capacity Management stellt sicher, dass die vorgehaltenen Rechner- und Speicherkapazitäten den Anforderungen des Kunden entsprechen und in Abstimmung mit der Budgetplanung kostengünstig zur Verfügung gestellt werden. Informationen über die Kosten werden im Rahmen der Kapazitätsplanung und Verfügbarkeit ermittelt. Die Verrechnung der Kapazität findet über die Leistungsverrechnung (Charging) statt. Die Kosten können, je nach Vereinbarung, mit dem einzelnen Kunden, mit dem Unternehmen als Ganzes oder über den Service an sich aufgeschlüsselt und verrechnet werden. Benötigen eine Abteilung oder einzelne Anwender besonders viel Plattenplatz, kann dies in Abstimmung zwischen Capacity Management und Financial Management entsprechend umgesetzt und in Rechnung gestellt werden.

Das Configuration Management kümmert sich um den Aufbau und die Pflege eines gesicherten Datenbestandes zu den Betriebsmitteln, den IT Services und deren Beziehungen zueinander zur Unterstützung aller anderen Service Management-Prozesse. Dies bezieht sich auf Daten zu Hardware, Software und anderen Configuration Items (CIs) sowie deren Beziehungen zueinander und betrifft auch Troubleshooting-Informationen und die Bestimmung der entsprechenden Auswirkungen innerhalb der IT-Infrastruktur. Die CMDB enthält allerdings auch Informationen aus dem Financial Management in Bezug auf die jeweiligen CIs, wie etwa die IT-Services und deren Verrechnung oder die Finanzdaten und die Produktrichtlinien (Policies). So stellt das Financial Management im Sinne eines Asset Managements betriebswirtschaftliche Informationen zu den IT-Komponenten bereit.

18 Security Management

Seit einigen Jahren sind die Themen Security und Security Management, nicht nur durch entsprechende Schadensmeldungen, in aller Munde. „Security“ wird als ein Synonym für Daten- und Netzwerksicherheit und den Datenschutz verwendet. „Security“ ist solange gewährleistet, wie Ihre Daten, Ihr System, Ihr Netzwerk oder Ihr Computer nicht durch Manipulationen, Schäden, Spionage, Sabotage oder Zerstörung zu Schaden kommen.

Mittlerweile gilt IT-Sicherheit als ein wichtiges Thema. Selbst große Firmen mussten zu der Einsicht gelangen, dass Sicherheit nur solange besteht, bis irgendjemand ihnen das Gegenteil beweist. Das gilt nicht nur für Hacker-Angriffe oder Virenwarnungen, sondern auch für das Thema Spionage und Datenmissbrauch. Die Erkenntnis, dass Unternehmens- und Mitarbeiterdaten ein schützenswertes Gut darstellen, und der sorgsame Umgang mit diesen Ressourcen stellt eine essenzielle Basis für den Unternehmenserfolg dar. Neben der firmeneigenen Motivation existieren auch externe Motivationsquellen, die der IT Security im Unternehmen einen besonderen Stellenwert einräumen: gesetzliche Bestimmungen wie der Sarbanes Oxley Act (SOX), KonTraG, BGB, AktG, GmbhG und HGB. Auch Basel II (Neuer Basler Akkord zur Eigenkapitalsicherung von Krediten) trägt zu dieser Entwicklung bei (siehe *Abbildung 18.1*).

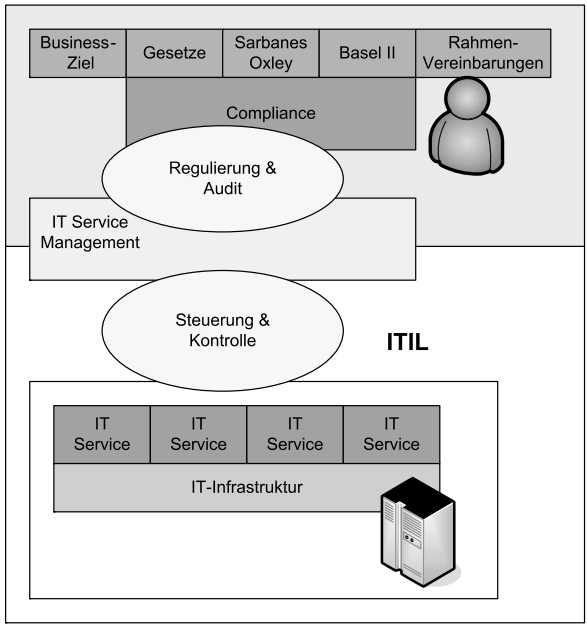


Abbildung 18.1:
Security Management im Spannungsfeld

Die Hauptaufgaben der Informationssicherheit bestehen in diesem Zusammenhang in dem kontrollierten zur Verfügung Stellen von Informationen und dem Schutz dieser Informationen vor unbefugtem Zugriff. Es geht um die beiden großen Bereiche Datenschutz und Datensicherheit. Die Themen rund um das Security Management sind vielfältig und allgegenwärtig: Passwörter, Firewalls, Intrusion Detection-Systeme, Viren- und Spam-Schutz.

18.1 Security Management nach ITIL

Security Management ist eine eigenständige ITIL-Disziplin, die vom OGC keinem der beiden ITIL-Bereiche Service Support und Service Delivery zugeordnet wurde. Dieser Prozess ist Gegenstand einer separaten Veröffentlichung. Security Management stellt eine übergreifende Disziplin dar, die alle anderen ITIL-Disziplinen tangiert. IT Security Management gehört im Gegensatz zum Service Support zum taktisch-strategischen Teil des IT-Bereichs mit operativen Auswirkungen. Vielfach wird es aus diesem Grund eher dem Bereich Service Delivery zugerechnet.

Security Management ist der Prozess zur Einführung und zur Erhaltung eines definierten Sicherheitsniveaus für Informationen, IT-Dienstleistungen und die IT-Infrastruktur. Es stellt sicher, dass den Geschäftsanforderungen entsprechende Sicherheitsrichtlinien implementiert und gepflegt werden. Dazu gehört, dass Security Incidents definiert behandelt werden. Diese Policies und Maßnahmen müssen mit Hilfe von Audits kontinuierlich überprüft, gemessen und bei Bedarf angepasst werden. Die Ergebnisse dieser Überprüfungen bilden die Basis für Reports, die über den Status der Sicherheitsmaßnahmen und deren Umsetzungsgrad berichten.

Security Management kümmert sich als Prozess um die definierten Ansprüche an die Security in Bezug auf Informationen und die IT Services im Unternehmen (*siehe Abbildung 18.2*). Dazu gehört auch die Reaktion auf einen sicherheitsrelevanten Zwischenfall. Security Incidents werden als Ereignisse betrachtet, die dem Unternehmen Schaden in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit von Daten und die entsprechenden Prozessen verursachen können.

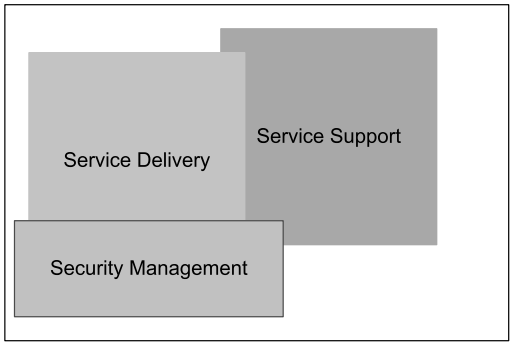


Abbildung 18.2: Security Management als eigenständige ITIL-Disziplin

Security Management gehört in die Management-Ebene, wo die notwendigen Verantwortlichkeiten erkannt und in Auftrag gegeben werden müssen, da es alle Bereiche des Unternehmens berührt. Das Engagement äußert sich auf strategischer Ebene

in Form von Vorgaben für das Security Management, entsprechender Informationspolitik sowie in Form von Informationsplänen. Auf operativer Ebene zeigt sich dies durch die Anschaffung von Sicherheitsprodukten/-Tools, Projekte sowie durch das Verhalten und die Aktivitäten der Mitarbeiter. Security Management ist Chefsache. Die Umsetzung Security-relevanter Maßnahmen ohne Management-Unterstützung ist nur in seltenen Fällen von Erfolg gekrönt.

Die Informationssicherheit sollte auf den Stellenwert der jeweiligen Informationen für das Unternehmen abgestimmt werden. Dieses Abstufungsmodell wird als Kompromiss dargestellt. Dieser bewegt sich zwischen den möglichen Sicherheitsmaßnahmen einerseits und dem Wert der Information sowie der Bedrohungen andererseits. Dies ist unter zwei Gesichtspunkten von Bedeutung. Zum einen kann ein Unternehmen nur dann funktionieren, wenn den Arbeitsabläufen rechtzeitig die richtigen und vollständigen Informationen zur Verfügung gestellt werden. Zum anderen reichen die Geschäftsabläufe eines Unternehmens durch die Verarbeitung von Informationen Produkte und Services nach außen, um vereinbarte Ergebnisse zu liefern, die oft ebenfalls als Informationen ausgegeben werden. Ist dem nicht so und können Ergebnisse nicht entsprechend den Zielvorgaben erreicht werden, kann der Geschäftserfolg des Unternehmens gefährdet sein. Diese Gefährdungen sollen durch den Einsatz der IT Security zumindest reduziert, wenn nicht sogar eliminiert werden. Dazu wird eine unternehmensweite Richtlinie aufgesetzt, die sich auch in den SLAs niederschlägt.

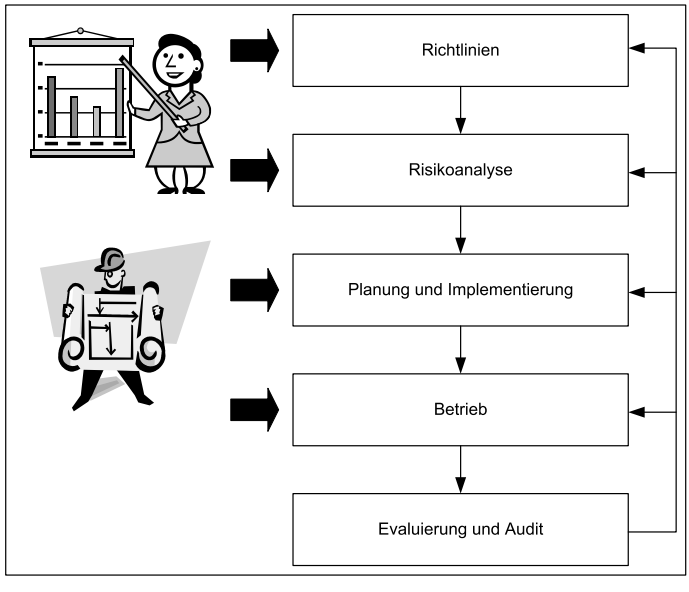


Abbildung 18.3: Security Management ist kein statischer Prozess

IT Security Management-Prozesse befassen sich jedoch nicht nur mit der Implementierung bedarfsgerechter IT Security. Hier geht es auch um eine kontinuierliche Überwachung der Sicherheitsmaßnahmen, um die Effektivität und Effizienz fortwährend bewerten zu können (*siehe Abbildung 18.3*). Daraus leitet sich eine Grundlage für neuerliche Anpassungen und weitere Maßnahmen ab. Dazu gehört, dass

die definierten Sicherheitsanforderungen und -maßnahmen auch bei geänderten Anforderungen oder einer sich verändernden IT-Umgebung gewährleistet werden. Security-Management ist niemals statisch. Die Aktivitäten innerhalb des Security Management sollten also ständig überprüft und überarbeitet werden, um ihre Effektivität zu erhalten. Das Security Management lehnt sich ebenso wie beispielsweise das Service Level Management an den Qualitätskreis von Deming an.

18.2 Begriffe und Definitionen des Security Management

Das Security Management ist auf die Gewährleistung der Sicherheit von Informationen ausgerichtet. Sicherheit (Safety) als Begriff wird hier als die Sicherheit vor bekannten Risiken und die größtmögliche Vorbeugung vor unbekannten Risiken verwendet. Schutz (Security) ist das Mittel, das zu diesem Zweck eingesetzt wird. Es ist der Wert der Information für das Unternehmen, der geschützt werden muss. Dieser Wert kann nur vom Unternehmen definiert werden und wird für den Bereich der IT-Organisation von den Aspekten der Vertraulichkeit, der Integrität und der Verfügbarkeit bestimmt (CIA, *siehe Abbildung 18.4*):

- Vertraulichkeit (Confidentiality): Schutz von Informationen vor unautorisierter Einsicht und unbefugter Benutzung. Es geht zum einen darum, Daten im Sinne des Datenschutzes zu schützen. Zum anderen muss gewährleistet werden, dass nur Personen, die Zugriff auf bestimmte Daten haben sollen, diesen auch bekommen. Alle anderen dürfen nicht auf diese Daten zugreifen (selektiver Datenzugriff).
- Integrität (Integrity): die Richtigkeit, die Vollständigkeit und der korrekte Zeitpunkt der Informationsübermittlung. Dies ist ein Grund, warum Verschlüsselungs- und Signierungsmechanismen zum Einsatz kommen.
- Verfügbarkeit (Availability): Verfügbarkeit über die Informationen zu jedem gewünschten Zeitpunkt innerhalb des vereinbarten Zeitraums. Voraussetzung hierfür ist die Kontinuität der entsprechenden IT-Mittel, die die Informationen bereitstellen. Daten müssen verfügbar sein.

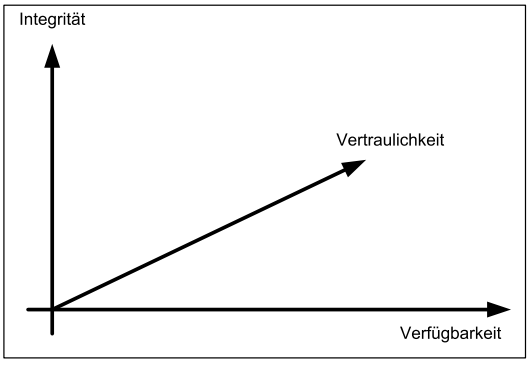


Abbildung 18.4: Kernfaktoren der Sicherheit

Daraus abgeleitete Aspekte sind die Privacy (die Vertraulichkeit und Integrität einer auf eine natürliche Person zurückzuführenden Information), Anonymität und Kontrollierbarkeit, d.h. die Möglichkeit, den richtigen Umgang mit der Information verifizieren und die richtigen Auswirkungen der Sicherheitsmaßnahmen nachweisen zu können.

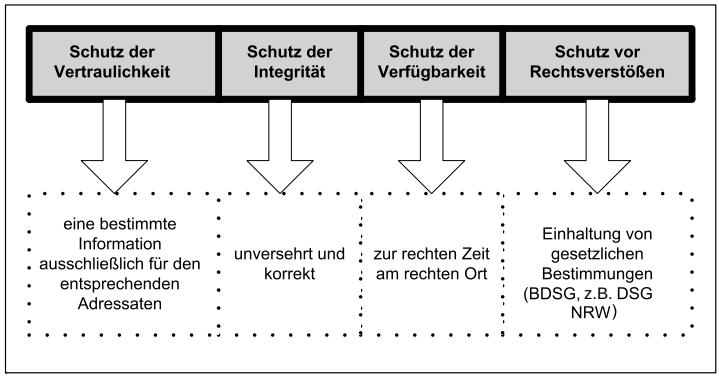


Abbildung 18.5: Aspekte der IT-Sicherheit

Für die Umsetzung dieser Anforderungen ist die IT-Organisation verantwortlich. Das Security Management stellt sicher, dass der IT Service stets auf einer mit dem Kunden vereinbarten Sicherheitsstufe erbracht wird. Das Security Management sorgt für die strukturelle Integration der Sicherheit in der IT-Organisation aus der Sicht des Service-Anbieters.

Ausgangspunkt bei der Erstellung des Sicherheitsparagraphen im SLA ist der Sicherheitsbedarf des Kunden (*siehe Abbildung 18.6*). Der Vertreter des Service-Abnehmers (der Kunde) und der Vertreter des Service-Anbieters (die IT-Organisation) führen diesbezüglich Verhandlungen. Im Servicekatalog werden auch die möglichen Sicherheitsmaßnahmen angeboten, wie etwa der Basisschutz, auch Security Baseline genannt. Über diesen Grundschutz hinaus kann der Kunde zusätzlichen Bedarf anmelden.

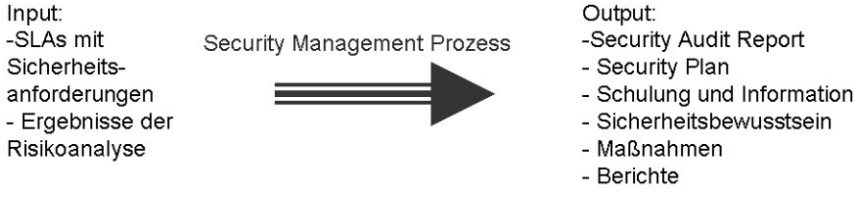


Abbildung 18.6: Der Security Management-Prozess

Das notwendige Maß an IT Security resultiert aus einer Risikoanalyse, die sowohl der Kundensicht (Business Perspective) als auch der technischen Sicht (Technical Perspective) entsprechen muss. Diese Analyse führt zu den Service Level Requirements für die IT-Sicherheit. Das Ergebnis dieser Analyse basiert auch auf dem aktuellen Status und der Qualität der momentan vorhandenen IT Security im Unternehmen. Die so entstandenen Richtlinien in Bezug auf die Security bilden die Basis

für Sicherheitskonzepte und –maßnahmen. All dies fließt als definierte Vereinbarung in die Service Level Agreements (SLAs) ein. Hieraus resultiert ein „Security Implementation Plan", in dem die notwendigen Sicherheitsmaßnahmen festgeschrieben werden. Die Maßnahmen dieses Plans werden implementiert und ständigen Reviews und Audits mit dem Ziel einer kontinuierlichen Verbesserung unterworfen. Dem Kunden wird darüber regelmäßig Bericht erstattet. So kann der Kunde auf der Grundlage dieser Berichte seine Anforderungen und Wünsche überprüfen und bei Bedarf anpassen. Darüberhinaus kann die IT-Organisation den Plan bzw. dessen Umsetzung modifizieren oder aber die Anpassung der Vereinbarungen in Bezug auf die IT Security im SLA anstreben.

Deswegen ist es auch wichtig, dass bei der Erstellung eines SLAs messbare Key Performance Indicators (KPIs) und Leistungskriterien definiert werden. Dabei stellen die Leistungsindikatoren (KPIs) die messbaren Größen (Metrik) dar. Die Leistungskriterien stehen für die erreichbaren Zahlenwerte der IT-Sicherheit. Die Lieferung der entsprechenden Kennbereiche und Zahlenwerte als Berechnungsgrundlage gestaltet sich oft als schwierig. Die Verfügbarkeit beispielsweise lässt sich anhand dieser Bewertung meist noch in einer Zahl ausdrücken, in Bezug auf die lntegrität und die Vertraulichkeit von Daten gestaltet sich diese Aktion als schwieriger. Security Management ist eine Aufgabe, die sich nicht auf die technische Überwachung reduzieren lässt.

18.3 Aufgaben und Aktivitäten des Security Management

Das Security Management ist ein zyklisches System, das sich mit der Steuerung, der Richtlinien-Definition (Policies) und der Organisation der Informationssicherheit auseinandersetzt. Dazu gehören auch die Planung, Implementierung, Evaluierung und Anpassung in Form von Aktualisierungen, falls dies notwendig ist. Wie in vielen anderen ITIL-Prozessen kommt auch dem Security Management die wichtige Aktivität des Reportings zu. Es ist unabdingbar, dass dem Kunden regelmäßig Rechenschaftsberichte von der IT-Organisation zur Verfügung gestellt werden. Nur so können die sicherheitsrelevanten Anforderungen aus den SLAs überprüft werden:

1. Steuerung, Grundsätze, Richtlinien und Organisation der Informationssicherheit: Die Steuerung organisiert und kontrolliert das Security Management selbst. Es steht als lenkende und kontrollierende Aktivität im Mittelpunkt des Prozesses (*siehe Abbildung 18.7*). Es legt die Sicherheitsgrundsätze und die Organisation der Informationssicherheit im Rahmen des Sicherheitskonzeptes des Unternehmens fest. Dabei werden Fragen beantwortet wie etwa: Wie kommen Sicherheitspläne zustande? Wie werden diese Pläne implementiert? Wie wird die Implementierung überprüft?

   Innerhalb dieser Aktivität geht es konkret um die Entwicklung und Implementierung der Policies (unter Berücksichtigung der Beziehungen zu anderen Unternehmensgrundsätzen). Diese führen in Interaktion mit den Zielvorgaben und allgemeinen Prinzipien zur Beschreibung der Teilprozesse. Auch Funktionen

und Verantwortliche für die Teilprozesse werden ermittelt. Hier wird zudem das Zusammenspiel mit anderen ITIL-Prozessen und deren Organisation definiert, wie etwa die allgemeinen Verantwortlichkeiten von Mitarbeitern.

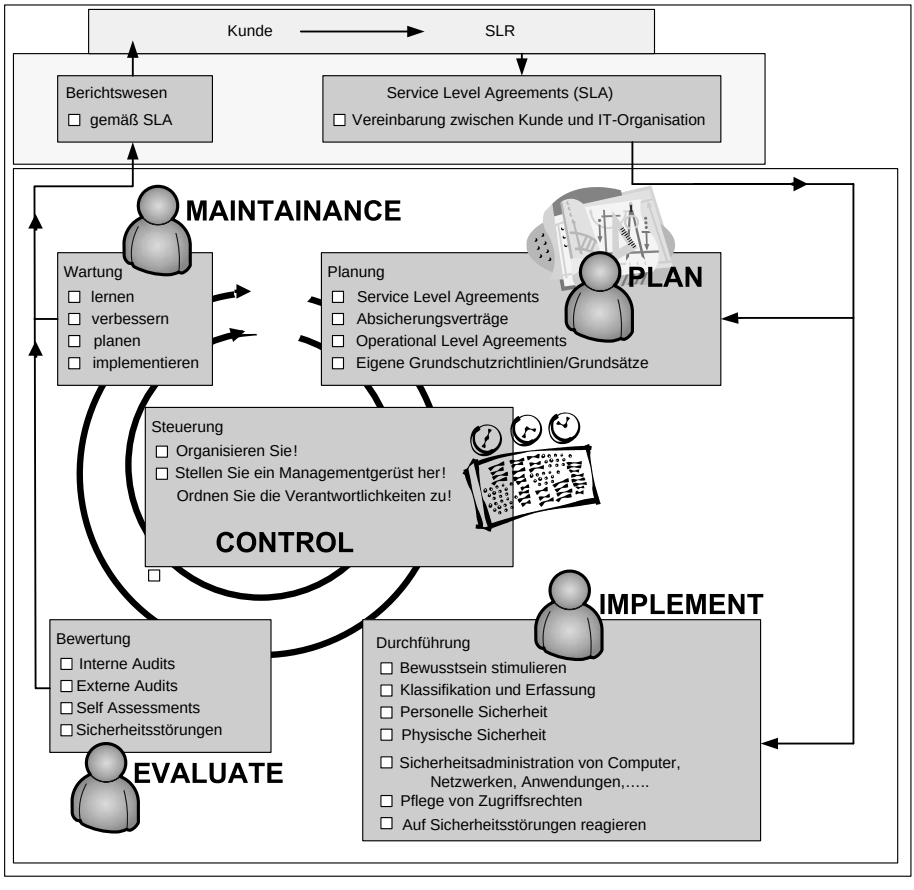


Abbildung 18.7: Abläufe des Security Management-Prozesses

Bei der Organisation in Sachen IT Security geht es um die Erstellung eines Rahmens anhand der Organisationsstruktur mit einer genauen Zuteilung von Verantwortlichkeiten. Dazu gehört die Einrichtung einer Steuerungsgruppe für Informationssicherheit im Zusammenhang mit einer entsprechenden Koordinierung. Wichtig sind auch eine Regelung zur Zusammenarbeit zwischen Organisationseinheiten und Partnern, die diesbezügliche interne und externe Kommunikation, Absprachen zur unabhängigen Beurteilung (IT Security-Audit) und zur Informationssicherheit in Verträgen mit Dritten.

2. Planung: Innerhalb dieses Subprozesses werden die Aktivitäten beschrieben, die dazu führen, dass die sicherheitsrelevanten Informationen in die SLAs einfließen. Dies betrifft auch die Absicherungsverträge (Underpinning Contracts), soweit diese spezifisch für die Sicherheit sind. Die allgemein formulierten Zielvorgaben

im SLA werden in den Operational Level Agreements (interne Vereinbarungen auf Betriebsebene, OLAs) differenziert und näher spezifiziert. OLAs können in diesem Zusammenhang als Spezifizierung der IT-Organisationseinheit gesehen werden.

Dieser Subprozess steht in enger Verbindung zum Service Level Management. Die Einzelheiten müssen gewährleisten, dass sämtlichen Sicherheitsanforderungen und -normen des Kunden nachweisbar entsprochen werden kann. Änderungen laufen unter der Kontrolle des Change Management, wobei der Security-Manager dafür Sorge zu tragen hat, dass die entsprechenden Informationen weitergegeben werden.

Security-Manager: Ein „Hut" im Security Management

Während in kleinen IT-Organisationen mehrere Prozesse von einer einzigen Person betreut werden können, sind in großen Organisationen zumeist mehrere Mitarbeiter mit einem Prozess befasst, z.B. im Security Management. Im letztgenannten Fall ist immer eine Person als Security-Manager zu benennen, die dann dafür verantwortlich ist, dass der Security Management-Prozess reibungslos funktioniert. Das Pendant auf der Kundenseite ist der (unternehmensweite) Sicherheitsbeauftragte.

3. Implementierung: Dieser Prozessabschnitt hat dafür Sorge zu tragen, dass die geplanten und festgeschriebenen Sicherheitsanforderungen auch wirklich umgesetzt werden. Die Forderungen können aber nur in die Praxis umgesetzt und von allen gelebt werden, wenn ein entsprechendes Bewusstsein und die nötige Motivation entwickelt wurden. Dazu gehören auch verständliche Dokumentationen und Prozeduren für alle Beteiligten.

   So ist besonders zu betonen, wie wichtig es ist, dass ein Security-Incident überhaupt als solcher erkannt wird. Dementsprechend müssen konkrete Vorgaben entwickelt werden, wie das Vorgehen bei Sicherheitsstörungen auszusehen hat. Hier sind ähnliche Aktivitäten wie in Bezug auf den „normalen Incident" notwendig, wie beispielsweise eine Störmustererkennung und ggf. eine Zuordnung zu Störungen, die in der Vergangenheit bereits aufgetreten sind. Auch die Registrierung eines Security Incident muss entsprechend vorgenommen werden.

   Weitere Stichworte zu dieser Aktivität sind Klassifizierung und Kontrolle von IT-Werkzeugen, personelle Sicherheit (Verpflichtungserklärungen, Schulungen, Richtlinien und Anweisungen), Sicherheit im IT-Betrieb (Trennung von Funktionen, Verhaltensregeln, Trennung von Produktions- und Testumgebung, Virenschutz, Datenträgerthemen, Implementierung spezieller Maßnahmen und Tools) und Zugriffsschutz (Zugriffsrechte und entsprechende Grundsätze, Sammlung und Pflege der sicherheitsrelevanten Einstellungen).

4. Evaluierung: Der Glauben an eine sichere Implementierung aus den SLA-Anforderungen reicht nicht aus. Umgesetzte sicherheitsrelevante Maßnahmen müssen immer wieder auf den Prüfstand gestellt werden. Zum einen, um zu kontrollieren, ob sie auch wirklich das tun, was sie tun sollen, nämlich vor bestimmten Szenarien Schutz und Sicherheit bieten. Zum anderen bieten neue technische

Errungenschaften auch im Sicherheitsbereich neue Möglichkeiten für die Implementierung. Kurz: Eine Evaluierung ist von größter Bedeutung. Diese Evaluierung ist nicht nur für die Bewertung des eigenen Unternehmens, sondern auch für den Kunden und andere Dritte erforderlich.

Dabei geht es neben der Überprüfung der geforderten Sicherheitsgrundsätze und der Implementierung von Sicherheitsplänen auch um eine allgemeine Sicherheitskontrolle für die IT-Komponenten und die Infrastruktur.

Evaluierung tangiert Standards und Richtlinien. Das Ergebnis hat Auswirkungen auf die aktuellen Grundlagen für den Security-Bereich. Sie kann auch Anlass zu Änderungen geben. In diesem Fall wird ein Request for Change (RfC) an das Change Management gestellt. Dabei werden drei Arten der Evaluierung unterschieden :

- Self Assessments (meist von den Prozessbeteiligten selbst durchgeführt)
- Interne Audits (von internen IT-Sicherheits-Auditoren durchgeführt)
- Externe Audits (von externen IT-Sicherheits-Auditoren durchgeführt)

Die Audits sollten wegen der erforderlichen Trennung der Funktionen nicht von denselben Mitarbeitern vorgenommen werden, die bereits andere Prozesse überwacht haben. Darüber hinaus sollte auch eine Evaluierung auf der Grundlage der gemeldeten Sicherheitsstörungen stattfinden, die an das Problem Management zur Zusammenfassung und Trenduntersuchung weitergeleitet werden. Die wichtigsten Aktivitäten sind:

5. Pflege und Wartung: Im Sinne der Anforderung einer ständigen Prozessverbesserung muss sich auch das Security Management diesem Zyklus von Plan-Do-Check-Act unterziehen. Die ständige Aktualisierung des Security Management-Prozesses bezieht sich auf die Infrastruktur, die Organisation und die Prozesse im Unternehmen. Dies umfasst auch die Sicherheitspläne, Handbücher, Maßnahmenkataloge und Vereinbarungen wie die Operation Level Agreements (OLAs).

   Die Aktualisierung der Sicherheitsmaßnahmen basiert auf den Ergebnissen der regelmäßigen Audits und Reviews der anderen Subprozesse und allgemeinen neuen Erkenntnissen im Sicherheitsbereich. Daraus können sich auch neue Anforderungen ergeben, die in die SLAs einfließen. Die Änderungen selbst erfolgen dann im Rahmen des normalen Change Management-Prozesses.

6. Reporting: Das Berichtswesen dient den anderen Subprozessen im Security Management als Basis für deren Entscheidungen (z.B. beim Review und bei der Evaluierung). Des Weiteren werden Berichte an den Kunden entsprechend der Maßgabe in den SLAs versendet. Regelmäßige Berichte helfen dem Kunden, nicht nur in Bezug auf das Security Management sich ein aktuelles Bild zu verschaffen. Die IT-Organisation kann dem Kunden gegenüber Rechenschaft über die gelieferten Sicherheitsservices ablegen. Zudem erhält der Kunde Berichte über die Sicherheitsstörungen. Daneben können Berichte auch Sicherheitsjahrespläne, Aktionspläne und eine Statusübersicht über die Implementierung von Informationssicherheit enthalten. Unter diesen Punkt fällt der Fortschritt der Realisierung in Bezug auf den Sicherheitsjahresplans. Dazu gehören auch eine Übersicht über implementierte oder noch zu treffende Maßnahmen, Schulungen und Ergebnisse zusätzlicher Risiko-Analysen. Die Identifikation von Trends

und Störungen informiert den Kunden über Vorfälle und Voraussagen. Es ist wichtig, dass Berichte nicht nur Statusinformationen über aktuelle Maßnahmen liefern, sondern auch, dass Informationen über die Auswirkungen der Maßnahmen kommuniziert werden.

18.4 Security Management im ITIL-Gesamtzusammenhang

Im ITIL-Regelwerk zum IT Service Management finden sich an verschiedenen Stellen Verweise auf Sicherheitsaufgaben. Generell gilt: Wenn Aktivitäten in anderen Prozessen gewünscht sind, dann muss eine Abstimmung mit diesen Prozessen stattfinden.

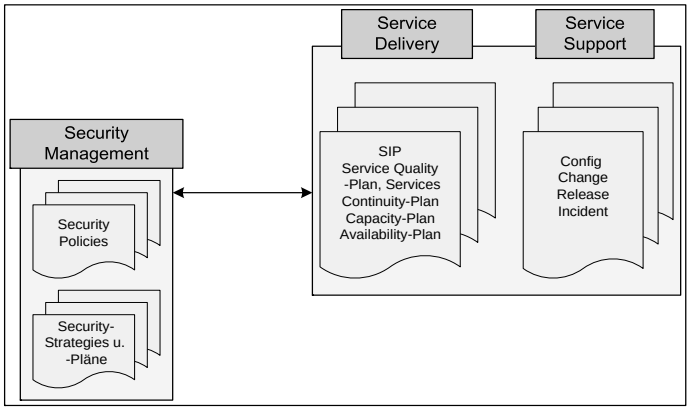


Abbildung 18.8: Security Management steht in Interaktion mit Service Support und Service Delivery

Notwendige Änderungen an der IT-Infrastruktur kommen nur über den Change Management Prozess zu Stande. Das Security Management liefert den nötigen Input. Verantwortlich für den Change Management-Prozess ist jedoch der Change-Manager, unter dessen Regie der Change umgesetzt wird. Allerdings entstehen viele sicherheitsrelevante Probleme erst durch unkoordinierte oder unkommunizierte Veränderungen (Changes). Daher sollten Changes, die mögliche Auswirkungen auf die IT-Sicherheit mit sich bringen, im Change Management besondere Berücksichtigung finden. Es ist allerdings nicht beabsichtigt, den Security-Manager bei jeder Änderung einzuschalten. Er ist jedoch ein möglicher Kandidat für das Change Advisory Board (CAB). Das Change Management kann auch die Aspekte der Verfügbarkeit, Vertraulichkeit und Integrität tangieren. Anhand dieser Risikoklassifizierung lässt sich der Change-Prozess entsprechend den Sicherheitsanforderungen durchführen und kommunizieren. Bereits die Service Level-Vereinbarungen (SLAs) und die korrespondierenden Einträge in der CMDB müssen Sicherheitsparameter enthalten.

Das Configuration Management arbeitet in Bezug auf die IT-Sicherheit Hand in Hand mit dem Security Management, dem Change Management und dem Service Level Management. Auch in Bezug auf diese Kooperation spielt die Configuration

Management Database (CMDB) eine wichtige Rolle. Über eine sicherheitsrelevante Klassifizierung werden CIs mit einem bestimmten Maßnahmenkatalog oder einem Verfahren verknüpft. Diese Verknüpfung bietet Informationen zur gewünschten Vertraulichkeit, Integrität und/oder Verfügbarkeit dieses CI und wird aus den Sicherheitsanforderungen des SLA abgeleitet. Die Klassifizierung in Sicherheitsstufen erfolgt auf der Grundlage einer Analyse, welche die Abhängigkeit der Unternehmensprozesse von den Informationssystemen und den eigentlichen Informationen untersucht.

Das Service Level Management sorgt dafür, dass Anforderungen und Vereinbarungen über die Services, die für die Kunden erbracht werden sollen, festgelegt, kontrolliert und befolgt werden. In diesen SLAs sollten die Vereinbarungen über die zu ergreifenden Sicherheitsmaßnahmen festgehalten werden. Insofern ist das Service Level Management für die Vorgaben des Security Management verantwortlich. Diese Vorgaben werden zur Überprüfung Analysen unterzogen. Diese Informationen bedingen den Rahmen für die mit dem Kunden vereinbarte Sicherheitsstufe im Service Level Agreement (SLA). Die Anforderungen an die Sicherheit der IT Services finden sich auch in den Service Level-Anforderungen (SLR) und im Servicekatalog der IT-Organisation. Die Definition des SLA stimmt das Security Management mit dem Service Level Management anhand der sicherheitsrelevanten Anforderungen ab. Für diese Abstimmung ist der Service Level-Manager verantwortlich. Auch die Inhalte von internen und externen Vereinbarungen (OLA, UC) spiegeln die Security-Anforderungen wider. Deshalb ist es wichtig, Leistungsindikatoren (KPIs) zu definieren, mit deren Hilfe die Kontrolle erfolgen kann, ob die geforderten Maßnahmen umgesetzt wurden.

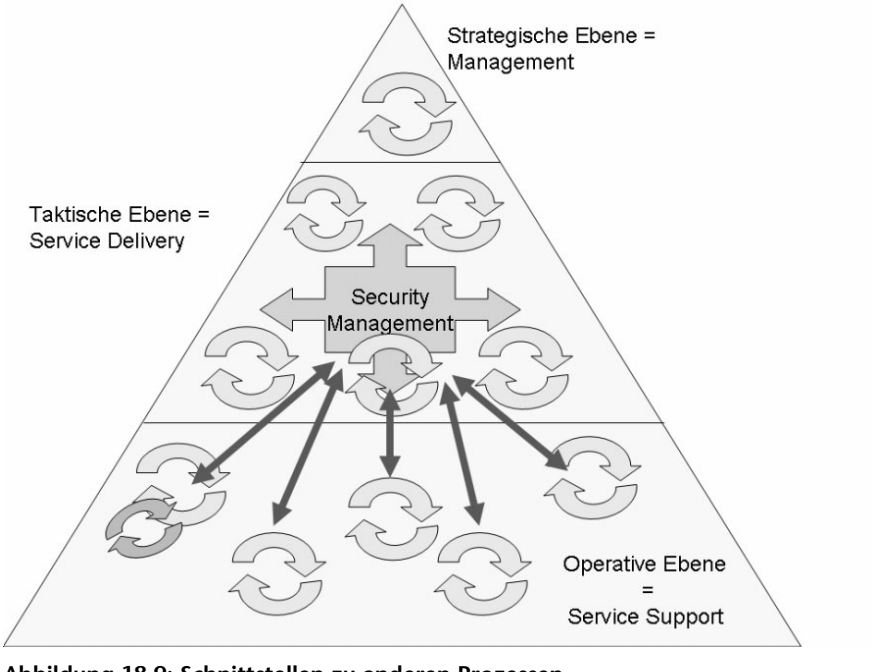


Abbildung 18.9: Schnittstellen zu anderen Prozessen

Im Incident Management erfolgt die Annahme, Erkennung und Registrierung von Security Incidents. Je nach Impact einer sicherheitsrelevanten Störung kann für diesen Prozess ein anderes Verfahren als für die normalen Störungen gelten. Es ist also äußerst wichtig, dass das Incident Management eine Sicherheitsstörung als solche erkennt. Bei Sicherheitsstörungen handelt es sich ohnehin um Störungen, welche die Einhaltung der Sicherheitsanforderungen aus dem SLA verhindern können, also die Einhaltung des SLAs gefährden. Es empfiehlt sich, in die SLA eine Übersicht über die Art der Störungen aufzunehmen, die als Sicherheitsstörungen zu betrachten sind.

Nur wenn eine Sicherheitsstörung erkannt wird, ist es möglich, das richtige Verfahren zur Behandlung dieses Incident-Typs einzuleiten. Neben dem jeweiligen Verfahren im SLA muss ein Weg für die Kommunikation im Hinblick auf Sicherheitsstörungen vereinbart werden, um eine Ausbreitung der Störung (Virenbefall) zu verhindern oder dafür zu sorgen, dass ein Sicherheitsloch (Firewall, DoS) möglichst schnell gestopft wird. Störungsmeldungen müssen nicht immer von Kundenseite oder einem Anwender herrühren. Auch das Security Management kann aufgrund von bestimmten Vorkommnissen einen Incident anzeigen.

Die Ursachen bei sicherheitsrelevanten Problemen liegen in der Hand des Problem Management. Auch die Initialaktionen zur Behebung von Sicherheitsmängeln werden vom Problem Management angestoßen. Ein Problem kann auch in Form eines Sicherheitsrisikos auftreten. Das Problem Management sollte in diesem Fall das Security Management in die Bearbeitung des Problems miteinbeziehen.

Auch auf das Release Management kommen besondere sicherheitsrelevante Anforderungen zu. Sämtliche Rollouts müssen über das Release Management kontrolliert und in Abstimmung mit dem Change Management ausgerollt werden. Mögliche Auswirkungen auf die Sicherheit sollten stets überprüft werden. Eine besondere Rolle kommt dem Release Management beim Stopfen von Sicherheitslöchern zu. Über das Installieren von Fixes oder Patches werden im Zuge der Softwareverteilung Risiken eliminiert. Rasches Handeln ist bei der Veröffentlichung möglicher Sicherheitsrisiken gefragt. Dabei sollte allerdings nicht vergessen werden, dass auch Patches nicht immer frei von Fehlern sind und diese getestet werden sollten. Hier ist ein Abwägen des Unternehmens zwischen Zeitdruck und Vermeidung von Ausfällen durch fehlerhafte Patches notwendig.

Availability Management und Security Management arbeiten eng zusammen. Das Thema Verfügbarkeit fließt unmittelbar in den Sicherheitsbegriff ein. Über das Availability Management wird aus den Geschäftsanforderungen ein kosteneffizientes und servicespezifisches Verfügbarkeitsniveau definiert, die Umsetzung geplant und die definierten Qualitätsparameter (Key Performance Indicators) überwacht. Dabei wird neben einer Optimierung der Verfügbarkeit durch Überwachung auch der Vergleich zur Service-Verfügbarkeit mit den SLAs umgesetzt. Da viele Sicherheitsmaßnahmen die Aspekte Verfügbarkeit, Vertraulichkeit und Integrität tangieren, ist eine Abstimmung hinsichtlich der zu ergreifenden Maßnahmen zwischen dem Availability Management, dem Continuity Management for IT Services und dem Security Management notwendig.

Das Continuity Management kümmert sich um die Erstellung von Plänen zur Wiederherstellung von IT Services nach einer Katastrophe und führt u.a. Risiko-Analysen durch (*siehe Abbildung 18.10*). Es kümmert sich darum, dass nach einem unvorhersehbaren Zwischenfall die Folgen für den IT Service auf ein definiertes Maß, das in den SLAs festgeschrieben wurde, beschränkt bleiben. Aufgrund der Sicherheitsaspekte dieses Themas bestehen Beziehungen zum Security Management.

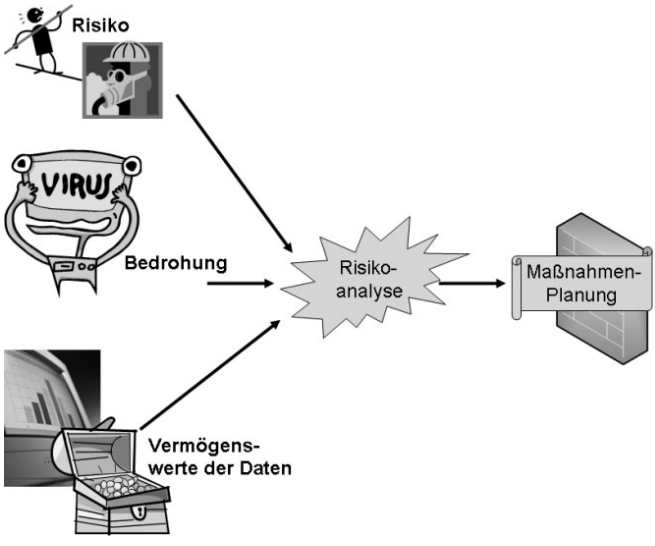


Abbildung 18.10: Aktivitäten des IT Continuity Management

Das Capacity Management kümmert sich um die Gewährleistung der Kundenanforderungen in Bezug auf eine rechtzeitige und kostengünstige Bereitstellung der erforderlichen und definierten Ressourcen. Die Anforderungen stammen aus den qualitativen und quantitativen Rahmen, die durch das Service Level Management erstellt werden. Fast alle Aktivitäten des Capacity Management stehen in einer Beziehung zur Verfügbarkeit. Da dieser Begriff nicht nur mit dem Availability Management in Verbindung steht, sondern auch ein Aspekt des Begriffes Sicherheit darstellt, existiert hier auch eine Verbindung zwischen Capacity Management und Security Management.

19 Beispielfragen zum Bereich Service Delivery

Aufgabe des Service Delivery ist die Durchführung der planerischen und steuernden Prozesse zur professionellen Durchführung der IT-Dienstleistungen auf taktischer Ebene. Ziel ist es, dass die Anforderungen zwischen Kunden und IT-Bereich bestmöglich getroffen, geplant und überwacht werden können. Dies steht im Zusammenhang mit einer besseren Kundenorientierung und der Anforderung, damit verbundene Aufwendungen wirtschaftlich optimal umzusetzen und verrechnen zu können. Zu den Modulen des Service Delivery zählen:

- Availability Management
- Capacity Management
- Continuity Management
- Financial Management for IT Services
- Service Level Management

Die nachfolgenden Fragen beziehen sich auf den Service Delivery-Set. Wichtig ist für Sie vor allem die Kenntnis über die genaue Aktivitätenabfolge innerhalb der Prozesse. Machen Sie sich klar, welches Ziel welcher Prozess hat und wo welche Verantwortlichkeiten liegen. Noch einmal zusammengefasst für diesen Bereich von ITIL ergeben sich folgende Punkte:

- Service Level Management: Vereinbarungen über IT Services, Bedürfnisse und Möglichkeiten, Abstimmung und Überwachung
- Availability Management: Misst und gewährleistet Verfügbarkeit, Mittel, Methoden, Techniken
- Continuity Management: Vorbereitung und Planung von Kontinuitätsmaßnahmen, Fokus: Kundenorganisation
- Capacity Management: Optimierung des IT-Ressourcen-Einsatzes, Management und Optimierung von Leistungen/Ressourcen, Schwerpunkt: Planung
- Financial Management: Betriebswirtschaftlich vertretbare Nutzung der IT Services, Budgeting, Accounting, Charging
- Security Management: Schutz der IT-Infrastruktur, SLAs, Gesetze, Anforderungen, Verträge, Integrität, Vertraulichkeit, Verfügbarkeit

IT Service Management nach ITIL besteht aus zwei Prozessgruppen:

- Service Support umfasst die Prozesse zur direkten Unterstützung der Nutzer im täglichen Betrieb (operationelle Ebene)
- Service Delivery befasst sich mit der mittel- bis langfristigen Planung und Verbesserung der IT Services (taktische Ebene).

Welcher ITIL-Prozess verhindert einen nicht autorisierten Datenzugriff?

A. Availability Management
B. IT Service Continuity Management
C. Release Management
D. Security Management

Lösung: D. Security Management: Bei diesem Prozess geht es um die Erfüllung der Sicherheitsanforderungen und der Schaffung eines IT-Grundschutzes. Availability Management beschäftigt sich mit der Verfügbarkeit. Continuity Management stellt sicher, dass Services nach einem Notfall wieder zur Verfügung stehen.

Es wurde eine Analyse bezüglich des Wachstums einer wichtigen Datenbank vorgenommen. Diese weist aus, dass die Speicherkapazität und ggf. andere Ressourcen aufgrund des weiteren Wachstums der Datenbank in der näheren Zukunft wahrscheinlich erweitert werden müssen. Welcher ITIL-Prozess muss dafür sorgen, dass diese Information rechtzeitig weitergeleitet wird, um das Entstehen von Speicherengpässen zu vermeiden?

A. Availability Management
B. Capacity Management
C. Change Management
D. Security Management

Lösung: A. Availability Management: Dieser Prozess muss die Verfügbarkeit der Services, der über die Anwendungen der Datenbank zur Verfügung gestellt werden, sicherstellen.

Welcher ITIL-Prozess ist für die Festlegung der Kosten für die zusätzliche Unterstützung durch den Service Desk verantwortlich?

A. Availability Management
B. Financial Management for IT Services
C. Incident Management
D. Service Level Management

Lösung: B. Financial Management for IT Services: Stichwort "Kosten"

In welchem Dokument legen Sie Anforderungen fest, die sich auf die Kapazität auswirken?

A. Im Kapazitätsplan
B. Im Service-Optimierungsprogramm
C. Im Servicequalitätsplan
D. In den Serviceanforderungen

Lösung: D. In den Serviceanforderungen werden die Vorgaben festgelegt, auf deren Basis der Service geplant, entwickelt und eingerichtet wird, um in der Konsequenz die Ausführung des Service Level Agreement SLA garantieren zu können. Der Servicequalitätsplan enthält Prozessparameter in Bezug auf die Management-Informationen.

Was ist eine andere Bezeichnung für Uptime?

A. durchschnittliche Zeit zwischen zwei Ausfällen (Mean Time Between Failures, MTBF)
B. durchschnittliche Zeit zur Wiederherstellung (Mean Time To Repair, MTTR)
C. durchschnittliche Zeit zwischen System-Zwischenfällen (Mean Time Between System Incidents, MTBSI)
D. Verhältnis zwischen MTBF und MTBSI

Lösung: A. MTBF. Dies ist die mittlere Zeit der Serviceverfügbarkeit, d.h. die produktive Zeit ohne Störungen oder Beeinträchtigungen. Alle anderen Möglichkeiten sind falsch.

Was ist eine Aktivität des IT Service Continuity Managements?

A. das Analysieren der Service-Zeiten
B. das Erstellen und die kontinuierliche Weiterbearbeitung eines Ausweichplans
C. das Reporting über die Verfügbarkeit
D. das Gewährleisten, dass Konfigurationselemente kontinuierlich aktualisiert werden

Lösung: B. Das Erstellen und die kontinuierliche Weiterbearbeitung eines Ausweichplans ist richtig. Dieser Plan, auch Verfügbarkeitsplan genannt, dient der Erhaltung bzw. Verbesserung der Verfügbarkeit. Das Reporting über die Verfügbarkeit ist eine Aktivität des Availability Management, dem ein Messen der Verfügbarkeit vorausgeht. Das Gewährleisten, dass die Konfigurationselemente kontinuierlich aktualisiert werden, ist eine Aktivität des Configuration Management, das dies in der CMDB realisiert.

Wie lautet die Definition des Begriffs Vertraulichkeit (Confidentiality) als Teil des Prozesses Security Management?

A. der Schutz der Daten vor unbefugter Einsichtnahme und Verwendung
B. die ständige Verfügbarkeit der Daten
C. die Kontrollierbarkeit der Daten auf Richtigkeit
D. die Korrektheit der Daten

Lösung: A. Der Schutz der Daten vor unbefugter Einsichtnahme und Verwendung ist die Beschreibung für Vertraulichkeit (Confidentiality), wie im Prozess Security Management verwendet. Die ständige Verfügbarkeit der Daten ist eine Beschreibung der Verfügbarkeit (Availability). Die Korrektheit der Daten ist Teil der Beschreibung von Integrität (Integrity).

Das Service Level Management ist unter anderem dafür zuständig, Service Level Agreements (SLAs) aufzustellen und mit Kunden darüber zu verhandeln. Was ist nicht Bestandteil einer SLA-Verhandlung?

A. ein Bericht zur Verfügbarkeit des Service in der jüngsten, zurückliegenden SLA-Periode
B. das Datum, zu dem ein SLA überarbeitet wurde
C. die Art, wie die Kosten umgelegt werden
D. Definitionen für Dringlichkeit (Urgency), Auswirkung (Impact) und Priorität (Priority)

Lösung: A. ein Bericht zur Verfügbarkeit des Service in der jüngsten, zurückliegenden SLA-Periode: SLA-Verhandlungen beziehen sich auf vertragliche Details zur Verfügbarkeit der Services und beinhalten kein Review.

Welcher ITIL-Prozess ist für den Entwurf eines Leistungsverrechnungssystems verantwortlich?

A. Availability Management
B. Capacity Management
C. Financial Management for IT Services
D. Service Level Management

Lösung: C. Financial Management for IT Services: Stichwort "Verrechnung"

Intermediate Recovery wird in Hinblick auf welches Zeitfenster verwendet?

A. 4 bis 8 Stunden

B. 4 bis 24 Stunden

C. 24 bis 72 Stunden

D. mehr als 72 Stunden

Lösung: C. 24 bis 72 Stunden. Immediate Recovery wird für einen Erwartungszeitraum zwischen 0 und 24 Stunden angesetzt. Intermediate Recovery bezieht sich auf einen Zeitraum zwischen 24 und 72 Stunden. Gradual Recovery eignet sich für einen Erwartungszeitraum von 72 Stunden und mehr.

Welche Beschreibung passt am besten auf die Zielrichtung des Capacity Management?

A. Sicherstellung, dass die Business-Bedürfnisse bezahlbar und erfüllbar sind

B. Bereitstellung wirtschaftlicher IT-Kapazitäten, um die vereinbarten Service Level zu erfüllen

C. Kostenreduzierung und Leistungslevel auf ein Minimum reduzieren

D. Sicherstellung, dass jederzeit ausreichend Kapazität vorhanden ist, um alle Kundenanforderungen zu erfüllen

Lösung: B. Bereitstellung wirtschaftlicher IT-Kapazitäten. Capacity Management funktioniert in Hinblick auf die Service Levels und deren Erfüllung. Geschäftsanforderungen legen mit Feedback aus der IT fest, ob bestimmte IT Services bezahlbar oder erfüllbar sind. SLA sind in Hinblick auf die Kosten definiert, um den festgeschriebenen Service bereitzustellen. Aus diesem Grund kümmert sich das Capacity Management vorwiegend um die Kapazitäten und Leistungen, wie sie in den SLAs definiert wurden.

Welcher ITIL-Prozess garantiert eine optimale und messbare Verfügbarkeit der IT Services?

A. Availability Management

B. Capacity Management

C. IT Service Continuity Management

D. Service Level Management

Lösung: A. Availability Management: Stichwort "Verfügbarkeit" und "messbar"

Welcher ITIL-Prozess ist für die Bestimmung der erforderlichen Hardware, die für die Unterstützung einer definierten Anwendung erforderlich ist, verantwortlich?

A. Availability Management

B. Capacity Management

C. Change Management

D. Configuration Management

Lösung: B. Capacity Management: Hier geht es um die Ermittlung der benötigten IT-Ressourcen.

20 Test-Simulation und typische Prüfungsfragen

Es bestehen keine besonderen Voraussetzungen für die von Ihnen angestrebte Zertifizierung. International ist das Prüfungsinstitut EXIN (*http://www.exin.nl*) zuständig, für den deutschsprachigen Raum hat die TÜV-Akademie (*http://www.tuev-sued.de*) diese Funktion übernommen. Die Bewertung Ihrer Examen wird von freiwilligen, unabhängigen und von TÜV/EXIN examinierten Korrektoren durchgeführt.

20.1 Zur Vorbereitung der Test-Simulation

Für das Ablegen der Prüfung zum Erwerb dieses Zertifikates ist keine Schulung – als zwingende Voraussetzung – erforderlich, allerdings ist der Besuch einer ITIL Foundation-Schulung oder vergleichbarer Trainings anzuraten. Bestanden hat der Teilnehmer, wenn er von den insgesamt 40 Multiple-Choice Fragen 65 % innerhalb von 60 Minuten richtig beantworten konnte. Jede Frage ist eine Multiple-Choice-Frage, die nur eine richtige Antwort zulässt. Während des Examens ist es nicht erlaubt, Literatur, Notizen oder einen programmierbaren Taschenrechner zu verwenden.

Die Höchstzahl der zu erreichenden Punkte beträgt 40. Für jede richtige Antwort bekommt der Prüfling einen Punkt. Bei 26 Punkten oder mehr hat der Teilnehmer die Zertifizierungsprüfung bestanden. Danach erhält er das offizielle ITIL Foundation-Zertifikat („Foundation Certificate in IT Service Management" nach EXIN).

Bei der Vorbereitung auf die Zertifizierung empfiehlt sich das Durcharbeiten von Literatur zum Thema ITIL. Die Originalliteratur des OGC ist vielfach schon zu detailliert und deckt mehr ab als in der Foundation-Zertifizierungsprüfung abgefragt wird. Hilfreich ist stets das Durcharbeiten von Selftestfragen, die zur Zeit allerdings nur in englischer Sprache kostenpflichtig vorliegen und von Ihnen bestellt werden können. Alternativ arbeiten Sie die Ihnen hier vorliegenden Fragen und Kommentare durch, um ein Gefühl für diese Art von Fragen in Bezug auf ITIL zu bekommen. Einige Fragen können Ihnen entweder genau so oder ähnlich in Ihrer Zertifizierungsprüfung begegnen. Überflüssig zu betonen, dass sich ein Zertifikatsanwärter durchaus intensiv mit dem Thema ITIL und IT Service Management auseinandergesetzt haben sollte, bevor die hier vorliegenden Fragen bearbeitet werden.

20.2 Beispielfragen und Braindumps

Die Ihnen hier vorliegenden Beispielfragen gliedern sich in die Frage, mögliche Antworten und eine Lösung mit Kommentar.

Was ist unter dem Begriff IT Service Management zu verstehen?

A. Eine effektive und effiziente Lieferung von IT Service-Leistungen mit einer gleich bleibenden Qualität, auf die sich der Anwender der IT Service-Leistung verlassen kann

B. Das Einrichten der Verwaltung der IT-Infrastruktur gemäß den Methoden in der IT Infrastructure Library

C. Die prozessbasierte Steuerung der IT-Infrastruktur, so dass die IT-Organisation dem Kunden auf professionelle Weise IT-Systeme liefern kann

D. Einer größeren Öffentlichkeit mehr Einblick in den IT Service geben

Lösung: A. ist richtig. Beachten Sie: IT Service Management umfasst mehr, als in der IT Infrastructure Library dokumentiert ist. Beim IT Service Management geht es gerade nicht (mehr) um IT-Systeme, sondern um IT Services.

Welche der nachfolgenden Aufgaben gehört zum Problem Management?

A. Koordinierung aller an der IT-Infrastruktur vorgenommenen Änderungen

B. Aufzeichnung aller Zwischenfälle für eine spätere Untersuchung

C. Genehmigung aller Änderungen, die in der Known Error-Datenbank vorgenommen werden

D. Die Bedürfnisse des Benutzers definieren und anhand dessen Änderungen an der IT Infrastruktur vornehmen

Lösung: C. Genehmigung aller Änderungen, die in der Known Error-Datenbank vorgenommen werden. Das Problem Management trägt die Verantwortung für diese Datenbank.

Daten in der Configuration Management Database (CMDB) dürfen nur nach vorheriger Genehmigung zu einer Änderung der Infrastruktur führen. Welcher Prozess erteilt diese Genehmigung?

A. Change Management

B. Configuration Management

C. Incident Management

D. Service Level Management

Lösung: A. Change Management: Dieser Prozess trägt die Verantwortung für Änderungen in der Infrastruktur. Stichwort ist hier „Genehmigung".

Sie arbeiten im Service Desk. Sie haben bemerkt, dass Sie und Ihre KollegInnen jeden Montagmorgen eine Reihe von Anrufen erhalten, die melden, dass eine Anwendung nicht verfügbar ist. Welcher Prozess wird von dieser Feststellung am deutlichsten profitieren, wenn Sie dies weitergeben?

A. Availability Management

B. Change Management

C. Problem Management

D. Incident Management

Lösung: C. Problem Management: Was das Service Desk an Fehlerfällen (Incidents) bemerkt, ist ein Symptom von dahinter liegenden Ursachen. Diese müssen untersucht werden, bevor sie an andere Prozesse weitergegeben werden können wie das Availability oder das Change Management. Das Problem Management ist immer der Prozess, der für die Ursachenforschung zuständig ist. Hier müssen Ursachen für Incidents identifiziert und aufgelöst werden.

Mit wem würden Sie in Ihrer Funktion als Finance Controller der IT-Abteilung eines großen Unternehmens bezüglich der Höhe des Geldbetrags verhandeln, der für das IT Service Delivery-Budget vorgesehen wird?

A. Chef-Buchhalter (Prokurist)

B. Financial Capacity Prozess Owner

C. Service Level-Manager

D. Kunde(n)

Lösung: Kunde(n): Der Kunde ist die Stelle, die ITIL als verantwortliche Entität für die Bezahlung des Delivery Service sieht.

Nach der erforderlichen Suche wurde die gemeinsame Ursache einer Reihe vergleichbarer Fehler gefunden. Dies führte zu einem erkannten Fehler (Known Error). Was hat in der Regel nun zu geschehen?

A. Alle Zwischenfälle müssen schnellstmöglich beseitigt werden.

B. Der Fehler muss durch eine Änderung behoben werden.

C. Der Fehler muss in die Configuration Management Database (CMDB) aufgenommen werden.

D. Das betreffende Problem muss identifiziert werden.

Lösung: B. Der Fehler muss durch eine Änderung behoben werden. Ein Request for Change (RfC) wird erstellt.

Der Change-Manager wird im Fall einer Änderungsanforderung (Request for Change, RFC) einige Aktivitäten starten. Was tut er, wenn es sich um eine komplexe Änderung handelt?

A. Die Änderung beim Problem Management anmelden

B. Die Änderung beim Incident Management anmelden

C. Die Änderung dem Change Advisory Board vorlegen

D. Die Änderung dem IT-Manager vorlegen

Lösung: C. Die Änderung dem Change Advisory Board vorlegen: Für kleinere Änderungen wird in der Regel kein solches Meeting zusammengerufen.

Was ist der Unterschied zwischen Besitzverwaltung (Asset Management) und Konfigurationsverwaltung (Configuration Management)?

A. Asset Management kümmert sich nur um die Besitzverwaltung; Configuration Management behandelt alles in der Infrastruktur.

B. Asset Management entspricht dem Configuration Management, aber betrifft nur die anderen Nicht-IT-Besitztümer wie Stühle und Tische.

C. Asset Management behandelt die finanziellen Aspekte der Configuration Items; Configuration Management behandelt ausschließlich die technischen Einzelheiten der Infrastruktur.

D. Configuration Management geht viel weiter als Asset Management, weil es auch die Beziehungen zwischen den Besitztümern (Assets) behandelt.

Lösung: D. Configuration Management geht viel weiter als Asset Management, weil es auch die Beziehungen zwischen den Besitztümern (Assets) behandelt. Die Komponenten werden hier nicht als Assets angesehen, sondern als CIs, die mit den entsprechenden Beziehungen in der CMDB dokumentiert werden.

Bei welchem ITIL-Prozess ist Mean Time Between Fallures (MTBF) ein allgemein gebräuchlicher Begriff?

A. Availability Management

B. Capacity Management

C. IT Service Continuity Management

D. Service Level Management

Lösung: A. Availability Management: Dazu gehören die verwandten Begriffe wie MTTR und MTBSI (siehe Abbildung 20.1).

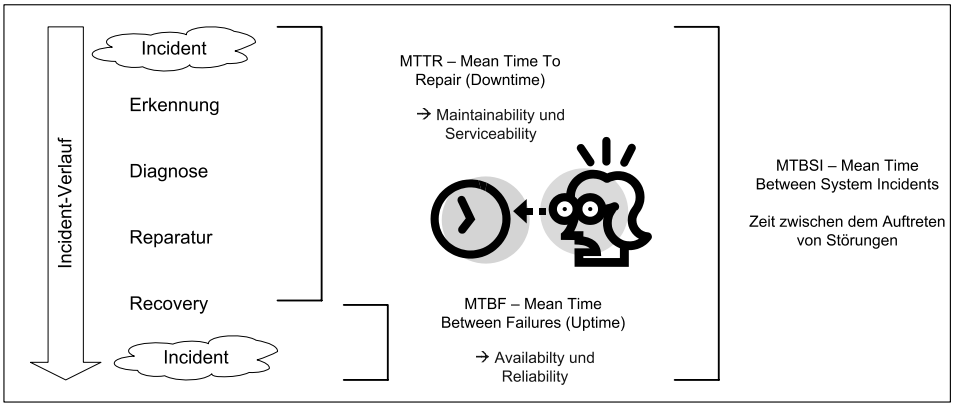


Abbildung 20.1: Messgrößen eines Incidents

Eine Firma beginnt mit dem Aufbau eines Intranets. Hinsichtlich der steigenden Zugriffe auf das Angebot muss die Kapazität des vorhandenen Netzwerkes erweitert werden. Welcher Prozess muss die Implementierung dieser Kapazitätserweiterung genehmigen?

A. Capacity Management
B. Change Management
C. Availability Management
D. Problem Management

Lösung: B. Change Management. Stichwort „genehmigen“

Das Beschaffungswesen einer elektronischen Fertigungsfirma hat vor kurzem einen Vertrag mit einem Ausrüster für PCs unterschrieben. Die ersten neuen Geräte werden geliefert und alle Anwendungen, die im Unternehmen verwendet werden, müssen sich vorab einem Test unterziehen. Die Fertigungsfirma besitzt eine gut strukturierte Produktions- und Testumgebung. Welcher Prozess autorisiert den Rollout der neuen Maschinen an die Anwender?

A. Release Management
B. Service Level Management
C. Change Management
D. Configuration Management

Lösung: C. Change Management: Das Schlüsselwort ist in diesem Fall „autorisieren“ oder „freigeben“.

Sie bemerken eine steigende Anzahl von Beschwerden eines Geschäftsbereiches bezüglich der Antwortzeiten einer Transaktionsanwendung und deren Aktivitäten. Der Capacity-Manager hat als Erklärung abgegeben, dass die momentan zur Verfügung stehenden Ressourcen werktags zwischen 09.30 h und 11.30 h sowie zwischen 14.00 h und 15.30 h überlastet sind. Welche der folgenden Möglichkeiten würde Abhilfe schaffen?

A. Ein Komitee ins Leben zu rufen, um die aktuellen Verfahren zu überprüfen

B. Anzahl der Arbeitskräfte erhöhen, die Überstunden machen sollen

C. Eine andere Verrechnungsrichtlinie einführen

D. Vertragsstrafen den SLAs hinzufügen

Lösung: C. Eine andere Verrechnungsrichtlinie einführen: Diese könnte die Kunden dazu bringen, die Hauptarbeitszeiten mit der entsprechenden Anwendung auf Zeiten mit niedrigeren Servicepreisen zu verlegen, die nicht im Peak-Bereich liegen.

Die IT-Abteilung möchte die ITIL-Prozesse einführen. Bei Verwendung des ITIL-Frameworks ist eine Reihe von Vorteilen und Verbesserungen für das entsprechende Unternehmen zu erwarten. Welche der folgenden Beschreibungen ist als Benefit einer solchen Umsetzung anzusehen?

A. Höhere Flexibilität und Anwendbarkeit dürften in Zusammenhang mit der Einführung von ITIL stehen.

B. Ein besserer IT-Beschaffungsprozess, der zu direkten Kosten-Ersparnissen führt

C. Veränderungen in Bezug auf das funktionale Arrangement der IT-Organisation

D. Höheres Prestige des Unternehmens nach Erscheinen der entsprechenden Pressemitteilung zur ITIL-Einführung

Lösung: A. Höhere Flexibilität und Anwendbarkeit dürften in Zusammenhang mit der Einführung von ITIL stehen: Das ist auf jeden Fall etwas, das die Unternehmen von ITIL erwarten.

Welcher der folgenden Punkte ist weder eine Aktivität noch ein Unterprozess des Capacity Management?

A. Business Capacity Management

B. Financial Capacity Management

C. Resource Capacity Management

D. Service Capacity Management

Lösung: B. Financial Capacity Management: Dies ist kein Unterprozess des Capacity Management.

Das IT Service Management unter Verwendung des ITIL Framework ist wichtiger als das Erreichen der Geschäftsziele.

A. Ich stimme dieser Aussage zu.

B. Ich stimme dieser Aussage nicht zu.

C. Diese Details muss ich mit der Geschäftsleitung/meinem Abteilungsleiter klären.

Lösung: B. Ich stimme dieser Aussage nicht zu: Wie in vielen Branchen geht es nicht nur um das Erreichen eines Teilziels, sondern um den Gesamtblick. IT und auch ITIL dienen keinem Selbstzweck, sondern haben eine Aufgabe: Das Unterstützen der Geschäftsziele.

Ihr Abteilungsleiter hat Sie gebeten, nach neuen und besseren Möglichkeiten zu suchen, um herauszufinden, was eigentlich die Geschäftsanforderungen für den IT-Bereich sind. Welchen Prozess ziehen Sie diesbezüglich heran?

A. Availability Management

B. Incident Management

C. Service Level Management

D. Service Desk

Lösung: C. Service Level Management: Service Level Management ist der Prozess, der am ehesten vorhandene Geschäftsanforderungen berührt und umsetzt. Dies wird durch Aktivitäten wie das Aufstellen von SLRs (Service Level Requirements) realisiert.

Der Begriff „Kunde" im Sinne von ITIL bezieht sich auf eine Person, die für den IT Service bezahlt.

A. Ich stimme dieser Aussage zu.

B. Ich stimme dieser Aussage nicht zu.

C. ITIL definiert diesen Begriff nicht.

Lösung: A. Ich stimme dieser Aussage zu: Der Kunde bezahlt für den Service, der Anwender nutzt ihn. Der Kunde versteht sich aber selbstverständlich selber als Endanwender.

Woraus entstand das Security Management?

A. Availability Management

B. IT Service Continuity Management

C. Incident Management

D. Problem Management

Lösung: A. Availability Management: Bereits kurz nach Entwicklung des originären ITIL-Frameworks in den 80er Jahren wurde das Security Management als eigenständiger Prozess definiert. Das Availability Management besitzt immer noch Elemente, die

dem Security Management zuzuordnen sind. Das Security Management stellt Leitsätze und Richtlinien auf, die das Availability Management betreffen und die es umzusetzen hat, beispielsweise die Verfügbarkeit.

Einmal eingerichtete ITIL-Prozesse sind quasi Selbstläufer, um die man sich zum Glück keine Gedanken oder gar Sorgen machen muss. ITIL-Prozesse sind in der Lage, sich selber zu protegieren und sich am Leben zu halten.

A. Ich stimme dieser Aussage zu.

B. Ich stimme dieser Aussage nicht zu.

C. Ich weiß nicht.

D. Es gibt keine ITIL-Prozesse.

Lösung: B. Ich stimme dieser Aussage nicht zu: Offensichtlich ist diese Aussage falsch. Prozesse wie Prozeduren und Arbeitsanweisungen entspringen Gedanken und Ideen. Ohne ständige Verbesserungen, um die Prozesse im Auge zu behalten, gerät der Prozess bei Nicht-Anwendbarkeit oder bei Anpassungen der Umgebung in Vergessenheit, verliert an Aktualität und Bezug oder wird abgelehnt.

Zählen Sie Service Support-Prozesse und einen entsprechenden Funktionsbereich auf.

A. Service Desk, Release, Incident, Availability, Configuration, Change

B. Service Desk, Release, Incident, Problem, Change

C. Financial Management for IT Services, Configuration, Availability, Service Level Management

D. IT Service Continuity Management, Service Desk, Change, Service Level Management, IT Service Continuity Management

Lösung: B. Service Desk, Release, Incident, Problem, Change

Der End-Anwender im Sinne von ITIL ist eine Person oder Gruppe, die einen IT Service nutzt.

A. Ich stimme dieser Aussage zu.

B. Ich stimme dieser Aussage nicht zu.

C. ITIL definiert den Begriff nicht.

Lösung: A. Ich stimme dieser Aussage zu: Der Endbenutzer ist die Person, die den Service nutzt, der Kunde zahlt für den entsprechenden Service. Eine Person oder Gruppe kann aber auch beides sein.

Welche der folgenden Optionen beschreibt den Begriff Service Management am ehesten? Service Management ist

A. Maintenance der technischen Infrastruktur, um sicherzugehen, dass die Kundenerwartungen verwaltet und erfüllt oder überschritten werden.

B. Geeignete Verwendung von Personen/Manpower, Prozessen und Technologien, um sicherzugehen, dass IT Service Delivery die Geschäftsbedürfnisse in effizienter und effektiver Weise befriedigt.

C. Schaffung der bestmöglichen Prozesse für die Praxis, die immer wieder verwendet werden können, und Sicherstellung, dass alle Mitarbeiter ein gemeinsames Verständnis der verwendeten Begriffe besitzen.

Lösung: B. Geeignete Verwendung von Personen/Manpower, Prozessen und Technologien, um sicherzugehen, dass IT Service Delivery die Geschäftsbedürfnisse in effizienter und effektiver Weise befriedigt: Das ist die am besten passende Beschreibung, IT Service Management umspannt die Bereiche Personen, Prozesse und Technologien.

Welcher Aspekt ist bei der Erfassung von sicherheitsrelevanten Zwischenfällen wichtig?

A. Die Person, die den Zwischenfall gemeldet hat

B. Entsprechende disziplinierende Maßnahmen

C. Qualifizierte Service Desk-Mitarbeiter

D. Erkennen eines sicherheitsrelevanten Zwischenfalls

Lösung: D. Erkennen eines sicherheitsrelevanten Zwischenfalls: Dies stellt aber auch die spezielle Anforderung dar, die nicht einfach für viele Mitarbeiter zu erfüllen ist. Um überhaupt adäquat reagieren zu können, ist das Erkennen eines solchen Falles unbedingte Voraussetzung.

Wie wird festgestellt, ob der IT Service Continuity Management-Plan in der Praxis funktioniert?

A. Durch Vergleich mit dem, was die Konkurrenten tun

B. Durch Überprüfung des ITSCM-Plans durch Dritte

C. Durch Test des ITSCM-Plans

D. Indem gewartet wird, bis ein Notfall eintritt und dann die Folgen überprüft werden

Lösung: C. Durch Test des ITSCM-Plans: Notfallpläne sollten stets vorab getestet werden. Auf diese Weise ist das Unternehmen nicht nur in der Lage, Probleme zu erkennen und zu beheben, die zur Verbesserung des Plans beitragen. Auch Aussagen über den ungefähren Zeitraum, die eine solche Maßnahme benötigt, können danach gemacht werden. Diese Tests sollten in regelmäßigen Abständen und bei Änderungen wiederholt werden.

Welche der folgenden Aufgaben gilt für jeden Prozess-Manager?

A. Für einen reibungslosen Verlauf des Prozesses zu sorgen

B. Die benötigte Hardware zu beschaffen

C. Daten zum Problem Management weiterzuleiten

D. Personalbewerbung

Lösung: A. Für einen reibungslosen Verlauf des Prozesses zu sorgen: Dafür ist er schließlich da. Es gibt diese Managerfunktion in jedem Prozess. Aber Achtung: Einen Service-Manager gibt es nicht – außer als ITIL-Zertifizierungstitel!

Der einwandfreie Betrieb einer bestimmten Anwendung erfordert die Installation der gleichen Version auf sämtlichen Systemen einer Client-/Server-Umgebung. Welcher Prozess ist für die Installation verantwortlich?

A. Configuration Management

B. Incident Management

C. Release Management

D. Change Management

Lösung: C. Release Management: Die aktive Umsetzung einer Änderung im Soft- oder Hardwarebereich erfolgt über das Release Management.

Ein neuer Service geht morgen in Betrieb. Was oder wer sollte am Service Desk vorhanden bzw. verfügbar sein?

- 1. Der Service Level-Manager, um Anleitungen zu geben
- 2. Anwendungsspezialisten, um Fragen zu beantworten
- 3. Dokumentation zum Service und ggf. eine Lösungsdatenbank
- 4. Der Zeitplan für die Durchführung von Changes (Forward Schedule of Changes)

A. 1 und 4

B. 3 und 4

C. 2, 3 und 4

D. Alle

Lösung: B. 3 und 4: Auf diese Weise können Rückfragen aus allen Bereichen zur Einführung des neuen Services beantwortet werden.

Die Netzwerkanwender erhalten wiederholt die Meldung, dass nicht genug Plattenplatz zur Verfügung steht. Da dieses Problem teilweise mit der Größe der verwendeten Software zusammenhängt, muss der Plattenplatz erweitert werden. In welchem Prozess erfolgt die formale Freigabe des Changes?

A. Problem Management

B. Incident Management

C. Release Management

D. Change Management

Lösung: D. Change Management. Hier erfolgt die Genehmigung des Changes als erste Aktion nach der Erfassung eines Changes.

In welchen Schritten läuft ein kontrollierter Change ab?

A. Erfassung des RFC – Priorisierung – Kategorisierung – (Impact-)Bewertung – Freigabe – Planung/Steuerung – Realisierung/Test – Implementierung – Review – Abschluss

B. Kategorisierung – lmpakt/Dringlichkeit bestimmen – Erfassung – Test – Realisierung/Implementierung – Abschluss

C. Identifikation – Registrierung – Zuordnung – Analyse – Realisierung – Test – Implementierung – Berichterstattung

D. Registrierung – Diagnose und Lösung – Klassifikation – Test – Implementierung – Abschluss

Lösung: A. Zuerst muss die Erfassung erfolgen. Review und Abschluss gehören stets dazu.

Was ist die Definitive Software Library (DSL)?

A. Ein sicherer und geschützter Arbeitsbereich, in dem Softwareänderungen durchgeführt werden können

B. Eine Library, die Backup-Kopien sämtlicher verwendeter Software beinhaltet

C. Eine geschützte Software Library, in der alle qualitätskontrollierten und freigegebenen Software-CIs gespeichert sind

D. Eine geschützte Software Library, in der alle aktuellen Software-Versionen gespeichert sind

Lösung: C. Eine geschützte Software Library, in der alle qualitätskontrollierten und freigegebenen Software-CIs gespeichert sind: Wichtig ist, dass sie geschützt ist und dass fehlerfreie Software dort abgespeichert wird.

Welche der Aussagen ist richtig?

A. Es ist Aufgabe des Change Management, die zu ändernden CIs zu identifizieren.

B. Das Change Management ist verantwortlich für die Changes in laufenden Projekten.

C. Das Change Management ist verantwortlich für das Aktualisieren von CI- Daten sowie Incidents, Problem-Daten und Known Error Records nach einem Change.

D. Das Change Management führt Datensätze aller Changes und ist verantwortlich für die Dokumentation, Überwachung und Review des Changes.

Lösung: D. Das Change Management führt Datensätze aller Changes und ist verantwortlich für die Dokumentation, Überwachung und Review des Changes: Das Review findet i.d.R. in Zusammenarbeit mit dem Problem Management statt.

Wofür ist das Release Management nicht verantwortlich?

A. Verteilung der Software an Remote-Standorte

B. Softwarefehler korrigieren

C. Release und Implementierung von Software in Produktivumgebungen

D. Das Sicherstellen, dass alle Elemente, die auf den Markt gebracht oder geändert werden, sicher sind und mit der Configuration Database (CMDB) verfolgt werden können

Lösung: B. Softwarefehler korrigieren: Das Release Management kann aufgrund der spezifischen Anforderungen natürlich jeden Fehler korrigieren.

In welchen Fällen ist nach der Implementierung eines Changes ein Change Review durchzuführen?

A. Immer

B. Auf Antrag der Person, die den RFC eingereicht hat

C. In regelmäßigen Abständen

D. Wenn ein weiterer Incident des gleichen Typs auftaucht

Lösung: A. Immer: Ein Review ist stets erforderlich, um einen Change sauber schließen zu können.

Welche Aussage ist richtig: Das Change Advisory Board (CAB) soll sicherstellen, dass beantragte Changes bewertet werden in Hinblick auf:

- Die voraussichtliche Auswirkungen des Changes auf die Services
- Die Folgen einer Nicht-Implementierung des Changes
- Die für die Implementierung erforderlichen Ressourcen
- Die voraussichtlichen Auswirkungen des Changes auf den Continuity-Plan (Notfallplan)

A. 1, 2 und 3

B. 2, 3 und 4

C. 1, 2 und 4

D. Alle

Lösung: D. Alle. Neben dem Change-Manager spielt das Change Advisory Board (CAB) bei weitreichenden Veränderungen eine wichtige Rolle. Es sollte die Auswirkungen des Changes auf die Geschäftsprozesse, die verwendete IT-Infrastruktur und unterstützte IT-Services, die Auswirkungen auch auf andere Services: Security, Office-Service, Transport,... und die Konsequenzen, wenn der Change nicht durchgeführt wird, berücksichtigen. Dazu gehört auch die Abschätzung der Ressourcen und Kosten, die für den Change benötigt werden, wie z.B. IT-Komponenten, Mitarbeiter, Zeit, Neuanschaffungen.

Welche Aktivität hat unmittelbar nach Annahme und Erfassung eines Zwischenfalls zu erfolgen?

A. Analyse und Diagnose

B. Klassifizierung

C. Matching

D. Problemlösung und -behebung

Lösung: B. Klassifizierung: Die Reihenfolge lautet: Störung annehmen und erfassen, Klassifizierung vornehmen und erste Unterstützung anbieten. Danach folgen Prüfung des Störmusters, Analyse und Diagnose des Incidents, Behebung und Wiederherstellung und zuletzt der Abschluss der Störung (siehe Abbildung 20.2).

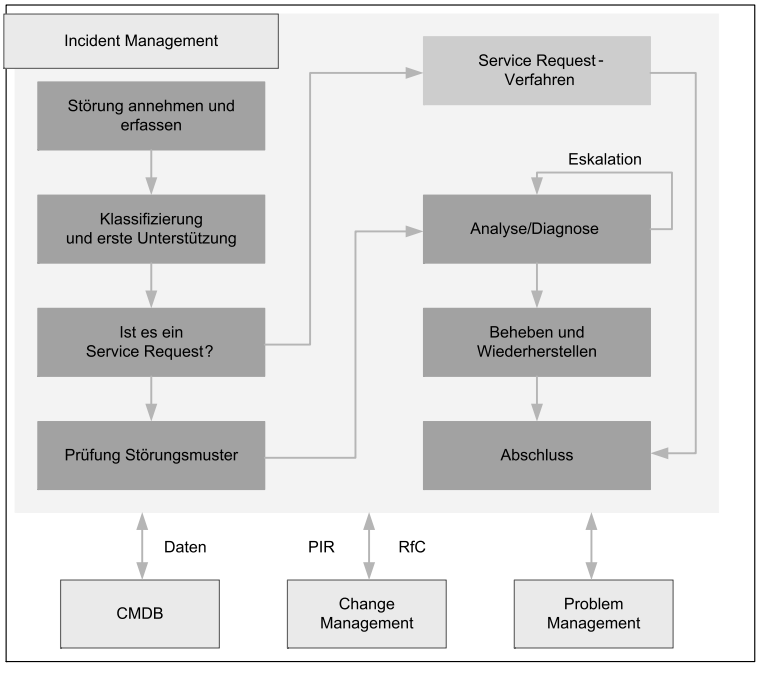


Abbildung 20.2: Incident Management-Aktivitäten

Wer oder was trägt die Verantwortung für den gesamten Change Management-Prozess?

A. Change Advisory Board

B. Change-Koordinator

C. Change-Manager

D. IT-Manager

Lösung: C. Change-Manager: Er hat die Verantwortung für den Prozess.

Eine Versicherung möchte gerne ein Support-Tool für ihr Service Desk einsetzen. Die IT-Abteilung möchte insbesondere wissen, welche Zwischenfälle immer wieder verstärkt auftreten. Was sollte diesbezüglich bei der Auswahl des Tools eine wichtige Rolle spielen?

A. Zwischenfall-Kategorisierung (Incident Categorisation)

B. Verbindung zum Change Management

C. Diagnose des Problems

D. Verbindung zum Service Level Management

Lösung: D. Verbindung zum Service Level Management: So kann beobachtet werden, welche SLAs gegebenenfalls aus dem Ruder laufen.

Sie arbeiten mit einer Web-Anwendung auf J2EE-Basis. Als Sie sich morgens anmeldeten, erschien die Meldung „Host not found". Sie konnten keine Verbindung zum UNIX-Server herstellen. Nachdem Sie Ihren Computern neu gestartet haben, war die Anmeldung erfolgreich. Dies trat nicht zum ersten Mal auf. Diese Woche mussten Sie Ihren Rechner bereits das dritte Mal neu starten. Aus diesem Grund wollen Sie dem Service Desk hierüber eine Meldung machen, damit der Fehler dort untersucht wird. Warum handelt es sich dabei?

A. Beschwerde

B. Bekannter Fehler

C. Problem

D. Zwischenfall

Lösung: D. einen Zwischenfall: Fehler oder Zwischenfälle (englisch: Incidents) sind Ereignisse, deren Ursache erst noch geklärt werden muss.

In welcher Weise nutzt das Problem Management die Configuration Management-Datenbank (CMDB)?

A. Das Problem Management erfasst ein Problem immer als ein Konfigurationselement.

B. Das Problem Management legt den Detaillierungsgrad des Konfigurationselements fest.

C. Das Problem Management sucht nach einer Lösung, wenn die CMDB nicht mit den derzeitigen physischen Zustand von Konfigurationselementen übereinstimmt.

D. Das Problem Management bezieht alle Probleme auf Konfigurationselemente.

Lösung: D. Das Problem Management bezieht alle Probleme auf Konfigurationselemente. Auf diese Weise ist eine schnelle und einfache Zuordnung von Problemen und möglichen Seiteneffekten möglich.

Was ist der Unterschied zwischen einem Prozess und einem Projekt?

A. Bei einem Projekt geht es – im Gegensatz zu einem Prozess – nicht um das Resultat.

B. Ein Prozess verläuft kontinuierlich und ist endlos, ein Projekt nicht.

C. Ein Prozess wird gestoppt, wenn das Ziel erreicht ist, ein Projekt nicht.

D. Ein Projekt verläuft kontinuierlich und ist endlos, ein Prozess nicht.

Lösung: B. Ein Prozess verläuft kontinuierlich und ist endlos, in dem Sinne, dass er immer wieder durchlaufen wird. Ein Projekt ist endlich: Laut DIN-Definition (DIN 69901) ist ein Projekt ein „Vorhaben, das im Wesentlichen durch die Einmaligkeit der Bedingungen in ihrer Gesamtheit gekennzeichnet ist, wie z.B. Zielvorgabe, zeitliche, finanzielle, personelle und andere Begrenzungen; Abgrenzung gegenüber anderen Vorhaben; projektspezifische Organisation."

Wann kann das Entwickeln, Testen und Implementieren einer Änderung (Change) anfangen?

A. Sobald die Auswirkungsanalyse (Impact Analysis) von den Mitgliedern des Change Advisory Board besprochen wurde.

B. Sobald ein gültiger Netzwerkplan für die Änderung vorliegt.

C. Sobald der Request for Change offiziell genehmigt ist.

D. Sobald der Request for Change klassifiziert ist.

Lösung: C. Sobald der Change genehmigt ist. Selbst dringende Änderungen müssen erst einmal genehmigt werden. Dabei geht es primär um formelle und nicht um technische Aspekte, wie beispielsweise ob der RfC alle erforderlichen Daten und Maßnahmen, Ansprechpartner und Kontaktdaten beinhaltet.

Wie trägt Problem Management zu einer höheren Lösungsrate des Service Desk bei?

A. Indem noch nicht gelöste Zwischenfälle analysiert werden

B. Indem Zwischenfälle mit dem Kunden evaluiert werden

C. Indem Zwischenfälle vermieden werden

D. Indem eine Datenbank mit Informationen/Wissen zur Verfügung gestellt wird

Lösung: D. Indem eine Datenbank mit Informationen/Wissen zur Verfügung gestellt wird: Diese sollte vom Problem Management gefüllt und gepflegt werden. Zudem sollte dieser Wissensspeicher mit Such- und Kategorisierungsfunktionen ausgestattet sein, um eine Zuordnung von Incidents, Problemen, Known Errors und Workarounds zu ermöglichen. Dies ist übrigens ein schönes Beispiel dafür, dass jeder Prozess eine eigene Datenbank haben kann.

Um Einblick in die Frage zu gewinnen, welche Konfigurationselemente wo installiert sind, wurde das Configuration Management eingerichtet. An welche Aktivität sollte bei der Einrichtung des Configuration Management auf jeden Fall gedacht werden?

A. Die Konfigurationselemente mit Aufklebern versehen
B. Die Definitive Software Bibliothek (DSL) für die Software-Konfigurationselemente einrichten
C. Ein Verfahren für Standard-Änderungsanträge festlegen
D. Die Beziehungen zwischen den Konfigurationselementen dokumentieren

Lösung: D. Die Beziehungen zwischen den Konfigurationselementen dokumentieren, um auf diese Weise Kategorisierung, Fehlersuche und Auswirkungen im Fehlerfalle zu ermöglichen. Die Beziehungen zwischen den CIs sind essenzieller Bestandteil der CMDB.

Die erfolgreiche Diagnose eines Problems führt zu einem bekannten Fehler. Wann kann der bekannte Fehler abgeschlossen werden?

A. Wenn ein Review der Änderung zu einem zufrieden stellenden Ergebnis geführt hat.
B. Wenn mit dem bekannten Fehler zusammenhängende Zwischenfälle nicht mehr auftreten
C. Wenn der Vorschlag zur Änderung beim Change Management erfasst ist
D. Wenn der Request for Change vom Change Advisory Board genehmigt ist

Lösung: A. Wenn ein Review der Änderung zu einem zufrieden stellenden Ergebnis geführt hat – und auch erst dann. Dies wird i.d.R. nach einem Change vom Problem Management durchgeführt.

Was ist ein Beispiel für ein Konfigurationselement?

A. Organigramm
B. Lieferant
C. Ort
D. Seriennummer

Lösung: A. Organigramm: Im Buch „IT Service Management" der itSMF wird das Organigramm als mögliches CI genannt, auch andere Dokumente wie der Servicekatalog können CIs darstellen.

Was ist die erste Aktivität bei der Durchführung des ITIL-Prozesses Release Management?

A. Release entwerfen und erstellen

B. Release testen

C. Release-Planung erstellen

D. Kommunikation und Vorbereitung des Releases

Lösung: C. Release-Planung erstellen: Erst planen, dann in Aktion treten. Dies gilt übrigens nicht nur für das Thema ITIL.

Welcher der folgenden IT-Prozesse oder Funktionen ist für die Lieferung des First-Line-Supports und die Unterstützung bei der täglichen Benutzung von IT Services verantwortlich?

A. Availability Management

B. Incident Management

C. Service Desk

D. Service Level Management

Lösung: C. Service Desk: Aufgrund der Fragestellung können Sie davon ausgehen, dass nicht nach einem Prozess („Aktivität") gefragt wird. Fragen dieser Art sind stets ein wenig heikel. Überlegen Sie sich, ob nach einem Prozess oder einer Funktion gefragt wird. Bei einem Prozess geht es stets um die mögliche Abbildung der Prozessaktivitäten.

In einer Organisation zieht die Vertriebsabteilung innerhalb des Gebäudes um. Nicht nur die Mitarbeiter, sondern auch ihre IT-Mittel ziehen um. Ein Service Desk-Mitarbeiter hat den Auftrag erhalten, die Workstations dieser Abteilung umzuziehen. In welchem ITIL-Prozess übernimmt dieser Mitarbeiter nun eine Rolle?

A. Change Management

B. Incident Management

C. Problem Management

D. Release Management

Lösung: D. Release Management: Hier geht es nicht nur um den Rollout von Hard- und Software, sondern auch um Umzüge. Das Release Management ist stets ein Prozess, der sich um jegliche Aktivitäten in diesem Bereich dreht und dort eine aktive Rolle übernimmt. Handelt es sich um kleine Umzüge, können sie auch vom Incident Management durchgeführt werden.

Bevor die Software in die Definitive Software-Bibliothek (DSL) installiert wird, wird sie auf Viren überprüft. Welcher ITIL-Prozess garantiert, dass nur virenfreie Software in der DSL gespeichert wird?

A. Application Management

B. Capacity Management

C. Configuration Management

D. Release Management

Lösung: D. Release Management. Zugelassene Versionen einer Applikation bewahrt der Prozess in der Definitive Software Library (DSL) sicher auf.

Der Service Desk des Lieferanten X erhält immer wieder den gleichen Incident Report. Es geht hierbei um die neueste Version einer Client-Server-Software. Der Zwischenfall lässt sich beheben, wenn die ältere Software-Version wieder installiert wird. Da die Ursache des Zwischenfalls noch immer nicht gefunden werden konnte, empfiehlt der Lieferant seinen Kunden, bei denen der Zwischenfall auftritt, vorübergehend wieder die alte Version zu installieren. Wofür ist dieser Rat ein Beispiel?

A. Bekannter Fehler

B. Problem

C. Workaround (Umgehungslösung)

D. Request for Change

Lösung: C. Workaround (Umgehungslösung): Dies entfernt zwar nicht die eigentliche Ursache des Problems, ermöglicht aber die Bereitstellung des Services für den Kunden.

Welcher ITIL-Prozess oder welche Funktion bearbeitet Störungen und Anwenderfragen?

A. Availability Management

B. Service Level Management

C. Problem Management

D. Service Desk

Lösung: D. Service Desk: Dies ist Aufgabe der ITIL-Funktion „Service Desk". Das Service Desk gilt als SPoC.

Was ist der Unterschied zwischen einem bekannten Fehler (Known Error) und einem Problem?

A. Bei einem bekannten Fehler ist die zugrundeliegende Ursache bekannt, bei einem Problem nicht.

B. Bei einem bekannten Fehler ist die Rede von einem Fehler in der IT-Infrastruktur, bei einem Problem nicht.

C. Ein bekannter Fehler ist immer Folge eines Zwischenfalls, ein Problem nicht immer.

D. Bei einem Problem wurden die relevanten Konfigurationselemente bereits bestimmt, bei einem bekannten Fehler nicht.

Lösung: A. Bei einem bekannten Fehler ist die zugrunde liegende Ursache bekannt, bei einem Problem nicht. Durch die Untersuchung eines Problems (Problem Control) wird die zugrunde liegende Ursache festgestellt. Somit kennt man die Ursache zu dem Problem. In diesem Augenblick spricht man von einem bekannten Fehler (Known Error). Einem Problem geht in der Regel mindestens ein Zwischenfall in der IT-Infrastruktur voraus. Bei der Beschreibung eines Problems sind die relevanten Konfigurationselemente noch nicht bekannt. Das Problem muss noch untersucht werden und wird am Ende der Untersuchung zu einem bekannten Fehler, wenn seine Ursache gefunden wurde.

Wer legt die Planung von einem Change (Änderung) fest?

A. Der Change-Manager

B. Das Change Advisory Board (CAB)

C. Der Kunde

D. Das IT Management

Lösung: A. Der Change-Manager ist die Person, die für den Change-Kalender die Endverantwortung trägt. Das Change Advisory Board (CAB) ist eine beratende Instanz, aber die Endverantwortung liegt beim Change-Manager.

Wer ist befugt, ein Service Level Agreement (SLA) zur Lieferung von IT-Dienstleistungen mit der IT-Organisation abzuschließen?

A. Service Level Management

B. Anwender

C. ITIL-Prozesseigentümer

D. Auftraggeber

Lösung: D. Der Auftraggeber ist befugt, ein Service Level Agreement (SLA) mit der IT-Organisation zur Lieferung von IT-Dienstleistungen abzuschließen. Der Anwender ist lediglich der Nutzer der Leistungen, der für seine Arbeit die IT-Dienstleistungen und Mittel nutzt.

Wenn in einer Windows-Umgebung eine neue Version eines Softwarepakets installiert wird, kann sich dies auf andere Softwarepakete auswirken. Welcher ITIL-Prozess überwacht, ob in dieser Situation andere Softwarepakete erneut getestet und installiert werden müssen?

A. Change Management
B. IT Service Continuity Management
C. Problem Management
D. Release Management

Lösung: A. Das Change Management sorgt dafür, dass die Risiken einer Änderung möglichst gering sind. Die tatsächlichen Aktionen (die neue Installation und das Testen anderer Pakete) können Aufgabe des Release Management sein, allerdings ist das Change Management für die Überwachung verantwortlich.

Der Availability-Manager will wissen, wie es mit der Wiederherstellung von IT-Komponenten aussieht. Bei wem muss er sich die erforderlichen Informationen einholen?

A. Beim Service Desk
B. Bei der technischen Administration
C. Beim Configuration-Manager
D. Beim Service Level-Manager

Lösung: C. Bei der Technischen Administration. Denn die Configuration Management Datenbank (CMDB) des Konfigurations-Managements enthält Informationen über den Grad der Störung, die Dauer der Störung usw.

Welcher der nachstehenden Begriffe bezeichnet das Ausmaß, in dem ein Zwischenfall (Incident) zu einer Abweichung vom normalen Serviceniveau führt?

A. Eskalation
B. Auswirkung
C. Priorität
D. Dringlichkeit

Lösung: B. Die Auswirkung (Impact) bestimmt das Ausmaß, in dem ein Zwischenfall zu einer Abweichung vom normalen Serviceniveau (Service Level) führt. Hier handelt es sich um einen Zwischenfall und (noch) nicht um eine Eskalation. Die Priorität wird durch die Auswirkung und die Dringlichkeit bestimmt; beide zusammen sind dann für die entsprechende Priorität verantwortlich.

Was ist die erste Aktivität, die im Problem Management-Prozess enthalten sein sollte?

A. Analysieren aller bestehenden Zwischenfälle

B. Klassifizieren von Problemen und Prioritäten setzen

C. Lösen von Problemen

D. Für die Managementinformationen sorgen

Lösung: A. Die Analyse aller bestehenden Zwischenfälle ist die erste Aktivität innerhalb des Subprozesses Problem Control.

Worüber berichtet ein Change-Manager der Organisation bezüglich eines ausgeführten Changes?

A. Über die Personalkosten

B. Über die Anzahl der Zwischenfälle (Incidents)

C. Über falsch registrierte Konfigurationselemente (CIs)

D. Über den Aufbau und die Zusammenstellung der Konfigurationselemente (CIs)

Lösung: B. Der Change-Manager gibt einen Bericht bezüglich der Anzahl der Zwischenfälle nach einem Change ab, um die Effizienz des Change Management-Prozesses darzustellen. Gerade in diesem Punkt zeigt sich, dass ITIL keine graue Theorie ist. In der Praxis ist es immer wieder auffallend, wie viele Changes die Ursache für nachfolgende Incidents sind.

Aus welcher Datensammlung können statistische Daten abgerufen werden, die Einblick in den Aufbau und die Zusammensetzung der IT-Infrastuktur geben?

A. Der Kapazitätssdatenbank (Capacity Database, CDB)

B. Der Configuration Management Database (CMDB)

C. Dem maßgeblichen Hardware-Lager (Definitive Hardware Store, DHS)

D. Der definitiven Software-Bibliothek (Definitive Software Library, DSL)

Lösung: B. Die Konfigurations-Management-Datenbank (Configuration Management Database, CMDB) enthält eine Aufzeichnung der gesamten IT-Infrastruktur und derer Komponenten (CIs) mit ihren wechselseitigen Beziehungen. Die CMDB gilt als Modell bzw. Abbild der IT-Infrastruktur.

Was ist nie eine Aktivität des Service Desk?

A. Die Abwicklung von (Standard) Requests for Change (RfC)

B. Die Abwicklung von Reklamationen über die Dienstleistung

C. Das Ermitteln der zugrunde liegenden Ursache von Zwischenfällen

D. Informationen über Produkte und Dienstleistungen erteilen

Lösung: C. Das Ermitteln der zugrunde liegenden Ursache von Zwischenfällen ist eine Aktivität des Problem Managements. Ursachenforschung gehört weder zum Prozess Incident Management noch zur Funktion Service Desk. Alle anderen erwähnten Aktivitäten können vom Service Desk übernommen werden (Achtung: Gefragt wurde „nie"!).

Welche der nachstehenden Kommunikationsformen gehört zu einem der taktischen Prozesse?

A. Anwender-Unterstützung auf dem Gebiet von Anwendungen
B. Rundschreiben des Service Desk über eine Anwendung
C. Besprechung eines Request for Change (RfC) in Bezug auf die Erweiterung einer Anwendung mit dem Antragsteller dieses RfC
D. Vereinbarungen über den Verfügbarkeitsprozentsatz einer gekauften Anwendung

Lösung: D. Vereinbarungen über den Verfügbarkeitsprozentsatz einer gekauften Anwendung werden im Prozess Service Level Management getroffen, einem taktischen Prozess. Die Anwender-Unterstützung auf dem Gebiet von Anwendungen findet im Prozess Incident Management, einem operativen Prozess, statt. Das Service Desk ist ebenfalls eine operativ arbeitende Abteilung. Der Service Support-Bereich enthält keine taktischen Kapitel.

Der PC eines IT-Anwenders funktioniert nicht mehr. Dies ist nicht das erste Mal, dass er mit einem defekten PC konfrontiert ist. Vor drei Monaten funktionierte der PC ebenfalls nicht. Er teilt die Störung dem Service Desk mit. Wovon ist hier die Rede?

A. Zwischenfall
B. Bekannter Fehler
C. Problem
D. Request for Change

Lösung: A. Es handelt sich um einen Zwischenfall. Es ist lange her, dass der letzte Zwischenfall auftrat. Der Zwischenfall ist nicht direkt mit der letzten Störung in Verbindung zu bringen.

Was ist ein Beispiel für einen Service Request?

A. Eine Reklamation zu einer Dienstleistung
B. Eine Störungsmeldung
C. Eine Verlegung der Apparatur
D. Die Bitte um Dokumentation

Lösung: D. Die Bitte eines Anwenders um Informationen, Empfehlungen, Dokumentationen oder ein neues Kennwort ist ein Service Request. Eine Störungsmeldung ist kein Service Request.

Womit beschäftigt sich das Pro-aktive Problem Management?

A. Mit dem Behandeln von Requests for Change
B. Die Trendanalyse und Identifizierung von möglichen Zwischenfällen und Problemen
C. Mit dem Verfolgen aller Störungen
D. Mit dem Verhindern des Auftretens neuer Änderungen infolge von vorgenommenen Änderungen

Lösung: B. Pro Active Problem Management beschäftigt sich mit der Trendanalyse und Identifizierung von möglichen Zwischenfällen und Problemen. So sollen Incidents durch entsprechende Aktionen vermieden werden. Mögliche Störungen werden frühzeitig erkannt, bevor diese Auswirkungen haben. Das Verhindern von neuen Anpassungen infolge von vorgenommenen Änderungen ist Aufgabe des Change Managements.

Welcher ITIL-Prozess liefert die wichtigsten und häufigsten inhaltlichen Beiträge für die Aktualisierung der Configuration Management-Datenbank (CMDB)?

A. Das Change Management
B. Das Configuration Management
C. Das Incident Management
D. Das Problem Management

Lösung: A. Das Change Management genehmigt laufend Änderungen in der IT-Infrastruktur und ist so verantwortlich dafür, dass Änderungen an den in der CMDB dokumentierten CIs vorgenommen werden. Das Configuration Management ist für die Pflege und für Audits zuständig. Das Incident Management und das Problem Management benutzen die CMDB lediglich.

Welche Person, die an einem Zwischenfall beteiligt ist, bestimmt, ob der Incident als abgeschlossen gelten darf?

A. Abnehmer von Dienstleistungen
B. Benutzer
C. Mitarbeiter des Service Desk
D. Service-Manager

Lösung: B. Benutzer: Dieser bestimmt immer, ob der Zwischenfall abgeschlossen wird und er wieder vernünftig arbeiten kann.

Was ist ITIL?

A. Eine Sammlung von Büchern, die als Modell für die Organisation von Prozessen in einem IT-Umfeld dienen
B. Eine Methode, nach der IT-Systeme einzurichten sind

C. Eine Sammlung von Richtlinien, die eingehalten werden müssen, wenn der Kunde nach der Norm ISO 9000 zertifiziert werden soll

D. Eine Verfahrensweise, bei der die von Kunden gemeldeten Zwischenfälle im Mittelpunkt stehen

Lösung: A. Eine Sammlung von Büchern, die als Modell für die Organisation von Prozessen in einem IT-Umfeld dienen. Die Originalliteratur in englischer Sprache stammt aus der Feder der OGC bzw. CCTA. Es ist eine Library!

Welcher ITIL-Prozess bzw. welche ITIL-Funktion fragt beim Kunden nach, ob ein Zwischenfall wirklich behoben ist?

A. Incident Management

B. Problem Management

C. Service Desk

D. Service Level Management

Lösung: C. Service Desk. Dies ist die Kontaktstelle zum Kunden.

Welcher ITIL-Prozess oder welche ITIL-Funktion hat die Aufgabe, eingehende Störungsmeldungen zu klassifizieren?

A. Change Management

B. Incident Management

C. Problem Management

D. Service Desk

Lösung: B. Das Incident Management (siehe Abbildung 20.3) klassifiziert Meldungen über eingehende Störungen.

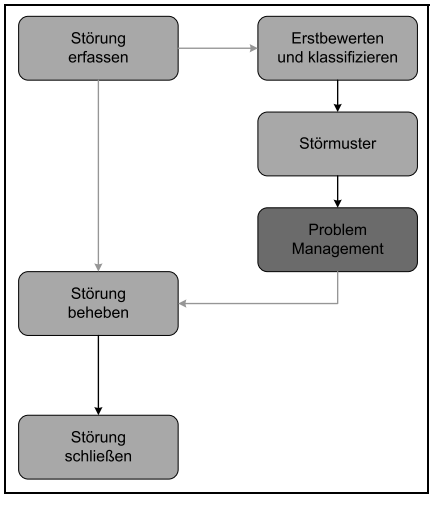


Abbildung 20.3: Aktivitäten im Incident Management

Im Change Management findet zwischen dem Akzeptieren eines Request for Change und dem Abschließen der Änderung eine Reihe von Aktivitäten statt. Welche der folgenden Aktivitäten wird als Erste ausgeführt?

A. Eintragen des Request for Change in den Zeitplan für Änderungen (FSC)

B. Entwickeln und Testen der Änderung

C. Festlegen der Dringlichkeit der Änderung

D. Implementieren der Änderung

Lösung: C. Festlegen der Dringlichkeit der Änderung: Dies ist Voraussetzung für alle weiteren Aktivitäten. Ansonsten wäre z.B. eine Planung gar nicht möglich.

Welcher Prozess steht nicht in direkter Beziehung zur Kunden-Organisation?

A. Change Management

B. Incident Management

C. Problem Management

D. Service Level Management

Lösung: C. Problem Management: Zwischen dem Problem Management und dem Kunden steht noch das Incident Management bzw. das Service Desk, die direkten Kontakt zum Kunden pflegen.

Ein Benutzer ruft das Service Desk mit der Beschwerde an, dass bei der Benutzung einer bestimmten Anwendung immer ein Fehler auftritt und dadurch die Verbindung mit dem Netzwerk unterbrochen wird. Welcher ITIL-Prozess ist für die Lokalisierung der Ursache verantwortlich?

A. Availability Management

B. Incident Management

C. Problem Management

D. Release Management

Lösung: C. Problem Management: Ursachenforschung ist stets Aufgabe dieses Prozesses.

Ein schwerer Fehler ist aufgetreten. Das zugewiesene Lösungsteam kann das Problem nicht innerhalb der vereinbarten Zeit beheben. Der Incident-Manager wird eingeschaltet. Von welcher Form der Eskalation ist hier die Rede?

A. Formelle Eskalation

B. Funktionale Eskalation

C. Hierarchische Eskalation

D. Operationelle Eskalation

Lösung: C. Hierarchische Eskalation, da hier eine Ebene „nach oben" gegangen wird (in der Linie).

Was ist die beste Beschreibung eines Problems?

A. Ein anderer Begriff für einen oder mehrere erkannte Fehler

B. Eine bekannte Ursache einer oder mehrerer Störungen

C. Eine unbekannte Ursache eines oder mehrerer Zwischenfälle

D. Ein erkannter Fehler mit einem oder mehreren Zwischenfällen

Lösung: C. Eine unbekannte Ursache eines oder mehrerer Zwischenfälle

Welcher ITIL-Prozess ist für die Aktualisierung der Konfigurations-Management-Datenbank (CMDB) verantwortlich?

A. Change Management

B. Configuration Management

C. Incident Management

D. Release Management

Lösung: B. Configuration Management: Kontrolle der IT-Infrastruktur und Pflege der entsprechenden Informationen sind Aufgaben des Configuration Management. Das Change Management stößt zwar viele Veränderungen an, pflegt aber nicht selber die CMDB, sondern übermittelt die relevanten Informationen an das Configuration Management.

In welchen Fällen muss nach der Implementierung einer Änderung eine Änderungsüberprüfung (Change Review) stattfinden?

A. Immer

B. Auf Anfrage der Person, die den Request for Change gestellt hat

C. Stichprobenartig

D. Wenn nach der Implementierung und der Änderung noch ein weiterer, gleichartiger Zwischenfall auftritt

Lösung: A. Immer: Dies ist fester Bestandteil des Prozesses. Diese Aktivität ist genauso zwingend notwendig wie Planung und Tests.

Control ist eine der Aktivitäten des Configuration Managements. Was beinhaltet diese Aktivität?

A. Die Aktualisierung aller Änderungen der Konfigurationselemente (Configuration Items, CIs) und ihre Beziehungen in der Konfigurations-Management-Datenbank (Configuration Management Database, CMDB)

B. Die Kontrolle, ob die Cls und ihre Attribute richtig in der CMDB stehen

C. Die Installation neuer CIs in der Betriebsumgebung

D. Die Inventarisierung der CIs

Lösung: A. ist richtig. Dagegen ist die Kontrolle, ob die CIs und ihre Attribute richtig in der Konfigurations-Management-Datenbank (Configuration Management Database, CMDB) stehen, keine Beschreibung für die Aktivität von Control, sondern von Verifizierung.

Welche Aktivität gehört zum Prozess Availability Management?

A. Das Klassifizieren von Requests for Change

B. Das Definieren der Auswirkungskodierung von Störungen

C. Das Identifizieren von Problemen in Bezug auf die Verfügbarkeit von IT Services

D. Das Messen der Verfügbarkeit des IT Service

Lösung: D. Messen ist neben der Berichterstattung die wichtigste Aktivität des Prozesses Availability Management. Die Ergebnisse aus den Aktivitäten Messen und Berichterstattung bilden die Basis für die Kontrolle der Service-Vereinbarungen, die Lösung von Problemsituationen und die Formulierung von Verbesserungsvorschlägen.

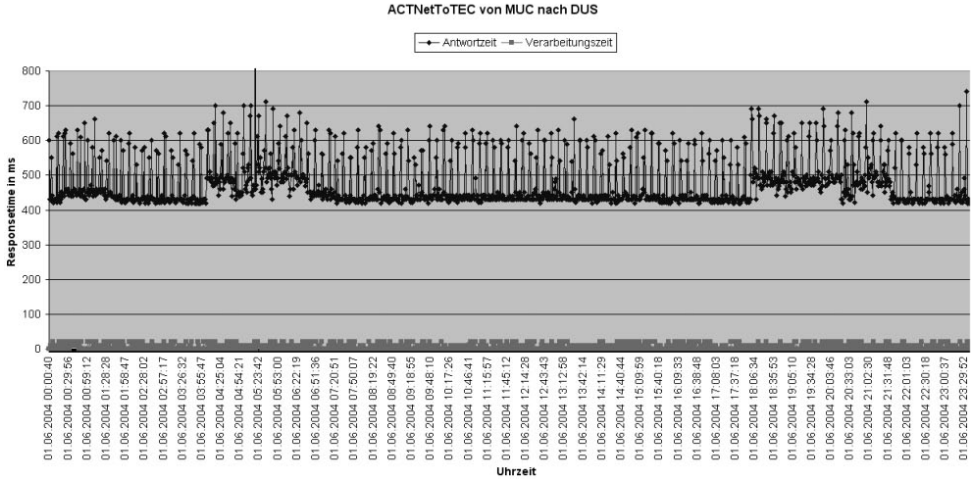


Abbildung 20.4: Beispielhaftes Messergebnis der Verfügbarkeit

In welchem Prozess wird mit dem Kunden über die Kosten der IT Serviceleistung diskutiert?

A. Availability Management

B. Capacity Management

C. Financial Management for IT Services

D. Service Level Management

Lösung: D. Service Level Management: Teil dieses Prozesses ist das Erstellen einer Service-Vereinbarung. Hierzu zählt auch der Zusammenhang zwischen gewünschten Dienstleistungen und den damit verbundenen Kosten.

Welche der folgenden Änderungen muss vom Change Management autorisiert werden?

A. Die Durchführung von Änderungen an einer Datensammlung (Datenbank) durch Anwender

B. Das erneute Setzen eines Kennworts

C. Das Hinzufügen eines neuen Anwenders in einem System

D. Der Umzug eines Druckers von der zweiten in die dritte Etage

Lösung: D. ist richtig. Dies stellt eine Änderung der IT-Infrastruktur dar, die Einfluss auf deren Funktion haben kann. Das erneute Setzen eines Kennworts ist keine Änderung (Change), sondern ein Service Request. Würde man jede Passwortänderung als Change betrachten, wäre der Change Management-Prozess schnell überlastet, durch Changes, die sich in der Regel nicht wesentlich auf die IT-Infrastruktur auswirken. Das Hinzufügen eines neuen Anwenders in einem System ist in der Regel kein Change, sondern ein Service Request.

Was muss als Attribut in die CMDB aufgenommen werden, um feststellen zu können, an welchen Konfigurationselementen (CIs) zur Zeit Wartungsarbeiten vorgenommen werden?

A. Ankaufdatum

B. Eigentümer

C. Ort

D. Status

Lösung: D. Status: Daran erkennen Sie, in welchem Zustand sich ein CI befindet (siehe Abbildung 20.5). Das Ankaufsdatum hat nichts mit der Wartung zu tun, genau so wenig wie alle anderen Angaben.

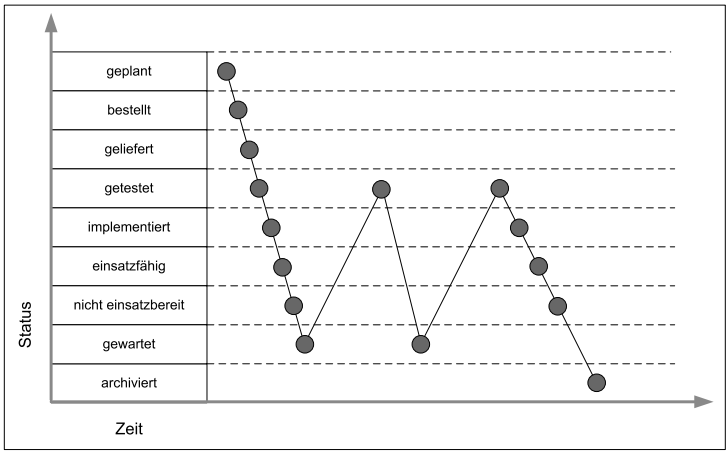


Abbildung 20.5: Status eines CI

Bei einem Server haben sich zwei Zwischenfälle (Incidents) ereignet. Es scheint, dass der Server durch seine vielen Verbindungen überlastet ist. Welche Maßnahme muss ein Availability-Manager in diesem Fall durchführen?

A. Er bittet den Capacity-Manager, die Kapazität des Servers zu vergrößern.

B. Er bittet den Problem-Manager, das Problem schnellstens zu untersuchen.

C. Er bittet den Security-Manager, zu untersuchen, ob evtl. zu viele Berechtigungen erteilt wurden.

D. Er bittet den Service Level-Manager, die Vereinbarungen in den Service Level Agreements (SLAs) zu überprüfen bzw. zu revidieren.

Lösung: B. ist richtig. Der erste Schritt besteht darin, zu bestimmen, was die tatsächliche Ursache der Zwischenfälle ist. Diese Überprüfung einzuleiten und zu überwachen ist Aufgabe des Problem-Managers. Erst wenn klar ist, dass die fehlende Kapazität Ursache des Problems ist, können weiter gehende Maßnahmen ergriffen werden. Es muss zuerst eine Untersuchung vorgenommen werden, bevor eine Vergrößerung der Kapazität des Servers durchgeführt werden kann. Bei der Implementierung des Servers war bekannt, wie viele Personen sich bei diesem Server einloggen können.

Welcher ITIL-Prozess oder welche ITIL-Funktion kennt die Aktivität, Zwischenfälle mit bekannten (dokumentierten) Lösungen in Verbindung zu bringen?

A. Change Management

B. Incident Management

C. Problem Management

D. Service Desk

Lösung: B. ist richtig. Dies ist eine konkrete Aktivität, die zum Prozess Incident Management gehört (Stichwort Störungsmuster). Das Change Management und das Problem Management beschäftigen sich nicht damit. Das Problem Management kümmert sich um die Untersuchung der zugrundeliegenden Ursache einer oder mehrerer Zwischenfälle.

Welchen Status bekommt ein Problem, wenn die Ursache dieses Problems bekannt ist?

A. Den Status „Incident“

B. Den Status „Known Error“

C. Den Status „Gelöst“

D. Den Status “Request tor Change”

Lösung: B. Status „Known Error“. Wenn die Ursache dieses Problems bekannt ist, bekommt es den Status bekannter Fehler (Known Error). Der Status 'Gelöst' ist nicht korrekt in der ITIL- Terminologie. Das Problem muss zuerst noch gelöst werden, wenn die

Ursache bekannt ist. Ein Request for Change (RfC) ist die logische Folge eines bekannten Fehlers (Known Error). Die Lösung des bekannten Fehlers kann durch die Anfrage und Ausführung eines Request for Change erfolgen.

Nachdem eine Änderung vorgenommen wurde, findet eine Auswertung statt. Wie bezeichnet ITIL diese Auswertung?

A. Zeitplan für Änderungen (Forward Schedule of Changes, FSC)

B. Review nach der Implementierung (Post Implementation Review, PIR)

C. Service-Entwicklungsplan (Service Improvement Program, SIP)

D. Serviceanforderungen (Service Level Requirements, SLRs)

Lösung: B. PIR ist korrekt. Ein Zeitplan für Änderungen (Forward Schedule of Changes, FSC) ist keine Auswertung, sondern ein Kalender mit einer Planung für die kommenden Änderungen. Ein Service-Entwicklungsplan (Service Improvement Programme, SIP) ist ebenfalls keine Auswertung. Serviceanforderungen (Service Level Requirements, SLRs) sind die Erwartungen, die ein Kunde an eine (neue) Dienstleistung stellt.

Aufgrund eines Defekts der Audiokarte eines Anwenders wurde diese durch eine neue ersetzt. Welcher ITIL-Prozess ist für die Registrierung dieser Aktivität verantwortlich?

A. Change Management

B. Configuration Management

C. Incident Management

D. Problem Management

Lösung: B. Das Configuration Management registriert neue Konfigurationselemente (Configuration Items, CI's) in der Configuration Management Database (CMDB). Das Change Management ist für die Genehmigung der Änderung verantwortlich, aber nicht für die Registrierung der geänderten Daten in der CMDB. Diese wird nur über das Configuration Management gepflegt.

Wo wird der Inhalt von Releases gespeichert?

A. In der Kapazitäts-Datenbank (GDB)

B. In der Configuration Management-Datenbank (GMOB)

C. Im Maßgeblichen Hardware-Lager (DHS)

D. In der Definitiven Software-Bibliothek (DSL)

Lösung: D. Der Inhalt von Releases wird in der Definitiven Software-Bibliothek DSL gespeichert.

Was wird in einen Service Level Agreement (SLA) aufgenommen?

A. Vereinbarungen in Bezug auf den zu liefernden Service
B. Die Verfügbarkeit des abgelaufenen Zeitraums
C. Ein Plan bzgl. der Vorgehensweise zur Implementierung des Prozesses Service Level Management
D. Detaillierte technische Beschreibungen des TCP-IP Protokolls

Lösung: A. Vereinbarungen in Bezug auf den zu liefernden Service. Die Einführuzng und Etablierung des Prozesses Service Level Management steht nicht in einem Service Level Agreement (SLA), sondern in einem Plan bzgl. der Vorgehensweise, wie dieser Prozess zu implementieren ist. Detaillierte technische Beschreibungen von Dienstleistungen sind nicht in einem guten SLA zu finden, da dieser nicht-technischen Charakter haben sollte.

Welcher ITIL-Prozess sorgt dafür, dass der IT Service im Fall einer Störung schnellstmöglich wiederhergestellt wird?

A. Change Management
B. Incident Management
C. Problem Management
D. Service Level Management

Lösung: B. Incident Management. Störungen gehen über das Incident Management ein. Das Incident Management versucht die Störungen schnellmöglich zu beheben.

Welche Informationen liefert der Prozess „Financial Management for IT Services" dem Service Level Management?

A. Die Verfügbarkeit von IT Services in einem bestimmten Zeitraum (Periode)
B. Die Kosten des Financial Management-Systems
C. Die Gesamtkosten der Netzwerk-Administration
D. Die Kosten pro Kunde bei den IT Services

Lösung: D. Die Kosten pro Kunde bei den IT Services. Dies ist einer der Punkte in Bezug auf die Kosten, die an das Service Level Management SLM berichtet werden. Das Umlegen der Kosten pro Service oder pro Kunde ist Teil eines Unterprozesses im Financial Management.

Welche Verantwortung hat der für die Sicherheit verantwortliche Security-Manager bei der Abfassung eines neuen Service Level Agreement (SLA)?

A. Übertragung der Serviceanforderungen für den Schutz von Informationen
B. Bestimmung der elementaren Sicherheitsanforderungen (Security Baseline) im Servicekatalog
C. Absicherung der Sicherheitsbestimmungen im SLA mit einem Operational Level Agreement
D. Berichterstattung über die technische Verfügbarkeit von Sicherheitskomponenten

Lösung: C. Absicherung der Sicherheitsbestimmungen im SLA mit einem Operational Level Agreement. Die tatsächliche Ausführung wird vom Security Management vorgenommen. Die Berichterstattung über die Verfügbarkeit gehört zum Aufgabenbereich des Availability Management.

Welcher ITIL-Prozess übernimmt die Regie über die Verteilung eines neuen Software-Releases?

A. Change Management
B. Configuration Management
C. Release Management
D. Service Level Management

Lösung: A. Change Management. Kontrolle und Regie der Verteilung von Releases finden unter der Verantwortung des Change Management statt. Das Release Management führt keine Regie über die Verteilung von Releases, sondern liefert sachliche Informationen über Releases und die Planung bzw. führt die Umsetzung durch.

In welchem ITIL-Prozess wird eine Analyse über mögliche Bedrohungen und Abhängigkeiten der Geschäftsprozesse von den IT Services erstellt und werden auf diesen Grundlagen Gegenmaßnahmen formuliert?

A. Availability Management
B. IT Service Continuity Management
C. Problem Management
D. Service Level Management

Lösung: B. IT Service Continuity Management. Das IT Service Continuity Management analysiert die Bedrohungen und Abhängigkeiten und legt relevante Gegenmaßnahmen fest. Ziel ist die Unterstützung des Business Continuity Managements (BCM), indem sichergestellt wird, dass die IT-Infrastruktur und -Dienste nach einer (unvorhersehbaren) Katastrophe innerhalb der vereinbarten Zeit kontrolliert wiederhergestellt werden können.

Wie wird innerhalb des Prozesses Capacity Management die Aktivität bezeichnet, mit der der Kapazitätsbedarf angepasst werden kann?

A. Application Sizing (Applikationsanpassung)

B. Demand Management (Bedarfsmanagement)

C. Modelling (Modellierung)

D. Tuning (Systemeinstellung)

Lösung: B. Das Demand Management ist mit der Anpassung des Kapazitätsbedarfs befasst. Das Application Sizing ist der Bereich, der Konzepte für die erforderliche Hardware entwickelt, um neue oder angepasste Applikationen in Betrieb zu nehmen. Das Modelling wird verwendet, um Konzepte für das „Verhalten" der Infrastruktur zu entwickeln. Das Tuning betrifft die optimale Einstellung von Systemen für die tatsächliche bzw. die zu erwartende Auslastung auf der Grundlage von gemessenen, analysierten und interpretierten Informationen.

Welcher ITIL-Prozess ist für das Erstellen eines Leistungsverrechnungssystems verantwortlich?

A. Availability Management

B. Capacity Management

C. Financial Management for IT Services

D. Service Level Management

Lösung: C. Financial Management for IT Services. Alle anderen Möglichkeiten sind falsch. Das Availability Management beschäftigt sich mit dem Management der Verfügbarkeit der IT Services. Capacity Management beschäftigt sich mit der Planung der zu erwartenden IT Service-Abnahmemengen. Das Service Level Management beschäftigt sich mit der Definition und Vereinbarung von Service Level Agreements.

Welcher Prozess verfolgt das Ziel, die IT-Dienstleistungen so schnell wie möglich wieder in Gang zu bringen, nachdem in einem Unternehmen eine längere Störung aufgetreten ist?

A. Availability Management

B. Capacity Management

C. IT Service Continuity Management

D. Problem Management

Lösung: C. IT Service Continuity Management: Dies entspricht der Definition dieses Prozesses.

Wo werden Vereinbarungen in Bezug auf das Security Management aufgezeichnet?

A. Konfigurations-Management-Datenbank (CMDB)

B. Service Level Agreement (SLA)

C. Definitive Software-Bibliothek (Definitive Software Library, DSL)

D. Kapazitätsplan (Capacity Plan)

Lösung: B. Service Level Agreement (SLA): Diese Vereinbarungen sind Bestandteil bzw. Unterprunkte zu den SLAs.

Wo wird die Planung von Änderungen (Changes) geführt?

A. In der CMDB (Configuration Management Database)

B. Im FSC (Forward Schedule of Change)

C. Im CAB (Change Advisory Board)

D. Im SIP (Service Improvement Program)

Lösung: B. Im FSC (Forward Schedule of Change): Hier wird die Terminplanung festgehalten und ggf. veröffentlicht.

Welches ist eine Aktivität des Service Desk?

A. Fungieren als erster Ansprechpunkt für den Kunden

B. Im Namen des Kunden die Störungsursache untersuchen

C. Lokalisieren der Ursache des Zwischenfalls

D. Fehlerquellen aus anderen Umgebungen zuordnen

Lösung: A. Das Service Desk ist der Single Point of Contact (SPoC).

Welche Rolle spielt ITIL in Bezug auf das IT Service Management?

A. Eine auf den besten Praxisbeispielen basierte Vorgehensweise

B. Internationale Norm für IT Service Management

C. Standardmodell für die IT-Dienstleistung

D. Theoretischer Rahmen für Prozesseinrichtung

Lösung: A. Eine auf den besten Praxisbeispielen basierte Vorgehensweise. ITIL ist weder standardisiert noch genormt.

Die Netzwerkadministratoren werden ständig von den Anwendern bei Problemen direkt angerufen oder angesprochen, so dass immer wieder Zeitkonflikte mit ihren geplanten Aufgaben auftreten. Sie haben kaum Zeit für die Verwaltung des Netzwerkes. Welcher ITIL-Prozess könnte diese Situation verbessern?

A. Change Management

B. Configuration Management

C. Incident Management

D. Problem Management

Lösung: C. Incident Management: Die Einführung dieses Prozesses würde verhindern, dass die Anwender die Fachabteilungen direkt kontaktieren und sie so vom Tagesgeschäft abhalten. Telefonnummern und direkte Ansprechpartner der nachgelagerten Fachabteilungen dürfen vom Incident Management nicht an die Anwender weitergegeben werden, um zu verhindern, dass das Incident Management unterlaufen wird und die Anwender sich doch wieder direkt an die Experten und bekannten Personen wenden.

Welcher der nachfolgenden Begriffe gehört zum Change Management?

A. Schätzung (Bewertung) nach der Implementierung (Post Implementation Review)

B. Notausgaben (Emergency Release)

C. Anfrage nach Service (Service Request)

D. Zeitliche Lösung (Workaround)

Lösung: A. Schätzung (Bewertung), auch PIR genannt. Dies gehört zum Change Management, wird aber über das Problem Management realisiert.

Einem Benutzer steht ein neuer PC zur Verfügung, der an das Firmen-Netzwerk angeschlossen wurde. Sein alter PC wird als Printserver für das lokale Netzwerk installiert. Welcher Prozess ist für die Registrierung dieser Änderung in der Configuration Management Database (CMDB) verantwortlich?

A. Change Management

B. Configuration Management

C. Problem Management

D. Release Management

Lösung: B. Configuration Management: Änderungen an der CMDB werden stets von diesem Prozess vorgenommen. Er ist verantwortlich für diese Datenbank und kein anderer Prozess ändert die Daten in der CMDB zu den CIs. Der Change Management-Prozess ist lediglich in der Lage, eine solche Änderung durch das Genehmigen eines Changes anzustoßen!

Die Speditionsfirma „LieferSchnell“ ist im Laufe der Jahre immer abhängiger von ihren Informationssystemen und den Leistungen der IT geworden. Daher wird beschlossen, die Stabilität der IT Services unter allen Umstanden sicherzustellen. Welcher Prozess wird dazu eingerichtet?

A. Availability Management

B. IT Service Continuity Management

C. Service Level Management

D. Service Management

Lösung: B. IT Service Continuity Management. Hier geht es um ein aktives Managen von Risiken. Selbst nach einem Katastrophenfall soll der Service schnellstmöglich wieder zur Verfügung stehen.

Die Daten für den Personalbereich sind nur befugten Benutzern zugänglich. Das Security Management unternimmt Schritte, dies zu gewährleisten. Welchen Sicherheitsaspekt garantiert das Security Management, wenn es derartige Schritte unternimmt?

A. Verfügbarkeit der Daten (Availability)

B. Integrität der Daten (Integrity)

C. Stabilität der Daten (Stability)

D. Vertraulichkeit der Daten (Confidentiality)

Lösung: D. Vertraulichkeit der Daten (Confidentiality): Dies muss sichergestellt werden, damit vertrauliche Daten nicht von Personen eingesehen werden können, die wie in diesem Fall den Datenschutz gefährden.

Ein Computer-Operator stellt fest, dass die Festplatte bald keine Speicherkapazität mehr hat. Welchem ITIL-Prozess muss er dies melden?

A. Availability Management

B. Capacity Management

C. Change Management

D. Incident Management

Lösung: D. Incident Management: Dieser Prozess dient als Anlaufstelle.

Für welche der folgenden Aktivitäten ist das Release Management verantwortlich?

A. Überprüfen, ob auf den Computern der Organisation illegale Software installiert wurde

B. Speichern der Originalkopien der gesamten gebrauchsfähigen Software der Organisation

C. Registrieren, wo welche Softwareversion erhältlich ist

D. Überprüfen, ob auf den Computern der Organisation ungetestete Software-Pakete installiert wurden

Lösung: B. Speichern der Originalkopien der gesamten gebrauchsfähigen Software der Organisation. Auf diese Weise wird sichergestellt, dass sämtliche Masterkopien in der DSL gespeichert werden.

Wofür benutzt das Service Level Management die Daten aus der Zwischenfallregistrierung des Service Desk?

A. Zum Erstellen des Dienstleistungsvertrages (Service Level Agreements, SLAs)

B. Zum Erstellen von Berichten über die Anzahl und Art der Zwischenfälle innerhalb eines bestimmten Zeitraums

C. Um anhand der Anzahl der gelösten Zwischenfälle die Verfügbarkeit der IT Services zu bestimmen

D. Um zusammen mit anderen Daten zu überprüfen, ob das vereinbarte Dienstleistungsniveau geliefert wurde

Lösung: D. Um zusammen mit anderen Daten zu überprüfen, ob das vereinbarte Dienstleistungsniveau geliefert wurde. Die Daten aus dem Reporting des Service Desk werden dem Service Level Management übergeben.

Das Service Desk hat diesen Monat über 4000 Anrufe entgegengenommen. Was fällt unter diese Anrufe?

A. Änderungen der Dienstleistungsverträge (Service Level Agreements, SLAs)

B. Meldungen über geänderte Configuration Items (CIs)

C. Anfragen an die IT-Organisation zur Anwenderunterstützung

D. Genehmigungen von Changes

Lösung: C. Anfragen an die IT-Organisation zur Anwenderunterstützung. Dies ist die Aufgabe des Service Desk.

Eine Handelsgesellschaft beabsichtigt die Fusion mit einem Konkurrenten. Die IT-Abteilungen sollen, einschließlich der IT-Infrastrukturen beider Firmen, zusammengelegt werden. Welcher Prozess ist für die Bestimmung der Festplatten- und Speicherkapazität der Anwendungen dieser vereinten IT-Infrastrukturen verantwortlich?

A. Application Management

B. Capacity Management

C. Computer Operations Management

D. Release Management

Lösung: B. Capacity Management: Gerade diese Situationen sind gute Beispiele für den Einsatz des Capacity Management. Capacity Management erstellt aus den Geschäftsanforderungen den Kapazitätsplan und überwacht dessen Einhaltung. Dabei wird zwischen Business, Service und Ressource Capacity Management unterschieden. Dazu gehören als Aktivitäten Application Sizing, Tuning, Servicemodellierung und Demand Management.

Welcher Begriff gehört nicht zum Financial Management für IT-Dienstleistungen (IT Services)?

A. Budgetieren (Budgeting)

B. Weiterberechnung (Charging)

C. Einkaufen (Procuring)

D. Tariffestlegung (Pricing)

Lösung: C. Einkaufen (Procuring): Standardfrage. Das Financial Management für IT Dienstleistungen besteht aus den Bereichen Budgeting, Charging und Pricing.

Anforderungen an das Dienstleistungsniveau (Service Level Requirements) werden im Prozess Service Level Management benutzt. Was repräsentieren diese Service Level Requirements?

A. Die Erwartungen und Bedürfnisse des Kunden bezüglich dieser Dienstleistung

B. Die Erwartungen der IT-Organisation in Bezug auf den Kunden

C. Die Bedingungen, die für den Dienstleistungsvertrag (Service Level Agreement, SLA) erforderlich sind

D. Einen Paragraphen des SLA mit Zusatzspezifikationen, die für die Ausführung des SLA erforderlich sind

Lösung: A. Die Erwartungen und Bedürfnisse des Kunden bezüglich dieser Dienstleistung: Über dieses Dokument definiert er seine Anforderungen.

Was ist eine der Zielsetzungen des Availability Management?

A. Einen Vertrag mit den Lieferanten abzuschließen

B. Überwachung der Verfügbarkeit eines Weiterberechnungssystems

C. Kontrolle der Zuverlässigkeit und des Dienstleistungsniveaus eines Configuration Item (CI), das gekauft und von Dritten gewartet wird

D. Planung und Verwaltung der Zuverlässigkeit und Verfügbarkeit der Dienstleistungsverträge (Service Level Agreements)

Lösung: C. Kontrolle der Zuverlässigkeit und des Dienstleistungsniveaus eines Configuration Item (CI), das gekauft und von Dritten gewartet wird

Welcher der nachstehenden Begriffe gehört zum IT Service Continuity Management?

A. Anwendungsdimensionierung (Application Sizing)

B. Empfindlichkeit (Vulnerablity)

C. Wartungsfähigkeit (Maintainability)

D. Reparaturvermögen (Resilience)

Lösung: B. Empfindlichkeit (Vulnerability): Thema Risikoeinschätzung

Was kann als Configuration Item (CI) angesehen werden?

A. Ein Anruf

B. Eine Dokumentation

C. Ein Zwischenfall

D. Ein Prozess

Lösung: B. Eine Dokumentation. Alle anderen Punkte stellen keine wirklichen greifbaren Items dar.

Wie unterstützt das Problem Management die Aktivitäten des Service Desk? Das Problem Management ...

A. ... löst ernste Zwischenfälle für das Service Desk.

B. ... untersucht alle Zwischenfälle, die das Service Desk löst.

C. ... entlastet das Service Desk, indem es die Lösung eines Problems direkt an den Benutzer weiterleitet.

D. ... stellt dem Service Desk Informationen über einen erkannten Fehler zur Verfügung.

Lösung: D. Das Problem Management stellt dem Service Desk Informationen über einen erkannten Fehler zur Verfügung. In einem solchen Fall werden Informationen zu einem Known Error kommuniziert und in die entsprechenden Datenbank eingepflegt.

Was versteht man unter einer Basiskonfiguration (Configuration Baseline)?

A. Eine Standardkonfiguration für die Configuration Management Database (CMDB)

B. Eine Beschreibung eines standardisierten CI

C. Ein Set von Configuration Items (CIs), das einmalig ausgeliefert wurde

D. Eine Standardkonfiguration, die an Benutzer ausgeliefert wird

Lösung: D. Eine Standardkonfiguration, die an Benutzer ausgeliefert wird: Eine so genannte Baseline besteht aus der Kopie einer Gruppe von „eingefrorenen CIs". Die entsprechenden Eigenschaften werden zu einem bestimmten Zeitpunkt dokumentiert und nicht weiter angepasst. Solche Ausgangskonfigurationen dienen oftmals als Ausgangspunkt für weitere Anpassungen oder als „Rückfallposition" (Rollback/Fallback).

Welche Rolle spielt die Definitive Software Library (DSL) im Prozess Release Management?

A. Ein (physischer) Speicherbereich für die Originalversionen der gesamten verwendeten Software

B. Ein Nachschlagewerk mit der gesamten Softwaredokumentation (Gebrauchsanweisungen und ähnliche Dokumente)

C. Ein Registrierungstool für alle Software-Items

D. Eine Art Configuration Management Database (CMDB) für Software

Die Abteilung Server-Betrieb der IT-Organisation hat zwecks Einhaltung eines Vertrages mit einem internen Kunden eine Vereinbarung mit einer externen Organisation getroffen. Worin wird die Vereinbarung mit der externen Organisation festgelegt?

A. Operational Level Agreement (OLA)

B. Service Level Agreement (SLA)

C. Service Level Requirements (SLRs)

D. Underpinning Contract (UC)

Lösung: D. Underpinning Contract (UC): Dies ist ein Vertrag mit einem externen Lieferanten (siehe Abbildung 20.6).

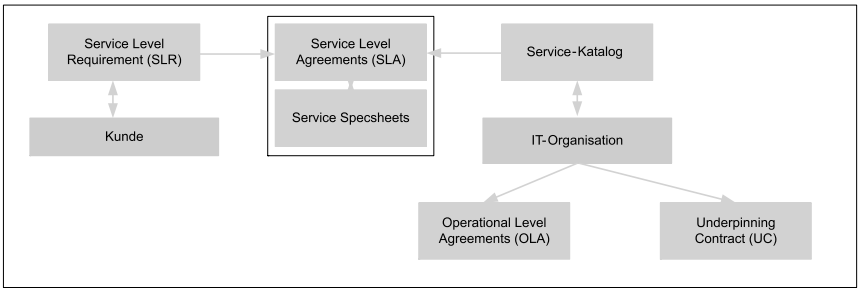


Abbildung 20.6: Begriffe des Service Level Management

Wie arbeitet Availability Management mit dem Security Management zusammen?

A. Indem Vereinbarungen über die Verfügbarkeit der Security Database getroffen werden

B. Indem Vereinbarungen hinsichtlich des Schutzes der Availability Database getroffen werden

C. Indem Grenzen für den Schutz aus den Anforderungen der Verfügbarkeit heraus bestimmt werden

D. Indem Maßnahmen über den Datenschutz verwirklicht werden

Lösung: D. Indem Maßnahmen über den Datenschutz verwirklicht werden

Welche Frage wird beantwortet, wenn eine Organisation Zukunftsbilder und Ziele festlegt?

A. Wie gelangen wir dorthin, wo wir sein wollen?

B. Wie wissen wir, ob wir dort sind oder nicht?

C. Wo wollen wir hin?

D. Wo befinden wir uns jetzt?

Lösung: C. Wo wollen wir hin? In diesem Zusammenhang wird oft der Begriff „Vision" verwendet (siehe Abbildung 20.7).

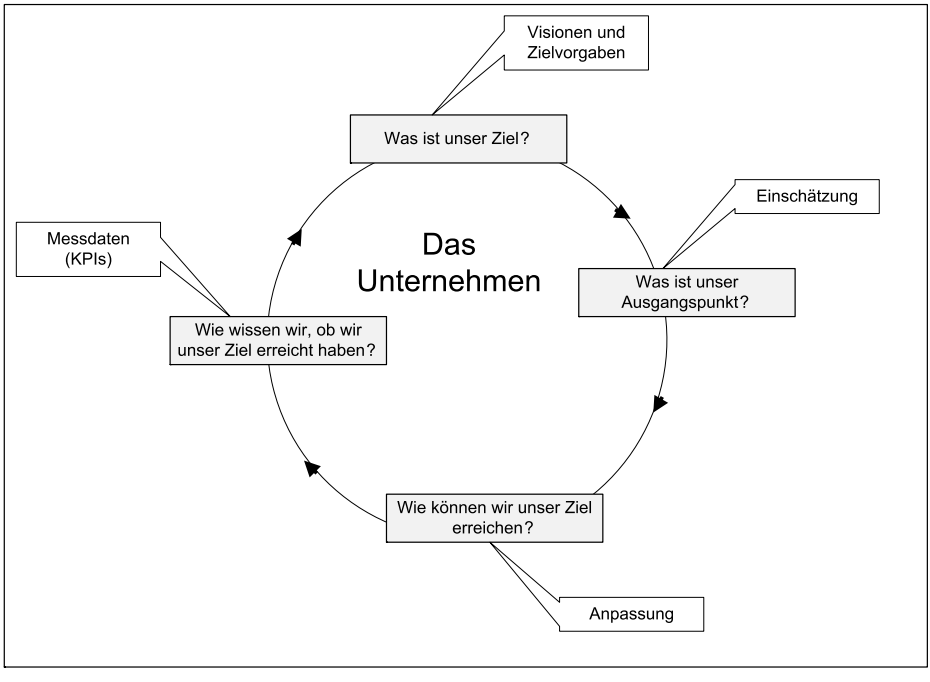


Abbildung 20.7: Optimierung der IT-Prozesse

Welche der nachfolgenden Aufgaben gehört zum Configuration Management?

A. Einberufen des Configuration Advisory Board

B. Physisches Verwalten der Software Items

C. Installieren der Apparatur am Arbeitsplatz

D. Zeichnen der Beziehungen zwischen den Configuration Items (CIs)

Lösung: D. Zeichnen der Beziehungen zwischen den Configuration Items (CIs) im Sinne der Informationspflege. Die Beziehungen zwischen den CIs helfen bei der Störungsdiagnose.

Welche der folgenden Aktivitäten liegt im Bereich des Incident Management?

A. Das Autorisieren von Changes

B. Das Durchführen von Ursachenanalysen der gemeldeten Störungen

C. Das Identifizieren und Dokumentieren der Probleme

D. Das schnellstmögliche Ingangsetzen der unterbrochenen Dienstleistung

Lösung: D. Das schnellstmögliche Ingangsetzen der unterbrochenen Dienstleistung. Die anderen genannten Lösungen liegen im Problem Management oder Change Management.

Welche Aussage trifft am ehesten auf den Begriff „Incident" zu?

A. Ein Vorfall, der von der erwarteten Standardleistung abweicht

B. Eine Serviceunterbrechung, deren Ursache noch nicht bekannt ist

C. Eine Frage oder Beschwerde, die der Anwender an den Service Desk richtet

D. Ein technisches Problem beim Kunden

Lösung: A. Ein Vorfall, der von der erwarteten Standardleistung abweicht. Der erwartete und via SLAs vereinbarte Service ist die Dienstleistung, die der Kunde und Anwender erwartet. Dazu zählt nicht nur eine absolute Unterbrechung des Services, sondern eine Minderung der damit im Zusammenhang stehenden Qualität.

Sie arbeiten in einer Organisation mit implementierten Service Support-Prozessen. Ein Anwender ruft an, um zu melden, dass er nicht mit der Anwendung Lotus Notes arbeiten kann. Dies ist ...

A. ein bereits bekannter Fehler

B. ein Problem

C. eine Störung

D. ein Request for Change

Lösung: C. Dies stellt eine Störung dar. Das erstmalige Auftreten eines solchen Zwischenfalls ist als Störung zu werten. Eine andere Zuordnung wäre nur dann möglich, wenn das Problem Management bereits aktiv war und das Incident Management oder das Service Desk mit Informationen zur Problemursache oder einem Known Error mit entsprechendem Workaround versorgt hätte.

Eine Anwenderin ruft das Service Desk an, um zu melden, dass ihr Lotus Notes Client ständig Netzwerkfehler meldet bzw. die Netzwerkverbindung jedes Mal zusammenbricht, wenn sie auf den Domino Server zugreift. Welche Funktion hat die Gesamtverantwortung dafür, dass die Ursache für diese Störung ermittelt wird?

A. Change Management

B. Incident Management

C. Problem Management

D. Service Desk

Lösung: C. Problem Management: Stichwort ist hier die Ursachenforschung, die stets in diesem Prozess verankert ist. Incident Management und Service Desk beschäftigen sich nicht mit dieser Aufgabe.

Welche Aufgabe liegt im Bereich des Problem Management (Problem Control)?

A. Proaktive Verhütung von Problemen

B. Identifizieren, Klassifizieren und Dokumentieren von Problemen

C. Verfassen von aussagekräftigen Problem-Berichten für das Management

D. Steigerung der Produktivität des Support-Personals

Lösung: B. Identifizieren, Klassifizieren und Dokumentieren von Problemen: Jede Störung, deren Ursache unbekannt ist, muss mit einem Problem verknüpft werden können. Das Thema Problemidentifizierung wird oft Problemkoordinatoren zugeordnet. Problem Control bezeichnet den deutschen Begriff Problembehandlung.

Aus welchem Hauptgrund sollte ein Service Desk eingerichtet werden?

A. Sicherstellen der zugesagten Funktionalität gemäß der getroffenen Vereinbarungen

B. Vermeiden von wiederkehrenden Problemen, damit die Anwender optimale Unterstützung bei der Ausführung ihrer Arbeit erhalten

C. Sicherstellen eines klar definierten Kontaktpunktes, an den sich alle Anwender mit Störungen, Anfragen, Bemerkungen und Beschwerden wenden können

D. Sichern der optimalen Verfügbarkeit von IT-Dienstleistungen für alle Anwender

Lösung: C. Sicherstellen eines klar definierten Kontaktpunktes, an den sich alle Anwender mit Störungen, Anfragen, Bemerkungen und Beschwerden wenden können: Dies ist die sogenannte Single Point of Contact-Funktion (SPOC).

Ein auszurangierender Server wird nächste Woche im Testumfeld verwendet. Welcher Prozess ist für die Registrierung der ausgeführten Änderung verantwortlich?

A. Change Management

B. Configuration Management

C. Service Desk

D. Problem Management

Lösung: B. Configuration Management. Das Change Management würde eine solche Änderung zwar genehmigen, das Umsetzen der Registrierung liegt aber beim Configuration Management. Die anderen Bereiche haben mit diesen Aktivitäten nur entfernt zu tun.

Die Hardware-Komponenten sowie die System- und Anwendungssoftware müssen in der CMDB erfasst sein. Welche (weiteren) Komponenten sind mögliche Configuration Items (CIs)?

1. Datenkommunikationseinrichtungen / 2. Mitarbeiter / 3. Dokumentationen

A. 1 und 2

B. 1 und 3

C. 2 und 3

D. 1, 2 und 3

Lösung: D. 1, 2 und 3

Was stellt die Basis für das IT Service Management dar?

A. Eine auf besten Praxisbeispielen basierte Vorgehensweise (Best Practise)

B. Ein Standardmodell für IT-Organisationen

C. Ein theoretischer Rahmen für die Einführung von Prozessen

D. Eine internationale Norm für IT Service Management

Lösung: A. Eine auf besten Praxisbeispielen basierte Vorgehensweise: Genau das stellt ITIL dar, und zwar in Form einer Bibliothek.

Welcher der folgenden Abläufe beschreibt den normalen Ablauf einer Fehlerbehebung?

A. Problem – Incident – Change – Known Error

B. Problem – Incident – Known Error – Change

C. Incident – Problem – Change – Known Error

D. Incident – Problem – Known Error – Change

Lösung: D. Incident – Problem – Known Error – Change: Ein Incident steht stets als Auslöser an erster Stelle und ein Change als Lösung an letzter Stelle der Aktionskette.

Nach einer genehmigten Änderung an der IT-Infrastruktur müssen die Daten in der CMDB modifiziert werden. Welcher Prozess erteilt die entsprechende Genehmigung für eine Änderung der Daten in der CMDB?

A. Configuration Management

B. Change Management

C. Release Management

D. Incident Management

Lösung: B. Change Management: Das wichtige Stichwort lautet hier „Genehmigung".

Welche Aussage ist in Bezug auf den Detaillierungsgrad der CMDB relevant?

A. Die Ausgeglichenheit zwischen dem Aufwand und der Genauigkeit der Informationen

B. Der Informationsbedarf von Incident und Problem Management

C. Die Informationen, die die Service-Organisation benötigt, um die gesteckten Ziele zu erreichen

D. Die Anzahl der Systeme und deren Beziehungen zur Infrastruktur

Lösung: C. Dier Informationen, die die Service-Organisation benötigt, um die gesteckten Ziele zu erreichen: IT Service Management dient stets zum Erreichen der gesteckten Business-Ziele. ITIL und IT sind kein Selbstzweck.

Prüfen Sie folgende Aussagen:

1. Der Service Desk stellt den täglichen Ansprechpartner für alle Anwender dar. Er ist für Anwenderprobleme im Zusammenhang mit der Nutzung der IT Services dar. Bei spezifischen Fragen zu bestimmten Themen werden die Anwender an die zuständigen IT-Abteilungen verwiesen.

2. Der Service Desk behebt alle Fehler und stellt nach einer Unterbrechung den normalen Servicebetrieb wieder her.

Welche der beiden Aussagen ist richtig?

A. 1

B. 2

C. Keine

D. Beide

Lösung: C. Keine: Der Service Desk verweist die Anwender auf keinen Fall an die fachspezifischen IT-Abteilungen und löst selber auch keine Fehler.

Beim Service Desk ruft eine Anwenderin an, die ihr Passwort nach ihrem Urlaub vergessen hat. Diese Störung betrifft nur diese eine Person. Der Mitarbeiter des Service Desk und die Anwenderin wissen beide, dass die Lösung der Anfrage nur Minuten dauern wird. Welche Schlussfolgerung ist anhand dieser Informationen zu ziehen?

A. Die Auswirkungen (Impact) sind hoch.

B. Die Priorität ist hoch.

C. Die Dringlichkeit ist hoch.

D. Es kann nichts Definitives über Auswirkung und Dringlichkeit gesagt werden.

Lösung: D. Es kann nichts Definitives über Auswirkung und Dringlichkeit gesagt werden: Schliesslich könnte es sich auch um ein Mitglied des Vorstands, den eigenen Chef, den Geschäftsführer und den Leiter der Abteilung XY handeln, der dringende Aktivitäten durchführen muss.

Wenn ein Fehler gemeldet wird, ist es wichtig, dass der Service mit möglichst geringen Auswirkungen für den Kunden wiederhergestellt wird. Dies ist hauptsächlich Aufgabe des folgenden Prozesses:

A. Configuration Management

B. Incident Management

C. Problem Management

D. Change Management

Lösung: B. Incident Management: Das Incident Management ist für die schnellstmögliche Wiederherstellung des definierten Betriebszustands eines Services zuständig.

Eine Palette von TFT-Monitoren inkl. Kabel wird geliefert. Der Status der gelieferten Hardware muss von „bestellt" in „auf Lager" geändert werden. Welcher Prozess erfasst diese Statusänderung?

A. Configuration Management

B. Incident Management

C. Problem Management

D. Change Management

Lösung: A. Configuration Management: Dieser ITIL-Prozess pflegt die CMDB.

Bei der Implementierung eines neuen Software-Pakets treten Fehler auf. Trotzdem wird die Entscheidung getroffen, das neue Release auszurollen. Welcher Prozess ist für die Aufzeichnung dieser Fehler verantwortlich, nachdem die Softwareverteilung erfolgreich abgeschlossen wurde?

A. Configuration Management

B. Problem Management

C. Release Management

D. Change Management

Lösung: B. Problem Management: Innerhalb der Fehlerbehandlung werden in Bezug auf das Change Management bekannte Fehler abgeschlossen.

Welche der folgenden Aussagen kann mit dem Begriff „proaktiv" belegt werden?

- 1. Known Error Control
- 2. Review von Incident- und Problem-Analyse-Reports zur Ermittlung von Trends
- 3. Vermeiden, dass sich Probleme mit Service A in Service X wiederholen
- 4. Identifizierung einer Incident-Ursache

A. 1 und 4

B. 1, 2 und 3

C. 2 und 3

D. 1 und 3

Lösung: C. 2 und 3: Trendanalyse ist stets als proaktive Tätigkeit anzusehen. Erkenntnisse bekannter Probleme als Hintergrundinfos für proaktive Tätigkeiten zu verwenden, dient ebenfalls einer Fehlervermeidung in der Zukunft.

In Kürze muss eine Abteilung mit neuen PCs versorgt werden, die alle neu zu installieren sind. Dabei kommt in der IT-Organisation die Frage auf, welche Verantwortung das Configuration Management hat und was nicht in dessen Zuständigkeit fällt. Für welche der folgenden Aktivitäten ist das Configuration Management nicht verantwortlich?

A. Das Prüfen der Vollständigkeit und Korrektheit der Informationen über die PCs

B. Das Prüfen der Funktionsfähigkeit der PCs

C. Das Aufzeichnen der Informationen bezüglich der PCs

D. Das Registrieren und Überwachen der Datenqualität über die PCs

Lösung: B. Das Prüfen der Funktionsfähigkeit der PCs: Ob und inwiefern ein PC funktioniert, ist, falls diesbezüglich ein Call beim Service Desk aufgegeben wurde oder nicht, Sache des Problem bzw. Incident Management.

Ein umfangreicher Change eines bestehenden Services soll geplant und implementiert werden. Für welche der folgenden Aktivitäten ist dabei das Configuration Management nicht verantwortlich?

A. Qualitätssicherung der Software-Module

B. Kontrolle aller Daten über die Software-Module

C. Benennung und Dokumentation der Daten über die Software-Module

D. Erfassung und Überwachung des Status der Software-Module

Lösung: A. Qualitätssicherung der Software-Module: Ob und inwiefern die Module funktionieren, muss innerhalb des Incident bzw. Problem Management herausgefunden werden.

Nach der Durchführung eines Changes im Netzwerkbereich können die Anwender auf bestimmte Systeme nicht mehr zugreifen. Welche Funktion ist für diesen Incident während seines gesamten Lebenszyklus zuständig?

A. Problem Management

B. Change Management

C. Service Desk

D. Configuration Management

Lösung: C. Service Desk: In der Regel liegen hier alle Informationen für Rückfragen, Zeitpläne und Ansprechpartner.

Der Prozentsatz der Supportanfragen, die ohne weiterführende Maßnahmen abgeschlossen werden können, ist ein Messkriterium für die Effektivität des:

A. Release Management
B. Configuration Management
C. Service Desk
D. Change Management

Lösung: C. Service Desk: Hier treffen die Anfragen der Anwender ein und hier kann ihnen auch direkt geholfen werden.

Welches ist keine Aufgabe des Service Desk?

A. Management-Berichte zu erstellen
B. Alle Störungen zu verfolgen und gegebenenfalls zu eskalieren
C. Die Ursache des Zwischenfalls zu lokalisieren
D. Die Benutzer über Status und Fortschritt ihrer Anfrage zu informieren

Lösung: C. Die Ursache des Zwischenfalls zu lokalisieren: Dies liegt im Bereich des Problem Management, Stichwort „Ursachenforschung".

Aus der erfolgreichen Problemdiagnose entsteht ein Known Error. Auf dessen Basis kann ein Request for Change (RfC) gestellt werden. Der Known Error kann geschlossen werden, wenn:

A. Ein Change Review zu einem zufrieden stellenden Ergebnis geführt hat
B. Der RfC beim Change-Manager eingereicht wurde
C. Der RfC vom Change Advisory Board (CAB) autorisiert wurde
D. Keine Incidents im Zusammenhang mit dem Known Error mehr auftreten

Lösung: A. Ein Change Review zu einem zufrieden stellenden Ergebnis geführt hat: Und auch erst dann darf der RfC geschlossen werden!

Zur Problembehebung muss eine Erweiterung des SANs inklusive Anpassung des Backups stattfinden. Durch welchen Prozess muss die formale Freigabe für die Umsetzung des Changes erfolgen?

A. Configuration Management
B. Release Management
C. Problem Management
D. Change Management

Lösung: D. Change Management: Genehmigungen kommen diesbezüglich stets aus dem Prozess Change Management, Stichwort „formale Freigabe"/„Genehmigung".

Warum sollten Mitarbeiter etwas über ITIL lernen?

A. Weil die Geschäftsprozesse von der Qualität der unterstützenden IT Services abhängen
B. Weil ITIL die einzige Methode für das Management verteilter IT-Umgebungen ist
C. Weil ITIL die erste Initiative im IT-Bereich ist, die herstellerunabhängig ist
D. Weil ITIL die ideale Aufbaustruktur einer IT-Organisation beschreibt

Lösung: A. Weil die Geschäftsprozesse von der Qualität der unterstützenden IT Services abhängen. ITIL ist kein Selbstzweck, sondern unterstützt Businessziele.

Welche der folgenden Prozesse leisten den größten Beitrag bei der Festlegung von Service Levels?

A. Service Level Management und Availability Management
B. Service Level Management und Continuity Management
C. Availability Management und Capacity Management
D. Capacity Management und Continuity Management

Lösung: A. Service Level Management und Availability Management

Wie trägt IT Service Management zur Verbesserung der Qualität der IT-Dienstleistung bei?

A. Indem Verträge zwischen internen und externen Kunden geschlossen werden
B. Durch allgemein anerkannte Normen der Service Levels
C. Indem in der IT-Organisation eine kundenfreundliche Behandlung gefördert wird
D. Indem Prozesse zur Verwirklichung der Dienstleistung eingerichtet werden, die einfach zu handhaben und aufeinander abgestimmt sind

Lösung: D. Indem Prozesse zur Verwirklichung der Dienstleistung eingerichtet werden, die einfach zu handhaben und aufeinander abgestimmt sind: Einfache Handhabung, Wiederverwendbarkeit und Stimmigkeit sind Kriterien, die für ITIL sprechen.

Zur Einhaltung eines Vertrages mit einem internen Kunden hat die IT-Abteilung eines Unternehmens eine Vereinbarung mit einem externen Lieferanten getroffen. Wie wird diese Vereinbarung mit dem externen Lieferanten bezeichnet?

A. Service Level Agreement (SLA)
B. Service Level Requirement (SLR)
C. Underpinning Contract (UC)
D. Operational Level Agreement (OLA)

Lösung: C. Underpinning Contract (UC): Stichwort ist hier „externe Lieferantenbeziehung".

Was ist ITIL?

A. Eine Bibliothek mit einer Serie von Büchern, die der IT-Organisation helfen, serviceorientierte Prozesse zu definieren

B. Eine Methode, nach der Informationssysteme einzurichten sind

C. Eine Sammlung von Richtlinien zur Zertifizierung nach Norm ISO 9000

D. Eine Anleitung für den kundenorientierten Aufbau einer IT-Organisation

Lösung: A. Eine Bibliothek mit einer Serie von Büchern, die der IT-Organisation helfen, serviceorientierte Prozesse zu definieren: nichts Mystisches, sondern lediglich eine Reihe von Büchern mit Best Practise-Inhalten.

Welche Aussage ist richtig?

1. SLAs sollen die Rollen und Verantwortlichkeiten für beide Parteien definieren.

2. SLAs sollen regelmäßig überwacht werden und es sollen Reports erstellt und verteilt werden.

3. Vor Unterzeichnung von SLAs sollte ein Review der unterstützenden Verträge erfolgen.

A. Alle

B. 1 und 2

C. 2 und 3

D. Keine

Lösung: E.*A. Alle*

Welche Aussage ist nicht richtig? Availability Level sind abhängig von:

A. Der Zuverlässigkeit der Komponenten (Reliability)

B. Den Kosten der Komponenten

C. Der Strapazierfähigkeit bei Ausfällen (Resilience)

D. Der Qualität von Wartung und Support

Lösung: B. Den Kosten der Komponenten. Dies gilt analog zu den Service Leveln.

Zu welchem der nachstehenden Begriffe sollte in einer strategischen Erklärung zum Service Management der IT-Organisation eine Aussage enthalten sein?

1. Servicequalität

2. Unternehmensziele

3. Kosteneffektivität

4. IT-Ressourcen

A. 1, 2 und 3
B. 1, 2 und 4
C. 2, 3 und 4
D. Zu keinem

Lösung: E.*B. 1, 2 und 4*

Security ist ein besonders wichtiges Element von

A. Financial Management for IT Services
B. Service Level Management
C. Availability Management
D. Capacity Management

Lösung: C. Availability Management. Diese beiden Prozesse arbeiten eng zusammen. Außerdem beeinflusst die Verfügbarkeit die Sicherheit.

Der Continuity-Plan einer IT Service-Organisation muss mindestens wie folgt überprüft und getestet werden:

A. Regelmäßig mindestens jährlich
B. Bei der Erstellung, danach jährlich und nach jedem signifikanten Change
C. Nachdem er erstellt wurde
D. Immer nach einem Notfall

Lösung: B. Bei der Erstellung, danach jährlich und nach jedem signifikanten Change: Hier spricht der gesunde Menschenverstand schon dafür, dass der Plan erst einmal nach der Erstellung geprüft und für den Ernstfall getestet wird. Dies gilt auch für jegliche Neuerungen, die den Plan wieder auf einen neuen Status setzen.

Wartbarkeit (Maintainability) ist definiert als:

A. Die vertraglichen Bedingungen, nach denen die Infrastrukturkomponenten gewartet werden
B. Die Fähigkeit eines CI, einen funktionstüchtigen Zustand beizubehalten oder wieder in diesen versetzt zu werden
C. Ein übergeordneter Begriff, der Serviceability, Resilience und Reliability umfasst
D. Die Fähigkeit von CIs, einen Service aufrechtzuerhalten, wenn ein oder mehrere CIs ausfallen

Lösung: B. Die Fähigkeit eines CI, einen funktionstüchtigen Zustand beizubehalten oder wieder in diesen versetzt zu werden wird als Wartbarkeit definiert. Oder anders ausgedrückt: Dies ist die Fertigkeit, Services und Komponenten wieder in den Zustand des normalen Betriebes zu versetzen (siehe Abbildung 20.8).

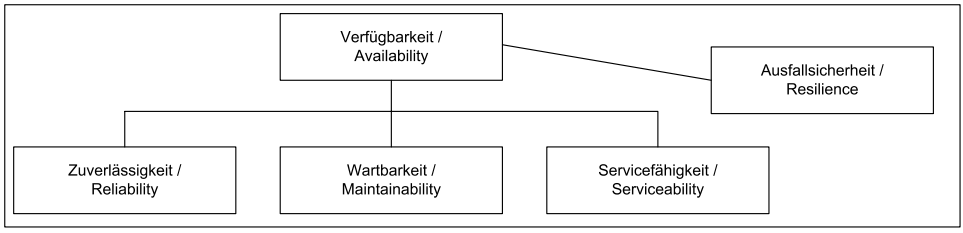


Abbildung 20.8: Einflussgrößen der Verfügbarkeit

Welche der nachfolgenden Berechnungen stellt die Verfügbarkeit von drei seriellen Configuration Items (CIs) dar?

A. 98/100 * 97,5/100 * 99/100 = 94,59

B. 98 + 97,5 + 99/100 = 94,59

C. 98/100 + 97,5/100 + 99/100 = ?

D. Keine

*Lösung: A. 98/100 * 97,5/100 * 99/100 = 94,59*

Ein Intermediate Recovery lässt sich beschreiben als:

A. Es gibt ein Remote Computer-Center, auf das im Notfall ausgewichen werden kann.

B. Es gibt eine Backup Computer-Installation mit den erforderlichen Ersatzkomponenten, ohne Daten und Applikationen.

C. Es gibt Ersatzkomponenten, die ein sofortiges Recovery ohne Serviceeinbußen ermöglichen.

D. Eine mobile Computereinheit

Lösung: B. Es gibt eine Backup Computer-Installation mit den erforderlichen Ersatzkomponenten, ohne Daten und Applikationen: Die zügige Wiederherstellung (Intermediate Recovery, Warm Standby) bezieht sich auf den Zugang zu einer vergleichbaren operativen Umgebung, in der innerhalb einer kurzen Umschaltzeit (24 bis 72 Stunden) die Services wieder zur Verfügung gestellt werden können. Es gibt hier drei Varianten: intern, extern, mobil.

SLAs sollten mindestens die folgenden Daten beinhalten:

A. Strafklauseln, Batch Turnaround-Zeiten, Online-Antwortzeiten, Verfügbarkeit, Durchsatz

B. Vertragsparteien, Continuity-Vereinbarungen, Dateninput, Servicezeiten

C. Datum der Vereinbarung, Dienstleistungsbeschreibung, Ort des Kunden, Turnaround-Zeiten

D. Dienstleistungsvereinbarungen, Vertragsparteien, Servicezeiten, Verfügbarkeit, Verantwortlichkeiten, Unterschriften

Lösung: D. Dienstleistungsvereinbarungen, Vertragsparteien, Servicezeiten, Verfügbarkeit, Verantwortlichkeiten, Unterschriften: Verträge ohne Unterschriften besitzen wenig Gültigkeit. Technische Details sind nicht unbedingt von Interesse.

Risk Management (CRAMM) ist ein wesentliches Element in zwei ITIL-Prozessen. Welche sind diese?

A. Problem Management und Capacity Management

B. Availability Management und Service Level Management

C. Availability Management und Continuity Management

D. Continuity Management und Capacity Management

Lösung: C. Availability Management und Continuity Management: Risk Management berührt den Begriff „Sicherheit", mit dem diese beiden Bereiche eng verzahnt sind.

Wofür ist der Continuity-Manager verantwortlich?

A. Die Entscheidung. welche Dienstleistungen nach einer Katastrophe noch erbracht werden

B. Die Gewährleistung, dass keine Katastrophen vorkommen können

C. Die Planung und Vorbereitung von Maßnahmen, damit die Dienstleistungen von einer Katastrophe überhaupt nicht beeinträchtigt werden

D. Die Erstellung von Plänen, die gewährleisten, dass nach einem Notfall die vereinbarten Service Levels innerhalb einer definierten Zeit wieder erreicht werden können

Lösung: D. Die Erstellung von Plänen, die gewährleisten, dass nach einem Notfall die vereinbarten Service Levels innerhalb einer definierten Zeit wieder erreicht werden können

Welche der folgenden Aufgaben liegt in der Verantwortung des Availability Management?

1. Planung und Überwachung der Verfügbarkeit der in den SLAs vereinbarten IT Services

2. Aushandlung der Availability Levels in den SLAs

3. Erfassung von Details zu auftretenden Kapazitätsproblemen

4. Auslösen von Changes der Infrastruktur

A. 1 und 2

B. 3 und 4

C. 1 und 4

D. Alle

Lösung: C. 1 und 4

Wie lautet der Fokus des Service Capacity Management?

A. Management der technischen Performance
B. Management der Leistung der IT Services auf Grundlage der SLAs
C. Ermittlung der Business Requirements
D. Ermittlung der Kundenanforderungen bezüglich der Kapazität

Lösung: B. Management der Leistung der IT Services auf Grundlage der SLAs. Das Service Capacity Management hat dafür zu sorgen, dass die Performance der Services gemäß den SLAs umgesetzt wird. Dabei hilft der Abgleich Service Achievement/ Service-Bedarf. Aktivitäten sind dabei: Überwachung, Analyse, Berichterstattung über die Leistungen der Services; Festlegen, was normale Belastungen für die Services sind; Nachfrage angleichen.

Wie lautet die strategische Zielsetzung für das Capacity Management?

A. Sicherstellen, dass die richtige IT-Kapazität bereit steht, um die Kundenanforderungen im aktuellen Beschaffungszyklus zu erfüllen
B. Sicherstellen, dass zu Zeiten des Spitzenbedarfs die richtige IT-Kapazität bereitsteht und dies möglichst niedrige Kosten verursacht
C. Sicherstellen, dass zu jeder Zeit eine kostenmäßig vertretbare IT-Kapazität bereitsteht, die auf die vereinbarten Anforderungen der Kunden abgestimmt ist
D. Sicherstellen, dass die Service Levels in Bezug auf die Kapazität auf alle Fälle eingehalten werden

Lösung: C. Sicherstellen, dass zu jeder Zeit eine kostenmäßig vertretbare IT-Kapazität bereitsteht, die auf die vereinbarten Anforderungen der Kunden abgestimmt Ist

Welche der folgenden Aussagen ist richtig?

A. Kapazitätspläne beantworten spezifische Fragen, z.B. wie die Performance für einen bestimmten Anwender verbessert werden kann.
B. Kapazitätspläne schlagen Lösungen für Performance-Probleme vor.
C. Kapazitätspläne zeigen, wann zukünftige Erweiterungen erforderlich sind, und geben die entsprechenden Kosten an.
D. Alle diese Aussagen sind richtig.

Lösung: C. Kapazitätspläne zeigen, wann zukünftige Erweiterungen erforderlich sind, und geben die entsprechenden Kosten an. Das Capacity Management stellt sicher, dass die vorgehaltenen Rechner- und Speicherkapazitäten den Anforderungen des Kunden entsprechen und kostengünstig zur Verfügung gestellt werden. Informationen über die Kosten werden im Rahmen der Kapazitätsplanung und Verfügbarkeit ermittelt.

Welche der folgenden Optionen ist kein Prozess aus dem Bereich Service Support?

A. Incident Management

B. Release Management

C. Service Desk

D. Configuration Management

Lösung: C. Service Desk: Diese Option wird zwar zum Bereich Service Support gezählt, stellt jedoch keinen Prozess, sondern eine Funktion dar.

Stichwort Qualität: Welche vier Schritte beinhaltet die ständige Verbesserung des Services innerhalb des Qualitätslebenszyklus?

A. Plan, Do, Check, Act

B. Do, Manage, Plan, Update

C. Check, Act, Action, Activity

D. Action, Strategy, Manage, Motivate

Lösung: A. Plan, Do, Check, Act: Diese Schritte sollen zur Erbringung einer guten Leistung wiederholt durchgeführt werden.

Welche der folgenden Optionen ist kein Prozess aus dem Bereich Service Delivery?

A. Service Level Management

B. IT Service Continuity Management

C. Availability Management

D. Service Capacity Management

Lösung: D. Service Capacity Management: Dies ist lediglich ein Unterprozess für das Capacity Management.

Wie lautet der Name des Qualitätsmesswerkzeug-Frameworks, das hauptsächlich in den USA verwendet wird und seinen Ursprung in Firmen wie General Electric oder Motorola hat?

A. Seven Hills

B. Four Fathers

C. Six Sigma

D. 12 Disciplines

Lösung: C. Six Sigma: Im Grunde genommen ist Six Sigma ein Begriff aus der Statistik, der als Synonym für Null-Fehler-Qualität steht. In einem Prozess, der Six Sigma erfüllt, entstehen unter bestimmten Rahmenbedingungen bezogen auf 1 Million Möglichkeiten nur 3,4 fehlerhafte Ergebnisse.

Six Sigma

Als zu Beginn der siebziger Jahre für den japanischen Schiffbau die Grundzüge eines Konzeptes namens „Six Sigma“ entwickelt wurden, ahnte noch niemand, dass heute ein regelrechter Hype um diese Qualitäts-Management-Strategie ausbrechen würde. Bei Motorola in den Achtzigern erstmals unternehmensweit angewendet und patentiert, gewann die Six Sigma-Methode laufend neue Anhänger.

Six Sigma als eine Prozess- und Qualitätsmanagementmethode hat eine Renaissance erfahren. Nach erfolgreicher Einführung in der produzierenden Industrie wird es nun verbreitet im Service- und Dienstleistungsbereich eingesetzt, um auch dort durch schlankere Prozesse mit kürzeren Durchlaufzeiten eine Null-Fehler-Qualität zu erzielen.

Das Ziel von Six Sigma ist ein Umdenken innerhalb des gesamten Unternehmens. Der Kern des Six Sigma-Ansatzes ist die ständige Verbesserung des Total Quality Management und die substanzielle Verbesserung von Geschäftsergebnissen. Es ist eine Messgröße für ein Qualitätsmanagement, das Perfektion als Ziel vor Augen hat. Das Six Sigma-Prinzip strebt Strategien an, die auf quantitativem Messen basieren und versuchen, Prozesse zu optimieren, Abweichungen bzw. Streuungen einzuschränken und Fehler oder Qualitätsprobleme aller Art zu eliminieren. Dazu werden etablierte Techniken der Qualitätssicherung mit einfachen und höheren Methoden der Datenanalyse und systematischem Training der Mitarbeiter aller Ebenen einer Organisation kombiniert. Zur Umsetzung von Six Sigma werden im Unternehmen eine Struktur und ein Team mit definierten Rollen und Verantwortlichkeiten benötigt.

Die folgenden Begriffe stellen Elemente dar, die einen Prozess beschreiben: Ziel, Input, Aktivitäten, Output, Metrik.

A. Ich stimme dieser Aussage zu.

B. Ich stimme dieser Aussage nicht zu.

Lösung: A. Ich stimme dieser Aussage zu: Ein Ziel ist stets essenziell und definiert im Grunde genommen den Zweck eines Prozesses, während die Metrik bestimmt, wie gut der Prozess läuft (siehe Abbildung 20.9).

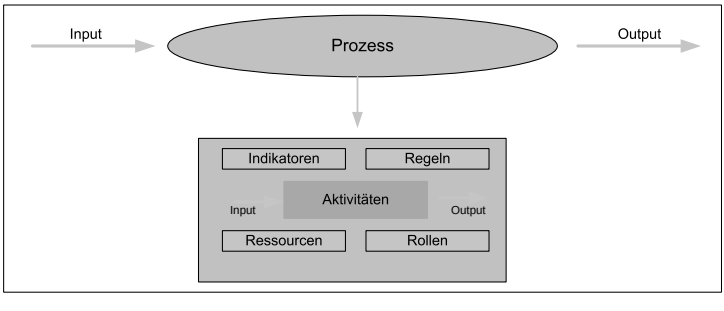


Abbildung 20.9: Allgemeine Prozessdarstellung

ITIL ist nur in folgenden Situationen oder Umgebungen anwendbar:

A. Große, multinationale Organisationen

B. Kleinere Unternehmen, die genug Flexibilität zum Wandel der Servicekultur besitzen

C. Neue Unternehmen, die Ihre IT von Grund auf neu aufbauen müssen

D. Wie jede gute Methodik ist ITIL absolut skalierbar.

Lösung: D. Wie jede gute Methodik ist ITIL absolut skalierbar. Die Praktiken und Prinzipien passen aber als Summe auch auf alle anderen Antworten.

Die ITIL-Prozesse, die über Service Support und Service Delivery definiert werden, besitzen keine Überlappungen oder Schnittstellen zueinander.

A. Ich stimme dieser Aussage zu.

B. Ich stimme dieser Aussage nicht zu.

Lösung: C. Ich stimme dieser Aussage nicht zu: Diese Aussage könnte nicht weiter von der Realität entfernt sein. Gerade diese Schnittstellen sind von großem Vorteil, wobei einige Bereiche eine stärkere Beziehung zueinander aufweisen als andere.

Wie lautet der Name des ersten Zertifizierungslevels der international anerkannten Zertifizierungsreihe für IT Service Management?

A. ITIL Practitioner

B. ITIL-Manager

C. ITIL Foundation

D. ITIL Best Practise Expert

Lösung: C. ITIL Foundation: Dies ist der Startpunkt für die ITIL-Zertifizierungen und gleichzeitig Voraussetzung für die nachfolgenden Zertifizierungsmöglichkeiten.

Der Owner des ITIL Framework ist das Office for Government Commerce (OGC) in England.

A. Ich stimme dieser Aussage zu.

B. Ich stimme dieser Aussage nicht zu.

Lösung: A. Ich stimme dieser Aussage zu: In der Vergangenheit war das CCTA für ITIL verantwortlich. Seit 2001 ist es das OGC.

Es existieren zwei Examenseinrichtungen, die die Examen für das IT Service Management zur Verfügung stellen: EXIN und ISEB.

A. Ich stimme dieser Aussage zu.

B. Ich stimme dieser Aussage nicht zu.

Lösung: A. Ich stimme dieser Aussage zu.

Sie haben Ihren Kollegen einige Aussagen zum Thema ITIL zusammengestellt, um ihnen zumindest einen groben Überblick geben zu können. Welche Definition würden Sie in Bezug auf das Problem Management verwenden?

A. Das Problem Management beschäftigt sich mit der Klassifizierung von Incidents bezüglich konkreter Probleme.

B. Das Problem Management sucht nach Informationen bezüglich der technischen Inhalte der Infrastruktur aus dem Configuration Management.

C. Das Problem Management zielt darauf ab, die Ursprungsursache von Incidents herauszufinden, um dann die entsprechenden Aktionen anzutriggern, die die Situation bereinigen oder zumindest verbessern.

D. Das Problem Management bezeichnet Aktivitäten, die in periodischen, regelmässigen Abständen und nicht jeden Tag durchgeführt werden.

Lösung: C. Das Problem Management zielt darauf ab, die Ursprungsursache von Incidents herauszufinden, um dann die entsprechenden Aktionen anzutriggern, die die Situation bereinigen oder zumindest verbessern: Hier geht es ganz klar um das Thema „Ursachenforschung".

Wie trägt IT Service Management zur Qualität der IT-Dienstleistung bei?

A. Indem Vereinbarungen zwischen internen und externen Kunden und Lieferanten in formalen Dokumenten festgelegt werden

B. Durch allgemein anerkannte Normen der Service Levels

C. Indem dafür gesorgt wird, dass unter allen Angestellten der IT-Organisation eine kundenfreundliche Behandlung gefördert wird

D. Indem Prozesse zur Verwirklichung der Dienstleistung eingerichtet werden, die einfach zu handhaben und aufeinander abgestimmt sind

Lösung: D. Indem Prozesse zur Verwirklichung der Dienstleistung eingerichtet werden, die einfach zu handhaben und aufeinander abgestimmt sind. ITIL ist kein Selbstzweck.

Zu welchem Prozess gehören Performance Management und Resource Management?

A. Availability Management

B. Capacity Management

C. IT Service Continuity Management

D. Service Level Management

Lösung: B. Capacity Management: Die drei Subprozesse des Capacity Management lauten Business Capacity Management, Service Capacity Management und Resource Capacity Management.

Eine Organisation hat den Prozess Incident Management eingerichtet. Dabei wurden mehrere Abteilungen eingerichtet, die sich mit dem Lösen von Zwischenfällen beschäftigen. Es gibt ein Lösungsteam für PC-Störungen, Netzwerk-Störungen, einen Service Desk und eine Gruppe von Spezialisten, die diese Teams unterstützen. In einer IT-Organisation werden die Unterstützungsgruppen in der Regel nach Niveaus gekennzeichnet, beispielsweise 1. Unterstützungsgruppe, 2. Unterstützungsgruppe usw. Wie würden Sie die Unterstützung hier einteilen können?

A. O. Niveau Service Desk, 1. Niveau beide Lösungsteams, 2. Niveau Spezialisten
B. 1. Niveau Service Desk, 2. Niveau PC-Lösungsteams, 3. Niveau Netzwerk-Lösungsteams, 4. Niveau Spezialisten
C. 1. Niveau Service Desk , 2. Niveau beide Lösungsteams, 3. Niveau Spezialisten
D. Alle Abteilungen auf Ebene O

Lösung: C. 1. Niveau Service Desk, 2. Niveau beide Lösungsteams, 3. Niveau Spezialisten: entsprechend First, Second und Third Level-Support

Firma ABC hält es für wichtig, dass jede Anfrage bezüglich eines neuen Arbeitsplatzes möglichst effizient und effektiv bearbeitet wird. Welcher ITIL-Prozess übernimmt diese Funktion?

A. Change Management
B. Customer Liaison (Kundenbetreuung Abnehmer)
C. Problem Management
D. Service Level Management

Lösung: A. Change Management

Die Konfigurationselemente (CIs) und die Configuration Management Database (CMDB) stehen in bestimmten Beziehungen zueinander. Wozu dienen diese Beziehungen?

A. Zur Verwaltung der CMDB
B. Zur Erfassung der CIs
C. Zur Kontrolle in Bezug auf die Richtigkeit der CIs
D. Zur Diagnostizierung von Störungen

Lösung: D. Die Beziehungen helfen bei der Diagnostizierung von Störungen. Die Zusammenhänge und Verknüpfungen zwischen den Verknüpfungen helfen, Störungen aufgrund der gebotenen Informationen leichter zu diagnostizieren.

Welcher Prozess verhindert einen nicht-autorisierten Datenzugriff?

A. Availability Management
B. IT Service Continuity Management

C. Security Management

D. Release Management

Lösung: C. Security Management. IT Security Management beschäftigt sich mit der Einführung und Durchsetzung eines definierten Sicherheitsniveaus für die IT-Umgebung. Dabei wird detailliert auf die Teilgebiete Vertraulichkeit, Integrität und Verfügbarkeit eingegangen.

Welcher Prozess garantiert eine optimale und messbare Verfügbarkeit der IT Services?

A. Availability Management

B. Capacity Management

C. Continuity Management

D. Service Level Management

Lösung: A. Availability Management. Beim Availability Management wird aus den Geschäftsanforderungen ein allgemeines sowie auch ein servicespezifisches Verfügbarkeitsniveau definiert, die Umsetzung geplant und die definierten Qualitätsparameter (Key Performance Indicators) überwacht.

Eine kundenorientierte SLA-Struktur beinhaltet:

A. Ein SLA, das alle Kundengruppen und alle verwendeten Services abdeckt

B. Ein nach Kundengruppen und allen verwendeten Services aufgeschlüsseltes SLA

C. Für jeden Service auf den Kunden konzentrierte und in Geschäftssprache verfasste SLAs

D. Ein SLA für jeden Service-Typ, entsprechend den Kundengruppen, die diesen Service verwenden

Lösung: B. Eine kundenorientierte SLA-Struktur beschreibt eine SLA-Struktur, in dem jede Kundengruppe einen SLA zugeordnet bekommt, der alle Services abdeckt.

Wie lautet die Aktivität, die darauf abzielt, den potenziellen Schaden oder Verlust einer Organisation aufgrund einer erheblichen Unterbrechung der geschäftskritischen Prozesse zu identifizieren?

A. Root Cause Analysis

B. Business Impact Analysis (BIA)

C. Service Outage Analysis (SOA)

D. Component Failure Impact Analysis (CFIA)

Lösung: B. Business Impact Analysis (BIA) ist eine Aktivität, die dem Continuity Management Informationen zu potenziellen Verlusten, die ein Unternehmen wahrscheinlich im Falle eines Desasters erleiden wird, als Basis zur Verfügung stellt.

Wofür steht beim Availability Management die Abkürzung SOA?

A. Serviceability of Applications

B. System Optimization Approach

C. Service Outage Analysis

D. Systematic Operational Adjustment

Lösung: C. Service Outage Analysis. SOA beschäftigt sich als strukturiertes Projekt mit der Verbesserung der Verfügbarkeit.

Welche Punkte der nachstehenden Liste gehören zu den Hauptverantwortlichkeiten des Capacity Management?

1. Modelling

2. Risikoanalyse

3. Application Sizing

4. DSL-Wartung

A. 1 und 2

B. 1 und 3

C. 2 und 4

D. 3 und 4

Lösung: B. 1 und 3. Modelling und Application Sizing werden als die Hauptaktivitäten angesehen. Risikoanalyse gehört nicht primär ins Capacity Management im Sinne der Kapazitätsplanung, sondern eher in den Bereich Continuity Management oder Availability Management. Die Wartung und Pflege der Definitive Software Library (DSL) ist beim Release Management angesiedelt.

Welche der folgenden Aussagen ist in Bezug auf die Detailtiefe und den Umfang (Scope) bei Einführung einer CMDB richtig?

A. Sie sollten keine detaillierten Informationen zu Komponenten sammeln, die nicht unter der Kontrolle des Change Management stehen.

B. Sie sollten sich keine großen Sorgen um das Change Management machen, zuallererst gilt es, die Datenbank zu füllen.

C. Sie sollten versuchen, so viele Informationen wie möglich zu allen Komponententypen zu sammeln.

D. Sie sollten die Wünsche der IT-Mitarbeiter berücksichtigen.

Lösung: A. Das Change Management als Basis zu verwenden, ist ein guter Ansatz für die Initiierung des Configuration Management. Schließlich können Sie auch nur die Komponenten verwalten und supporten, die über das Change Management verändert werden können. Sie sollten keine detaillierten Informationen zu Kompo-

nenten sammeln, die nicht unter der Kontrolle des Change Management stehen. Die Definition des richtigen Scopes für die CMDB ist ein erfolgskritischer Faktor für dieses Unterfangen. Alle Wünsche der IT-Abteilung umzusetzen sollte nur ein frommer Wunsch bleiben. Zu viele Informationen würden die Datenbank überfluten und die Verwaltung erschweren.

Welche Relationen werden über die CMDB zwischen Incidents und Problemen beschrieben?

1. Ein Incident zu einem Problem (1:1)
2. Ein Incident zu vielen Problemen (1:n)
3. Viele Incidents zu einem Problem (n:1)

A. 1 und 3
B. 1 und 2
C. 2 und 3
D. Alle

Lösung: A. 1 und 3. In den meisten Fällen lässt sich ein Incident anhand der spezifischen Informationen genau einem Problem zuordnen oder es treten mehrere Incidents zu einem Problem auf, z.B. wenn das Problem so große Auswirkungen hat, dass es viele Anwender trifft, die alle einen Incident melden.

Es gibt enge Verbindungen zwischen dem Service Level Management und …

1. Incident Management
2. Availability Management
3. Configuration Management
4. IT Service Continuity Management
5. Change Management

A. Alle
B. 2 und 4
C. 1, 3 und 5
D. 2, 3 und 5

Lösung: A. Alle. Das Service Level Management sitzt im Herzen der ITIL-Pyramide und bildet die Basis für die Anforderungen an die IT Services. Das Service Level Management benötigt den Output von jedem der genannten Prozesse, um eine hohe Kundenzufriedenheit zu erzielen.

Um ein neues Service Desk Management-Tool zu implementieren, muss die Kapazität des Service Desk-Servers erweitert werden. Wer ist verantwortlich für das Management des Requests hinsichtlich der zusätzlichen Kapazität?

A. Capacity-Manager

B. Financial-Manager

C. Service Level-Manager

D. Change-Manager

Lösung: D. Change-Manager, da dies eine Veränderung (Change) der produktiven Umgebung betrifft. Das Capacity Management mag auch davon betroffen sein, aber der Change wird nicht hierüber abgewickelt.

In Bezug auf die Verbindung zwischen Incident Management und Problem Management: Ein Problem kann ohne einen korrespondierenden Incident bestehen. Ist die Aussage korrekt?

A. Ja

B. Nein

C. Weiß ich nicht

D. Keine Angabe

Lösung: A. Ja. Ein Problem kann ohne korrespondierenden Incident existieren. Während des proaktiven Problem Management können Probleme entdeckt werden, für die es keinen Incident gibt.

Welche der folgenden Daten können keinen Input für das Change Management darstellen?

A. RFCs

B. CMDB-Informationen

C. Incident-Informationen

D. Forward Schedule of Changes (FSC)

Lösung: A. Incident-Informationen. Alle anderen Informationen dienen dem Change Management als Input.

Zur Beschreibung eines ITIL-Prozesses sind bestimmte Angaben erforderlich. Hierzu gehören die Ziele und Ergebnisse (Outputs). Was gehört noch dazu?

A. Aktivitäten

B. Genehmigungen

C. Ressourcen

D. Personal

Lösung: A. Aktivitäten. Ein Prozess stellt eine sich wiederholende Abfolge von Aktivitäten dar.

Wovon hängt die Priorität eines Zwischenfalls ab?

A. Von den Auswirkungen und der Dringlichkeit eines Zwischenfalls
B. Von den Auswirkungen und der Dringlichkeit eines Problems
C. Von dem zu erwartenden Aufwand und den Auswirkungen des Zwischenfalls
D. Von dem zu erwartenden Aufwand und den Kosten des Zwischenfalls

Lösung: A. Von den Auswirkungen und der Dringlichkeit eines Zwischenfalls. Dies sind die beiden Größen, die die Prioritätseinstufung beeinflussen (siehe Abbildung 20.10).

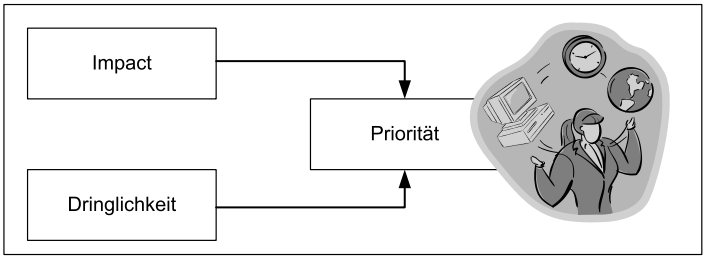


Abbildung 20.10: Größen im Zusammenhang mit der Priorität

Mean Time Between Failures (MTBF) bezeichnet:

A. Mittlere Zeit zwischen dem Auftreten von Störungen
B. Mittlere Service-„Ausfallzeit“
C. Produktive Zeit ohne Störungen oder Beeinträchtigungen
D. Keines davon

Lösung: C. Produktive Zeit ohne Störungen oder Beeinträchtigungen: Die Zeit zwischen der Wiederherstellung eines Services und dem Auftreten des nächsten Fehlers

ITIL definiert drei unterschiedliche Release-Typen. Diese beinhalten:

A. Complete, Medium, Small
B. Package, Medium, Full
C. Medium, Package, Complete
D. Delta, Full, Package

Lösung: D. Delta, Full, Package: Full bezeichnet alle Komponenten eines Releases, die zusammengestellt, getestet, verteilt und zusammen implementiert werden. Delta steht für die CIs, die durch das Release verändert werden. Package bezeichnet die individuellen Releases, entweder Full oder Delta, die zu einem Package zusammengefügt werden.

Welches sind Beispiele für einen IT Service?

1. LAN
2. Mail
3. Verrechnungssystem
4. Oracle-Datenbank

A. Keines

B. Alle

C. 1 und 3

D. 2 und 3

Lösung: D. 2 und 3: ITIL definiert einen IT Service als die Bereitstellung in Beziehung stehender Komponenten zur Unterstützung von Geschäftsprozessen. Ein Verrechnungssystem wird über eine Kombination unterschiedlicher Komponenten bereitgestellt.

Ihre Kollegin ist Service Desk-Managerin in einer relativ großen Organisation. Sie sollen sie bei der Dokumentation der Ziele für das Incident Management unterstützen. Wählen Sie die passende Aussage:

A. Den vereinbarten Service so schnell wie möglich wiederherzustellen

B. Minimierung nachteiliger Auswirkungen von Incidents und Problemen auf den Geschäftsbereich

C. Sicherstellung, dass standardisierte Methoden und Prozeduren für die effiziente und prompte Incidentbehandlung verwendet werden

D. Negative Auswirkungen von Fehlern in der IT auf das Geschäft zu minimieren und das Wiederauftreten von Incidents zu vermeiden

Lösung: A. Den vereinbarten Service so schnell wie möglich wiederherzustellen ist das primäre Ziel des Incident Management. Dies minimiert automatisch negative Auswirkungen auf den Geschäftsbetrieb. Zwischen Incident Management und Problem Management herrscht eine Art Konflikt, da der eine Prozess versucht, den Service so schnell wie möglich wiederherzustellen (Incident Management), während der andere Prozess eine andauernde Fehlerkorrektur durchführen möchte, unabhängig von den unmittelbaren Auswirkungen (Problem Management, siehe Option D).

A Glossar

A

Asset

Komponente eines Businessprozesses

Availability (Verfügbarkeit)

Übergeordneter Begriff für die Qualitätsmerkmale Zuverlässigkeit, Wartbarkeit, Servicefähigkeit und Sicherheit.Availability Management stellt einen Prozess dar, der die optimierte Nutzung von IT-Ressourcen, die Implementierung von Sicherheitsrichtlinien sowie die Überwachung der Servicevereinbarung ermöglicht.

B

Balanced Scorecard (BSC)

Konzept zur Umsetzung Ihrer Unternehmensstrategie. Eine BSC (ausgewogenes Kennzahlensystem) beginnt bei der Vision und Strategie des Unternehmens und definiert auf dieser Basis kritische Erfolgsfaktoren (KEF).

Build Management

Gehört zum Release Management. Die SW- oder HW-Komponenten, die zu einem neuen Release gehören, sollten auf klar festgelegte Weise zusammengesetzt bzw. in einer bestimmten Reihenfolge installiert werden, die damit reproduzierbar wird. Dieser Prozess wird oft automatisiert, ist damit zuverlässiger und führt immer zu einem einheitlichen Ergebnis. Sobald das neue Release in die kontrollierte Testumgebung gelangt, unterliegt das Build Management der Verantwortung des Release Management.

Business Capacity Management (BCM)

Subprozess des Capacity Management

C

CAB/EC

CAB Emergency Committee, für dringende Changes, Prozess Change Management

CAB

Change Advisory Board, Prozess Change Management

Capacity Management Database (CDB)

- Output und Eckpfeiler des Prozesses Capacity Management
- Enthält verschiedene Arten von Daten: Business, Service, Technik, Finanzen, Nutzung
- Evtl. zusammen mit CMDB

Capacity Plan (Kapazitätsplan)

Prozess Capacity Management. Zeigt den zukünftigen Kapazitätsbedarf und die dadurch wahrscheinlich entstehenden Kosten auf. Beinhaltet Infos über HW-Bedarf, Leistungsanforderungen an Systeme, Kostenvorgaben

CCTA

Central Computers and Telecommunications Agency (veralteter Begriff) – die Institution, die für die Erstellung und Aktualisierung von ITIL zuständig ist (jetzt OGC)

CDB

Capacity Management Database

CFIA

Component Failure Impact Analysis

Change

Das Hinzufügen, Ändern oder Herausnehmen von genehmigter, unterstützender oder grundlegender Hardware, Software, Anwendungen, Dokumentationen u.a.

Change Advisory Board (CAB)

Gehört zum Change Management. Beratende Funktion bei Bewertung und Autorisierung von Changes. Personen, die Change bzgl. Auswirkungen, Kosten, Ressourcen, Dringlichkeit usw. bewerten. Es sollten i.A. vertreten sein: Change-Manager (Vorsitz), Service Level-Manager, Application-Manager, Vertreter der Geschäftsbereiche, Problem-Manager, Release-Manager, Finanzabteilungsmanager, weitere Personen je nach Fachabteilung

Change Model

Prozess Change Management. Modellierung eines größeren Changes vor seiner Implementierung, unter Zusammenarbeit mit Capacity Management u.a. Beteiligten, um alle eventuellen Schwierigkeiten vor der Planung und Durchführung zu erkennen und zu beseitigen. Erleichtert auch Impactbestimmung. Für kleinere Changes gibt es Standard-Modelle.

Change-Kategorie

Prozess Change Management. Beschreibt die Auswirkungen, die ein beantragter Change voraussichtlich auf die IT-Organisation selbst hat, d.h. Bedarf an Ressourcen (Zeit, Geld, Mitarbeiter):

- Standardchange: Routine-Change, vorgegebener Ablauf, Genehmigung besteht grundsätzlich
- Geringer Impact: geringe Auswirkung, wenig Ressourcen erforderlich; Change-Manager kann Change autorisieren (oder delegieren an Service Desk)
- Signifikanter Impact: Deutliche Auswirkung; viele Ressourcen; RFC muss von CAB oder CAB/EC geplant und autorisiert werden
- Erheblicher Impact: Bedeutende Auswirkungen, erheblicher Ressourcenbedarf. RFC muss der Geschäftsführung zur Genehmigung vorgelegt werden, dann an CAB zur weiteren Planung.

Charging

Leistungsverrechnung, Subprozess des Financial Management for IT Services

CI (Configuration Item)

Komponente der IT-Infrastruktur, die für die Lieferung der Services benötigt wird. Sie ist eindeutig identifizierbar, kann sich ändern (Changes), muss verwaltet werden (Status). CIs haben eine Kategorie, Relationen, Attribute und einen Status.

CI-Kategorie

CIs fallen unter bestimmte Kategorien wie z.B. Hardware, Software, Netzwerk, Umgebung, Dokumentation, Services, Daten (von ITIL empfohlen). Auch Mitarbeiter können CIs sein.

CI-Varianten

CIs mit identischer Basisfunktion, jedoch geringen Unterschieden (z.B. der gleiche Drucker mit Zusatzspeicher). CI-Varianten haben den gleichen Namen, aber verschiedene Versionsnummern.

CMDB

Configuration Management Database, enthält alle relevanten Daten über die verwalteten CIs und alle Relationen/Beziehungen zwischen den dokumentierten CIs. Beim Entwurf der CMDB muss man den Umfang/Scope (welche CI-Kategorien) und den Detaillierungsgrad (CI-Level) festlegen, bis zu dem man die CIs verwalten will.

Component Failure Impact Analysis (CFIA)

Risikoanalyse: Welche Komponente kann welche Störung in welchem Umfang verursachen? Wichtig für Availability Management, kann aber auch vom Capacity Management und/oder Availability Management durchgeführt werden.

Configuration Baseline

Konfiguration eines bestehenden Produktes/Services zu einem bestimmten Zeitpunkt, der, falls nötig, später wiederhergestellt werden kann

Configuration Item

Siehe CI

Cost (Kosten)

Aufwand, verursacht durch eine bestimmte Maßnahme oder einen bestimmten Bereich

Costing (Kostenrechnung)

Prozess zur Identifizierung der Kosten und zur entsprechenden Zuordnung zu bestimmten Geschäftsbereichen oder Aktivitäten

Cost Unit

Kleinste verrechenbare Einheit pro Ressource; gehört zu Financial Management

CPD

Change Planning Document (Change Management)

CRAMM

Methode in den Prozessen Availability und Continuity Management; CRAMM steht für computer risk analysis and management method. Es wurde als wissenbasiertes Risiko-Management vorgestellt, das dem britischen Sicherheitsstandard BS 7799 entspricht und nach ISO 17799 zertifiziert ist. Mit dem Ergebnis der Analyse in Form eines Reports kann das Management Schwachstellen und Risiken in den IT-gestützten Geschäftsprozessen, der IT und Technik und anderen Bereichen wie Facilities und Personal erfassen, bewerten und beseitigen.

D

Definitive Hardware Store (DHS)

Prozess Release Management. Analog zur DSL sollte es einen Bereich für die sichere Speicherung/Lagerung von definitiver Ersatz-Hardware geben. Diese sollte auf demselben Level gewartet werden wie die HW der Produktivumgebung. Details zu dieser HW sollten in der CMDB dokumentiert sein, damit die Ersatz-HW im Falle einer Störung zur Lösung genutzt werden kann.

Definitive Software Library (DSL)

Prozess Release Management. Speicher, in dem autorisierte SW (auch Zwischenversionen) sicher aufbewahrt wird und aus dem heraus die SW verteilt wird. Unterliegt der Qualitätsprüfung (Viren, Lizenzen, Tests, Vollständigkeit), ist Basis für Release-Erstellung. Physisch kann es sich um verschiedene elektronische Medien in verschiedenen Formaten, Dateien, Dokumentationen handeln. Die DSL enthält die Master-Kopien der gesamten kontrollierten SW eines Unternehmens: Hierzu gehören sowohl gekaufte SW als auch selbst entwickelte SW, sowie Master-Kopien von Systemdokumentationen in elektronischer Form. Die genaue Konfiguration der DSL sollte vor Beginn der Implementierung definiert werden (und in Release-Grundsätzen dokumentiert). DSL sollte von den Libraries der Test- und Entwicklungsumgebung getrennt werden.

Delta-Release

Dabei werden nur die seit der letzten Version geänderten CIs ersetzt .

DHS

Definitive Hardware Store

Direkte Kosten

Prozess Financial Management. Entstehen durch Nutzung eines bestimmten Services, direkt einem Kunden und/oder Service zuweisbar.

Dringlichkeit

Incident Management: Auswirkung des Incidents auf geschäftliche Termine: Wie schnell muss Lösung erfolgen (z.B. sind geschäftliche Termine gefährdet?). Basis für Dringlichkeitsstufen: vordefinierte Checklisten

DSL

Definitive Software Library

E

Effektiv

Effekt (Wirkung, Erfolg): tatsächlich, wirklich bzw. wirkungsvoll (im Verhältnis zu den eingesetzten Mitteln), lohnend

Effizient

„Besonders wirtschaftlich“, „leistungsfähig“

Error Control

Zweiter Subprozess im Problem Management. Erkennung, Aufzeichnung, Klassifizierung und Bearbeitung von bekannten Fehlern

Eskalation

ITIL unterscheidet funktionale Eskalation im Sinne von Weiterleitung eines Incidents/Problems bis hin zur Lösung und hierarchische Eskalation, d.h. Einbeziehung einer höheren Entscheidungsinstanz bei auftretenden Fragen bzgl. eines Incidents (d.h. Abweichung vom üblichen Prozessverlauf), z.B. wenn absehbar ist, dass eine Lösung nicht zeitgerecht gefunden werden kann oder die Störung einen besonders großen Impact hat. Der Incident wird durch hierarchische Eskalation noch nicht zum Problem!

F

Fixkosten

Nutzungsunabhängige Kosten, Bsp.: Miete, Gehälter, Versicherung, SW-Lizenzen, HW-Wartungsverträge, Festpreis-Aufträge, usw. (Prozess Financial Management)

Forward Schedule of Changes

Change-Plan: Plan mit Informationen und Daten zu allen geplanten Changes. Gehört zum Change Management. Die entsprechenden Auswirkungen auf Services und Verfügbarkeit stehen im Projected Service Avalability-Dokument (PSA).

FSC

Forward Schedule of Changes

Full-Release

Dabei werden alle Komponenten einer Release-Einheit ersetzt, unabhängig davon, ob sie sich geändert haben oder nicht (Release Management).

G

Gradual Recovery

Allmähliche Wiederherstellung (mind. 72 Stunden) nach einem Notfall; Prozess ITSCM (Continuity Management)

I

ICTIM

ICT Infrastructure Management; es beschreibt vier Managementbereiche:

- Design and Planning
- Deployment
- Operations
- Technical Support

Immediate Recovery

Sofortige Wiederherstellung binnen weniger Stunden nach einem Notfall; Prozess ITSCM (Continuity Management)

Impact

Grad der Beeinträchtigung der Geschäftsaktivitäten des Kunden und Grad der Gefährdung der Service Level und die damit zusammenhängenden Auswirkungen auf das Kundengeschäft, oft gemessen anhand der Zahl der betroffenen Anwender oder Systeme; Bestimmung des Impacts im Incident Management/Service Desk und Problem Management

Incident

Jedes Ereignis, das nicht zum normalen (gemäß SLA) Servicebetrieb gehört und das eine Serviceunterbrechung oder -verschlechterung verursacht oder verursachen kann. Dies umfasst technische Störungen, automatische Systemwarnungen, Anfragen, Service Requests, RFCs .

Incident-Kategorie

Beschreibt den Störungsbereich (z.B. Hardware-Fehler, Software-Fehler, Service Request, usw.). Muss noch nicht das betroffene CI benennen (Prozess Incident Management/Service Desk).

Incident-Klassifizierung

Incident kategorisieren, Incident Matching, Incident priorisieren; Prozess Incident Management (Service Desk).

Incident-Lebenszyklus

Der Status eines Incident spiegelt seine aktuelle Position im Lebenszyklus wieder (*neu, angenommen, scheduled, assigned, in Bearbeitung, wartend, beschlossen, geschlossen*).

Incident-Matching

Durchsuchen der Datenbank(en), ob ähnliche Incidents dort schon dokumentiert sind und ob es dazu passende Known Errors oder Probleme gibt. Ziel: Finden einer schnellen Lösung; Prozess Incident Management (Service Desk)

Indirekte Kosten

Können keinem bestimmten Service oder Kunden zugerechnet werden (Bsp. Sekretärin, Strom, Wasser) (Prozess Financial Management).

Integrität (Integrity)

Begriff für die Richtigkeit, die Vollständigkeit und den korrekten Zeitpunkt der Informationsübermittlung. Dies ist ein Grund, warum Verschlüsselungs- und Signierungsmechanismen zum Einsatz kommen.

Intermediate Recovery

Zügige Wiederherstellung (24 bis 72 Stunden) nach einem Notfall; Prozess ITSCM (Continuity Management)

ITSC-Plan

Notfallplan, Prozess ITSCM (Continuity Management)

IT Service/-Dienstleistung

Die von den IT-Systemen zur Verfügung gestellte Palette von Funktionen, um einen oder mehrere Geschäftsbereiche/-Prozesse zu unterstützen. Ein IT Service geht vom einfachen Zugriff auf ein Programm bis hin zur Bereitstellung einer gesamten Umgebung inkl. Funktionen, Applikationen, Produkte. Dies auch plattformübergreifend und über verschiedene Kommunikationstechnologien. Auch der Support der eigentlichen Funktionalität gehört dazu.

Kurz: Die Summe aller technischen und nicht-technischen Interaktionen zwischen Kunden- und Dienstleisterseite

IT Service Management

Beschreibt den Wandel der Informationstechnik in Richtung Kunden- und Serviceorientierung. Von Bedeutung sind die Gewährleistung und Überwachung von IT Services. Auf diese Weise können kontinuierlich die Effizienz, die Qualität und die Wirtschaftlichkeit der jeweiligen IT-Organisation verbessert werden.

itSMF

Das IT Service Management-Forum stellt die weltweit einzige unabhängige und international anerkannte Organisation für IT Service Management. Das itSMF hat es sich zum Ziel gesetzt, als unabhängiger und nicht kommerzieller Verein die aktuellen Erkenntnisse und Methoden im Bereich des IT-Managements zu fördern und bekannt zu machen.

K

Known Error

Bekannter Fehler. Problemursache und zumindest der Workaround sind bekannt. Endgültige Lösung kann durch einen Change umgesetzt werden.

KPI

Key Performance Indicator: Um die Prozessqualität beurteilen zu können, sind klar definierte Parameter und messbare Ziele nötig, sog. Leistungsindikatoren.

Kunde

Der Auftraggeber, der mit dem Service-Provider über den Service verhandelt und dafür bezahlt, i.A. die Unternehmensführung oder ein Abteilungsleiter

M

Maintainability

Siehe Wartbarkeit

MTBF

Mean Time between Failures: mittlere Dauer der (Service-) Verfügbarkeit (Availability).

MTBSI

Mean Time between System Incidents: Mittlere Zeit zwischen dem (erneuten) Auftreten von Störungen, Maß für die Zuverlässigkeit (Reliability)

MTTR

Mean Time To Repair: mittlere Service-Ausfallzeit bzw. zur Wiederherstellung benötigte Zeit; Maß für die Wartbarkeit einer Komponente

O

OLA

Operational Level Agreement

Operational Level Agreement (OLA)

Service-Vertrag mit internem Lieferanten/Dienstleister. Verträge mit externen (UC) und internen (OLAs) Lieferanten sollen die Einhaltung und Erfüllung der SLAs sicherstellen. Bei Anpassungsbedarf sollten wenn möglich OLA oder UC an das SLA angepasst werden, nicht umgekehrt (Kundensicht).

P

Package-Release

Hier werden zusammengehörige SW-Cls gemeinsam in die Testumgebung und dann in die Produktivumgebung eingeführt (z.B. Desktop-Umgebung, die aus eMail, Emulator, Office-Suite und BS besteht) .

PIR

Post Implementation Review

Post Implementation Review

Ordnungsgemäße und vollständige Behebung eines Fehlers durch einen durchgeführten Change überprüfen und Kontrolle, ob Folge-lncidents aufgetreten sind, ob Ziele des Changes erreicht, ob der Kunde damit zufrieden ist

Pricing

Preisfestlegung, Aufgabe des Charging (Subprozess des Financial Management for IT Services).

Priorität

Vorrangigkeit, mit der ein Incident Problem/RfC zu behandeln ist; wird vergeben auf Basis von Impact und Dringlichkeit. Die erste Priorisierung erfolgt am Service Desk, gemeinsam mit Anwender. Basis ist hier eine vordefinierte Checkliste. Durch die Priorisierung kann man leichter eine Bearbeitungsreihenfolge festlegen und Ressourcen zuweisen.

Priorität	Wann zu beheben? Was passiert bei Nicht-Behebung? Gefahren?
Dringend	sofort, unmittelbar; sonst Gefahr erheblicher Auswirkungen auf das Geschäft; führt zu bestimmtem Verfahren für schnelle Bearbeitung, typischerweise umgehende CAB-Sitzung
Hoch	schnell, heute noch; potenzieller Schaden
Mittel	baldmöglichst, innerhalb einer Woche; Change behebt lästige Fehler oder fehlende Funktionalität (kann geplant werden)
Tief	wenn nichts anderes vorliegt, zum nächsten Wartungstermin; Change bringt geringfügige Verbesserung, für die keine vertragliche Notwendigkeit besteht

Proaktives Problem Management

Subprozess im Problem Management. Langfristige Reduzierung von Incidents durch frühzeitige Fehlererkennung und -behebung.

Problem Control

Erster Subprozess im Problem Management. Umwandlung eines Problems in einen Known Error

Problem

Die unbekannte Ursache eines oder mehrerer Incidents (die bei Abschluss des Incidents nicht in jedem Fall behoben ist). Ein Incident wird i.A. dann zum Problem erklärt (laut ITIL), wenn er häufig auftritt, einen großen Impact hat, wenn auch das Incident Management keinen Workaround dafür finden konnte oder wenn der Incident erstmalig auftritt. Generell trifft der Incident-Manager die Entscheidung, wann ein Incident zum Problem wird.

Untersucht wird die Ursache i.A. nur dann, wenn ein Incident sich häuft oder einen großen Impact hat und man (deshalb) die Ursache des Incidents wissen und beheben will.

Prozess

Ein Prozess ist nach ISO 8402 durch folgende Eigenschaften charakterisiert:

- Er besteht aus einer Menge von Mitteln und Tätigkeiten. Zu den Mitteln können Personal, Geldmittel, Anlagen, Einrichtungen, Techniken und Methoden gehören. Diese Mittel und Tätigkeiten stehen in Wechselbeziehungen.
- Ein Prozess erfordert Eingaben.
- Ein Prozess gibt Ergebnisse aus.

PSA

Projected Service Availability

Q

Qualität

Qualität wird laut ISO 402 als Gesamtheit der Eigenschaften und Kennzeichen eines Produkts bzw. eines Service verstanden, die zur Erfüllung der festgelegten oder selbstverständlichen Bedürfnisse wichtig sind.

Qualitätskreis von Deming

Dieses stellt die Qualität in den Vordergrund und beschreibt eine kontinuierliche Qualitätsverbesserung durch einen Zyklus, der als „Plan-Do-Check-Act“ (PDCA-Modell) bezeichnet wird.

R

RCM

Resource Capacity Management

Relationen (Beziehungen zwischen CIs)

CIs haben untereinander Beziehungen wie A ist Teil von B. ITIL schreibt die Art der Beziehungen nicht vor, sie werden im Prozess-Design definiert. Dabei geht es um Fragen wie etwa

- Welche CIs sind für die Erbringung des Services erforderlich?
- Welcher Service hängt von welchen CIs ab?

CI-bezogene Records aus anderen Prozessen sind auch selbst CIs: Change Record, Known Error Record, Problem Record, Incident Record. Auch SLAs sind CIs und weisen Relationen zu anderen CIs auf. Die Beziehungen sind außerdem wichtig bei der Störungsdiagnose.

Release

Eine Sammlung von neuen und/oder geänderten CIs, die getestet und zusammen in die Produktivumgebung eingeführt werden. Jeder Release ist ein Change, aber nicht jeder Change ist ein Release.

Release-Art bzw. -Typ

Umfang des Releases im Bezug auf das, was sich seit dem letzten Release geändert hat:

- Delta Release: Release enthält nur die CIs, die seit dem letzten Release geändert wurden (Bsp. Service Pack).
- Full Release: Alle Komponenten werden zusammen entwickelt, getestet, verteilt und implementiert (z.B. das ganze Word-Programm).
- Package Release: Einzelne, voneinander unabhängige Releases, sowohl Full Releases als auch Delta Releases, werden zu einem Paket für die Freigabe geschnürt, z.B. wenn der ganze Arbeitsplatz inklusive Betriebssystem und Applikationen neu aufgesetzt wird.

Release-Einheit (Unit)

Der Umfang, in dem ein Release normalerweise freigegeben wird, z.B. als Suite (z.B. MS Office), Applikation (z.B. MS Word), Modul (z.B. Word-Rechtschreibprüfung)

Release-Nummerierung

Stellt sicher, dass jedes Release durch eine eindeutige Nummer identifizierbar ist

Release-Richtlinien

Enthalten Angaben zu Release-Einheiten, Release-Nummerierung, Release-Häufigkeit, Notfallrelease, Voll-, Package-, Delta Release, dringenden Changes

Reliability (Zuverlässigkeit)

Fähigkeit einer Komponente, die benötigte Funktionalität für eine definierte Dauer und unter definierten Umständen zu liefern

Resilience (Fehlertoleranz)

Strapazierfähigkeit von Komponenten. Fähigkeit einer Komponente oder eines Services, betriebsfähig zu bleiben, wenn eine oder mehrere andere Komponenten ausgefallen sind

Resource Capacity Management

Subprozess des Capacity Managements

RfC

Request for Change. Antrag auf Änderung (Change) an einer oder mehreren CIs

Risk Analysis (Risikoanalyse)

Analyse von Schwachstellen und Risiken, unter Berücksichtigung der Bedrohungen für die Vermögenswerte.

Risk Management

Auswahl und Anwendung von Gegenmaßnahmen zur Minimierung der Risiken im IT Service Management

S

Safety (Sicherheit)

Sicherheit vor bekannten Risiken und die größtmögliche Vorbeugung vor unbekannten Risiken

Schwachstellen

Schwachstellen der Vermögenswerte in ihrer spezifischen Umgebung. So hat z.B. ein PC mit Diskettenlaufwerk und ohne Antiviren-SW eine Schwachstelle bzgl. Viren (Security).

Security:

Security Management ist zwar ein eigener Prozess, wird aber soweit wie möglich in andere ITIL-Prozesse integriert, indem bestimmte Security-Aspekte von diesen übernommen werden. Dies wird beispielsweise durch die Implementierung von Schutzmaßnahmen im Rahmen des Availability Management zur Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit von Daten und somit zur Gewährleistung kontinuierlicher Services realisiert.

Service Achievement

Aktueller erreichter und an den Kunden gelieferter Service Level

Service Capacity Management

Subprozess des Capacity Management

Service Desk

Eine zum Incident Management gehörende Funktion.

Service Improvement Program (SIP)

Internes Projekt zur Identifizierung und Einführung messbarer Verbesserungen innerhalb eines Arbeitsbereiches/Prozesses

SCM

Service Capacity Management

Servicekatalog

Beschreibt die gesamte Palette der Services sowie die verschiedenen Service Level, die die IT liefern kann (Service-Beschreibung, Funktionalitäten, Wartungszeiten usw.), die Service-Charakteristiken, die Service-Erbringer. Enthält auch eine Übersicht über die Kunden pro Service, ggfs. Einzelheiten.

Service Level Agreement (SLA)

Vertrag zwischen IT-Organisation und Kunden, der einen zu erbringenden Service und dessen Service Level genau definiert. SLA muss bestehende Verträge berücksichtigen. Mindestangaben in SLA:

- Einfache Servicebeschreibung und Leistungsmerkmale
- Service-Zeiten und -Verfügbarkeit
- Reaktionszeiten gegenüber den Usern, Reaktionszeiten bei RfCs, Reaktions- und Behebungszeiten bei Störungen
- Zielvorgaben für Verfügbarkeitmaßgaben und Security
- Pflichten auf beiden Seiten
- Kritische Geschäftszeiten und Ausnahmen (Feiertage, Eskalation usw.), Unterschriften

Die Messkriterien sollten aussagekräftig sein. Es muss klar sein, ob die Messkriterien den Mindestwert, den Worst Case, die erwarteten Werte oder die Zielwerte für die Service Level beschreiben. Es kann sinnvoll sein, die nicht beinhalteten Dienstleistungen aufzuführen, z.B. muss der Kunde wissen, welche Gefahren drohen, falls keine Sicherheitsmaßnahmen getroffen werden.

Service Level Requirement (SLR)

Vom Kunden definierte Anforderung an einen Service. Basis für die Erstellung der SLAs

Service Quality Plan (SQP)

Dokumentierter Plan und Spezifizierung interner Ziele zur Gewährleistung der vereinbarten Service Level. Interne Service-Beschreibung, ausgerichtet auf die IT-Mitarbeiter, enthält Plan mit Servicekatalog, Verträgen und IT-Planung sowie verschiedene Datenblätter

Service Request

Jeder Incident, der nicht auf einem Fehler in der IT-Infrastruktur beruht (Auskünfte, Anfragen, Support für bestimmte Applikationen, Beschwerden u.a.)

Serviceability (Unterstützende Vertragsvereinbarungen)

Dieser Begriff definiert die von externen Lieferanten bereitzustellenden Leistungen, um die mit dem Kunden getroffenen Vereinbarungen bzgl. Verfügbarkeit zu untermauern. Servicefähigkeit basiert also auf Drittverträgen mit externen Service-Providern

Single Point of Failure

IT-Komponente ohne Backup-/Cluster-Fähigkeit, die Impact verursachen kann und die unbedingt identifiziert werden muss, z.B. mittels CFIA

SIP

Service Improvement Program

SLA

Service Level Agreement

SLM

Service Level Management

SLR

Service Level Requirement

SPOC

Single Point of Contact. Das Service Desk wird in der Regel als SPoC bezeichnet, da dies die primäre Kontaktstelle für Kunden und Anwender darstellt.

SQP

Service Quality Plan

Stand-by-Option

Wiederherstellungsalternative für den Notfall

Status

CIs haben Status wie z.B.: (CI ist) in Entwicklung, in Testphase, produktiv, in Reparatur, bestellt, auf Lager, im Archiv, usw.

Schutz (Security)

Mittel, das zum Zweck der Sicherheit eingesetzt wird

U

Underpinning Contract (UC)

Service-Vertrag mit externem Lieferanten/Dienstleister (d.h. IT ist hier selbst der Kunde)

Verträge mit externen (UC) und internen (OLAs) Lieferanten sollen die Erfüllung der SLAs sicherstellen. Bei Anpassungsbedarf sollten wenn möglich OLA oder UC an SLA angepasst werden, nicht umgekehrt (Kundensicht).

V

Variable Kosten

Nutzungsabhängige Kosten, z.B. Überstunden, Verbrauchsmaterial, Telekommunikation, Spesen, usw.

Verfügbarkeit

Zu einem bestimmten Zeitpunkt oder während einer bestimmten Zeitdauer zu erfüllen. Wird i.A. als Verhältniszahl bzw. Grad (in Prozent) bezogen auf die vereinbarten Service-Zeiten ausgedrückt. Sowohl die Gesamtdauer eines Ausfalls als auch die Häufigkeit von Ausfällen beeinträchtigen die Servicequalität.

Vulnerability

Begriff aus ITSCM, bezeichnet Empfindlichkeit bzw. Schwachstellen der IT-Systeme/- Services gegenüber Risiken/Bedrohungen. Kann durch Risikoanalyse (CRAMM) ermittelt werden.

W

Wartbarkeit (Maintainability)

Fähigkeit einer Komponente oder eines Services, in einen funktionierenden Zustand zurückzukehren. Gemessen durch MTTR

Workaround

Vermeidung/Beseitigung eines Incidents oder Problems durch schnelle bzw. zeitlich begrenzte Umgehungslösung. Dadurch kann der User den Service wieder nutzen, ggfs. mit Einschränkungen, z.B. indem er bei Druckerausfall auf einen anderen Drucker ausweichen kann.

Workload

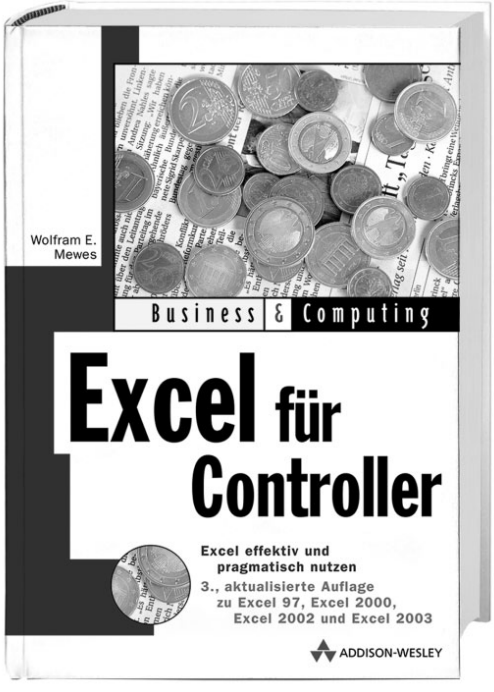
Arbeitslast, Nutzlast auf bestimmte Services oder Komponenten

Z

Zuverlässigkeit (Reliability)

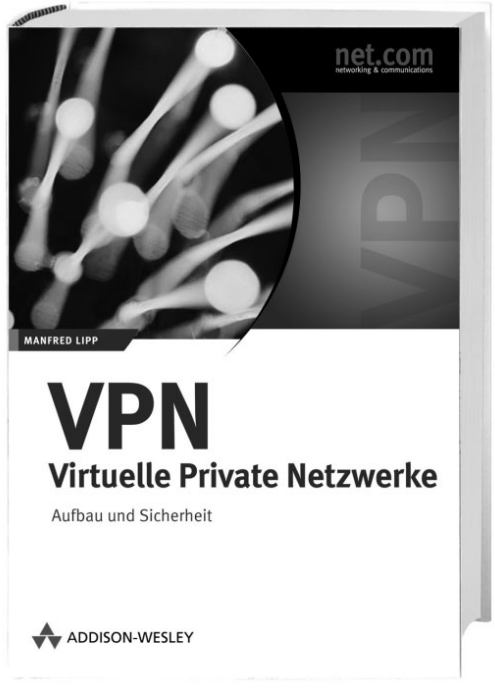
Fähigkeit einer Komponente, die benötigte Funktionalität für eine definierte Dauer und unter definierten Umständen zu liefern

Stichwortverzeichnis



In der 3. Auflage zeigt Ihnen Wolfram E. Mewes auf bewährte Weise, wie Sie als Controller (und als User) alle Excel-Funktionen effektiver nutzen. Neben den finanzmathematischen Funktionen beschreibt er unter anderem, wie Sie selber Automatisierungsmöglichkeiten in VBA programmieren können. Weitere Schwerpunkte sind die Anbindung von Excel an Datenbanken, die Analyse mit Hilfe von Pivot-Tabellen sowie OLAP. Der unentbehrliche Begleiter für die tägliche Arbeit im Controlling, für Excel-Versionen von Excel 97 bis inklusive Excel 2003.

Wolfram E. Mewes
ISBN-13: 978-3-8273-2122-1
ISBN-10: 3-8273-2122-0
44.95 EUR [D]

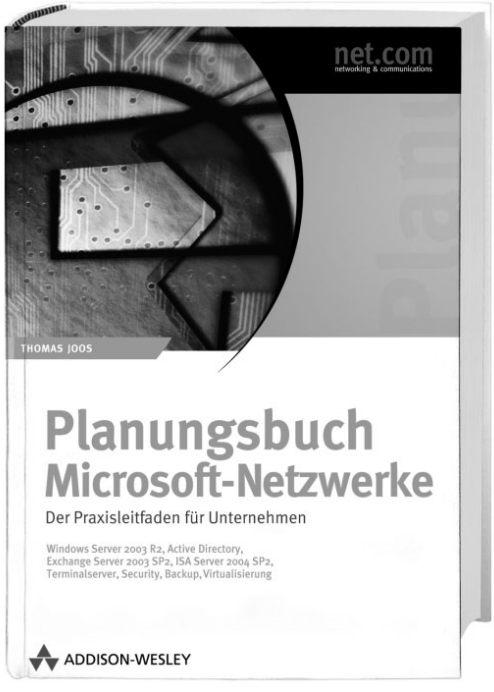


Mit einem VPN lassen sich Daten sicher über öffentliche Netzwerke transportieren. Nach einer kurzen Einführung in die Grundlagen widmet sich Autor Manfred Lipp ausführlich der VPN-Integration in Sicherheitsarchitekturen und SSL-VPNs. Ein weiterer Schwerpunkt liegt auf dem Einsatz von Microsoft VPN-Clients sowie VoIP und QoS im VPN. Im abschließenden Praxisteil beschreibt er anhand von mehreren Beispielszenarien, wie Sie ein VPN implementieren. Das Buch richtet sich an all diejenigen, die ein VPN betreiben oder planen, dies zu tun, und sich deshalb etwas intensiver mit der zugrunde liegenden Technologie befassen möchten. Neben theoretischen Erwägungen und der Erklärung heutiger VPN-Standards wird das Ganze durch etliche Tipps und Designbeispiele abgerundet.

Manfred Lipp
ISBN-13: 978-3-8273-2252-2
ISBN-10: 3-8273-2252-9
49.95 EUR [D]

Nutzen Sie die Stärken von Excel! Dieses Buch mit allen Tabellenmodellen, Diagrammen und Makros auf CD zeigt Ihnen, wie Sie Ihre Projekte schnell und effizient budgetieren, planen und steuern. War Ihnen herkömmliche Projektsoftware bisher zu teuer oder zu kompliziert? Hier sind die Lösungen von Excel-Experte Ignatz Schels. Sie werden staunen, wie Ihre Projekte plötzlich gelingen!

Ignat Schels
ISBN-13: 978-3-8273-2309-3
ISBN-10: 3-8273-2309-6
39.95 EUR [D]



IT-Leiter, -Administratoren und -Berater erhalten mit diesem Buch kompetente Informationen zur Planung eines Netzwerks mit Microsoft-Technologien (Windows Server 2003 R2, Exchange Server 2003 SP2, ISA 2004 SP2, WSUS, SharePoint u.v.m.). Themen sind u.a. Viren-und Spamschutz, Notfallkonzepte, VPN und Terminalserver. Sie finden einen Vergleich der verschiedenen Serverversionen und Speichermedien und erfahren alles über das perfekte Zusammenspiel der wichtigsten Produkte.

Thomas zoos
ISBN-13: 978-3-8273-2386-3
ISBN-10: 3-8273-2386-X
59.95 EUR [D]