



Thema:

**ITIL-konformes Inventar- und Help Desk-Management  
für kleine und mittlere Organisationen**

**Diplomarbeit**

Fakultät für Informatik  
Arbeitsgruppe Wirtschaftsinformatik - Managementinformationssysteme

Themensteller: Prof. Dr. rer. pol. habil. Hans-Knud Arndt

Betreuer: Prof. Dr. rer. pol. habil. Hans-Knud Arndt

vorgelegt von: Alexander Prösdorf

Abgabetermin: 03. Oktober 2011

## Inhaltsverzeichnis

Inhaltsverzeichnis .....	II
Verzeichnis der Abkürzungen und Akronyme .....	III
Abbildungsverzeichnis .....	IV
Tabellenverzeichnis .....	V
1 Einführung .....	1
2 Grundlagen.....	3
2.1 IT Infrastructure Library .....	3
2.2 Service und Service Management .....	6
2.3 Funktionen und Prozesse.....	7
2.4 Configuration Item .....	8
2.5 Kleine und mittlere Organisationen .....	9
3 Service Operation .....	13
3.1 Service Operation als Produktionsstätte der IT .....	13
3.2 Event Management.....	14
3.3 Incident Management.....	18
3.4 Request Fulfilment .....	25
3.5 Problem Management.....	27
3.6 Access Management.....	31
3.7 Service Desk.....	33
3.7.1 Der Service Desk als Single Point of Contact.....	33
3.7.2 Klassifizierung von Service Desks .....	34
3.7.3 Planung und Bereitstellung des Service Desk.....	35
3.7.4 Technische Ausstattung .....	37
3.7.5 Leistungsfähigkeit und Kundenzufriedenheit .....	39
3.7.6 Service Desk und Help Desk in der Gegenüberstellung .....	41
4 Methodische Überlegungen .....	43
4.1 Das Fachkonzept .....	43
4.2 Architektur integrierter Informationssysteme .....	44
4.3 Grundsätze ordnungsmäßiger Modellierung.....	45
5 Fachkonzept für ein integriertes Service Desk- und Inventarmanagement .....	47
5.1 Organisationsmodell.....	47
5.2 Datenmodell .....	50
6 Prototypische Realisierung .....	56
Literaturverzeichnis .....	57

## **Verzeichnis der Abkürzungen und Akronyme**

CI	Configuration Item
CMS	Configuration Management System
CTI	Computer Telephony Integration
EPK	Ereignisgesteuerte Prozesskette
ERM	Entity-Relationship-Modell
GoM	Grundsätze ordnungsmäßiger Modellierung
IT	Informationstechnik
ITIL	IT Infrastructure Library
KEDB	Known Error Database
KMU	Kleine und mittlere Unternehmen
SLA	Service Level Agreement
OLA	Operational Level Agreement

## **Abbildungsverzeichnis**

Abb. 5.1 Aufbauorganisation der IT-Organisation.....	49
Abb. 5.2 Beispiel Martin-Notation .....	50
Abb. 5.3 Datenmodell.....	51

## **Tabellenverzeichnis**

Tab. 3.1 Help Desk und Service Desk in der Gegenüberstellung. ....	42
Tab. 5.1 Beschreibung der Informationsobjekte, ihrer Attribute und Beziehungen.....	52

## 1 Einführung

Die IT Infrastructure Library (ITIL), hat sich von seit der ersten Version im Jahr 1998 zu einer weltweit anerkannten Best-Practice-Sammlung für kundenorientiertes IT-Service Management entwickelt. Derzeit ist die Version 3 verfügbar. Eine Aktualisierung der Version 3, die als 2011 Edition eingeführt werden soll, befindet sich in Arbeit. Die Aktualisierung verspricht eine Straffung der Struktur und Reduktion bezüglich inhaltlicher Inkonsistenzen. Auch Begrifflichkeiten werden klarer herausgearbeitet.

Sowohl zur Umsetzung und Einführung der ITIL als auch zu Praxiserfahrungen befindet sich eine Vielzahl von Publikationen auf dem Markt. Die Publikationen befassen sich jedoch überwiegend mit dem Einsatz der ITIL in großen Unternehmen sowie Hochschulen.

Grundsätzlich richtet sich ITIL nach Angaben der Herausgeber an Organisationen von jeglicher Größe und Typ. Dennoch lassen sich nicht alle in den ITIL-Kernpublikationen formulierten Richtlinien, Prozesse und Funktionen uneingeschränkt auf kleine und mittlere Organisationen skalieren. Dies ist nicht zuletzt eine Frage der Wirtschaftlichkeit. Dem hohen Aufwand für die Realisierung von ITIL-Prozessen und Funktionen steht ein eher kleines Volumen von zu bearbeitenden Anfragen, Störungen und zu betreibender Infrastruktur gegenüber. Kostenvorteile, die sich beispielsweise aus der beschleunigten und koordinierten Abwicklung von Störungen ergeben, stellen sich später ein.

Dennoch sind insbesondere die gewinnorientierten kleinen und mittleren Organisationen, d.h. die kleinen und mittleren Unternehmen (KMU) die sozial und wirtschaftlich vorherrschende Unternehmensform in Deutschland. Sie stellen 99,7 % der gewerblichen Betriebe sowie Freiberufler, bei ihnen arbeiten 79,5 % der sozialversicherungspflichtig Beschäftigten (vgl. IfM Bonn (2011b)).

IT Service Management gemäß der ITIL kann auch kleine und mittlere Organisationen dabei unterstützen, bei dynamischen und sich schnell ändernden Marktbedingungen Flexibilität zu beweisen und für interne und externe Kunden IT-Dienstleistungen in hoher Qualität zur Verfügung zu stellen.

In dieser Arbeit sollen zwei Ausschnitte aus der ITIL - Publikation Service Operation betrachtet werden, das Inventarmanagement und der Help Desk. Die Umsetzung des Help Desk erfolgt in der ITIL durch die umfangreiche Funktion Service Desk, die als Kontaktstelle zwischen Anwendern und IT - Organisation steht.

Die Arbeit geht zuerst auf Grundbegriffe und Konzepte der ITIL ein und beschreibt diese. Auf weitere Grundlagen, die für diese Arbeit von Bedeutung sind, wird eingegangen. Es folgt eine genaue Betrachtung der Prozesse in der Publikation Service Operation. Im gleichen Kapitel schließt sich die Beschreibung von Aufbau, Organisation und Nutzung der Funktion Service Desk an.

Kapitel vier widmet sich grundsätzlichen methodischen Überlegungen, die bei der Entwicklung des Fachkonzepts zu berücksichtigen sind.

Im fünften Kapitel folgt das Fachkonzept für das integrierte Service Desk- und Inventarmanagement und Verwendung der Methoden, die in Kapitel vier eingeführt wurden. Das Kapitel 6 stellt schließlich die prototypische Implementierung vor.

## **2 Grundlagen**

### **2.1 IT Infrastructure Library**

Die IT Infrastructure Library (ITIL) ist ein prozessorientierter Best-Practice-Ansatz für die Umsetzung eines IT-Service Managements in Organisationen jeglicher Größe und Art. ITIL ist nach Angaben der Herausgeber der am häufigsten angewendete erfahrungsbasierte Ansatz und international etabliert. Dieser beschreibt das Management und die Bereitstellung von IT-Services im Kontext ihres Lebenszyklus (vgl. Buchsein et al. (2008) S.6).

Grundprinzip der ITIL ist die bestmögliche Ausrichtung der IT-Organisation an den Anforderungen und Geschäftsprozessen des Kunden. Somit ist die IT-Unterstützung von Geschäftsprozessen als strategische Ressource anzusehen und einer der entscheidenden Erfolgsfaktoren von Geschäftsmodellen. Für diese Unterstützung des Geschäftsprozesses wird in den ITIL-Publikationen der Begriff Service verwendet, der nachfolgend noch definiert wird (vgl. Buchsein et al. (2008) S.11f.).

Innerhalb der ITIL bildet die Publikation Service Strategy den Kern. Service Design, Service Transition und Service Operation bilden die Schale um diesen Kern. Die Publikation Continual Service Improvement bildet die äußere Hülle, die Kern und Schale umgibt. Jede der Publikation beschreibt eine Phase im Service Management von IT-Dienstleistungen<sup>1</sup>.

Die ITIL ist grundsätzlich für alle Organisationstypen geeignet, da die Gestaltung, Strukturierung und Umsetzung an den individuellen Bedürfnissen der einzelnen Organisation ausgerichtet werden muss. Sie bietet insofern keine fertigen Methoden, bei denen es genügen würde, diese eins zu eins zu implementieren. Die in der ITIL beschriebenen Prozesse verlaufen horizontal durch die Organisation.

Durch die Einführung von ITIL sollen die folgenden Ziele erreicht werden können (vgl. Olbrich (2008) S. 4):

- Effektive und zielorientierte Gestaltung von Prozessen, Aufgaben und Rollen
- Beschleunigung der praktischen Umsetzung und Ausrichtung an den geschäftlichen Anforderungen
- Einheitliche Begriffsbildung und -verwendung und somit Reduzierung kommunikativer Missverständnisse

---

<sup>1</sup> Es werden in dieser Arbeit die englischen Original-Bezeichnungen der Publikationen verwendet, weil auch die deutschsprachigen Übersetzungen der ITIL - Publikationen die englischen Titel verwenden.



- Verbesserung der Kommunikation innerhalb der Organisation und nach außen und damit frühzeitige Aufdeckung von Änderungsbedarf und Problempotential
- Steigerung der Qualität der Serviceerbringung bei Kostensenkung
- Transparenz über alle Arbeitsabläufe mit einhergehender Verbesserung der Zufriedenheit von Kunden und Mitarbeitern

ITIL stellt nicht einen umfassenden Standard dar, sondern ist eine allgemein gehaltene Sammlung von Erfahrungen und Bewährtem. ITIL ist dennoch mit dem Standard ISO/IEC 20000 abgestimmt und ermöglicht somit eine Zertifizierung nach diesem Standard.

ITIL beschreibt somit nur, was zu tun ist, jedoch nicht, wie dies erreicht werden kann. Detaillierte Methodenbeschreibungen können schon deshalb nicht Bestandteil von ITIL sein, weil dafür eine Zielausrichtung auf eine bestimmte Organisationsform, Organisationsstruktur oder Branche in den Publikationen vorgenommen werden müsste. Die konkrete Umsetzung und Einführung der in der ITIL beschriebenen Prozesse und Funktionen wird nur dann gelingen, wenn das formulierte Ziel über den Wunsch nach ITIL-Konformität bzw. ITIL-Einführung hinausgeht. Geeignete beispielhafte Ziele sind der Wunsch nach Kostensenkung in der IT-Organisation, die Reduzierung von Durchlaufzeiten oder einer verbesserten Transparenz von Prozessen. Damit bestehen nämlich Zielvorgaben, die sich anschließend auch durch Definition zugehöriger Kennzahlen messen lassen (vgl. Beims (2010) S. 11 f.; Stych/Zeppenfeld (2008) S. 124 ff.).

Tatsächlich sind einige Konzepte und Methoden der ITIL nur dann sinnvoll umzusetzen, wenn die Organisation und der zugehörige IT-Bereich eine gewisse Größe besitzen.

Auf die Inhalte und Zielsetzungen der fünf ITIL-Kernpublikationen soll nachfolgend kurz eingegangen werden.

#### 1. Band: Service Strategy

Die Publikation Service Strategy ist der Ausgangspunkt des Lebenszyklus von Services. Es umfasst Empfehlungen und Methoden, mit denen das Service Management ausgelegt, entwickelt und implementiert werden kann, und dies nicht nur als Fähigkeit der Organisation, sondern auch mit dem Ziel der Entwicklung strategischer Werte. Prinzipien bezüglich der Praxis des Service Managements werden vermittelt, um sicherzustellen, dass sich der Lebenszyklus von Services jederzeit am Bedarf des

Kerngeschäfts ausgerichtet. Die behandelten Themen umfassen weiterhin die Entwicklung von Märkten und Servicekatalogen, organisatorisches und finanzielles Management sowie der Umgang mit Kosten und Risiken. Damit richtet es sich vorrangig an Geschäftsführer, leitende Mitarbeiter und Entscheider in der Organisation (vgl. Cannon/Hinrichs (2007) S. 6; Beims (2010) S. 16).

## 2. Band: Service Design

Der Band Service Design stellt Leitlinien bereit, die Design und Entwicklung von kundenorientierten und innovativen Services und Service Management Prozessen ermöglichen. Die strategischen Ziele aus der vorherigen Phase Service Strategy werden hiermit umgesetzt. Neben den neu zu entwickelnden Services befasst sich diese Phase auch mit Veränderungen und Verbesserung an bestehenden Services. Die folgenden Management-Prozesse werden beschrieben: Servicekataloge, Servicelevel, Kapazitätsplanung, Verfügbarkeit, Servicewiederherstellung, Informationssicherheit und Lieferanten (vgl. Cannon/Hinrichs (2007) S. 7; Beims (2010) S. 17).

## 3. Band: Service Transition

Die Phase Service Transition bzw. Serviceüberführung unterstützt Organisationen bei Planung und Management von Serviceänderungen und der Überführung der entwickelten Services in die produktive Geschäftsumgebung. Neben dem Change Management und dem Release- und Deployment Management werden auch Prozesse wie das Management von Service Assets und Konfigurationen sowie Test und Validierung von Services beschrieben (vgl. Cannon/Hinrichs (2007) S. 7; Beims (2010) S. 17).

## 4. Band: Service Operation

Die Publikation Service Operation bzw. Servicebetrieb betrachtet den operativen täglichen Betrieb von Services und Infrastruktur. Prozesse wie Incident- und Problem Management sind Kernthemen dieser Phase, auf die in einem eigenen Abschnitt dieser Arbeit noch im Detail eingegangen wird (vgl. Cannon/Hinrichs (2007) S. 7; Beims (2010) S. 17).

## 5. Band: Continual Service Improvement

Der Band Continual Service Improvement bzw. Kontinuierliche Serviceverbesserung stellt Vorgehensweisen bereit, um für den Kunden Wertschöpfung und Nutzen der Services zu steigern, die im Verlauf der Phasen Service Design, Service Transition und Service Operation definiert, eingeführt und betrieben werden. Qualität, Effizienz und

Effektivität von Services werden auf Basis von Feedback-Kreisläufen gesteigert (vgl. Cannon/Hinrichs (2007) S. 7; Beims (2010) S. 17).

## 2.2 Service und Service Management

Der Begriff Service wird in den Publikationen der ITIL wie folgt definiert: "Ein Service ist eine Möglichkeit, einen Mehrwert für Kunden zu erbringen, indem das Erreichen der von den Kunden angestrebten Ergebnisse erleichtert oder gefördert wird. Dabei müssen die Kunden selbst keine Verantwortung für bestimmte Kosten und Risiken tragen." (Cannon/Hinrichs (2007) S. 14).

Services ermöglichen es, Ergebnisse zu verbessern, indem die Leistung gesteigert und die Wirkungen von Einschränkungen reduziert werden. Somit kann das gewünschte Ergebnis mit einer höheren Wahrscheinlichkeit erreicht werden (vgl. Cannon/Hinrichs (2007) S. 14).

Im Blickpunkt stehen somit das Erreichen der angestrebten Ergebnisse und die Erbringung eines Mehrwerts für die Geschäftsprozesse der Organisation.

Wenn die von der IT-Organisation zu erbringenden Services die folgenden Merkmale umfassen, so handelt es sich um IT-Services (vgl. Buchsein et al. (2008) S.13):

- Services werden vom Anbieter, also z.B. der konkreten IT-Organisation für einen oder mehrere Kunden bereitgestellt
- Services unterstützen unter Einsatz der Informationstechnologie die Geschäftsprozesse des Kunden und leisten hierbei einen Mehrwert
- Services bestehen aus einer Kombination der Produktionsfaktoren Personen, Prozesse und Technologie
- Services werden unter Zuhilfenahme von Service Level Agreements vereinbart

STYCH hält fest: "Ein IT-Service ist immateriell, unteilbar, zeitlich begrenzt, individuell, standortbezogen und kann nicht zurückgerufen werden." (vgl. Stych/Zeppenfeld (2008) S. 138).

Ein IT-Service wird vom Kunden als zusammenhängendes Ganzes wahrgenommen. Ein IT-Service wird mit Hilfe einer oder mehrerer IT-Systeme bereitgestellt, wodurch Geschäftsprozesse ermöglicht bzw. unterstützt werden (vgl. Stych/Zeppenfeld (2008) S. 138).

Service Management wird von der ITIL-Primärliteratur wie folgt definiert: "Das Service Management ist die Gesamtheit der spezialisierten organisatorischen Fähigkeiten, die zur Generierung eines Mehrwert für Kunden in Form von Services verfügbar sind." (Cannon/Hinrichs (2007) S. 13).

IT Service Management zielt darauf ab, eine optimale Unterstützung der Geschäftsprozesse einer Organisation durch die IT-Organisation zu erbringen. Dabei steht die Ausrichtung auf die Bedürfnisse der internen und externen Kunden im Vordergrund. IT Service Management wird in seinen Methoden und Fähigkeiten durch Praxis, Wissen und Erfahrung geprägt. Die Fähigkeiten der Organisation bestehen aus Funktionen und Prozessen, um die Services während ihres Lebenszyklus zu managen. Die vorhandenen Fähigkeiten und Ressourcen sind so auszurichten, dass sie nutzenstiftende und werthaltige Services liefern können (vgl. Cannon/Hinrichs (2007)).

### **2.3 Funktionen und Prozesse**

Funktionen im Sinne der ITIL sind "Organisationseinheiten, die auf die Ausführung bestimmter Aufgaben spezialisiert sind und für bestimmte Ergebnisse verantwortlich sind." (Cannon/Hinrichs (2007) S. 14).

Sie verfügen als in sich geschlossene Einheiten über spezifische Ressourcen und Fähigkeiten, die für die Erbringung der Leistung erforderlich sind. Durch sie wird die Struktur und Stabilität von Organisationen gewährleistet. Innerhalb der Funktionen sind Rollen mit zugehörigen Berechtigungen definiert, die für festgelegte Abläufe und deren Ergebnisse verantwortlich sind. Die Kommunikation zwischen den Funktionen ist entscheidend für die Leistungsfähigkeit der gesamten Organisation und wird über gemeinsam genutzte Prozesse definiert. Funktionsübergreifende Steuerung und Koordination wird durch definierte Prozessmodelle ermöglicht (vgl. Cannon/Hinrichs (2007) S. 14 f.)

Damit unterscheidet sich der Funktionsbegriff in der ITIL von dem Funktionsbegriff in der Wirtschaftsinformatik.

Nach SCHEER kennzeichnen Funktionen jeweils einen Vorgang. Durch Funktionen werden Objekte erzeugt oder verändert. Funktionen lassen sich bis auf die Ebene von Elementarfunktionen jeweils in Teilfunktionen zerlegen, um die Komplexität zu reduzieren (vgl. Scheer (1998) S. 19).

Diese Auffassung des Funktionsbegriffs ist eher vergleichbar mit dem Prozessbegriff im ITIL-Verständnis. Demnach beschreibt ein Prozess einen strukturierten Satz an Aktivitäten, durch deren Ausführung ein definiertes Ziel erreicht werden soll. Der Prozess wandelt somit die Eingabefaktoren in zu erwartende Ergebnisse um. Aktivitäten innerhalb eines Prozesses werden von verwendeten Fähigkeiten und Ressourcen beeinflusst. Ein Prozess kann Richtlinien, Standards, Leitlinien und Arbeitsanweisungen definieren (vgl. Cannon/Hinrichs (2007) S. 281).

Prozesse haben mehrere Eigenschaften: Sie sind messbar anhand verschiedener Kriterien, wie Kosten, Qualität, Produktivität. Prozesse haben spezifizierte Ergebnisse, die zu erreichen sind. Die Ergebnisse von Prozessen sind ebenso messbar.

Außerdem hat ein Prozess Abnehmer der entsprechenden Ergebnisse, die für diese von Nutzen sind und definierte Erwartungen zu erfüllen haben. Die Abnehmer können sich innerhalb oder außerhalb der Organisation befinden. Weiterhin reagiert ein Prozess auf Ereignisse, welche diesen kontinuierlich oder schrittweise verlaufen lassen (vgl. Cannon/Hinrichs (2007) S. 15).

## **2.4 Configuration Item**

Unter der Bezeichnung Configuration Item (CI) werden in der ITIL alle Komponenten zusammengefasst, „die verwaltet werden müssen, um einen IT Service bereitstellen zu können. Informationen zu den einzelnen CIs werden in einem Configuration Record innerhalb des Configuration Management Systems erfasst und über den gesamten Lebenszyklus hinweg [...] verwaltet.“ (Cannon/Hinrichs (2007) S. 261).

Konkrete beispielhafte Ausprägungen von CIs sind IT-Services, Hardware, Software, Gebäude, formale Prozessdokumentationen und Service Level Agreements (SLA). Das Configuration Management System ist ein Werkzeug mit integrierter Datenbank, die ein Anbieter von Services, also bspw. die IT-Organisation, verwendet, um die CIs zu administrieren (vgl. Cannon/Hinrichs (2007) S. 261).

Im weiteren Verlauf der Arbeit soll unter Inventar und Configuration Item das Gleiche verstanden werden.

## 2.5 Kleine und mittlere Organisationen

Die Formulierung „kleine und mittlere Organisationen“ beschreibt verschiedene Formen von Organisationen, sowohl hinsichtlich des Organisationszwecks als auch der Organisationsgröße.

Organisationen sind soziale, zeitlich relativ stabile Systeme, bestehend aus Individuen. Sie verfolgen gemeinsame Ziele. Nach ihren Zielen können Organisationen klassifiziert werden.

Organisationen können einerseits Sachleistungen bzw. Dienstleistungen erbringen, wie Produktionsbetriebe und Dienstleistungsunternehmen. Sie können auch das Ziel haben, auf ihre Umgebung zu wirken. Dies streben beispielsweise Behörden, staatliche Sicherheitsorgane, Parteien und Gewerkschaften an.

Eine andere Form von Organisationen bilden jene, die das Ziel haben, Personen zu verändern. Sie werden auch als Non-Profit-Organisationen bezeichnet. Dies können beispielsweise Schulen, Universitäten, Beratungsstellen und Justizvollzugsanstalten sein (vgl. Schewe (2011)).

Im Bereich der Unternehmen hat das Institut für Mittelstandsforschung eine Definition formuliert, um die kleinen und mittleren von den großen Unternehmen abzugrenzen.

Als kleine Unternehmen gelten demnach die unabhängigen Unternehmen mit bis zu neun Beschäftigten und einem Jahresumsatz von weniger als 1 Mio. EUR. Die Unternehmen, die bis zu 499 Beschäftigte haben und einen Jahresumsatz von weniger als 50 Mio EUR generieren, fallen unter die Gruppe der mittleren Unternehmen. Wenn kleine und mittlere Unternehmen gemeinsam betrachtet werden, wird häufig die Abkürzung KMU verwendet. Weiterhin schließt auch der Begriff Mittelstand immer die kleinen Unternehmen mit ein. Die Rechtsform der Unternehmen ist unerheblich für die Einordnung. Unternehmen, welche die zuvor genannten Grenzen überschreiten, werden als Großunternehmen bezeichnet (vgl. IfM Bonn (2011a)).

Es gibt einige entscheidende Unterschiede in den Merkmalen kleiner bzw. mittlerer Unternehmen (KMU) gegenüber großen Unternehmen. Dies bezieht sich sowohl auf die IT-Organisation als auch auf die Gesamtorganisation. Einige Merkmale werden im Folgenden im Überblick dargestellt.

Die folgenden Eigenschaften von KMU beeinflussen die Arbeitsweise und das Tagesgeschäft der IT-Organisation:

- Nur einen oder wenige Unternehmensstandorte

- Kleine Anzahl von IT-Anwendern
- Unterdurchschnittliches Verhältnis von IT-Mitarbeitern zu Anwendern
- Begrenzte finanzielle Ressourcen im Vergleich zu großen Unternehmen
- Kleine Budgets und Mitarbeiterzahlen
- Unterproportionales Verhältnis von IT-Support-Mitarbeitern zu Anwendern im Vergleich zur Branchen – Durchschnitt
- Geringe finanzielle Mittel für Maßnahmen, deren Nutzen noch nicht sicher ist.
- Begrenzter Zeitrahmen, in denen sich Verbesserungen rentieren bzw. sich als nützlich erweisen müssen.

Insbesondere zeichnen sich kleine und mittlere Unternehmen durch eine stark informell geprägte Unternehmenskultur und Atmosphäre aus. Die Mehrheit der Mitarbeiter ist untereinander persönlich bekannt, man kennt in etwa die Standpunkte, Reaktionen, Vorurteile und Perspektiven der Anderen.

In größeren Unternehmen sind Prozesse und Abläufe stärker formalisiert, die Kommunikation ist unpersönlicher.

Dabei ist Formalismus für viele der ITIL-Verfahren- und Methoden unbedingt erwünscht, durch den Verzicht werden Zeit- und Kostenrisiken in Kauf genommen. Als Beispiele seien hier Aktivitäten im Rahmen des Configuration Managements oder des Change Managements genannt. Formalismus ist ein entscheidendes Kriterium für das Management von Services.

Kleine Organisationen, seien es nun kleine Unternehmen, Abteilungen oder Teams, fühlen sich in der Regel dem Teamgeist und den gemeinsamen Zielen verpflichtet und ermöglichen auch über die Teamgrenzen hinaus eine engere Zusammenarbeit.

Personen in kleinen Organisationen sind häufig für mehrere Rollen verantwortlich. Die Kommunikation zu Themen, die von gemeinschaftlichem Interesse sind, wird so erleichtert. Allerdings verstärkt dies die Tendenz zu informeller Kommunikation zwischen der IT-Organisation und den Kunden. Einerseits können somit Probleme mit einem Minimum an Kommunikationsaufwand gelöst werden, andererseits könnten somit Themen ohne eine ausreichende Betrachtung, Abstimmung, Dokumentation bzw. finanzielle Freigabe zur Umsetzung kommen, was nicht wünschenswert ist.

Kleinere und mittlere Unternehmen verfügen außerdem über eine stärkere Reaktionsfreudigkeit und Flexibilität gegenüber den Bedürfnissen ihrer internen und externen Kunden.

Die Umsetzung von Initiativen und Ideen kann trotz unvollständiger Planung frühzeitig begonnen werden. Änderungen und Erweiterungen können einfacher eingefügt werden, da Entscheidungsträger besser verfügbar sind und der Kommunikationsaufwand insgesamt geringer ist.

Dienstleistungen und Services richten sich außerdem häufig an eine geringere Zahl von Nutzern im Unternehmen, weshalb die Anforderungen einfacher kontrollierbar und an den tatsächlichen Bedarf anpassbar sind.

Mitarbeiter in kleinen und mittleren Organisationen kennen die Liefer- und Prozesskette der Produkte und Leistungen des Unternehmens besser und dies gilt auch für Unternehmensangehörige, die für das IT Service Management verantwortlich sind. Somit können diese ihre Leistungen stärker am Bedarf und am Unternehmenszweck ausrichten.

Kleine und mittlere Organisationen können es sich dagegen häufig nicht leisten, für bestimmte Tätigkeiten ausgewiesene Spezialisten bereitzuhalten, solange diese Spezialfähigkeiten nicht das Kerngeschäft der Organisation betrifft. Dies gilt auch und insbesondere im IT-Bereich.

Beispielsweise verfügen insbesondere kleine Organisationen häufig nicht über Mitarbeiter, die speziell für die Wartung und den Betrieb eines Microsoft-Exchange - Servers ausgebildet und zertifiziert sind. Kleinere Anpassungen der Software können von ggf. von überdurchschnittlich erfahrenen IT-Anwendern vorgenommen werden. Sobald jedoch anspruchsvolle Probleme gelöst werden müssen oder ein Versionswechsel durchgeführt werden soll, werden häufig die Leistungen eines externen Dienstleisters in Anspruch genommen.

Kleine und mittlere Organisationen sind häufig vor allem aus finanziellen Erwägungen heraus gezwungen, sich auf die Fähigkeiten und Mitwirkung einzelner Personen mit spezialisiertem Fachwissen zu verlassen und sind in einem besonderen Maße von ihnen abhängig. Diese in der englischsprachigen ITIL-Literatur als "Heroes" bzw. "Helden" bezeichneten Personen lösen auftretende Störfälle und Probleme zügig und kompetent. Bei ihrer Abwesenheit kann die Organisation jedoch in einen kritischen Zustand gelangen. In einem bestimmten Umfang kann dieses Risiko akzeptiert werden, jedoch sollte sich die Organisation darüber stets im Klaren sein. Insbesondere besteht jederzeit



die Gefahr, dass ein solcher "Held" die Organisation verlässt und damit die Verfügbarkeit einzelner Fähigkeiten nicht mehr gegeben ist.

Hier kann Dokumentation und formalisierte Kommunikation bezüglich getroffener Entscheidungen und durchgeführter Handlungen innerhalb der Organisation helfen, die Folgen der Nichtverfügbarkeit eines "Helden" zu reduzieren.

Wenn jedoch Überlebensfähigkeit der Organisation von einzelnen "Helden" abhängt, ist es sinnvoll und angemessen, weitere Personen auf das erforderliche Spezialwissen zu trainieren. Im Zusammenhang mit dem Mangel an Spezialisten steht der Umstand, dass in kleinen und mittleren Organisation auf eine kleinere Wissensbasis zurückgegriffen werden kann, allein aufgrund der geringeren Anzahl an Mitarbeitern.

Der einzelne Mitarbeiter ist eher Generalist und besetzt verschiedene Rollen in der Organisation. Spezialisierte Fähigkeiten werden dann nach Bedarf von Drittanbietern bezogen.

Kleine und mittlere Organisationen können bezüglich ihrer IT-Organisationskosten nicht von den Skaleneffekten profitieren, wie sie für größere Organisationen zu erzielen sind. Die Kosten der IT pro Anwender sind relativ gesehen höher, so z.B. für Hardware- und Software-Lizenzen, Schulungskosten für IT-Mitarbeiter und externe Beratungsleistungen.

Ein weiterer Aspekt ist die sogenannte Pro-Kopf-Komplexität, welche die "small means simple"-These widerlegt. Tatsächlich sind die Aufgaben in kleinen und mittleren Organisationen eher komplex. Der Bedarf nach einfachen Standard-Konfigurationen ist in kleinen spezialisierten Arbeitsgruppen geringer, ein höherer Anteil der Anwender verlangt nach stärker individualisierten Techniken und Verfahren. Dies kann sich dann in höherer Komplexität und Vielfalt der Incidents, der Configuration Items und ihrer Verknüpfung untereinander, sowie der Hard- und Software äußern.

Weiterhin trifft es zu, dass in kleinen und mittlere Organisationen insgesamt weniger Rollen zu besetzen gibt, somit sind auch die Aufstiegsmöglichkeiten für einzelne Mitarbeiter, und insbesondere in den hier betrachteten IT-Abteilungen entsprechend beschränkt (vgl. Taylor/Macfarlane (2009); S. 25 ff.).

Alle diese Fakten müssen bei Planung, Entwicklung, Bereitstellung und Betrieb von IT-Services in kleinen und mittleren Organisationen berücksichtigt werden.

## 3 Service Operation

### 3.1 Service Operation als Produktionsstätte der IT

Die Publikation Service Operation beschreibt Prozesse, Funktionen und Empfehlungen, mit denen Effizienz, Effektivität und Stabilität bei der Bereitstellung und dem Support von IT-Services gewährleistet und verbessert werden kann. Service Operation befasst sich also mit dem Management der den Kunden angebotenen Services und stellt den Betrieb innerhalb der vereinbarten Service-Level sicher.

Dies umfasst auch das Management der für die Servicebereitstellung eingesetzten Technologie und Infrastruktur unter Einsatz von Verfahren zur Leistungsmessung und Monitoring. ITIL bezeichnet die Service Operation als "Produktionsstätte der IT".

Der tatsächliche Geschäftsnutzen der in den vorherigen Phasen Service Strategie, Service Design und Service Transition durchgeführten Aktivitäten und Methoden zeigt sich bevorzugt in der Phase Service Operation. (vgl. Cannon/Hinrichs (2007); S. 3)

Die Realisierung der vorgenannten Erwartungen ist jedoch mit unterschiedlichen Zielkonflikten verbunden:

Interne Sicht der IT vs. externe Sicht des Kerngeschäfts

Stabilität vs. Reaktionsfähigkeit

Servicequalität vs. Servicekosten

Reaktives Verhalten vs. Proaktives Verhalten

Für die Phase Service Operation sind fünf Kernprozesse beschrieben, auf die in den nachfolgenden Seiten detaillierter eingegangen wird.

- Event Management
- Incident Management
- Problem Management
- Request Management
- Access Management

Weiterhin sind für die Durchführung der Prozesse der Service Operation-Phase die nachfolgenden Funktionen erforderlich:

- Service Desk
- Technical Management
- IT Operations Management
- Application Management

Von diesen Funktionen soll nur der Service Desk genauer beschrieben, da dieser für die fachkonzeptionelle Entwicklung in dieser Arbeit erforderlich ist.

### **3.2 Event Management**

Das Event Management hat das Ziel, Ereignisse, die in der IT-Infrastruktur auftreten, zu erkennen, diese zu bewerten und geeignete Steuerungsmaßnahmen einzuleiten. Das Event Management ist daher die Basis des operativen Monitorings und der operativen Steuerung. IT-Komponenten sollten überwacht werden, um Funktionsstörungen möglichst frühzeitig zu entdecken und Auswirkungen auf die unterstützten Geschäftsprozesse gering zu halten.

Das Event wird definiert als jedes wahrnehmbare Ereignis, das von Bedeutung für die Bereitstellung von IT-Diensten oder das Management der IT-Infrastruktur ist. Bei Events handelt es sich zumeist um Benachrichtigungen, die von einem Configuration Item, einer Monitoring-Software oder einem IT-Service generiert werden.

Events sind der Auslöser verschiedener IT-Service Management-Prozesse, Aktivitäten und auch automatisierter Vorgänge. Innerhalb des Event Management-Prozesses muss gewährleistet werden, dass Event-Benachrichtigungen nach dem Senden durch entsprechende Software auch empfangen und weiterverarbeitet wird.

Es muss hier angemerkt werden, dass Monitoring und Event Management nicht dasselbe sind, jedoch eng miteinander verknüpft. Das Event Management dient dazu, Benachrichtigungen hinsichtlich des Status von IT-Infrastruktur und Diensten zu erzeugen und weiterzuleiten. Das Monitoring ist weiter gefasst, obwohl es technisch gesehen erforderlich ist, um Benachrichtigungen auszulösen. Monitoring-Agenten fragen zwar kontinuierlich den Status von Geräten ab, Events werden jedoch nur unter

definierten Bedingungen ausgelöst (vgl. Cannon/Hinrichs (2007); S. 42 f.; Beims (2010) 136 f.).

Es wird zwischen verschiedenen Event-Typen unterschieden, die jeweils unterschiedliche Maßnahmen auslösen (vgl. Cannon/Hinrichs (2007); S. 46 f.; Beims (2010) 137 f.):

**Informativ (Informational):** Es sind keine Maßnahmen als Reaktion auf das Event erforderlich, da es keine Ausnahme darstellt. Events dieser Art werden ggf. für einen definierten Zeitraum in Systemprotokolldateien gespeichert und informieren über den Status eines Geräts oder Dienstes oder den erfolgreichen Abschluss einer Aktivität. Beispiel: Ein Gerät meldet sich am Netzwerk an. Ein Druckauftrag wird erfolgreich abgeschlossen.

**Warnung (Warning):** Ein Messwert eines Geräts oder Dienstes nähert sich einem definierten Grenzwert oder untypisches Verhalten wurde festgestellt. Personen, Prozesse oder Überwachungssoftware werden informiert, um die Situation zu überprüfen und Maßnahme einzuleiten, die eine Ausnahme verhindern können. Beispiel: Die Festplattenauslastung eines Servers hat den Schwellwert von 80 % erreicht und nähert sich dem 90 %-Grenzwert.

**Ausnahme (Exception):** Ein Dienst oder ein Gerät läuft nicht in einwandfreiem Zustand, Totalausfall, reduzierte Leistungsfähigkeit oder Funktionseinschränkungen sind eingetreten. Dies bedeutet nachteilige Folgen für Geschäftsprozesse oder eine Verletzung der SLA. Maßnahmen zur Überprüfung und Entstörung sind normalerweise erforderlich. Üblich sind die Öffnung eines Incidents und/oder eines Requests for Change. Beispiel: Ein Datei-Server ist ausgefallen. Ein Netzwerkknoten ist nicht erreichbar.

In der konkreten Anwendungssituation des Event Managements sollten die Abgrenzungen der verschiedenen Event-Typen klar definiert sein.

Der Event-Management-Prozess umfasst die folgenden Schritte (vgl. Cannon/Hinrichs (2007); S. 44 f.; Beims (2010) 137 f.):

### *Event-Eintritt*

Events treten kontinuierlich auf, nicht alle werden jedoch registriert und weitergeleitet. In den Entwurfs- und Entwicklungsphasen von IT-Diensten und IT-Infrastrukturen sollte bereits berücksichtigt werden, welche Events erkannt werden müssen.

### *Event-Benachrichtigung*

Für das Event Management wird die Funktionalität einer Vielzahl von Geräten oder System genutzt, Status-Informationen oder definierte Ereignisse zu übermitteln. Das kann entweder durch Abfrage von Daten des Geräts erfolgen, das sog. Polling, oder das Gerät ist selbst in Lage, Benachrichtigungen zu übermitteln, sobald definierte Bedingungen eintreten. Die Implementierungen solcher Polling- bzw. Benachrichtigungsmechanismen basieren häufig auf dem verbreiteten Standard Simple Network Management Protocol (SNMP).

### *Event-Erkennung*

Event-Benachrichtigungen, die generiert wurden, werden unmittelbar danach von Software-Agenten oder Management-Software erkannt, die auf dem Gerät oder System laufen, das die Benachrichtigung erzeugt hat.

### *Event-Filterung*

Nur bei einem kleineren Anteil auftretenden Events muss eine Reaktionsmaßnahme eingeleitet werden. Der überwiegende Anteil wird nur in Protokolldateien aufgezeichnet. Die Filterung hat damit zum Ziel, festzulegen, ob ein Event für die Verarbeitung an eine Management-Software weitergeleitet wird oder ob es ignoriert wird.

### *Event-Kategorisierung und -Zuordnung*

Die bei der Filterung als relevant eingestuften Ereignisse werden klassifiziert, um entscheiden zu können, welche Reaktionen erforderlich sind. Die Organisation erstellt Kategorien nach ihrem Bedarf, mindestens sollten jedoch die zuvor beschriebenen Event-Typen Informativ, Warnung und Ausnahme definiert sein. Auch die Kategorisierung in anderen Dimensionen sowie eine Priorisierung der Events kann durchgeführt werden. Außerdem kann in dieser Phase bestimmt werden, ob schon von weiteren Geräte bzw. Diensten gleichartige Events bekannt sind - dann erfolgt eine entsprechende Zuordnung.

### *Auslösung (Trigger)*

Auf die Kategorisierung und Zuordnung von Events können automatisiert Antworten eingeleitet werden, dies wird als Trigger bezeichnet. So können bspw. Incident Trigger darunter sein, mit denen durch einen automatisiert erzeugten Datensatz der Incident-Management-Prozess ausgelöst wird. Auch Change Management Prozesse können durch entsprechende Trigger gestartet werden. Typisch sind auch Skripte, die Stapelverarbeitungsaufträge anstoßen.

### *Maßnahmenauswahl*

In dieser Phase werden die verschiedenen Maßnahmen, die als Antwort auf das Event möglich sind, ausgewählt und durchgeführt. Mehrere Maßnahmen können dabei kombiniert werden.

### *Maßnahmen überprüfen*

In großen Organisationen wird tagtäglich eine Vielzahl von Events generiert, somit ist es nicht möglich, alle durchgeführten Maßnahmen und Aktivitäten zu überprüfen. In kleineren Organisationen wird sehr wahrscheinlich die Kapazität dafür fehlen. Dennoch sollten die wichtigen Ereignisse und Ausnahmen einer manuellen Nachbetrachtung unterzogen werden. Diese Ergebnisse sollten auch Grundlage des kontinuierlichen Verbesserungsprozesses sein.

### *Event schließen*

Die meisten Events werden weder geöffnet noch geschlossen. Insbesondere Events vom Typ Informativ werden meist nur erfasst. Events, die jedoch einen Incident, ein Problem oder einen Change generiert haben, sind mit diesen über einen Datensatz verknüpft und werden geschlossen, wenn auch der zugeordnete Managementprozess abgeschlossen ist.

Betrachtungen hinsichtlich der Effizienz und Effektivität des Event Management Prozesses sollten die folgenden Kennzahlen berücksichtigen:

- Anzahl der Events, unterschieden nach Kategorie und Bedeutung
- Anteil der Events, bei denen ein Eingriff durch Mitarbeiter erforderlich wurde
- Anteil der Events, durch die Changes oder Incidents erzeugt wurden

- Anteil der Events, die durch bekannte Fehler (Known Errors) oder Probleme (im Sinne der ITIL - Definition ausgelöst wurden
- Anteil der Events, die sich wiederholten
- Anzahl und Anteil der Events, unterteilt nach technischen Plattformen bzw. Anwendungen

### **3.3 Incident Management**

Incident Management befasst sich mit Ereignissen, die den normalen Betrieb von Diensten und Services beeinträchtigen oder stören. Wichtigstes Ziel ist die möglichst schnelle Wiederherstellung des Normalbetriebs und die Vermeidung bzw. Minimierung der nachteiligen Folgen für die Geschäftsprozesse. Als Normalbetrieb von Services ist hierbei der Betrieb innerhalb der Grenzen des SLA festgelegt.

Ein Incident im Sinne der ITIL ist definiert als eine ungeplante Unterbrechung oder Qualitätsbeeinträchtigung eines IT-Services. Als Incident wird ebenso der Ausfall eines Configuration Items betrachtet, auch wenn dieser noch nicht zu einer Störung eines Services geführt hat.

Das Incident Management ist ein Prozess, der über den gesamten Lebenszyklus eines Incident für diesen verantwortlich ist. Das Incident Management hat jedoch nicht zum Ziel, die Ursache einer Störung oder Beeinträchtigung zu finden und zu beseitigen, denn dies ist Bestandteil des Problem Managements.

Mit Unterstützung des Incident Managements kann die Produktivität der Anwender gesteigert werden und die bestmögliche Verfügbarkeit und Qualität der bereitgestellten Services ermöglicht werden.

Incidents werden von Mitarbeitern der IT-Organisation gemeldet, über den Service Desk infolge der Meldungen von Anwendern ausgelöst oder über Schnittstellen vom Event Management übermittelt. Die Mehrzahl der übermittelten Events verursachen jedoch keine Incidents, sondern zeigen den Normalbetrieb an.

Auf Basis von SLAs werden für jede Phase der Incident-Bearbeitung Zeitvorgaben festgelegt. Die Dokumentation dieser Zielzeiten erfolgt in sog. Operational Level Agreements (OLAs) und Verträgen mit externen Dienstleistern, falls diese eingesetzt werden. Die Zielzeiten sind weiterhin Handlungsgrundlage für das Eskalieren von Incidents.

Für Incidents, die gleichartig sind und wiederholt auftreten, sollten Standard-Incident-Modelle hinterlegt werden. In diesen wird dokumentiert, welche konkreten Schritte zur Bearbeitung des Incidents und Wiederherstellung des Services durchgeführt werden sollten. Dies umfasst auch personelle Zuständigkeiten, Zeitvorgaben und Eskalationsregeln.

Incidents, die unmittelbar große Auswirkungen auf die Geschäftsprozesse haben, werden als Major Incidents bezeichnet und erfordern besondere Maßnahmen zur Wiederherstellung des Service, darunter kürzere Zeitvorgaben und höhere Priorisierungen. Ab wann ein Incident ein Major Incident ist, sollte in den Prozessvorgaben des Incident Managements bzw. in der Beschreibung des Service festgehalten werden (vgl. Cannon/Hinrichs (2007); S. 53 ff.; Beims (2010) 141 ff.)

Der Incident Management Prozess umfasst die folgenden Schritte (vgl. Cannon/Hinrichs (2007); S. 55 ff.; Beims (2010) 143 ff.):

#### *Incident - Identifizierung*

Um die Behandlung eines Incident einzuleiten, muss er als solcher identifiziert werden. Anwender melden sich über Telefon, Webportal oder E-Mail beim Service Desk, weil die Auswirkungen des Incident sie in ihrer Aufgabenerfüllung beeinträchtigen. Automatisierte Meldungen können den Anlauf des Incident Management Prozesses beschleunigen, ggf. noch bevor die Auswirkungen die Anwender erreichen.

#### *Incident-Erfassung*

Jeder Incident wird in einem Incident-Datensatz aufgezeichnet und mit verschiedenen Attributen versehen, unabhängig davon, ob diese über den Service Desk gemeldet werden oder durch das Event Management System. Dies ermöglicht eine effektive Nachverfolgung und gewährleistet, dass auch die Support-Gruppen, die den Incident später bearbeiten, über den gleichen Informationsstand verfügen. Die während des Lebenszyklus des Incident entstehenden Information sowie die durchgeführten Aktivitäten werden dem Incident-Datensatz hinzugefügt.

Die folgenden Informationen sollten im Verlauf des Incident-Lebenszyklus in seinem Datensatz hinterlegt werden:

- Eindeutige Identifikationsnummer
- Kategorie-Einstufung des Incident
- Auswirkungen des Incident



- Dringlichkeit des Incident
- Priorität auf Basis von Auswirkungen und Dringlichkeit
- Zeitstempel der Erfassung
- Name bzw. Kennzeichen der Person oder Gruppe, die den Incident erfasst hat
- Art der Incident-Meldung (Telefon, E-Mail, Event-Management-System usw.)
- Name und Kontaktdaten des Anwenders, der den Incident gemeldet hat
- Art der Kommunikation mit dem Anwender
- Beschreibung der Symptome
- Status (Erfasst, in Bearbeitung, gelöst, geschlossen)
- Zuordnung des / der betroffenen Geräte / Dienste / Configuration Items
- Zuordnung zu eventuell bekannten Fehlern oder Problemen
- Auflistung der durchgeführten Aktivitäten zur Lösung des Incident
- Zeitstempel bei Lösung des Incident
- Kategorie zum Zeitpunkt des Abschlusses
- Zeitstempel beim Schließen des Incident

### *Incident-Kategorisierung*

In diesem Prozess-Schritt erfolgt die fachliche Einordnung des Incident in eine Kategorie. Das Kategorisierungsschema muss zuvor anhand des Bedarfs und der konkreten Situation in der IT-Organisation aufgestellt werden. Eine Vorgehensweise zur Aufstellung eines Kategorisierungsschemas findet sich am Ende dieses Abschnitts

Mit der Festlegung der Kategorie kann bereits eine Vorentscheidung für die Support-Gruppe fallen, die den Incident bearbeiten soll. Außerdem wird in dieser Phase überprüft, ob der erfasste Sachverhalt auch tatsächlich einem Incident entspricht. Zum Beispiel könnten Anwender bei der Erfassung über Webformulare aus Unwissenheit versehentlich auch den Typ Incident auswählen, obwohl es sich tatsächlich um einen

Service Request handelt. Liegt ein Service Request vor, muss dieser aus dem Incident Management-Prozess herausgenommen werden und an den Request Fulfilment-Prozess weitergegeben werden.

#### *Incident- Priorisierung*

Die Ermittlung der Priorität eines Incident erfolgt unter Berücksichtigung der Dimensionen Dringlichkeit (d.h wie schnell eine Lösung benötigt wird) und Auswirkungen. Die Anzahl der von der Service-Beeinträchtigung betroffenen Anwender ist eine Möglichkeit, die Auswirkungen zu beurteilen. Aber auch die Anzahl der beeinträchtigten Services oder die zu erwartenden finanziellen, rechtlichen oder Reputationsfolgen sind ein Maßstab. In diesem Schritt kann fallweise auch entschieden werden, dass der Incident ein Major Incident ist. Das Priorisierungssystem kann in Form einer Codierungsmatrix angelegt werden, wobei konkrete Werte für alle Kombinationen aus Dringlichkeitsstufe (Hoch, Mittel, Niedrig) und Auswirkungsstufe (Hoch, Mittel, Niedrig) berücksichtigt werden.

#### *Incident-Erstdiagnose*

Der Service-Desk-Mitarbeiter versucht in dieser Phase, eine unmittelbare Lösung für den Incident zu finden, dies kann noch während der telefonischen Meldung des Anwenders geschehen. Dafür sollten Diagnoseskripte, eine Datenbank der bekannten Fehler und Umgehungsmöglichkeiten (Workarounds) zur Verfügung stehen. Der Incident kann in dieser Phase geschlossen werden, wenn eine Lösung bereitgestellt und umgesetzt werden kann.

#### *Incident- Eskalation*

Die Eskalation hat zum Ziel, zu entscheiden, ob die Incident-Bearbeitung an andere Support-Gruppen weitergegeben werden muss. Dafür werden organisationsintern Regeln innerhalb der sog. Operational Level Agreement (OLA) festgelegt. Falls eine Eskalation erfolgt, werden die betroffenen Anwender darüber informiert. Der Service Desk bleibt jedoch weiterhin bis zum Abschluss der Incident - Bearbeitung für diesen verantwortlich. Zwei Arten der Eskalation werden unterschieden.

Die Funktionale Eskalation erfolgt, wenn der Service Desk den Incident aufgrund von fehlendem Wissen oder Fähigkeiten oder infolge von Zeitüberschreitungen nicht lösen kann. Es erfolgt eine Weitergabe an und die Bearbeitung von Support-Gruppen, die auf nächster Ebene den Second-Level-Support oder Third-Level-Support abdecken. Auch externe Kapazitäten kommen hier in Betracht, beispielsweise der Support der Hardwarehersteller.

Die Hierarchische Eskalation muss vorgenommen werden, wenn es sich um Incidents mit hoher Priorität handelt. Weiterhin gilt dies für Incidents, bei denen absehbar ist, dass die weiteren Schritte der Bearbeitung mehr Zeit benötigen, als dies in den Regeln von OLA und SLA vereinbart wurde. Die hierarchische Eskalation folgt der fachlichen Führungshierarchie der Organisation, d.h. es erfolgt die Benachrichtigung leitender Mitarbeiter, damit diese nach Bedarf weitere Maßnahmen einleiten und Kapazitäten bereitstellen können.

#### *Untersuchung und Diagnose*

Die an der Bearbeitung des Incident beteiligten Support-Gruppen untersuchen und bewerten die Störung und deren Auswirkungen. Die einzelnen Aktivitäten werden im Datensatz zum Incident dokumentiert. Bei einfachen Incidents erfolgt dieser Schritt beim First-Line-Support, der in der Regel vom Service Desk abgebildet wird. Bei funktionaler Eskalation führen die nachfolgenden Support-Gruppen dies ebenso durch. Die in Frage kommenden Lösungen werden so herausgearbeitet.

#### *Lösung und Wiederherstellung*

Nachdem eine Lösungsmöglichkeit für den Incident identifiziert wurde, muss diese angewendet und getestet werden. Verschiedene Ansätze kommen dabei in Betracht. Der Anwender kann unter Hilfeleistung des Service Desk selbst Schritte durchführen, welche die Störung beheben. Alternativ kann der Service Desk zentral Schritte zur Störungsbehebung, wie den Neustart eines Dienstes oder Servers durchführen. Auch externe Lieferanten, wie Hardwarehersteller oder spezialisierte Supportdienstleister können Lösungen bereitstellen. Die Support-Gruppe, welche die Lösung implementiert und getestet hat, gibt den Incident zurück an den Service Desk und dokumentiert die Lösung.

#### *Incident-Abschluss*

Der Service Desk überprüft in dieser Phase, ob die Lösung vollständig und wirksam ist und ob der Anwender damit einverstanden ist. Ebenso wird die Dokumentation der Incident-Bearbeitung geprüft, um sicherzustellen, dass ein historisch vollständiger Datensatz vorliegt. Zusammen mit den an der Bearbeitung des Incident beteiligten Support-Gruppen sollte geklärt werden, ob mit einem erneuten Auftreten einer gleichen oder vergleichbaren Störung zu rechnen ist. In diesem Fall sollte ein Problem Record erstellt werden, um den Problem Management Prozess einzuleiten. Abschließend kann der Incident formal als geschlossen gekennzeichnet werden.

Die folgenden Kennzahlen sind geeignet, die Effektivität und Effizienz des Incident Management Prozesses zu beurteilen:

- Gesamtzahl der Incidents je Betrachtungszeitraum
- Anzahl Incidents nach Status (Erfasst, In Arbeit, geschlossen)
- Umfang des aktuellen Rückstands der nicht abgeschlossenen Incidents
- Anteil der Major Incidents
- Zeitspanne von der Öffnung eines Incidents bis zur Schließung
- Durchschnittliche Kosten je Incident
- Anteil der falsch zugewiesenen bzw. falsch kategorisierten Incidents
- Anteil der Incidents, die direkt vom Service Desk abgeschlossen wurden

Mit der Kategorisierung des Incidents soll der zu bearbeitende Sachverhalt grob eingeordnet werden, wobei hiermit ggf. schon eine Ursachenanalyse verbunden ist. Dafür ist es erforderlich, das ein Kategorisierungsschema aufgestellt wird, das von der Hauptebene der Kategorien auf zwei bis drei Unterebenen verzweigt.

Je nachdem, auf welchem Wege der Incident den Service Desk erreicht, ist die Kategorisierung mehr oder weniger genau bzw. richtig.

Ein Endanwender, der die Kategorien über das Webportal erfasst, wird im Einzelnen die Kategorien nicht so zuordnen können, wie dies ein technisch-administrativer Mitarbeiter aus der IT-Abteilung kann. Daher sollte es demzufolge auf jeder Kategorieebene auch immer die Auswahl "unbekannt" geben.

Ein allgemein gültiges Kategorisierungsschema gibt es nicht, es sollte jeweils anhand der konkreten informationstechnischen Ausgestaltung der Organisation ausgerichtet sein. Die nachfolgend beschriebene Methodik für die Entwicklung eines Kategorisierungsschemas bietet sich an, wenn nur wenig Datenmaterial bezüglich der tatsächlichen oder zu erwartenden Incidents vorliegen und es organisatorisch möglich ist, das Kategorisierungssystem in der Praxis zu testen.

Zuerst sollte im Rahmen eines Brainstormings innerhalb der IT-Gruppe ermittelt werden, welche Incident-Themen besonders häufig auftreten. Die hierbei festgestellten

Themen bilden die oberste Kategorie. Zusätzlich sollte die Kategorie "Sonstige" hinzugefügt werden. Die so ermittelten Kategorien werden in das Service-Desk - Werkzeug eingepflegt, mit dem die Incidents erfasst werden. In der Testphase werden anschließend Incidents gesammelt.

Wenn etwa 30-50 Incidents je Kategorie vorhanden sind, folgt eine Analyse der aufgezeichneten Daten. So zeigt sich, ob es sich lohnt, tatsächlich bestimmte Kategorien auf oberster Ebene anzuordnen. Die Untersuchung der Kategorie "Sonstige" bringt Hinweise, welche weiteren Kategorien auf der obersten Ebene eingerichtet werden sollen. Außerdem kann durch Analyse der oberen Kategorien festgestellt werden, wie durch Aufspaltung aus diesen die Unterkategorien gebildet werden.

Diese Form der Analyse kann dann nach einer bestimmten Zeitphase wiederholt werden, um das Kategorisierungsschema auf seine Gebrauchstauglichkeit und Relevanz hin zu prüfen. Weitere Kategorien auf den einzelnen Ebenen können so hinzugefügt werden. Auch ein existierendes Kategorisierungsschema, das keine zufriedenstellenden Ergebnisse bringt, kann nach dem zuvor beschriebenen Ansatz analysiert und angepasst werden.

Falls das Kategorisierungsschema nicht mit dieser Methodik entwickelt und getestet werden kann - weil es z.B. in einer kleinen Organisation lange dauern würde, bis sich die Menge von 30-50 Incidents je Kategorie angesammelt hat, könnte auch ein sehr einfaches Schema, das sich an der Infrastruktur orientiert, verwendet werden.

Ein beispielhaftes Schema könnte wie folgt aussehen:

1. Hardware
  - a. Server
  - b. Arbeitsplatzrechner
  - c. Ausgabegeräte
2. Software
  - a. Betriebssystem
  - b. Standardsoftware
  - c. Eigenentwickelte Software
3. Netzwerk

- a. LAN
- b. WLAN
- c. Internet

### **3.4 Request Fulfilment**

Das Request Fulfilment ist ein Prozess, der sich mit der Bearbeitung von Anwenderanfragen aller Art beschäftigt, die sich nicht auf Störungen und Beeinträchtigungen des Geschäftsbetriebs beziehen. Diese werden in der ITIL als Service Request bezeichnet. Sie unterscheiden sich von Incidents dadurch, dass sie in der Regel geplant werden können, während Incidents Ereignisse sind, die ungeplant auftreten.

Auf diesem Weg können Anwender Standarddienste und -leistungen von der IT-Organisation beziehen, für die ein definierter Genehmigungsprozess existiert. Die verfügbaren Leistungen und Informationen, die Anwender abrufen können, werden mit dem Kunden innerhalb der SLA vereinbart und in einem Service-Katalog an die Anwender kommuniziert.

Die Produktivität der Anwender in der Organisation lässt sich durch die Bereitstellung des Request Fulfilment-Prozesses verbessern und Verwaltungsaufwand für Bereitstellung von Diensten und Leistungen kann reduziert werden.

Häufig handelt es sich um kleinere Änderungswünsche - sog. Changes, die häufig nachgefragt werden, aber in der Umsetzung geringe Kosten und geringes Risiko - technischer oder organisatorischer Art - bedeuten. Aufgrund dieser Eigenschaften wird daher in der ITIL empfohlen, diese getrennt von den Incident Management- und Change Management-Prozessen zu bearbeiten. Dennoch muss die Organisation zuvor im Einzelnen festlegen, wenn welcher Management-Prozess ausgelöst werden muss.

Beispiele für Service Requests sind Anfragen hinsichtlich Passwortrücksetzung, Anträge auf Installation einer benötigten Software oder der physische Umzug von Arbeitsplatzcomputern, aber auch Auskunftsanfragen.

Es ist sinnvoll, den Aufgabenbereich des Service Desk so zu erweitern, dass dieser auch die Service Requests als solche bearbeitet.

Eine Vielzahl von konkreten Service Request - Typen tritt immer wieder auf, weshalb für diese sog. Request Models hinterlegt werden sollen. Sie definieren, vergleichbar zu den Incident-Modellen, die Schritte für eine konsistente und SLA-adäquate Bearbeitung (vgl. Cannon/Hinrichs (2007); S. 64 f.; Beims (2010) 151 f.).

Die folgenden Prozessaktivitäten kennzeichnen das Request Fulfilment (vgl. Cannon/Hinrichs (2007); S. 65 ff.; Beims (2010) 152 ff.):

#### *Menüauswahl*

Anwender wählen eine definierte Standard-Leistung aus dem Service-Katalog aus und kommunizieren diesen Wunsch an den Service Desk, wodurch der Service Request ausgelöst wird. Die Auswahl dieser Leistungen kann durch die Anwender auch über eine Menüsteuerung in einem Webformular erfolgen und an den Service Desk übermittelt werden. Dabei sollte vom Anwender bzw. Kunden festgelegt werden, bis wann der Abschluss des Service Request erwartet wird, also die Leistung zur Verfügung stehen sollte.

#### *Finanzielle Genehmigung*

Die meisten Service Requests verursachen Kosten, weshalb sichergestellt werden muss, dass diese auch in Rechnung gestellt werden können und ausgeglichen werden. Die zu erwartenden Kosten müssen zunächst ermittelt werden. Anschließend soll die Freigabe von einem dazu berechtigten fachlichen Verantwortlichen eingeholt werden, nach Möglichkeit über einen Workflow-Prozess.

#### *Weitere Genehmigungen*

Auch Genehmigungen, die sich auf die Einhaltung organisationsinterner oder gesetzlicher Vorschriften beziehen, müssen von den verantwortlichen Mitarbeitern eingeholt werden.

#### *Ausführung*

Nach den Genehmigungen kann die Ausführung in die Wege geleitet werden. Einfache Anfragen werden direkt von Mitarbeitern des Service Desk bearbeitet. Auch die Weitergabe des Service Request zur Bearbeitung an andere Support-Gruppen ist je nach Anfrage auch möglich. Der Service Desk behält jedoch die Verantwortung für Überwachung und Steuerung des Service Request und informiert die Anwender bzw. Kunden.

### *Abschluss*

Falls andere Support-Gruppen den Service Request bearbeitet haben, geben diese nach Beendigung ihrer Maßnahmen den Service Request zurück an den Service Desk. Der Service Desk schließt den Service Request unter Berücksichtigung der Tätigkeiten ab, wie sie auch für den Abschluss von Incident-Vorgängen vorgesehen sind und stellt sicher, dass der Anwender die Ausführung akzeptiert. Die Kostenverrechnung bzw. Rechnungsstellung wird veranlasst.

Die folgenden Kennzahlen sind für die Beurteilung von Effektivität und Effizienz des Request Fulfilment geeignet:

- Anzahl der Service Requests im Betrachtungszeitraum
- Anzahl Service Requests nach Status (Erfasst, In Arbeit, geschlossen)
- Umfang des aktuellen Rückstands der nicht abgeschlossenen Service Requests
- Durchschnittliche Bearbeitungszeit eines Service Requests
- Durchschnittliche Kosten eines Service Requests nach Typ

### **3.5 Problem Management**

Ein Problem im Sinne der ITIL ist die unbekannte Ursache eines oder mehrerer Incidents. Das Problem Management befasst sich als Prozess mit dem Lebenszyklus dieser Probleme. Ziel ist die Vermeidung von wiederholt auftretenden Incidents und der Reduzierung von Auswirkungen der nicht vermeidbaren Incidents.

Zu den Aktivitäten des Problem Management gehört es, die Ursachen von Incidents aufzudecken. Das Problem Management sorgt dafür, dass Maßnahmen zur dauerhaften Beseitigung der Probleme durch Steuerungsprozesse wie das Change Management und das Release Management implementiert werden.

Weiterhin umfassen die Aufgaben des Problem Managements die Administration von Informationen zu Problemen, zu Workarounds sowie zu Lösungen. Dies hilft, Anzahl und Auswirkungen von Incidents über den Zeitverlauf zu verringern. Zu diesem Zweck werden Wissensdatenbanken und eine Datenbank der bekannten Fehler und zugehöriger Workarounds, die sog. Known Errors Datenbank gepflegt.



Bei Workarounds handelt es sich um Maßnahmen, welche die Auswirkungen von Incidents oder Problemen reduzieren sollen, solange es keine dauerhafte abschließende Lösung dafür gibt.

Das Problem Management steht in enger Beziehung zum Incident Management und kann gemeinsame Schemata zur Kategorisierung, Priorisierung und Auswirkungsabschätzung verwenden. Auch die Known Error Datenbank steht dem Incident Management zur Verfügung, um schnell und effektiv Incidents bearbeiten zu können.

Weitere Schnittstellen bestehen zu fast allen anderen der in den ITIL-Publikationen beschriebenen Management-Prozesse. Beispielhaft seien hier das Configuration Management, das Release and Deployment Management und das Service Level Management genannt (vgl. Cannon/Hinrichs (2007); S. 67 f.; Beims (2010) 154 f.).

Zwei wesentliche Hauptströmungen kennzeichnen das Problem Management:

Proaktives Problem Management zielt auf die frühzeitige Identifikation von Schwachstellen und die Vermeidung zukünftiger Probleme ab. Es ist damit im Grundsatz ein Gedanke des Continual Service Improvement und wird in der entsprechenden ITIL-Publikation behandelt.

Reaktives Problem Management ist mit Identifikation, Analyse und Beseitigung von Problemen ein Kernprozess der Service Operation und besteht aus den folgenden Aktivitäten (vgl. Cannon/Hinrichs (2007); S. 68 ff.; Beims (2010) 156 ff.):

#### *Problem-Erkennung*

Die Erkennung von Problemen kann über mehrere Wege stattfinden. Möglich ist, dass der Service Desk einen Incident zwar gelöst hat, die Ursache aber unbekannt ist und davon ausgegangen werden muss, dass sich Incidents aufgrund der gleichen Ursache wiederholen. Weiterhin können Support-Gruppen bei der Analyse von Incidents zu dem Ergebnis kommen, dass diesen eine oder mehrere unbekannte Ursachen zugrunde liegen. Auch Hardware-Hersteller können Informationen zu Problemen bereitstellen, die gelöst werden müssen.

#### *Problem-Erfassung*

In diesem Schritt werden die detaillierten relevanten Informationen zu einem Problem in einem Datensatz angelegt, der während der Bearbeitung des Problems entsprechend

aktualisiert wird. Wichtig ist außerdem eine Verknüpfung zwischen Problem-Datensatz und Incident-Datensatz, der den Prozess ausgelöst hat.

#### *Problem-Kategorisierung*

Für die Kategorisierung sollte nach Möglichkeit das gleiche Kategorisierungsschema wie für die Incident-Kategorisierung verwendet werden, womit auch die Zuordnung von Mitarbeitern mit dem entsprechenden Wissen verbunden ist.

#### *Problem-Priorisierung*

Die Priorisierung dient unter Berücksichtigung von Häufigkeit und Auswirkungen der zugrundeliegenden Incidents dazu, die Kapazitäten und Zeitfenster für die Bearbeitung des Problems auszuwählen. Die Priorisierung erfolgt analog zur Codierungsmatrix, wie sie auch für die Priorisierung von Incidents vorgeschlagen wird.

#### *Problem-Untersuchung und -Diagnose*

Mit verschiedenen Techniken und Methoden wird versucht, die Ursache für das zu bearbeitende Problem zu ermitteln. Die konkreten Möglichkeiten hängen dabei auch von Schweregrad, den Auswirkungen und den zur Verfügung stehenden Kapazitäten ab. Neben anderen Techniken kommt die Anwendung von chronologischen Analysen, Brainstorming-Methoden oder Erstellung von Ishikwa-Diagrammen in Frage.

#### *Erstellen eines Known Error-Datensatzes mit Workaround*

Mit der Bereitstellung eines Workarounds kann das Problem vorübergehend und zeitlich begrenzt umgangen werden. Dennoch muss weiter an einer dauerhaften Lösung gearbeitet werden. Wenn ein Workaround verfügbar ist, bleibt der Problem-Datensatz weiterhin geöffnet. Die Verfügbarkeit eines Workarounds wird in der Known Error-Datenbank dokumentiert.

#### *Problem-Lösung*

Wird ein Lösungsansatz gefunden, kann dieser zur dauerhaften Behebung des Problems implementiert werden. Es muss sichergestellt werden, dass durch diese Lösung keine anderen Services und Systeme in ihrer Stabilität gefährdet werden. Bei funktionalen Änderungen ist es zumeist erforderlich, diese mittels eines Request for Change über das Change Management zu realisieren. Somit kann die Lösung erst eingesetzt werden, wenn diese dort genehmigt und freigegeben wurde.

Es gibt weiterhin Problem-Fälle, in denen die Realisierung einer dauerhaften Lösung aus Gründen der Wirtschaftlichkeit nicht gerechtfertigt werden kann. Der Problem - Datensatz wird dann nicht geschlossen, ein Workaround muss im zugehörigen Known Error-Datensatz jedoch unbedingt dokumentiert werden.

#### *Problem-Abschluss*

Die Aufzeichnungen bezüglich der Aktivitäten zur Lösung des Problems sollten abschließend auf Vollständigkeit geprüft werden. Wenn die Problemlösung aktiv ist, kann der Problem-Datensatz sowie der oder die verknüpften Incident-Datensätze formal als geschlossen gekennzeichnet werden. Wichtig ist außerdem die Aktualisierung des Known Error-Datensatzes, um zu kennzeichnen, dass eine dauerhafte Lösung bereitgestellt wurde.

#### *Nachbetrachtung von schwerwiegenden Problemen*

Sofern der Prozess ein schwerwiegendes Problem, ein sog. Major Problem bearbeitet hat, erfolgt eine Nachbetrachtung. Hierbei soll festgestellt werden, wie Problemlösungsfähigkeiten verbessert werden können und das erneute Auftreten vergleichbarer Major Problems verhindert werden kann. Die Prozessvereinbarungen grenzen dabei die Major Problems von den Problems ab.

Die Beurteilung von Effektivität und Effizienz des Problem Management kann durch die folgenden Kennzahlen ermöglicht werden:

- Gesamtzahl der im Betrachtungszeitraum erfassten Probleme
- Anteil der Problem-Lösungen, die innerhalb der Grenzen der SLA durchgeführt wurden
- Anzahl und Anteil der Probleme, bei denen die Ziellösungszeit überschritten wurde
- Bestand an noch nicht abgeschlossenen Problemen
- Durchschnittliche Kosten für die Bearbeitung eines Problems
- Anzahl der schwerwiegenden Probleme nach Status (Erfasst, In Arbeit, Geschlossen)

### 3.6 Access Management

Das Access Management ist ein Prozess, der die Rechte der Anwender zur Nutzung von IT-Services steuert. Dazu müssen Anwender korrekt identifiziert werden. Das Access Management unterstützt die Organisation im Management des geistigen Eigentums und ihrer Daten und berücksichtigt dabei die Aspekte Vertraulichkeit, Verfügbarkeit und Integrität. Anwender erhalten somit Zugriff auf die Dienste und Daten, die sie für die Erfüllung ihrer Aufgaben benötigen. Audits hinsichtlich der Daten- und Dienstnutzung werden erleichtert und im Fall von Missbrauch können Zugriffsrechte zentral und schnell zurückgezogen werden. Auch die Begriffe Berechtigungsmanagement oder Identitätsmanagement sind für den Access Management Prozess gebräuchlich.

Die Koordination und Steuerung des Access Management kann durch das IT-Betriebsmanagement oder bevorzugt durch den Service Desk abgebildet werden. Zur Initiierung des Prozesses können auch Services Requests über den Service Desk verwendet werden.

Für das Access Management werden die Konzepte Zugriff, Identität, Rechte und Service bzw. Servicegruppen verwendet.

Zugriff beschreibt den Umfang und Level von Servicefunktionalitäten oder Daten, die ein Anwender nutzen darf. Mit Hilfe der Identität kann ein Anwender von einem anderen Anwender unterschieden werden. Dies erfolgt über die Zuordnung von Attributen, wie Name, Kontaktdaten, Nummern von Ausweisdokumenten.

Rechte beziehen sich auf die konkreten Einstellungen, mit denen ein Anwender Zugang zu einem Service oder einer Servicegruppe hat. Typische Zugriffsebenen sind Lesen, Schreiben, Ausführen, Löschen.

Anwender nutzen meist mehrere Services und Anwender mit ähnlichen Aufgaben nutzen gleiche oder ähnliche Services. Um das Berechtigungsmanagement zu vereinfachen, erfolgt die Steuerung über Anwendergruppen und Servicegruppen (vgl. Cannon/Hinrichs (2007); S. 77 f.; Beims (2010) 160 f.).

Die folgenden Aktivitäten kennzeichnen den Prozess Access Management (vgl. Cannon/Hinrichs (2007); S. 78 f.; Beims (2010) 161 f.):

#### *Zugriffsanforderung*

Die Anforderung von Zugriffsrechten kann auf verschiedenen Wegen erfolgen. Dies kann beispielsweise über Personaladministrationssysteme erfolgen, wenn ein Mitarbeiter eingestellt wird. Auch Service Requests oder für diesen Zweck eingerichtete

Webformulare eignen sich hierfür. Der Servicekatalog beschreibt die Regeln für Anforderung von Zugriffsrechten.

### *Verifizierung*

Die Verifizierung stellt sicher, dass der anfragende Anwender die Person ist, die sie behauptet, zu sein. Dies kann über eine systemgestützte Abfrage von Benutzernamen und Passwort geschehen. Weiterhin wird geprüft, ob der Anwender berechtigt ist, die angefragten Zugriffsrechte zu erhalten. Hierzu muss die Rolle des Anwenders in der Organisation sowie die damit verbundenen Rechte betrachtet werden.

### *Rechteerteilung*

Den identifizierten und berechtigten Anwendern werden in diesem Schritt die Zugriffsrechte auf Basis der Rollen erteilt. Berücksichtigt werden müssen an dieser Stelle ggf. auftretende Rollenkonflikte. So ist es möglich, dass einem konkreten Anwender in der einen Rolle der Zugriff auf einen Service gewährt wird, in einer anderen Rolle wird der Zugriff auf den gleichen Service jedoch nicht gewährt. Hierfür müssen entsprechende Regeln vereinbart werden. Durch den Access Management-Prozess wird jedoch an dieser Stelle nicht entschieden, ob ein Zugriffsrecht erteilt wird. Stattdessen werden die Vorgaben umgesetzt, die auf der Grundlage der Unternehmensanforderungen in den Phasen Service Strategy und Service Design erstellt wurden.

### *Überwachen des Identitätsstatus*

Während der Zugehörigkeit des Anwenders zur Organisation können sich dessen Rollen ändern und damit auch die Services, auf die er zugreifen muss. Als Beispiele sollen hier Beförderungen, Tätigkeitswechsel oder Versetzungen genannt werden. In diesen Fällen muss das Access Management aktiv werden.

### *Protokollieren des Zugriffs*

Die Überwachung und Aufzeichnung des ordnungsgemäßen Gebrauchs der Zugriffsrechte der Anwender ist Kernbestandteil dieser Aktivität. Die dafür geeigneten technischen Mittel und Monitoring-Maßnahmen müssen in den Servicebetriebsprozessen berücksichtigt werden.

### *Rücknahme oder Einschränkung von Rechten*

Auch die Entziehung von Zugriffsrechten gehört zu den Aufgaben des Access Managements. Dies ist im Falle von Kündigungen von Mitarbeitern oder

Tätigkeitswechseln erforderlich. Wenn Anwender andere Zugriffsebenen benötigen oder geänderte Rollen einnehmen, werden ihre Rechte eingeschränkt.

Die folgenden Kennzahlen sind für die Beurteilung von Effektivität und Effizienz des Access Management - Prozesses geeignet:

- Anzahl der Zugriffsanforderungen je Betrachtungszeitraum
- Zugriffsgewährungen nach Arbeitsgruppen, Abteilungen und Services
- Anzahl von Incidents im Zusammenhang mit Zugriffsrechten

### **3.7 Service Desk**

#### **3.7.1 Der Service Desk als Single Point of Contact**

Der Service Desk ist die zentrale und einzige operative Anlauf- und Kommunikationsschnittstelle (Single Point of Contact, SPOC) gegenüber den Anwendern bzw. Kunden und eine Koordinationsstelle für IT-Organisationsstrukturen und IT-Prozesse. Er nimmt Wünsche, Anfragen und Störungsmeldungen entgegen und bildet damit Teile des Incident Management-Prozesses, des Request Management-Prozesses sowie des Access Management-Prozesses ab. Es handelt sich damit um eine Funktion im Sinne der ITIL und nicht um einen Prozess.

Die zuvor genannten Meldungen bzw. Anfragen erreichen den Service Desk über Telefonanrufe, Webportale oder automatisiert vom Infrastruktur-Monitoring (Infrastruktur-Events).

Ein gut strukturierter und organisierter Service Desk kann die Leistungsfähigkeit des IT-Bereichs herausstellen und deren Wahrnehmung als dienstleistungsorientierte Organisation stärken. Die Zufriedenheit der Kunden wird verbessert, Qualität und Geschwindigkeit der Bearbeitung von Kunden- und Anwenderanfragen wird optimiert. Die Bereitstellung eines Service Desk verbessert die Auslastung der Mitarbeiter des IT-Bereichs und führt außerdem zu höherer Produktivität der Mitarbeiter in den Kerngeschäftsfeldern, da diese sich auf ihre eigentliche Aufgabe konzentrieren können. Die IT-Infrastruktur unterliegt einer besseren Steuerung, die Häufigkeit negativer Einwirkungen auf die Kerngeschäftsprozesse können reduziert werden. (vgl. Cannon/Hinrichs (2007); S. 124 f.; Beims (2010) 163 f.):

Im Folgenden sollen die Ziele und Aufgaben des Service Desk festgehalten werden, die im weitesten Sinne der möglichst zügigen Wiederherstellung der Arbeitsfähigkeit der Anwender dienen (vgl. Cannon/Hinrichs (2007); S. 125 f.; Olbrich (2008) S. 18 f.):

- Entgegennahme, Dokumentation und Auswertung aller Incidents, Service Requests und Zugriffsanforderungen
- Bearbeitung der Incidents und Service Requests, die sich im Sinne eines First-Level-Supports lösen lassen
- Einschätzung und Weiterleitung von Incidents und Service Requests, die sich nicht innerhalb vereinbarter Fristen lösen lassen, an den Second-Level- und Third-Level-Support
- Koordination des Second-Level- und Third-Level-Support, Überwachung und Steuerung offener Incidents und Service Requests
- Regelmäßige Benachrichtigung der Anwender hinsichtlich ihrer noch nicht abschließend bearbeiteten Incidents und Service Requests
- Einhaltung der Service Level Agreements (SLA)
- Erstellen von Berichten für die Leitungsebene der IT-Organisation bzw. der Gesamtorganisation
- Ermittlung und Verbesserung der Anwender- und Kundenzufriedenheit durch Umfragen und Kontaktpflege

### **3.7.2 Klassifizierung von Service Desks**

Für die Struktur von Service Desks existieren drei typische Formen: lokal, zentralisiert und virtuell (vgl. Cannon/Hinrichs (2007); S. 125 f.).

Der lokale Service Desk ist örtlich nahe oder innerhalb der Gruppe der Anwender angesiedelt. Somit lässt sich durch die Präsenz eine schnelle und kundennahe Betreuung realisieren und die Kommunikation vereinfachen. Wird jedoch der Service Desk zur Betreuung von eher kleinen Standorten errichtet, kann dies dazu führen, dass das Service Desk-Personal nicht vollständig ausgelastet ist, obwohl es dennoch zur Entgegennahme von Störungsmeldungen bereitgehalten werden muss. Dies kann jedoch in Kauf genommen werden, wenn bestimmte Umstände, wie sprachliche oder kulturelle Unterschiede, Zeitverschiebungen oder besonders spezialisierte Anwendergruppen

diesen Ressourceneinsatz rechtfertigen. Allerdings wird durch diese dezentrale Struktur die Zusammenarbeit zwischen den jeweils lokalen Service Desks an den unterschiedlichen Standorten erschwert; Wissensaustausch findet nur in begrenzter Form statt. Auch müssen für jeden Standort die entsprechenden nachgelagerten Unterstützungsstellen bereitgehalten werden.

Ein zentraler Service Desk an einem Standort unterstützt mehrere Anwenderstandorte gleichzeitig. Eine höhere Effizienz wird dadurch erreicht, dass ein höheres Incident bzw. Service Request -Aufkommen von im Vergleich zu lokalen Service Desks insgesamt weniger Mitarbeitern bearbeitet wird; eine höhere Auslastung stellt sich somit ein.

Außerdem entsteht schneller eine größere Datenbasis von bearbeiteten Vorgängen, so dass mehr Routine im Umgang mit Incidents und Service Requests entwickelt wird. Eine kundennahe Betreuung wird mit zunehmender Größe schwieriger, der Administrationsaufwand für die Service Desk-Organisation nimmt zu. Dennoch kann es erforderlich sein, von Zeit zu Zeit auch Mitarbeiter an die Anwender-Standorte zu entsenden, wobei deren Einsatz aber vom zentralen Service Desk koordiniert wird.

Der virtuelle Service Desk ist physisch an mehreren Standorten präsent, verwendet jedoch das gleiche Werkzeug sowie eine gemeinsame Datenhaltung. Er vereint damit die Vorteile von zentralen und lokalen Service Desk-Strukturen. Für den Anwender wirkt diese Organisationsform wie ein zentralisierter Service Desk, der beispielsweise immer über eine einheitliche Rufnummer zu erreichen ist. Mit verstärktem Aufwand für Administration und technischen Ressourcen ist zu rechnen, auch wenn sich für den virtuellen Service Desk Potentiale wie Outsourcing und Offshoring ergeben. Kontinuierliche Servicequalität muss jedoch über alle physikalischen Standorte sichergestellt werden (vgl. Olbrich (2008) S. 21 ff.; Cannon/Hinrichs (2007); S. 125 ff.; Stych/Zeppenfeld (2008) S. 45 ff.).

### **3.7.3 Planung und Bereitstellung des Service Desk**

Der Service Desk soll über eine feste Rufnummer, über eine feste E-Mail-Adresse und über eine spezifische Kontaktseite innerhalb des Intranets der Organisation erreichbar sein. Allen IT-Anwendern müssen die Möglichkeiten zur Kontaktaufnahme mit dem Service Desk bekannt sein. Dies kann durch entsprechende Beschriftung von Telefonen und der Computer-Hardware vereinfacht werden. Auch innerhalb des Intranets sollten Hinweise zur Erreichbarkeit des Service Desks an häufig besuchten Seiten hervorgehoben platziert sein. Um im Falle von Störungen die Identifizierung



von betroffener Hardware zu erleichtern, ist es unbedingt erforderlich, diese mit lesbaren eindeutigen Attributen zu versehen. Dies kann z.B. eine Inventar-Nummer oder IP-Adresse sein, sofern diese statisch vergeben wird.

Als schwierig stellt sich die Planung der personellen Kapazität des Service Desk dar. Hierfür sind Prognosen und statistischen Analysen zu Anzahl und zu Art der Störungsbzw. Anfrageaufkommens erforderlich. Dabei bezieht sich die Analyse auch auf die Art der Kontaktaufnahme, da für synchrone Kommunikation wie Telefon oder Chat eine andere Planung vorgenommen werden muss als für asynchrone Kommunikation wie z.B. E-Mail. Es sollte sichergestellt werden, dass auch bei hohem Anrufaufkommen die Erreichbarkeit des Service Desk den Vereinbarungen der Service Level Agreements gerecht wird. Zu Spitzenzeiten sollten die Kapazitäten des Service Desk durch externe Dienstleister oder Second-Level-Mitarbeiter aufgestockt werden können (vgl. Cannon/Hinrichs (2007); S. 128 f.).

Die folgenden weiteren Faktoren beeinflussen die Planung und Konfiguration des Service Desks:

- Erwartungen der Anwender und Kunden
- Anforderung und Bedarf hinsichtlich der IT-Unterstützung der Geschäftsprozesse; dies bedeutet, dass auch die kritischen Geschäftsprozesse herausgestellt werden müssen
- Umfang, Struktur und Komplexität der unterstützten IT-Infrastruktur
- Anzahl und IT-Affinität von Kunden und Anwendern, denen der Service Desk zur Verfügung steht
- Typen von Incidents und Service Requests
- Grad der Spezialisierung und Kundenanpassung der von der IT-Organisation angebotenen Services und Dienstleistungen
- Zeitplanung der Service Desk - Abdeckung, ggf. mit Berücksichtigung von Vor-Ort-Betreuung durch Mitarbeiter
- Technische Ausstattung des Service Desk mit Kommunikationsmitteln und Softwarewerkzeugen
- Fähigkeiten und Ausbildungsstand der Service Desk-Mitarbeiter

Die Anforderungen an den Fähigkeitsstand und die Ausbildung der Service Desk-Mitarbeiter können sehr unterschiedlich sein und hängen davon, welches Ziel, insbesondere hinsichtlich der Lösungszeit, der Service Desk verfolgt. Dabei besteht zwischen den Antwort- und Lösungszeitzielen und den Kosten ein direkter Zusammenhang; je kürzer diese Zeiten sein sollen, umso höher sind die durch höheren Ressourceneinsatz zu erwartenden Kosten.

Wichtig ist außerdem die kontinuierliche Weiterbildung durch interne und externe Schulungen, sowohl in Bezug auf die eingesetzten Technologien als auch hinsichtlich der nicht-fachlichen Fähigkeiten und der Kommunikationsfähigkeiten. (vgl. Cannon/Hinrichs (2007); S. 129 f.).

In Bezug auf das Qualifikationsniveau des Service Desk kann zwischen drei Arten unterschieden werden.

Beim sogenannten *Unskilled Service Desk* beschränken sich Mitarbeiter darauf, Incidents und Service Requests entgegenzunehmen, zu erfassen und nur bei einfachen Fällen eine Erstlösung anzustreben. Aufwendigere Vorgänge werden an die nächsten Ebenen der Support-Struktur, wie Second-Level und Third-Level-Support weitergegeben.

Der *Skilled Service Desk* verfügt darüber hinaus über zusätzlich Erstlösungskompetenz und kann somit mehr Fälle selbst lösen, ohne diese weitergeben zu müssen.

Wesentlich mehr Wissen und Erfahrung benötigen Mitarbeiter, wenn deren Einsatz für den Typ *Expert Service Desk* vorgesehen ist. Denn für diesen ist neben einer umfangreichen Erstlösungskompetenz auch die dauerhafte Behebung, d. h. eine Problemlösung der Vorfälle vorgesehen (vgl. Olbrich (2008) S. 24).

#### **3.7.4 Technische Ausstattung**

ITIL empfiehlt für die Funktion Service Desk verschiedene unterstützende Werkzeuge, damit die Mitarbeiter ihre Rolle vollumfänglich ausfüllen können.

Die meisten Incidents und Service Requests werden dem Service Desk über Anrufe durch die Anwender mitgeteilt. Eine zuverlässige und leistungsfähige Ausstattung der Telefonarbeitsplätze, die auch über Headsets verfügen sollten, ist daher unerlässlich.

Der Service Desk sollte organisationsweit über eine einheitliche Rufnummer erreicht werden können. Anrufer könnten hierbei mittels entsprechenden Optionsansagen über die Telefontastatur weitergeleitet werden, um gleich den richtigen Ansprechpartner für ihr Anliegen zu erreichen. Die Menüführung sollte hierbei klar und eindeutig sein, so dass der Anrufer mit einiger Sicherheit die richtige Auswahl treffen wird.

Es ist außerdem zweckmäßig, wenn durch die Verbindung von Telefonanlage und Arbeitsplatzcomputer des Service Desk-Mitarbeiters (Computer Telephony Integration, CTI) der Anrufer mit Hilfe einer Datenbank erkannt wird. So können bei der Aufnahme von Incidents und Service Requests die Kontaktdaten des Anrufers übernommen werden. Auch Rückfragen der Anrufer zu bereits im System erfassten Vorgängen lassen sich beschleunigt abwickeln, da auch hier unmittelbar der entsprechende Datensatz auf dem Arbeitsplatzcomputer des Service Desk-Mitarbeiters angezeigt wird.

Um Leistungsfähigkeit der Telefonie-Unterstützung des Service Desk beurteilen zu können und außerdem den Bedarf planen zu können, ist es erforderlich, die folgenden Messwerte zu dokumentieren - möglichst unterstützt durch die CTI - Software:

- Anzahl der eingehenden Anrufe und ggf. auf die einzelnen Optionen (s.o.) entfallenden Anteile
- Annahmezeiten bzw. Warteschleifenzeiten
- Anzahl nicht angenommener Anrufe
- Anzahl angenommener Anrufe je einzelnen Service Desk-Mitarbeiter - sofern betrieblich und rechtlich zulässig
- Durchschnittliche Gesprächsdauer je Anruf

(vgl. Cannon/Hinrichs (2007); S. 181)

Die Werkzeuge bzw. Softwarekomponenten des Service Desk sollten so weit wie möglich ineinander integriert sein, wobei das Configuration Management System (CMS) die Kernkomponente bildet.

Diese sollte Zugriff auf eine Datenbank mit bereits bekannten Fehlern und Problemen, die sogenannte Known Error-Datenbank (KEDB) haben. Dabei besteht eine direkte Verknüpfung der Configuration Items mit bereits dokumentierten bekannten Fehlern.

Die KEDB hält Details zu Lösungen bereit, mit denen bereits zuvor aufgetretene Incidents und Probleme behoben wurden. Die einzelnen Einträge der KEDB müssen über ein Kategorisierungssystem bzw. eine Verschlagwortung durchsuchbar gemacht werden. Im Falle von Incidents / Problemen müssen die bekannten Fehler schnell durchsucht werden können, um Überschneidungen aufzudecken.

Neben durchgehend laufenden Monitoring-Werkzeugen müssen dem Service Desk auch Diagnose-Werkzeuge zur Verfügung stehen, um die Ursachen von Ausfällen im Einzelfall zu ermitteln. Hierzu eignen sich Skripte, die unter Verwendung der jeweils eingesetzten Technologien und Betriebssysteme automatisiert Abfragen vornehmen und Messungen durchführen. Die Eingrenzung von Incidents sollte somit erleichtert und beschleunigt werden (vgl. Cannon/Hinrichs (2007); S. 181 f.).

### **3.7.5 Leistungsfähigkeit und Kundenzufriedenheit**

Zum Kerngedanken der ITIL gehört es, dass die Leistungsfähigkeit aller Prozesse und Funktion des IT-Service Managements kontinuierlich gemessen werden. Somit sind auch für den Service Desk Kennzahlen zu definieren, durch deren Interpretation Effizienz, Effektivität sowie Reifegrad festgestellt und Verbesserungspotential aufgedeckt werden kann.

Beim Einsatz von Kennzahlen muss darauf geachtet werden, dass die Messergebnisse nicht in falsche Zusammenhänge gebracht werden bzw. falsche Schlussfolgerungen gezogen werden. Die wesentlichen Gütekriterien der Messgrößen, wie Objektivität, Reliabilität und Validität sind zwingend zu gewährleisten.

Beispielsweise lässt sich aus dem Zuwachs bei der Anzahl der bearbeiteten Störungen nicht unmittelbar eine gesteigerte Effizienz des Service Desk ableiten. Die statistische Auswertung und Interpretation muss alle begleitenden Umstände berücksichtigen und auch Messungen aus früheren Zeiträumen zum Vergleich heranziehen.

Die folgenden Kennzahlen sind geeignet für die Leistungsmessung und Steuerung des Service Desk (vgl. Cannon/Hinrichs (2007) S. 133):

- Erstlösungsquote: Anteil der Incident-Meldungen, die ohne Weitergabe des Vorgangs an andere Support-Gruppen gelöst werden, dabei Unterteilung auf die verschiedenen Kommunikationswege, wie Telefon, E-Mail usw.
- Durchschnittliche Lösungszeit von Incidents: Messung und Mittelwertbildung des Zeitraums zwischen Öffnung und Abschluss eines Incidents; hierbei Unterteilung in Incidents, die ohne Eskalation vom First-Level-Support bearbeitet wurden, und solche, die an nachgelagerte Support-Gruppen weitergegeben wurden
- Durchschnittskosten für die Bearbeitung eines Incidents: Anfallende Gesamtkosten des Service Desk geteilt durch die Anzahl der entgegen genommenen Incidents
- Anteil der Incidents, die innerhalb der in den Service Level Agreements vereinbarten Zielzeiten bearbeitet und abgeschlossen wurden
- Anzahl der eingehenden Incidents mit Zuordnung auf definierte Tages- und Wochenabschnitte, um eine Planung der vorzuhaltenden Personalkapazität zu ermöglichen

Zusätzlich zu den oben genannten harten Kennzahlen sollten sich die Verantwortlichen des Service Desk auch dafür interessieren, wie zufrieden Kunden und Anwender mit der Leistung des Service Desk sind. Dies kann über verschieden Formen von Umfragen realisiert werden.

Eine mögliche Realisierungsform wäre eine Telefonbefragung, bei der ein bestimmter Anteil der Anwender zeitnah nach der Lösung ihrer gemeldeten Incidents kontaktiert wird. Ein mit dem betreffenden Incident zuvor nicht befasster Service Desk-Mitarbeiter oder ein Gruppenleiter stellt dem Anwender etwa 4-6 Fragen im Zusammenhang mit der von ihm gemeldeten Störung. Die Fragen sollten so konzipiert sein, dass der Anwender in der Lage ist, diese zu beantworten.

Diese können sich beispielweise auf die Zufriedenheit mit der erzielten Lösung oder auf die Kommunikationskompetenz des Service Desk-Mitarbeiters beziehen, der den Incident bearbeitet hat. Sinnvoll ist hier die Verwendung von beispielsweise 5-stufigen Skalen, bei denen z.B. die Werte 1 für "sehr zufrieden" bis 5 für "Überhaupt nicht zufrieden" zur Auswahl stehen. Dies vereinfacht die statistische Auswertung der Umfragen. Drücken die Ergebnisse Unzufriedenheit mit dem Service Desk aus, sollten die Verantwortlichen Maßnahmen zur Verbesserung der Kunden- bzw. Anwender-zufriedenheit veranlassen.

Weitere mögliche Umfrageformen sind die persönliche Befragung, Gruppenbefragungen sowie Umfragen über Briefpost, E-Mail oder Webformulare (vgl. Cannon/Hinrichs (2007) S. 133).

### **3.7.6 Service Desk und Help Desk in der Gegenüberstellung**

Das Aufgabenfeld eines Service Desk ist, wie zuvor bereits beschrieben sehr umfangreich und ist damit erheblich breiter als das eines Help Desks, der eher auf die Leistung von Hilfestellung ausgelegt ist.

Der Service Desk bildet die zentrale Schnittstelle zwischen Anwendern bzw. Kunden und der IT-Organisation. Es bietet neben Erstunterstützung, Störungslösung, Annahme von Anfragen und Beschwerden weitere Dienstleistungen, die im besten Fall in einem Leistungskatalog dokumentiert sind. Der Service Desk ist eher als Leitstelle zu verstehen, welche Daten und Fakten zur Störung abfragt um dann zentralisiert Maßnahmen zur Entstörung zu koordinieren und teils auch durchzuführen.

Jedoch sind kombinierte Formen, also Help Desks, die auch Service Desk-Funktionalitäten anbieten, häufig in der Praxis anzutreffen.

Auch ist es typisch, dass der Help Desk aus dem Unternehmen ausgelagert ist bzw. als externe Leistung eingekauft wird und somit mehrere Kunden bedient. Er kann daher nicht zwingend vertieftes Wissen bezüglich Prozessen und Kerngeschäften des Kunden bereithalten (vgl. Wallner/Rüdiger (2008), S. 16 f.).

Die Tabelle 3.1 liefert eine Gegenüberstellung von Service Desk und Help Desk anhand verschiedener Kriterien.

**Tab. 3.1:** Help Desk und Service Desk in der Gegenüberstellung (vgl. Wallner/Rüdiger (2008), S. 17).

<b>Kriterium</b>	<b>Service Desk</b>	<b>Help Desk</b>
Ausrichtung zum Kunden	Ausschließliche und zentrale Kontaktstelle (Single Point of Contact, SPOC)	Nicht zwingend die zentrale Kontaktstelle
Unternehmensaufgabe	Verbindung zwischen IT und Kerngeschäft bzw. zentrale Schnittstelle zwischen Anwendern bzw. Kunden und der IT-Organisation	Auf IT-Support ausgerichtet
Geschäftsgrundlage	Klar formulierte Service Level Agreements (SLA) sowie regelmäßige Revisionen der SLA	Klar formulierte SLA
Kenntnis des Kunden	Umfangreiche Kenntnis der Prozesse, Funktionen und Produkte des Kunden	Teilkennntnisse des Kerngeschäfts
Qualitätsmanagement	Qualitätsmanagement durch Berichtswesen und Qualitätssicherungsaktivitäten	Berichtswesen
Messgrößen	Key Performance Indicators (KPI)	Keine oder wenig ausgeprägte KPI-Kultur
Kommunikation	Sprachen nach Bedarf des Kunden	Sprachen nach Bedarf des Kunden
Norm / Richtlinie	ITIL	Umsetzung von ITIL-Ausschnitten bzw. Mischformen aus Help Desk und Service Desk
Aktivitäten	Incident Management, Access Management, Service Requests, Problem Management	Häufig Konzentration auf Trouble Ticketing
Softwareunterstützung	Integriertes Softwarewerkzeug, nach Möglichkeit über alle ITIL-Prozesse	Einzelne Softwarewerkzeuge nach je nach angebotenen Diensten

## 4 Methodische Überlegungen

### 4.1 Das Fachkonzept

Kernaufgabe dieser Arbeit ist die Entwicklung eines Fachkonzepts als Vorarbeit für eine softwaretechnische Umsetzung des Inventar- und Service Desk-Managements. Deshalb soll an dieser Stelle eine kurze Begriffsklärung eingefügt werden.

Das Fachkonzept beschreibt die Spezifikation der relevanten fachlichen Anforderungen an eine Softwareanwendung. Die Spezifikation des Fachkonzepts wird in unterschiedlichen Sichten betrachtet. Dies sind einerseits die funktionalen, dynamischen Aspekte und andererseits die strukturellen Aspekte, die Datenstrukturen. Auch die Gestaltung der Organisationsebene, wie das Aufbauorganisationsmodell, können in das Fachkonzept eingebunden werden.

Das Informationsmodell, das für das Fachkonzept erstellt wird, beinhaltet die Informationsobjekte. Diese Informationsobjekte werden zum einen im Gesamtzusammenhang, betrachtet, d.h. ihre Beziehungen zueinander. Weiterhin werden die Informationsobjekte im Detail beschrieben, wobei neben der Bedeutung des Informationsobjekts auch deren Eigenschaften formuliert werden (vgl. Alpar et al. (2008), S. 167 f.).

RAUTENSTRAUCH / SCHULZE definieren das Fachkonzept als eine "(semi-)formale, implementierungsunabhängige Beschreibung einer betriebswirtschaftlichen Konzeption" (Rautenstrauch/Schulze (2003), S.227).

Das Fachkonzept soll die Funktionalitäten und Fähigkeiten der zu entwickelnden Software beschreiben. Für die Formulierung der Anforderungen werden semantische Modelle unterschiedlichen Abstraktionsgrads verwendet. Die Modelle abstrahieren von allen technischen Aspekten der Realisierung und beschreiben die fachlichen Aspekte, die für das Verständnis der Interaktionen mit den Nutzern und die Umsetzung der Anforderungen benötigt werden. Als Träger des betriebswirtschaftlichen Anwendungskonzepts ist es langfristig angelegt.

Es schließt sich der Systementwurf an, bei dem das Fachkonzept zum DV-Konzept konkretisiert wird. Das DV-Konzept umfasst Aspekte der technischen Realisierung und dient damit als Grundlage für die Implementation (vgl. Laudon et al. (2006), S. 578; Scheer (1998), S. 14 f.; Gadatsch (2008), S. 128).



## 4.2 Architektur integrierter Informationssysteme

Mit der Architektur integrierter Informationssysteme (ARIS) wurde von SCHEER eine Methodik für die ganzheitliche Betrachtung der Geschäftsprozesse entwickelt, die inzwischen das Niveau eines Industriestandards erreicht hat (vgl. Laudon et al. (2006); S. 582 f.).

Es werden fünf Sichten für die Betrachtung eines Informationssystems unterschieden: Organisationssicht, Funktionssicht, Datensicht, Leistungssicht und Steuerungssicht. Innerhalb jeder Sicht existieren die drei Beschreibungsebenen Fachkonzept, DV-Konzept und Implementierung.

Die Organisationssicht beschreibt die Aufbauorganisation mit den Aufgabenträgern der zu modellierenden Organisation. Dazu werden mit Hilfe von Organigrammen Standorte, Organisationseinheiten und Rollen mit ihren Beziehungen untereinander dargestellt.

Mit Hilfe der Funktionssicht werden die Vorgänge, welche die Input-Leistungen zu Output-Leistungen transformieren, zusammengefasst. Funktion unterstützen Ziele und werden durch diese gesteuert. Mit Hilfe von Funktionsbäumen erfolgt auf unterschiedlichen Aggregationsstufen die Darstellung der Funktionen und ihrer Beziehungen untereinander.

In der Datensicht werden die relevanten Informationsobjekte mit ihren Eigenschaften und Beziehungen zueinander beschrieben. Zu diesem Zweck hat sich das von CHEN entwickelte Entity-Relationship-Diagramm als Defacto-Standard etabliert.

Die Leistungssicht beschreibt die Sach- und Dienstleistungen der Organisation, welche die Ergebnisse von Prozessen sind. Für die Leistungssicht werden Produktmodelle verwendet.

Die Steuerungssicht integriert die vier Basissichten Organisationssicht, Funktionssicht, Datensicht und Leistungssicht. Prozesse werden innerhalb der ARIS-Methode als Abfolgen von Funktionen verstanden. Diese Abfolgen von Funktionen werden ereignisorientiert modelliert. Die Ausführung von Funktionen wird durch Ereignisse ausgelöst und kann wiederum selbst Ereignisse auslösen. So lassen sich Ketten von Funktionsausführungen darstellen, die mit Hilfe von "und" sowie "oder" - Verknüpfungen auch komplexe Geschäftsprozesse in der Organisation beschreiben. Diese Form von Diagramm wird als Ereignisgesteuerte Prozesskette (EPK) bezeichnet (vgl. Laudon et al. (2006); S. 582 f.; Gadatsch (2008), S. 130 f.; Scheer (2002), S. 32 ff.).

### 4.3 Grundsätze ordnungsmäßiger Modellierung

Bei der Modellierung komplexer Sachverhalte von Organisationen können naturgemäß mehrere die Realität zutreffend abbildende Modelle entstehen. Zur Steigerung der Qualität von Modellen eines Fachkonzepts wurden von BECKER ET AL. die Grundsätze ordnungsmäßiger Modellierung aufgestellt. Sie stellen Gestaltungsempfehlungen dar, mit denen die Modelle bedarfsgerecht und unter Reduzierung der Vielfalt der Modellvarianten erstellt werden können. Außerdem kann somit die Vergleichbarkeit und Integrationsfähigkeit der Modelle erleichtert werden.

Der *Grundsatz der Richtigkeit* umfasst die syntaktische sowie semantische Richtigkeit. Die syntaktische Richtigkeit beinhaltet die Vollständigkeit und Konsistenz des Modells. Die Vollständigkeit wird angenommen, wenn alle als erforderlich geltenden methodischen Konstrukte des verwendeten Metamodells tatsächlich vorhanden sind. Konsistenz wird angenommen, wenn alle im Modell verwendeten Objekte und Notationen im Metamodell definiert sind. Semantische Richtigkeit erfordert die strukturerhaltende und verhaltenstreue Abbildung sowie semantische Konsistenz und Aktualität des Modells gegenüber der Realität.

Der *Grundsatz der Relevanz* fordert, dass alle zu modellierenden Sachverhalte aus dem Umfang der realen Sachverhalte berücksichtigt werden. Durch Zerlegung in Teilmodelle kann eine Relevanzanalyse vorgenommen werden. Die Relevanz umfasst die modellierten Objekte, die Modellierungsmethode und die Anwendung der Modellierungsmethode.

Der *Grundsatz der Wirtschaftlichkeit* fordert, dass Erstellungsaufwand, Verwendungsdauer, Beständigkeit und Flexibilität des Modells in einem betriebswirtschaftlich akzeptablen Verhältnis zum Nutzen des Modells stehen. Wirtschaftliche Modellierung kann erreicht werden durch Nutzung von Referenzmodellen und die Wiederverwendbarkeit von Bestandteilen des Modells.

Der *Grundsatz der Klarheit* fordert, dass allen denkbaren Betrachtern bzw. Nutzern des Modells dieses klar erscheint. Klarheit umfasst vor allem Kriterien der grafischen Darstellung, wie Strukturiertheit, intuitive Zugänglichkeit, Übersichtlichkeit und Lesbarkeit.

Der *Grundsatz der Vergleichbarkeit* ist sichergestellt, wenn die Metamodelle, die verwendet werden, ineinander überführt werden können. Außerdem ist dies durch die Berücksichtigung von Konventionen bei Bezeichnern und Modellkonstrukten zu erreichen.

Der *Grundsatz des systematischen Aufbaus* fordert, dass Teilmodelle sowohl innerhalb einer Sicht als auch sichtenübergreifend integriert werden können. Die Sichtenintegration erfolgt beispielsweise in ARIS in der Steuerungssicht durch die Prozessmodelle. Die Prozessmodelle bilden damit ein sichtenübergreifendes Metamodell, das den systematischen Aufbau gewährleisten kann.

(vgl. Becker et al. (1995); S. 435 ff.; Rautenstrauch/Schulze (2003); S. 253 ff.)

## **5 Fachkonzept für ein integriertes Service Desk- und Inventarmanagement**

### **5.1 Organisationsmodell**

Das Organisationsmodell für die Aufbauorganisation einer kleinen bzw. mittleren IT-Organisation wird in Abbildung 5.1 dargestellt. Als Modelltyp wird das Organigramm verwendet.

Die Organisationseinheit (OE) IT-Organisation verfügt über mehrere untergeordnete OE und wird von der Rolle Leiter IT fachlich und disziplinarisch geführt.

Die OE Service Desk wird von der Rolle Leiter Service Desk fachlich und disziplinarisch geführt. Personen der Rolle Mitarbeiter Service Desk nehmen Service Requests und Incidents entgegen. Incidents werden im Rahmen des First-Level-Supports von den Mitarbeitern des Service Desk bearbeitet. Funktionale Eskalation zum Second-Level-Support erfolgt zu den Fachgruppen Technical Management, Application Management und IT Operations Management, die hierfür erfahrene Spezialisten bereitstellen.

Die hierarchische Eskalation von Incidents in der Funktion Service Desk erfolgt in Richtung des Incident Managers und bei Bedarf an den Leiter Service Desk.

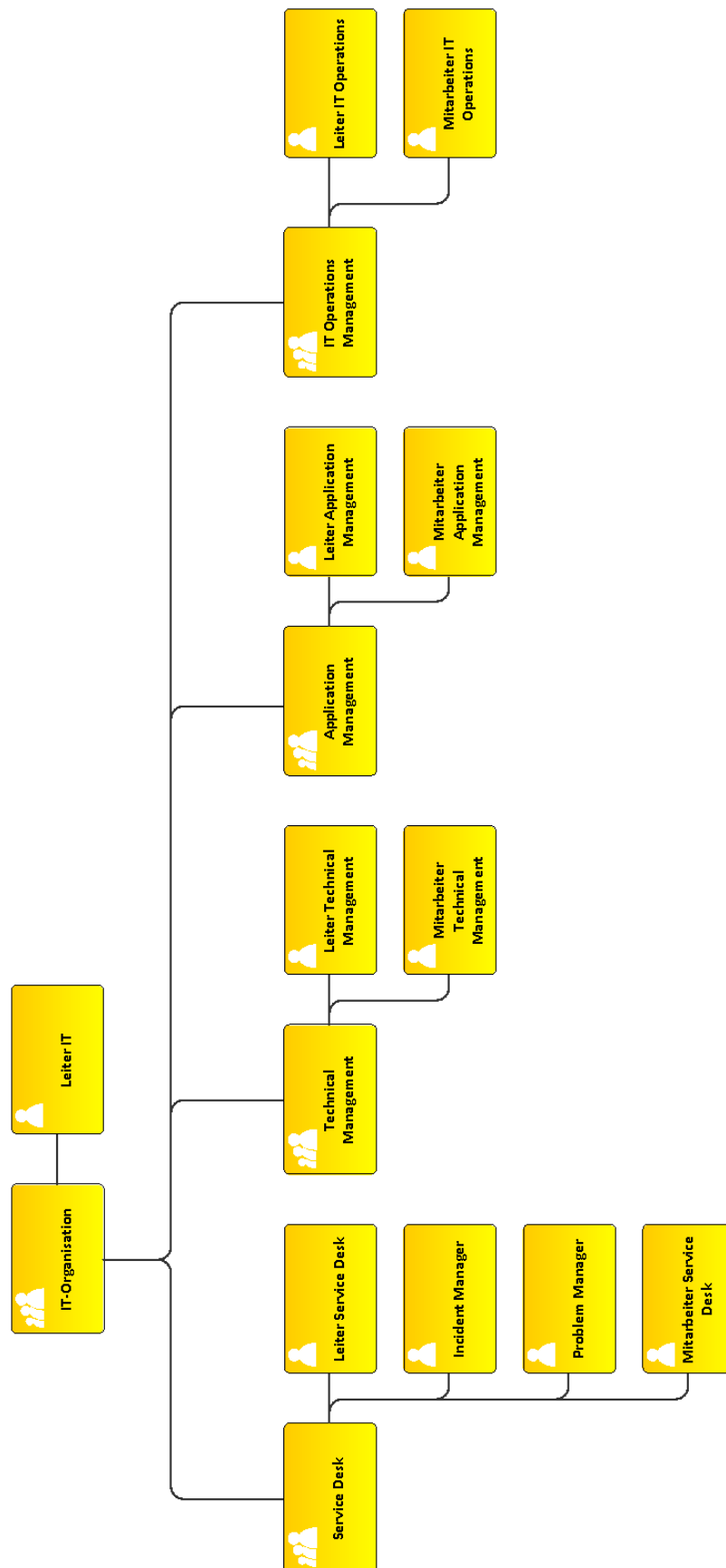
Personen der Rolle Mitarbeiter Service Desk bearbeiten außerdem initial die eingehenden Service Requests. Falls weitere Aktivitäten für Bearbeitung eines Service Requests erforderlich sind, wird die OE IT Operations Management mit einbezogen. Weiterhin können OE zur Erfüllung des Service Request herangezogen werden, die nicht zur IT-Organisation gehören, wie Einkaufsabteilung oder das Liegenschaftsmanagement.

Personen der Rolle Mitarbeiter Service Desk nehmen außerdem Anfragen hinsichtlich der Access Management-Prozesse entgegen. Sie prüfen diese auf Zulässigkeit gegenüber den Vorgaben der Organisation und geben Nutzungsrechte frei.

Die Rolle Problem Manager verantwortet die stabile und funktionierende Ausführung des Problem Management-Prozesses. Er ist Schnittstelle zu externen Partnern und für den formalen Abschluss von Problem-Datensätzen zuständig. Außerdem stellt er Teams aus Mitarbeitern der fachlichen OE zusammen, welche die tiefgehende Diagnose und Lösung von Problemen durchführen.

Die Rolle Incident Manager verantwortet den Incident Management-Prozess und entwickelt diesen bedarfsgesteuert weiter. Er koordiniert außerdem die Aktivitäten der an der Incident-Bearbeitung mitwirkenden Rollen, wie die Mitarbeiter Service Desk als First-Level-Support und die Mitarbeiter der Fachgruppen, die den Second-Level-Support bereitstellen.

Die OE Technical Management, Application Management und IT Operations bilden die spezialisierten Fachgruppen innerhalb der IT-Organisation. Sie sind damit der Second-Level-Support für Incidents, Probleme und Service Requests, die beim Service Desk eingehen. Sie werden jeweils vom Leiter der OE fachlich und disziplinarisch geführt und umfassen jeweils weitere Personen der Rolle Mitarbeiter.



**Abb. 5.1:** Aufbauorganisation der IT-Organisation

## 5.2 Datenmodell

Das Datenmodell in Abbildung 5.3 beschreibt unter Verwendung des Entity-Relationship-Diagramms die Informationsobjekte des integrierten Service Desk- und Inventarmanagement – Werkzeugs.

Die Informationsobjekte werden als Entitäten mit ihren Attributen sowie den Relationen zwischen den Entitäten beschrieben. Die Relationen verwenden für die Angabe der Kardinalitäten die sog. Martin-Notation. Die Abbildung 5.2 enthält ein Beispiel für die Angabe der Kardinalitäten unter Verwendung der Martin-Notation. Die Angaben im Diagramm lesen sich von oben nach unten wie folgt:

- Eine Person ist geboren in minimal einem, maximal einem Ort.
- Eine Person ist gestorben in minimal Null, maximal einem Ort.
- Eine Person macht Ferien in minimal Null, maximal vielen Orten.
- Eine Person war bereits in minimal einem, maximal vielen Orten.

An den Relationen sind außerdem die Rollenbezeichnungen der Entitäten angetragen.

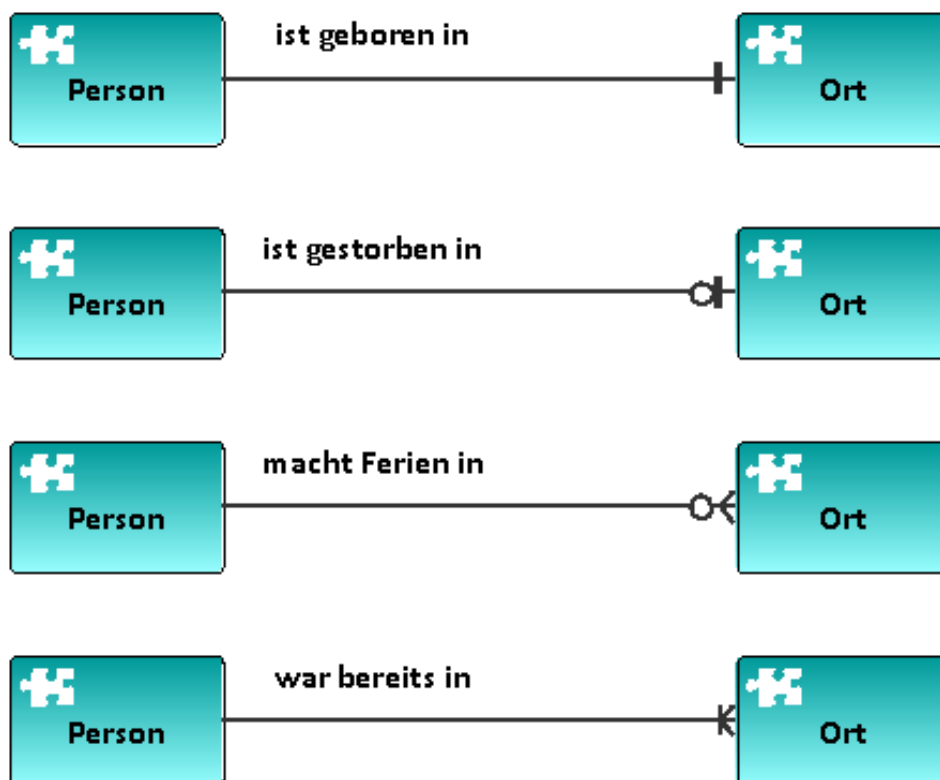


Abb. 5.2: Beispiel Martin-Notation

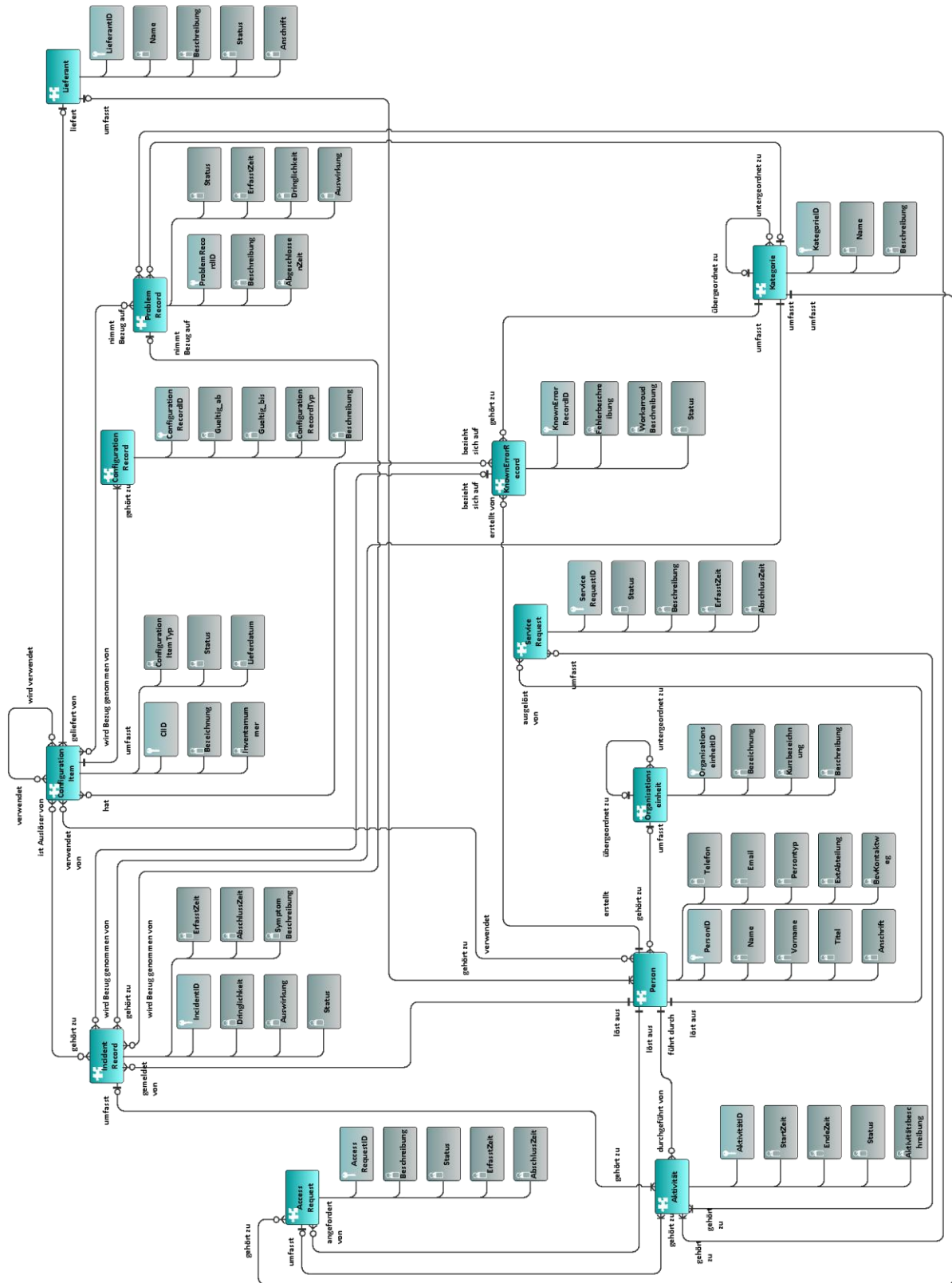


Abb. 5.3: Datenmodell



**Tab. 5.1** Beschreibung der Informationsobjekte, ihrer Attribute und Beziehungen

Entität	Attributname	Bedeutung bzw. Wertebereich	Datentyp
Kategorie	KategorieID	Primärschlüssel	Primärschlüssel
	Name	Bezeichner für die Kategorie	Text
	Beschreibung	Beschreibung für die Kategorie	Text

Beziehungen:

Einer Kategorie können keine, eine oder mehrere Kategorien untergeordnet sein.

Eine Kategorie ist keiner oder einer Kategorie übergeordnet.

Die Entität Kategorie wird verwendet von ProblemRecord, IncidentRecord, KnownErrorRecord und AccessRequest.

Lieferant	LieferantID	Primärschlüssel	Primärschlüssel
	Name	Bezeichner für Lieferant	Text
	Beschreibung	Zusätzliche Information	Text
	Status	Aktiv   Beendet	Aufzählung
	Anschrift	Anschriftendaten	Verbund

Beziehungen:

Lieferanten können ConfigurationItems liefern.

Lieferanten sind Personen zugeordnet. Diese fungieren als Ansprechpartner des Lieferanten.

Aktivität	AktivitätID	Primärschlüssel	Primärschlüssel
	StartZeit	Startzeit der Aktivität	Zeitstempel
	EndeZeit	Abschlusszeit der Aktivität	Zeitstempel
	Status	Status der Aktivität: Zugewiesen   In Arbeit   Abgeschlossen	Aufzählung
	Aktivitätsbeschreibung	Beschreibung einer einzelnen Aktivität, die vorgenommen wurde bzw. vorzunehmen ist	Text

Beziehungen:

Eine Aktivität wird von einer Person durchgeführt werden bzw. ist von einer Person durchgeführt worden.

Eine Aktivität gehört entweder zu einem ProblemRecord oder zu einem IncidentRecord oder zu einem AccessRequest oder zu einem ServiceRequest.

Person	PersonID	Primärschlüssel	Primärschlüssel
	Name	Nachname der Person	Text
	Vorname	Vorname der Person	Text
	Titel	Titel der Person	Text
	Anschrift	Anschriftendaten der Person	Verbund
	Telefon	Telefonnummer	Text
	Email	Email-Adresse der Person	Text
	Personentyp	Intern   Extern	Aufzählung
	BevKontaktweg	Bevorzugter Kontaktweg der Person: Email   Telefon   Fax   Brief	Aufzählung

---

 Beziehungen:

Eine Person kann eine oder mehrere Aktivitäten durchführen.

Eine Person kann einen oder mehrere AccessRequests auslösen

Eine Person kann einen oder mehrere IncidentRecords auslösen

Eine Person kann zu einem Lieferanten gehören

Eine Person kann ein oder mehrere ConfigurationItems verwenden

Eine Person kann eine oder mehrere KnownErrorRecords erstellen

Eine Person kann zu einer Organisationseinheit gehören

---

Organisations- einheit	Organisations- einheitID	Primärschlüssel	Primärschlüssel
	Bezeichnung	Langbezeichnung der Organisationseinheit	Text
	Kurzbezeichnung	Kurzbezeichnung der Organisationseinheit	Text
	Beschreibung	Beschreibung der Organisationseinheit	Text

## Beziehungen:

Eine Organisationseinheit kann einer anderen Organisationseinheit untergeordnet sein.

Eine Organisationseinheit kann einer oder mehrerer Organisationseinheiten übergeordnet sein

Eine Organisationseinheit kann eine oder mehrere Personen umfassen.

---

AccessRequest	AccessRequestID	Primärschlüssel	Primärschlüssel
	Beschreibung	Beschreibung der Zugriffsrechanforderung	Text
	Status	Bearbeitungsstatus der Zugriffsrechanforderung: Erfasst   In Arbeit   Abgeschlossen	Aufzählung
	ErstelltZeit	Datum der Erfassung der Zugriffsrechanforderung	Zeitstempel
	AbschlussZeit	Datum des Abschlusses der Bearbeitung der Zugriffsrechanforderung	Zeitstempel

## Beziehungen:

Ein AccessRequest umfasst eine oder mehrere Aktivitäten.

Ein AccessRequest ist einer Kategorie zugeordnet.

Ein AccessRequest wurde von einer Person angefordert

---

IncidentRecord	IncidentID	Primärschlüssel	Primärschlüssel
	Dringlichkeit	Incident-Dringlichkeit: Niedrig   Mittel   Hoch	Aufzählung
	Auswirkung	Incident-Auswirkung: Niedrig   Mittel   Hoch	Aufzählung
	Status	Status des Incident: Offen   In Arbeit   Abgeschlossen	Aufzählung
	ErfasstZeit	Zeitpunkt der Incident-Erfassung	Zeitstempel
	AbschlussZeit	Zeitpunkt des Incident-Abschlusses	Zeitstempel

	Symptom Beschreibung	Beschreibung der Incident-Symptome	Text
--	-------------------------	------------------------------------	------

**Beziehungen:**

Ein IncidentRecord umfasst eine oder mehrere Aktivitäten

Ein IncidentRecord ist einer Kategorie zugeordnet

Ein IncidentRecord wurde von einer Person gemeldet

Ein IncidentRecord kann einem oder mehreren ConfigurationItems zugeordnet sein.

Ein IncidentRecord kann in Verbindung zu einem ProblemRecord stehen.

Ein IncidentRecord kann in Verbindung zu einem KnownErrorRecord stehen.

ProblemRecord	ProblemRecordID	Primärschlüssel	Primärschlüssel
	Beschreibung	Beschreibung des Problems	Text
	Status	Status des Problem: Offen   In Arbeit   Abgeschlossen	Aufzählung
	ErfasstZeit	Zeitpunkt der Problem-Erfassung	Zeitstempel
	Abgeschlossen Zeit	Zeitpunkt des Problem-Abschlusses	Zeitstempel
	Dringlichkeit	Problem-Dringlichkeit: Niedrig   Mittel   Hoch	Aufzählung
	Auswirkung	Problem-Auswirkung: Niedrig   Mittel   Hoch	Aufzählung

**Beziehungen:**

Ein ProblemRecord kann auf einen oder mehrere ConfigurationItems Bezug nehmen

Ein ProblemRecord kann auf einen oder mehrere IncidentRecords Bezug nehmen

Ein ProblemRecord ist einer Kategorie zugeordnet

Ein ProblemRecord umfasst eine oder mehrere Aktivitäten

KnownError Record	KnownError RecordID	Primärschlüssel	Primärschlüssel
	Fehler beschreibung	Detailbeschreibung des bekannten Fehlers	Text
	Workaround Beschreibung	Beschreibung für die vorübergehende Abhilfe des bekannten Fehlers	Text
	Status	Status des bekannten Fehlers: In Arbeit   Gültig   Archiviert	Aufzählung

**Beziehungen:**

Ein KnownErrorRecord kann sich auf einen IncidentRecord beziehen

Ein KnownErrorRecord kann sich auf einen oder mehrere ConfigurationItems beziehen

Ein KnownErrorRecord wurde von einer Person erstellt.

Ein KnownErrorRecord gehört zu einer Kategorie.

ConfigurationItem	CIID	Primärschlüssel	Primärschlüssel
	Bezeichnung	Bezeichnung des ConfigurationItem	Text
	Inventarnummer	Eindeutige Inventarnummer, physischen ConfigurationItems zugeordnet	Integer

	ConfigurationItem Typ	Typ des ConfigurationItem: Hardware   Software   Service   Dokument   Andere	Aufzählung
	Status	Status des ConfigurationItem: In Planung   Im Test   In Betrieb   In Wartung   Archiviert	Aufzählung
	Lieferdatum	Datum der Bereitstellung des ConfigurationItem	Datum

**Beziehungen:**

Ein ConfigurationItem kann von einem oder mehreren anderen ConfigurationItems verwendet werden.

Ein ConfigurationItem kann eines oder mehrere andere ConfigurationItems verwenden

Ein ConfigurationItem umfasst einen oder mehrere ConfigurationRecords

Ein ConfigurationItem kann Auslöser eines oder mehrerer IncidentRecords sein

Ein ConfigurationItem kann einen oder mehrere KnownErrorRecords haben

Ein ConfigurationItem kann in Beziehung zu einem oder mehreren ProblemRecords stehen

Ein ConfigurationItem kann von einem Lieferanten bereitgestellt werden

Ein ConfigurationItem kann von einer oder mehreren Personen verwendet werden

Configuration Record	Configuration RecordID	Primärschlüssel	Primärschlüssel
	Guelteig_ab	Zeitpunkt, ab dem der ConfigurationRecord gültig ist	Zeitstempel
	Guelteig_bis	Zeitpunkt, bis zu dem ein ConfigurationRecord gültig ist	Zeitstempel
	ConfigurationRecordTyp	Typ des ConfigurationRecords: Standort   Lizenzschlüssel   SLA   Installationsparameter   Konfigurationsparameter	Aufzählung
	Beschreibung	Wert des angegebenen ConfigurationRecordTyp	Text

**Beziehungen:**

Ein ConfigurationRecord gehört zu einem ConfigurationItem

## 6 Prototypische Realisierung

Die prototypische Implementierung des integrierten Service Desk- und Inventarmanagements erfolgt als Datenbank in Lotus Domino / Notes

Lotus Domino / Notes ist ein dokumentenorientiertes, verteiltes Datenbanksystem des Herstellers IBM. Die Serverkomponente trägt die Bezeichnung Lotus Domino, die Client-Anwendung wird unter der Bezeichnung Lotus Notes ausgeliefert.

Der Besonderheit von Lotus Domino / Notes liegt in der Eigenschaft als dokumentenorientiertes System. Das zuvor beschriebene Entity-Relationship-Modell lässt sich diesem Fall nicht unmittelbar als relationale Datenbank implementieren.

Die Datenbank organisiert die Daten somit nicht über ein festes Datenschema, sondern verwaltet diese als einzelne Dokumente. In Lotus Domino / Notes werden die Dokumente mit Hilfe von Masken angelegt und wieder bearbeitet. Für jedes Dokument, das eine beliebige Zahl von Datenfeldern haben kann, wird jeweils die zugehörige Maske gespeichert, um diese bei der Bearbeitung wieder zu verwenden.

Die Ansicht von erzeugten Dokumenten in Listenform erfolgt über Sichten, die in Abhängigkeit vom konkreten Informationsbedarf angelegt werden können. Es werden jeweils Spalten definiert, die angezeigt werden sollen. Für jede Sicht wird festgelegt, ob alle in der Datenbank enthaltenen Dokumente – unabhängig von Bedingungen angezeigt werden sollen, oder nur die Dokumente, die mit einer bestimmten Maske angelegt wurden.

Für die jeweiligen Informationsobjekte bzw. Entitäten aus dem Datenmodell werden Masken angelegt, welche die Erfassung eines Datensatzes als Dokument ermöglichen. Für jedes Attribut des Datenmodells wird ein Datenfeld in der Maske angelegt. Für den Wertebereich des Datenfeldes wird ein geeigneter Datentyp ausgewählt, z.B. Text, RichText oder Dialogfelder, wenn es sich bei den Attributen des Datenmodells um Aufzählungstypen handelt.

Um Mengen von Dokumenten zu betrachten und zur Bearbeitung auszuwählen, werden jeweils für die Informationstypen bzw. Entitäten Sichten erstellt. Der Bezug zur verwendeten Maske wird sichergestellt. Verknüpfungen zwischen Entitäten werden über Dialoglisten hergestellt, die auf bereits angelegte Sichten zugreifen. In einem Dokument kann somit der Bezug zu einem anderen Dokument hergestellt werden. So lässt sich beispielsweise ein ConfigurationRecord einem Configuration Item zuordnen.

## Literaturverzeichnis

- Alpar, P.; Grob, H. L.; Weimann, P.; Winter, R. (2008): Anwendungsorientierte Wirtschaftsinformatik: Strategische Planung, Entwicklung und Nutzung von Informations- und Kommunikationssystemen. 5. Aufl., Wiesbaden.
- Becker, J.; Rosemann, M.; Schütte, R. (1995): Grundsätze ordnungsmäßiger Modellierung. Wirtschaftsinformatik, 37. Jg., Heft 5, S. 435-445.
- Beims, M. (2010): IT-Service-Management in der Praxis mit ITIL 3: Zielfindung, Methoden, Realisierung. München.
- Buchsein, R.; Victor, F.; Günther, H.; Machmeier, V. (2008): IT-Management mit ITIL V3. 2. Aufl., Wiesbaden.
- Cannon, D. L.; Hinrichs, B. (2007): ITIL Service Operation. London
- Gadatsch, A. (2008): Grundkurs Geschäftsprozess-Management: Methoden und Werkzeuge für die IT-Praxis: eine Einführung für Studenten und Praktiker. Wiesbaden.
- IfM Bonn (2011a): IfM Bonn Institut für Mittelstandsforschung Bonn. <http://www.ifm-bonn.org/index.php?id=89>. 18. September 2011
- IfM Bonn (2011b): IfM Bonn Institut für Mittelstandsforschung Bonn. <http://www.ifm-bonn.org/index.php?id=99>. 18. September 2011.
- Laudon, K. C.; Laudon, J. P.; Schoder, D. (2006): Wirtschaftsinformatik : eine Einführung. München u. a.
- Olbrich, A. (2008): ITIL kompakt und verständlich. 4. Aufl., Wiesbaden.
- Rautenstrauch, C.; Schulze, T. (2003): Informatik für Wirtschaftswissenschaftler und Wirtschaftsinformatiker. Berlin u. a.
- Scheer, A. W. (1998): Wirtschaftsinformatik: Referenzmodelle für industrielle Geschäftsprozesse. 2. Aufl., Berlin u. a.
- Scheer, A. W. (2002): ARIS - vom Geschäftsprozess zum Anwendungssystem. 4. Aufl., Berlin u. a.
- Schewe, G. (2011): Definition: Organisation | Wirtschaftslexikon Gabler. <http://wirtschaftslexikon.gabler.de/Definition/organisation.html>. 20. September 2011.
- Stych, C.; Zeppenfeld, K. (2008): ITIL. Berlin u. a.
- Taylor, S.; Macfarlane, I. (2009): ITIL V3 small-scale implementation. 3. Aufl., London.
- Wallner, G.; Rüdiger, A. (2008): Help Desk oder Service Desk? Information week, 12. Jg., Heft 3, S.16-17.

## **Abschließende Erklärung**

Ich versichere hiermit, daß ich die vorliegende Diplomarbeit selbständig, ohne unzulässige Hilfe Dritter und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Magdeburg, den 3. Oktober 2011