HANSER

Leseprobe

Christian Wischki

ITIL®V2, ITIL®V3 und ISO/IEC 20000

Gegenüberstellung und Praxisleitfaden für die Einführung oder den Umstieg

ISBN: 978-3-446-41977-3

Weitere Informationen oder Bestellungen unter

http://www.hanser.de/978-3-446-41977-3

sowie im Buchhandel.

Teil I:
ITIL(v2)

1 ITIL V2 – Einleitung und Überblick

Was ist ITIL eigentlich?

ITIL (IT Infrastructure Library) ist ein Framework für den Betrieb einer IT. Das Ziel von ITIL ist, Ansätze, Methoden und Architekturen (Prozesse) für den Betrieb und für die Betreuung der zu liefernden IT-Services nach dem „Best-Practice-Prinzip“ anzubieten und damit eine optimierte, serviceorientierte und qualitätsgesicherte IT-Service-Struktur zu ermöglichen. Dabei muss sich die praktische Umsetzung immer an den spezifischen Anforderungen und Bedürfnissen eines Unternehmens orientieren, nicht nur an den technischen Anforderungen, sondern vor allem auch an den sozialen, politischen und kulturellen Belangen. Man kann ITIL mit folgenden Aussagen charakterisieren:

- ITIL ist keine Projektmethode, sondern eine prozess- und kundenorientierte Betriebsmethode.
- ITIL dient im Grunde als „Best-Practice-Ansatz“ und als Framework für den IT-Betrieb.
- ITIL ist keine verbindliche Norm (die passende Norm ist ISO/IEC20000), kein Tool, keine Vorschrift und schon gar keine Formularvorlage.
- ITIL ist service-, produkt-, technologie- und herstellerunabhängig.
- ITIL liefert auch eine gemeinsame Sprachbasis für die „IT-Prozess-Spezifikation“ der verschiedenen IT-Betriebsbereiche.
- ITIL betrachtet die IT als Ganzes, sieht diese als serviceorientierte Organisation und versteht vor allem die Fachabteilungen als deren Kunden.
- ITIL ist definitiv keine „Out of the Box“-Lösung.
- ITIL empfiehlt, was zu beachten und was zu tun ist, aber nicht, *wie* es zu tun ist.
- ITIL macht Vorschläge, und zwar dazu,
  - welche Prozesse entwickelt werden sollten,
  - welche Rollen definiert werden sollten,
  - welche Aufgaben definiert werden sollten,
  - welche Abhängigkeiten abgebildet werden sollten.

Während sich ITIL in der Version 1 in der Praxis nicht einmal ansatzweise durchsetzen konnte, verzeichnete ITIL V2 einen durchschlagenden Erfolg. Man kann inzwischen sogar behaupten, dass ITIL V2 den De-facto-Standard für einen IT-Betrieb darstellt, jedoch nicht in der von ITIL V2 ursprünglich definierten Form, die eine Sammlung von acht Büchern umfasst:

- Service Support
- Service Delivery
- Security Management
- ICT Infrastructure Management
- Software Asset Management
- Application Management
- Planning to implement Service Management
- Business Perspective

Der große Erfolg von ITIL V2 besteht darin, dass sich die Anwender das aus dem von der OGC (Office of Government and Commerce) definierten ITIL V2 für die Praxis herausgezogen haben, was wirklich praxisrelevant ist und für die meisten IT-Organisationen und ihre IT-Services einen guten und lebbaren Best-Practice-Ansatz darstellt. Von den oben genannten acht von der OGC definierten Büchern haben sich in der Praxis nur zwei Bücher durchgesetzt, nämlich Service Support und Service Delivery. Hinzu kommt ein überschaubarer Security-Management-Prozess, der aus dem Band „Security Management“ entstanden ist. Abbildung 1.1 zeigt als „Big Picture“ das praxisrelevante ITIL V2.

ITIL 2.0 – Überblick

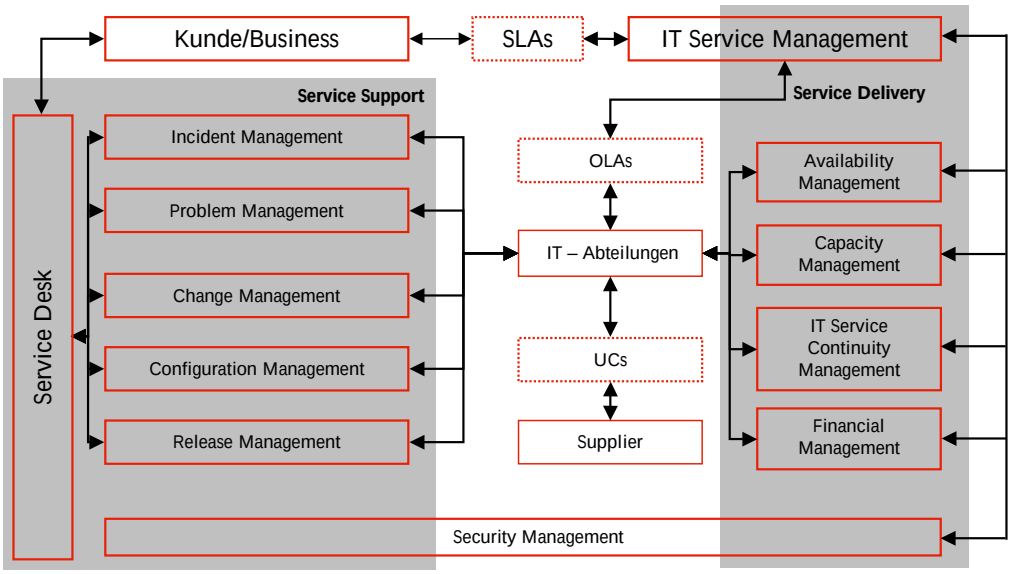

Abbildung 1.1 ITIL 2.0 in der für die Praxis relevanten Ausprägung

Im Rahmen des Service-Delivery, einem taktischen Prozessbereich, werden die zu liefernden IT-Services mit dem Kunden vereinbart, entwickelt, realisiert und dann über den Change-Management-Prozess in den produktiven Betrieb – in den Bereich des Service Supports – überführt. Der Service Support ist dann auch für den Support der IT-Services verantwortlich.

Die Prozesse des Service Delivery

- **Service Level Management** – Vereinbaren, Überwachen, Steuern, Sicherstellen und Optimieren aller Service Level Agreements (SLAs), Operation Level Agreements (OLAs) und Underpinning Contracts (UCs) sowie der ihnen zugrunde liegenden Service-Qualitäten.
- **Availability Management** – Planen, Steuern, Sicherstellen, Überwachen und Optimieren der aktuellen und vor allem auch der zukünftigen Verfügbarkeit von IT-Services und deren Komponenten.
- **Capacity Management** – Planen, Steuern, Sicherstellen, Überwachen und Optimieren der aktuellen und vor allem auch der zukünftigen IT-Service-Kapazitätsanforderungen.
- **IT Service Continuity Management** – Die Überlebensfähigkeit eines Unternehmens nach einem Katastrophenfall unter ökonomischen Geschichtspunkten gewährleisten.
- **Financial Management** – Die Gesamtkostenbetrachtung und -transparenz, Total Cost of Ownership (TCO), bezogen auf alle Services und auf einzelne Configuration Items (CI), die Unterstützung der Kostenoptimierung durch Synergie- und Einsparungsanalysen und die permanente Kontrolle der Investitionsstrategie, Return of Investment (ROI).
- **Security Management** – Die Gewährleistung der Vertraulichkeit, der Integrität und der „Verfügbarkeit“ der Daten innerhalb der IT im vorgegebenen Umfang sowie das frühzeitige Erkennen, Klassifizieren und ggf. Beseitigen allgemeiner Bedrohungen und Sicherheitslücken.

Praxistipp

Obwohl das Service Level Management laut ITIL im Bereich des Service Delivery angesiedelt ist, sollte es in der Praxis jedoch – wie das Security Management – eher übergreifend für die Bereiche Service Support und Service Delivery gesehen werden, da es letztendlich die gesamte Verantwortung über alle IT-Services dem Kunden gegenüber hat.

Die Prozesse des Service Support

- **Service Desk** – Stellt eine Funktion in ITIL dar, welche Aufgaben von Prozessen übernehmen kann, meist die des ersten Ansprechpartners in der IT für den Kunden.
- **Incident Management** –Die zügige Wiederherstellung der IT-Service-Leistungen im Störungsfall gemäß der vereinbarten SLAs; gleichzeitig das Minimieren der Beeinträchtigung der Geschäftsprozesse im Störungsfall (reaktiv).

- **Problem Management** – Die Ursachen von Störungen und Problemen detailliert untersuchen und entsprechende dauerhafte und nachhaltige Lösungen finden (proaktiv & reaktiv).
- **Change Management** – Optimierung aller Services über alle Prozesse hinweg durch richtige Entscheidungen über die eingereichten Änderungsanträge.
- **Configuration Management** – Die Bereitstellung von aktuellen und historischen Informationen über die verfügbaren IT-Services, die damit verbundenen IT-Infrastruktur-Konfigurationselemente und deren Beziehungen untereinander.
- **Release Management** – Die Minimierung der Beeinträchtigung der Serviceumgebung durch eine zielgerichtete sowie qualitätsgesicherte Planung und Steuerung der Releases.

Fazit

Wie sich eine IT durch die Einführung von ITIL-Prozessen verändert, lässt sich treffend mit diesem Vergleich darstellen: Der Kunde bzw. das Business erhält von der IT keine Waschmaschinen mehr, sondern saubere Wäsche, d.h. der Kunde bzw. das Business erhält von der IT keine IT-Leistungen mehr, sondern Business- und IT-Services. Eine Einführung von ITIL bringt Ihnen eine Reihe von Vorteilen:

- ITIL führt zu mehr Qualitätssicherung und -steigerung.
- ITIL führt zu mehr Kostentransparenz.
- ITIL führt zu transparenten und optimierten IT-Services und somit auch zu optimierten IT-Service-Strukturen.
- ITIL führt zu einer optimierten Unterstützung des Business durch die IT.

Dem stehen auch Nachteile gegenüber:

- ITIL kann, wenn es falsch interpretiert und eingeführt wird, zu weniger Eigeninitiative, zu weniger Dynamik und zu weniger proaktivem Engagement („Let's do it") im Unternehmen führen.
- Eine Einführung von ITIL ist anfangs immer mit entsprechendem Aufwand und Kosten verbunden (es werden hierbei jedoch auch stets Quickwins erzielt).

Leider sind in ITIL V2 teilweise auch sehr wichtige Bestandteile eines IT-Services nicht in einem mit deren Praxisrelevanz in Bezug stehenden, notwendigen Detaillierungsgrad beschrieben, wie beispielsweise

- die Wartungsprozesse: Gerade in der IT gibt es fast keine Services, die nicht regelmäßig gewartet werden müssen. Wartungsprozesse sind in der ITIL-V2-Praxis in den proaktiven Teil des Problem Managements eingegliedert, da sie zur Störungsvermeidung beitragen.
- die Überführung der im Service Delivery entwickelten IT-Services in den Service Support: In der ITIL-V2-Praxis geschieht dies durch den Change-Management-Prozess, der auch die Schnittstellte zwischen dem Service Support, dem Service Delivery und dem Projekt Management darstellt.

- die Betrachtung der IT-Services über deren gesamten Lebenszyklus: In der ITIL-V2-Praxis findet das innerhalb des Prozesses „Service Level Management“ statt. So wird zum Beispiel das in der IT-Praxis stets notwendige End-Of-Life eines Services vom Service Level Management initiiert und dann durch das Change Management realisiert, da die Abschaltung eines IT-Services nichts anderes als eine Änderung an einem bestehenden IT-Service darstellt.

2

2 ITIL V2 – Der Service Desk

Der Service Desk ist unter ITIL Anlaufpunkt für alle Kunden und Anwender. Sie tragen dort ihre Anliegen zu einem oder mehreren von der IT zu erbringenden Services vor. Der Service Desk sollte laut ITIL immer als SPOC (Single Point of Contact) aufgebaut sein, um als einzige Kontaktstelle zwischen der IT und den Kunden und Anwendern zu fungieren. Ein anderer gängiger Begriff hierfür ist „One Face to the Customer".

Der Vorteil liegt darin, dass sich die Kunden und Anwender der IT-Services ihre Ansprechpartner in der IT nicht merken müssen. Sie kontaktieren einfach immer den Service Desk, der dann für die Koordination und Weiterleitung der Kundenanliegen innerhalb der IT zuständig ist.

Bemerkung

Der Service Desk heißt bei größeren ITs oft auch „Call Center" bzw. „Help Desk" bei mittleren und kleinen ITs. Andere gängige Bezeichnungen sind „Customer Hotline" oder „Customer and Care Center". ITIL hat den Begriff Service Desk absichtlich gewählt, um zu signalisieren, dass das Ziel von ITIL darin besteht, dem Kunden einen Service zu bieten und nicht nur eine Leistung zu erbringen.

Der Service Desk hat einerseits die Aufgabe, die Interessen der Kunden bzw. der Anwender gegenüber der IT zu vertreten, stellt aber andererseits auch die Visitenkarte und das „Gesicht" der IT gegenüber den beiden Zielgruppen dar.

Praxistipp

Analog zum Auftreten des Service Desks nimmt der Kunde die IT subjektiv wahr. Wenn der Service Desk als „schlecht" oder „inkompetent" empfunden wird, so hat die IT sofort das gleiche Image – egal wie gut sie wirklich funktioniert. Schon aus diesem Grund ist ein gut funktionierender Service Desk essenziell wichtig für das Image der IT.

2.1 Der Service Desk als Funktion

Der Service Desk ist kein Prozess im eigentlichen Sinne, sondern als eine Funktion definiert und auch als solche zu verstehen – genau genommen als Schnittstellenfunktion. Der Unterschied zwischen einem Prozess und einer Funktion besteht darin, dass Funktionen Aufgaben von mehreren Prozessen übernehmen können, jedoch meist für sich selbst keine dediziert definierten Aufgaben besitzen.

Der Service Desk bildet die Schnittstelle zwischen dem Kunden/Anwender und der IT-Organisation. Im Grunde lassen sich die Anliegen der Kunden/Anwender, die den Service Desk kontaktieren, in drei Kategorien einteilen:

- Meldung von Störungen (Incident)
- Stellen von Anfragen (Service Request)
- Meldung von Beschwerden (Complaint)

Für alle drei Bereiche sollte der Service Desk auch jeweils einen eigenen Prozess bzw. eine Vorgehensweise definieren.

Eine Störung liegt vor, wenn der IT-Service, so wie im SLA (Service Level Agreement) definiert, nicht mehr verfügbar ist. Eine Anfrage stellt im Grunde einen Wunsch des Kunden dar, z.B. nach einer Dokumentation, nach einem neuen Feature etc. Eine Beschwerde bringt meist den Unmut des Kunden bzw. des Anwenders über den erbrachten IT-Service zum Ausdruck. Sie stellt keine Störung dar, sondern meist den Wunsch nach einem besseren Service.

Praxistipp

In der Praxis geschieht es häufig, dass ein Kunde eine Störung meldet, die aber im Grunde keine darstellt. Im klassischen Beispiel meldet der Kunde beim Service Desk eine zu langsame Applikation. Ob dies nun eine Störung oder eine Beschwerde darstellt, hängt ausschließlich vom SLA ab. Sofern in diesem definiert ist, dass die Applikation eine maximale Antwortzeit von beispielsweise fünf Sekunden nicht überschreiten darf, diese jedoch zehn Sekunden dauert, dann stellt dies eine Störung dar. Sind im SLA aber keine Antwortzeiten von Applikationen geregelt, so ist dies keine Störung. Die Aussage des Kunden reflektiert dann nur den Wunsch nach einem schnelleren Antwortverhalten der Applikation – also eine Anfrage. Die Inhalte aller SLAs sind somit Voraussetzung für den Service Desk, um überhaupt zwischen Störung und Anfrage unterscheiden zu können.

2.2 Organisationsformen des Service Desks

Ziel ist es, den Service Desk so zu organisieren bzw. aufzustellen, dass er sowohl die Ansprüche der Kunden/Anwender als auch die der IT optimal erfüllen kann. Jedes Unternehmen und jede IT muss seinen passenden Weg finden und entwickeln. ITIL beschreibt hierzu drei mögliche Organisationsformen: den zentralen, den dezentralen und den virtuellen Service Desk.

2.2.1 Der zentrale Service Desk

Dieser ist im Grund über seine Geografie definiert. Er ist an genau einem Ort vorhanden, von dem aus er alle Anliegen der Kunden und Anwender bedient. Diese Organisationsform des Service Desks passt vor allem für solche Unternehmen, die in einer einzigen kulturellen, sprachlichen und evtl. auch geografischen Region aktiv sind, jedoch keine lokale Nähe zum Kunden/Anwender benötigen, weil sich beispielsweise alles Notwendige auch Remote, d.h. von der Ferne aus, erledigen lässt.

2.2.2 Der lokale Service Desk

Dieser ist an einem oder auch an verschiedenen Standorten, aber stets direkt beim Anwender oder Kunden vor Ort positioniert. Diese Organisationsform eignet sich vor allem für solche Unternehmen, bei denen eine Anwesenheit der IT vor Ort notwendig ist bzw. entsprechende Vorteile mit sich bringt. Ein einfaches Beispiel sind Unternehmen, die aus Sicherheitsgründen bei Störungen keinen Remote-Zugriff auf ihr System erlauben, was dann stets eine Behebung vor Ort erfordert.

2.2.3 Der virtuelle Service Desk

Diese Organisationsform ist standortunabhängig und kann sowohl zentral als auch dezentral organisiert sein. Für den Anwender ist nicht mehr ersichtlich, wo sein Anliegen entgegengenommen und bearbeitet wird, und im Grunde besteht fast kein persönlicher Kontakt mit dem Kunden oder Anwender. Es kommen vor allem standortunabhängige Kommunikationsformen wie Internet, E-Mail, Telefon etc. zum Einsatz.

Diese Organisationsform des Service Desk eignet sich vor allem für sogenannte „Global Player“. Sie vereint alle Vorteile des lokalen und zentralen Service Desks und eliminiert die entsprechenden Nachteile.

Unabhängig davon, ob ein lokaler, zentraler oder virtueller Service Desk zum Einsatz kommt, muss man sich in einem zweiten Schritt Gedanken darüber machen, wie dieser funktionieren und welche Aufgaben der verschiedenen anderen Prozesse er übernehmen soll.

2.3 Service Desk mit oder ohne fachliche Lösungskompetenz

Wie gesagt, stellt der Service Desk im Grunde „nur“ die Anlaufstelle für Anliegen des Kunden und der Anwender dar. Er kann aber auch Aufgaben von anderen Prozessen übernehmen, z.B. Teile des Incident Managements (Störungsmanagement).

2.3.1 Der Service Desk ohne fachliche Lösungskompetenz

Abbildung 2.1 zeigt einen Service Desk ohne fachliche Lösungskompetenz. Hier eruiert der Service Desk nur, ob es sich bei der gemeldeten Störung um eine Applikations- oder Infrastrukturstörung handelt: Funktioniert beispielsweise eine der Applikationen am PC des Kunden nicht mehr oder handelt es sich um Probleme an dessen PC (Hardware) bzw. an der Infrastruktur (Netzwerk, Server etc.)?

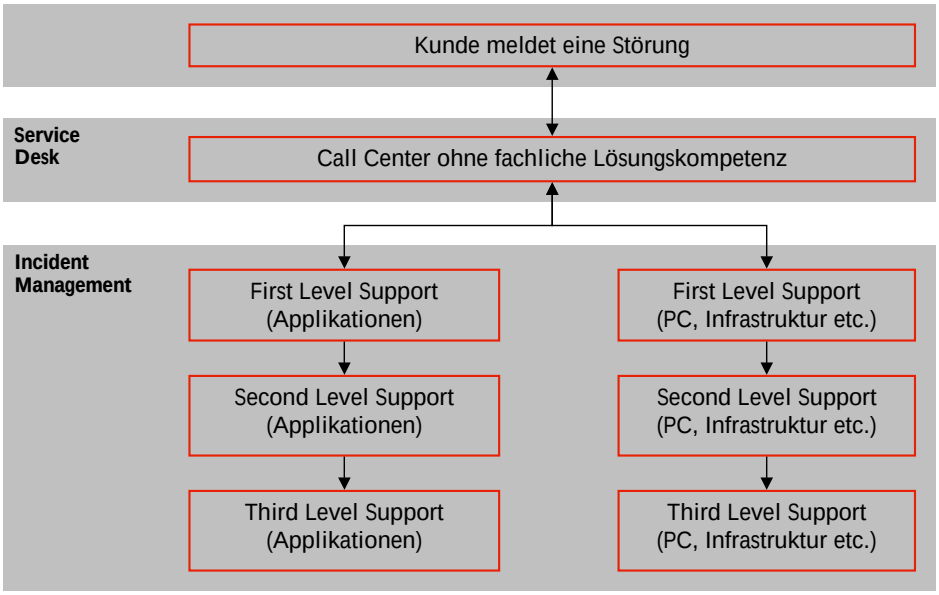

Abbildung 2.1 Struktur eines Service Desks ohne fachliche Lösungskompetenz

Praxistipps

Ein Service Desk ohne fachliche Lösungskompetenz kommt vor allem bei einer IT oder einem Service-Provider mit einer sehr großen Anzahl von Kunden zum Einsatz. Hier sind zunächst die zum Support berechtigten Kunden zu identifizieren, um sicherzustellen, dass keine „Spaßmeldungen“ oder Anwender ohne Support-Berechtigung die IT- bzw. Support-Organisation unnötig belasten und dementsprechende Kosten verursachen.

Auch wenn eine IT ihren Kunden viele IT-Services anbietet und damit verbunden ein entsprechend breites Know-how vorhanden sein muss, bietet sich ein Service Desk ohne fachliche Lösungskompetenz an. In diesem Fall ist es besser, wenn der Service Desk zusammen mit dem Anwender nur ermittelt, welcher Service die Störung verursacht hat, und das Problem dann zur Bearbeitung an eine nachgelagerte Support-Einheit weiterreicht.

2.3.2 Der Service Desk mit fachlicher Lösungskompetenz

Abbildung 2.2 zeigt einen Service Desk mit fachlicher Lösungskompetenz. In diesem Fall übernimmt der Service Desk Teile der Aufgaben des Incident Managements. Als First Level Support versucht bereits der Service Desk, die Störung zu beheben.

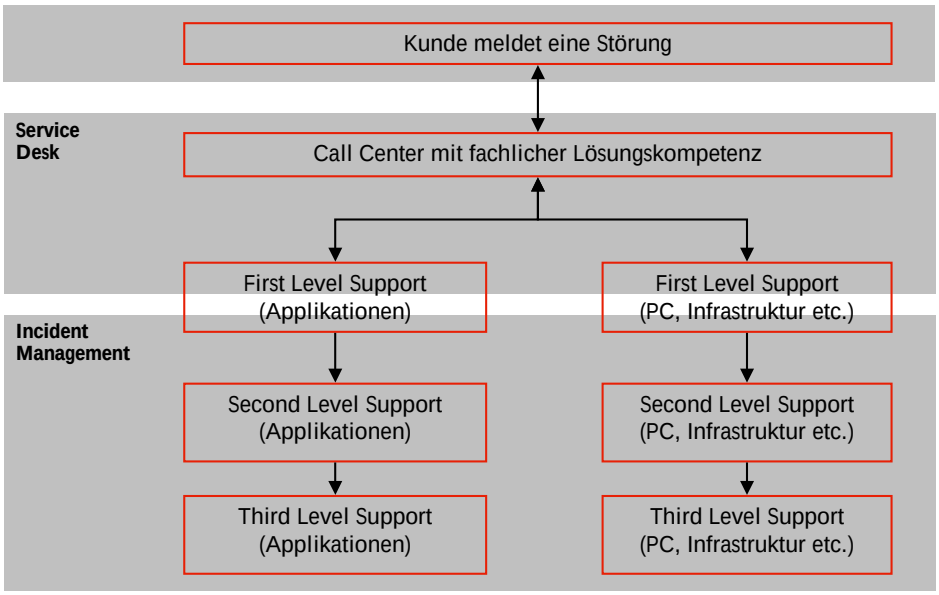

Abbildung 2.2 Struktur eines Service Desks mit fachlicher Lösungskompetenz

Praxistipps

Ein Service Desk mit fachlicher Lösungskompetenz wird beispielsweise bei Services eingesetzt, in denen kein oder nur wenig Spezialwissen notwendig ist, um eine Störung beheben zu können, z.B. im PC-Bereich der IT, dem sogenannten Front-End-Bereich. Die Frage eines Service-Desk-Mitarbeiters, ob beim Kunden der Monitor oder der mit dem Arbeitsplatz verbundene PC eingeschaltet ist, muss kein hochbezahlter IT-Spezialist stellen.

Eine weitere Einsatzmöglichkeit liegt vor, wenn nur wenige und/oder bereits technisch versierte Kunden/Anwender ihr Anliegen dem Service Desk melden dürfen. In diesem Falle erwartet der Anwender einen Ansprechpartner im Service Desk, der mit ihm auf gleichem technischem Niveau kommunizieren kann. Im Service Desk muss deshalb entsprechendes fachliches Know-how vorhanden sein, da sich als Kunde meist der Applikationsverantwortliche persönlich meldet.

Hinweise

Die Verantwortung für die Störung verlagert sich durch das Weiterreichen an eine andere Support-Einheit nicht. Der Service Desk bleibt immer „Owner“ der Störung und ist für deren Behebung dem Kunden gegenüber verantwortlich.

Eine Störung ist erst dann behoben, wenn der Kunde bzw. der Anwender bestätigt, dass sein Service wieder funktioniert – und nicht, wenn die IT bzw. der Service-Provider der Meinung ist, dass es so sein sollte.

Ziele und Aufgaben des Service Desks

Wie bereits erwähnt, besitzt der Service Desk für sich selber keine Ziele und Aufgaben, da er eine Funktion und keinen Prozess darstellt.

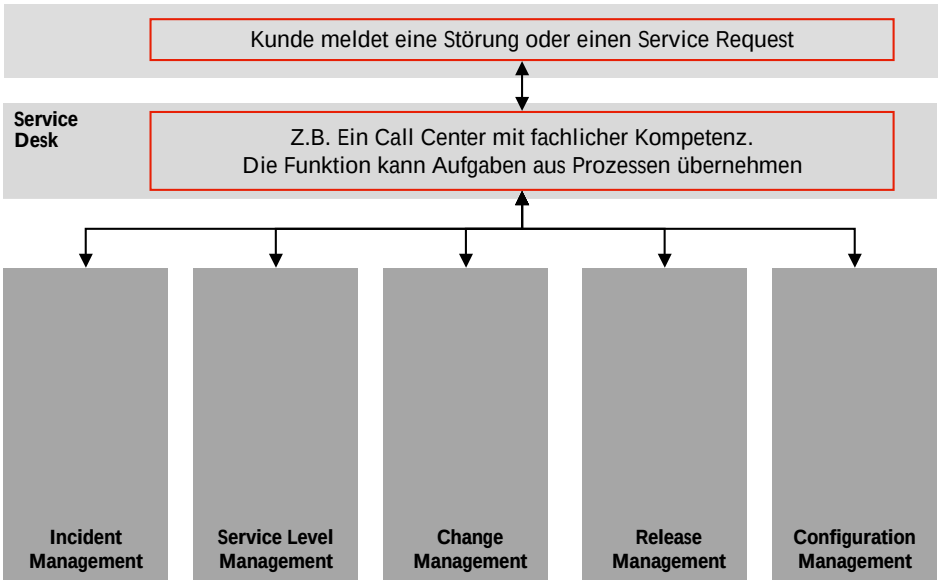

Abbildung 2.3 Prozesse, die beispielsweise ihre Aufgaben an den Service Desk auslagern

Da der Service Desk jedoch seine Aufgaben von anderen Prozessen übernimmt (siehe Abbildung 2.3), übertragen sich auch deren Ziele und Aufgaben auf den Service Desk. In der Praxis erledigt der Service Desk folgende Aufgaben für die genannten Prozesse:

- First Level Support im Incident Management
  - Garantiert die in den SLAs vereinbarte Erreichbarkeit der IT-Organisation
  - Stellt eine zielgerichtete und lösungsorientierte Kommunikation mit dem Anwender dar
  - Ist verantwortlich für die Annahme und Klassifikation von Störungen
  - Entlastet die Experten durch effektives Weiterleiten von Störungen samt der vollständigen Störungsinformationen
  - Stellt die effektive Koordination und Einsatzzuordnung der nachfolgenden Service-Support-Einheiten sicher
  - Überwacht die Störungsbearbeitung und stellt die Kundenzufriedenheit sicher
- Change Management
  - Stellt die vollständige Erfassung der RFCs (Request for Changes) sicher
  - Informiert den Antragsteller eines jeden RFC über die Entscheidung, ob dieser realisiert wird oder nicht
- Configuration Management
  - Führt bei Bedarf Audits und Reviews bzgl. der Konfigurationen der verschiedenen CIs (Configuration Items) durch
- Release und Deploy Management
  - Informiert die Anwender über neue Releases oder Services

- Service Level Management
  - Nimmt Anfragen (Service Requests) und Beschwerden (Complaints) der Anwender/Kunden entgegen

Der Service Desk fungiert aber in jedem Fall als „Single Point Of Contact“ (SPOC) und stellt die „Visitenkarte“ der IT-Organisation für deren Anwender und Kunden dar.

2.4 Schnittstellen zu anderen Prozessen

Die wichtigsten Schnittstellen des Service Desks zu anderen ITIL-Prozessen sind beispielsweise wie folgt:

- **Incident Management** – Die überwiegende Mehrheit aller Calls sind Störungsmeldungen, die an das Incident Management weitergeleitet werden.
- **Configuration Management** – Den Störungen werden mögliche CIs aus der CMDB zugeordnet.
- **Change Management** – Service Requests werden mittels RFCs erfasst und dann seitens des Change Managements bearbeitet.
- **Service Level-Management** – Der Service Desk informiert beispielsweise den Anwender proaktiv über Service-Veränderungen oder neue Services.

2.5 Zusammenfassung

Ziele des Service Desks

- Garantiert die in den SLAs vereinbarte Erreichbarkeit der IT-Organisation
- Ist der Single Point Of Contact (SPOC) für den Anwender
- Sorgt für effektive Koordination und Einsatzzuordnung der nachfolgenden Service-Support-Einheiten
- Bietet zielgerichtete und lösungsorientierte Kommunikation mit dem Anwender
- Stellt eine ausgezeichnete „Visitenkarte“ der IT-Organisation für den Anwender dar

Aufgaben des Service Desks

- Annahme und Klassifikation von Incidents (und ggf. auch von Anfragen → Service Requests)
- Übernahme von Aufgaben anderer Prozesse wie zum Beispiel:
  - First Level Support im Incident Management
  - Erfassung der RFCs im Change Management
  - Audits und Reviews für das Configuration Management.

- Entlastung der Experten durch ein effektives Weiterleiten der Requests und Störungen inkl. der vollständigen Störungsinformationen
- Überwachen der Störungsbearbeitung und der Kundenzufriedenheit

Key Performance Indikatoren

- Erreichbarkeit (und auch Verfügbarkeit)
- Anzahl und Verhältnis der richtig und/oder falsch weitergeleiteten Störungen zu den gesamten Störungsmeldungen
- Maximale, minimale und durchschnittliche Warte- und Bearbeitungszeit
- Maximale, minimale und durchschnittliche Lösungszeit (Service Desk immer als Owner)
- Und vieles mehr, je nach Bedarf bzw. je nach Service …

3

3 ITIL V2 – Das Incident Management

Der Incident-Management-Prozess zählt für den Anwender zu den sichtbarsten Prozessen einer IT-Organisation. In diesem Prozess werden Störungen möglichst effektiv behoben, sodass der Service, wie im SLA (Service Level Agreement) vereinbart, wieder gewährleistet ist. Dazu ist es notwendig, Prozeduren für die Aufzeichnung, die Priorisierung, das Management der Auswirkungen, die Auswirkungsanalysen für das Business, die Klassifizierung, die Aktualisierung, die Eskalation, die Lösung und das formelle Schließen von Incidents zu entwickeln, zu definieren und einzuführen.

Praxistipps

In der Praxis kommt man nur in äußerst seltenen Fällen mit einem einzigen, überschaubaren Incident-Prozess aus. Bei der Entwicklung der Incident-Management-Prozesse gilt die Faustregel: Die Anzahl der von der IT zu erbringenden Services – sowohl dem Kunden bzw. Anwender als auch den internen IT-Services gegenüber – entspricht auch der Anzahl der zu entwickelnden Incident-Management-Prozesse. Selbstverständlich ergeben sich im Zuge der Entwicklung häufig entsprechende Synergie-Effekte.

Die Qualität eines IT-Services bzw. einer IT wird in der Praxis oft anhand der Durchlaufzeit von erfolgreich bearbeiteten Incidents gemessen, was allerdings für die wahre Qualität des IT-Services keine Aussagekraft hat. Das Incident Management dient dazu, auftretende Störungen und somit fehlende Qualitäten eines IT-Services im produktiven Betrieb zu beheben. Entscheidend für dessen Qualität ist jedoch die Anzahl der Anwender bzw. Kunden. Gute IT-Services bzw. IT-Systeme zeichnen sich stets durch wenige Störungsmeldungen trotz vieler Anwender aus.

Um den Incident-Management-Prozess effektiv entwickeln und ausführen zu können, muss vorab festgelegt sein, was überhaupt eine Störung (Incident) darstellt:

- Ein Incident ist ein Ereignis, eine Störung oder ein Zwischenfall, der bedingt durch eine nicht geplante betriebsbedingte Aktion (Maintenance), eine tatsächliche oder potenzielle Unterbrechung oder auch Minderung des im SLA vereinbarten Service verursacht wurde.
- Ein Service Request ist eine Anfrage des Kunden, der *keinen* Incident im eigentlichen Sinne darstellt, da der im SLA vereinbarte Service nicht gestört ist. Klassische Service

Requests stellen Anfragen bzgl. Service-Erweiterung (neue Funktionen, zusätzlichen Support etc.), Dokumentation oder Unterstützung der Anwender dar.

- Ein Complaint ist eine Beschwerde des Kunden und bedeutet ebenfalls *keinen* Incident im eigentlichen Sinne, da auch hier der im SLA vereinbarte Service nicht gestört ist. Eine Beschwerde führt in der Praxis oft zu einem Service Request, ist jedoch erst einmal kein solcher.

Entscheidend bei einem Incident-Management-Prozess ist, dass eine Störungsmeldung – egal ob sie von einem Monitoring System oder von einem Anwender stammt – eindeutig identifizierbar ist, und ob es sich wirklich um eine Störung handelt oder nicht. Vor allem bei eingehenden Anwendermeldungen ist häufig der Unterschied zwischen Incident, Service Request und Complaint nicht erkennbar, wenn das entsprechende SLA dem Incident Management nicht bekannt ist.

Praxistipp

Grundlage für die Definition einer Störung ist immer das jeweilige SLA – nicht der vom Anwender gefühlt zu erbringende Service der IT-Organisation. Im SLA sind die zu erbringenden Services und deren Levels definiert. Nur wenn diese nicht erfüllt sind, liegt ein Incident vor.

3.1 Der Incident-Management-Prozess

Abbildung 3.1 zeigt einen Incident-Management-Prozess, bei dem der Kunde bzw. das Business stets über den gesamten Zyklus einer berichteten Störung (oder auch einer Service-Anfrage) hinweg informiert und im Falle einer Minderung des vereinbarten Service-Levels proaktiv benachrichtigt und über die vereinbarten eingeleiteten Maßnahmen informiert werden sollte.

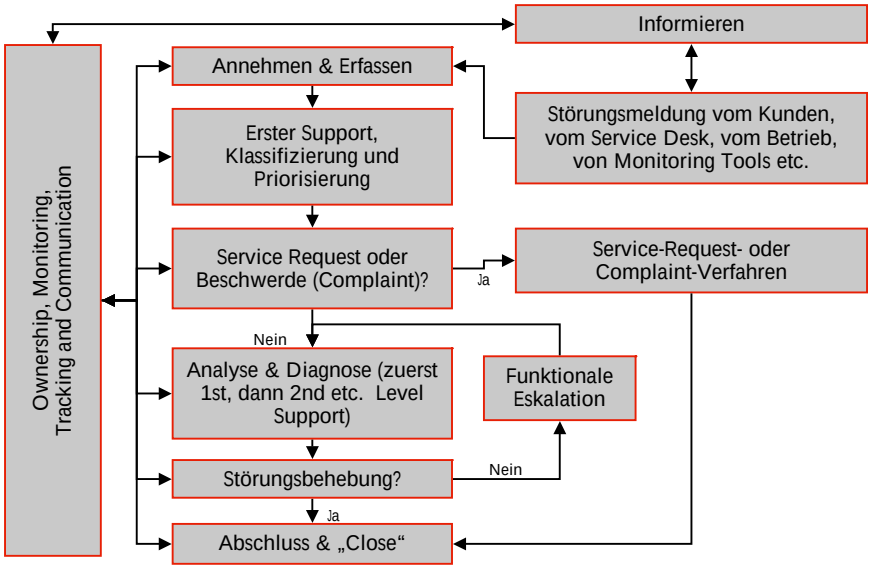

Abbildung 3.1 Incident-Management-Prozess – in Anlehnung an den ITIL Service Support

Praxistipp

Alle beim Incident Management involvierten Personen sollten Zugriff auf relevante Information wie bekannte Fehler, Problemlösungen und Workarounds besitzen sowie auf die Configuration Management Database (CMDB) zugreifen können, da die darin enthaltenen Informationen entscheidend für eine erfolgreiche und schnelle Störungsbearbeitung sind.

3.1.1 Identifikation von Störungen

Störungen werden in der Praxis entweder vom Anwender identifiziert und gemeldet – was allerdings für die IT kein gutes Zeugnis darstellt – oder durch ein Monitoring-System der IT, was auf eine effektive Funktionsweise der IT hindeutet.

Praxistipp

Wenn Störungen durch ein oder mehrere Monitoring-Systeme automatisch identifiziert werden, dann ist ein entsprechendes Event-Management-System – eine Art Interpretationsschicht, welche zwischen der Monitoring-System-Ebene und dem Incident Management angesiedelt ist – eine stets hierfür essenzielle Notwendigkeit, da beispielsweise nicht gleich jedes von der Monitoring-System-Ebene identifizierte, dedizierte Ereignis für sich selber einen Incident darstellt, aber in Kombination mit einem oder mehreren anderen identifizierten Ereignissen dann eventuell wieder doch.

3.1.2 Erfassung von Störungen

Alle Incidents müssen aufgezeichnet werden. Das Incident Management überprüft, ob die Störungsinformationen – egal ob automatisiert oder manuell – auch wirklich Störungen darstellen. Sollten sie sich als Störung herausstellen, werden sie erfasst, was in der Praxis mittels eines Ticketing-Tools erledigt wird. In der Regel gilt: pro Incident ein Ticket.

Bei der Störungserfassung ist großer Wert darauf zu legen, dass die Störungsinformationen stets vollständig erfasst sind – und vor allem ist auf das entsprechende Configuration Item (CI – siehe Kapitel 6, *Configuration Management*) zu referenzieren, was eine Verbindung zwischen Ticketing-Tool und Configuration Management Database (CMDB – siehe Kapitel 6, *Configuration Management*) erfordert. Anschließend folgt die Klassifizierung und Priorisierung des Incidents.

3.1.3 Klassifizierung und Priorisierung

Bei der Klassifizierung von Incidents unterscheidet man zwischen normalen und großen (Major) Incidents. Beim Major Incident sind in der Regel sehr viele Anwender und/oder IT-Services betroffen, was dann eine entsprechende Priorisierung des Incidents zur Folge hat. Die Priorität eines Incidents ergibt sich stets aus der Kombination von Auswirkung (z.B. Anzahl der betroffenen Anwender) und Dringlichkeit (z.B. produktives System oder Testsystem), wobei Major Incidents stets nicht nur eine hohe Priorität haben, sondern auch vor allen anderen Incidents absolut vorrangig zu bearbeiten sind.

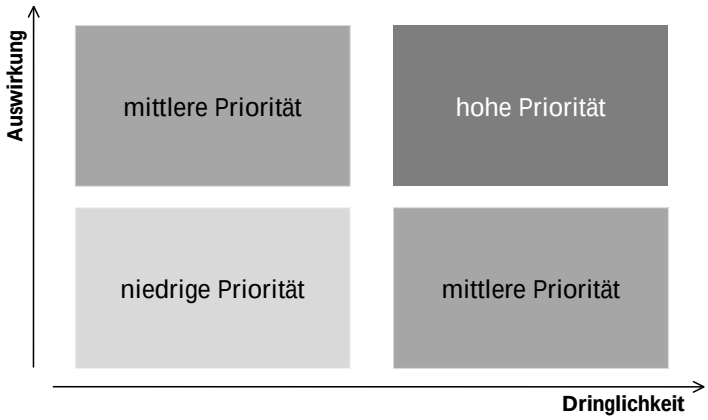

Abbildung 3.2
Prioritätsmatrix

Praxistipp

In der Praxis unterhält eine IT-Service-Organisation häufig mehrere SLAs und auch mehrere IT-Services. Hier sollte man die in ITIL definierte Priorisierungsmatrix (siehe Abbildung 3.2) um eine weitere Dimension der verschiedenen SLAs erweitern, da in jedem SLA normalerweise andere Reaktions-, Lösungs- und Wiederherstellungszeiten sowie zusätzliche Vertragsstrafen vereinbart sind, was vor allem bei größeren Unternehmen und externen IT-Dienstleistern der Fall ist. Die Handhabung der Priorität ist dann ohne ein entsprechendes Ticketing- und Service-Management-Tool, in dem die diesbezüglich relevanten Details aller SLAs erfasst sind, fast unmöglich.

Major Incidents sollten stets über einen eigenen Prozess klassifiziert und gehandhabt werden, da sie fast immer Störungen darstellen, die besonders große Auswirkungen auf die Kunden und das Business zur Folge haben. Meist entstehen dabei sehr hohe Kosten und Aufwände, weil große oder signifikante Teile eines IT-Services oder auch mehrere IT-Services nicht mehr verfügbar sind.

3.1.4 Diagnose und Analyse

Anschließend erfolgt eine Erstdiagnose und -analyse der Störung, jedoch nur in der dafür notwendigen Tiefe, um die Störung zu beheben. Probate Mittel sind:

- Eine Knowledge-Database oder Known-Error-Database (Wissensdatenbank – siehe Kapitel 4, *Problem Management*). In dieser sind unter anderem bekannte Fehler sowie deren Behebungen oder Workarounds hinterlegt.
- Eine Configuration Management Database (CMDB – siehe Kapitel 6, *Configuration Management*)

Sollte im First-Level-Support die Störung nicht behoben werden können, findet eine entsprechende Eskalation – eine funktionelle Eskalation – in den nächsthöheren Support-Level statt. Dieser versucht dann, die Störung zu beheben, oder eskaliert sie in den für ihn nächsthöheren Level. Das Ganze geht solange, bis die Störung behoben ist.

Bemerkungen

Das Gegenteil einer funktionellen Eskalation ist die hierarchische Eskalation – beispielsweise zum Incident Manager, der für den gesamten Incident-Prozess verantwortlich ist. Dieser Weg wird in der Praxis meistens nur bei Beschwerden seitens des Anwender beschritten oder wenn ein Major Incident vorliegt. Gravierende Entscheidungen wie beispielsweise der Neustart eines gesamten Rechenzentrums trifft normalerweise nicht der Support-Mitarbeiter, sondern der Incident Manager.

Es ist ein weitverbreiteter Irrtum, der First-Level-Support würde das Incident Management darstellen und der Second-Level-Support das Problem Management. Beide Prozesse haben in diesem Fall nichts miteinander zu tun. Innerhalb des Incident Managements existieren verschiedene Support-Level – angefangen vom First-Level-Support, der in der Praxis oft in den Service Desk ausgelagert ist, über den Second- bis hin zum Third-, Fourth-, Fifth-Level-Support etc., je nach den Anforderungen. Das Ende dieser Kette stellt meist der Support des Herstellers dar. Alle diese Support-Levels liegen jedoch innerhalb des Incident Managements und haben im Grunde nichts mit dem Problem Management zu tun.

Praxistipp

Bei Major Incidents und normalen Incidents mit einer hohen Priorität sollten in jedem Fall mittels eines Problem-Tickets, welches durch das Incident Management eröffnet werden sollte, eine Root-Cause-Analyse (Ursachenanalyse) seitens des Problem Managements initiiert werden, um so sicherzustellen, dass die Ursache der Störung identifiziert und auch nachhaltig behoben wird.

3.1.5 Störungsbehebung und Abschluss

Ist die Lösung bekannt, wird die Störung durch das Incident Management behoben und der Störungsmelder diesbezüglich informiert. Erst wenn der Anwender oder das meldende System bestätigt, dass die Störung behoben ist, wird sie vom Incident Management geschlossen – und nicht, wenn die IT-Organisation der Meinung ist, dass die Störung behoben ist.

Praxistipps

In der Praxis stellt man den Lifecycle eines Incidents mittels verschiedener Zustände dar, beispielsweise Incident in Bearbeitung = Störung wird bearbeitet; Incident fixed = Die IT ist der Meinung, dass die Störung jetzt behoben ist; Incident closed = Der Anwender hat bestätigt, dass die Störung behoben ist, oder das Monitoring-System meldet diese Störung nicht mehr. Jedoch sind weder Monitoring-Systeme noch Anwender unfehlbar. Tritt die gleiche Störung beim selben Anwender oder beim selben Monitoring-System zeitnah wieder auf, sollte es möglich sein, dieselbe Störung wieder zu eröffnen bzw. zu reaktivieren, was in der Praxis meist den Zustand „ReOpen“ bedeutet. Meldet jedoch ein anderer Anwender oder ein anderes Monitoring-System die gleiche Störung, so sollte dieses als eigene und neue Störung im Incident Management behandelt werden. Melden viele Anwender zeitnah die gleiche Störung, ist von einem Major Incident auszugehen.

Major Incidents bzw. Infrastruktur-Störungen werden meist nicht gleich bei der ersten Störungsmeldung als solche identifiziert. Ein sicheres Anzeichen dafür sind dann sich sehr schnell häufende gleiche oder ähnliche Meldungen. In diesem Fall sollte ein Major Incident eröffnet und alle bis dahin diesbezüglichen normalen Störungen auf diesen gemappt werden, damit sie beim Schließen des Major Incidents ebenfalls automatisch geschlossen werden. Weitere auf einen Major Incident bezogene Störungen braucht man dann nicht mehr erfassen, da es sinnlos

ist, dieselbe Störung x-mal aufzunehmen. Die IT sollte aber alle Anwender proaktiv über den Major Incident informieren, damit sie sich bei einer ihnen vorliegenden Störung nicht beim Service Desk melden – das verursacht nur unnötigen Aufwand.

Es ist nicht Aufgabe des Incident Managements, die Ursache der Störung zu finden und zu beheben. Dafür ist das Problem Management zuständig, was in der Praxis leider oft nicht berücksichtigt wird. Das Ziel des Incident Managements besteht darin, den Service so schnell wie möglich wiederherzustellen und die dafür notwendigen Diagnosen und Analysen durchzuführen. Wenn beispielsweise die Wiederherstellung des im SLA geforderten Service-Levels am schnellsten durch einen Neustart des Servers zu erreichen ist, dann stellt dies für das Incident Management die Lösung der Störung dar – unabhängig von deren Ursache. Allerdings lassen sich in der Praxis nicht alle Störungen ohne entsprechende Ursachenanalyse beheben. Dann eröffnet man ein entsprechendes Problem-Ticket, das in Bezug zum Incident-Ticket steht. Anschließend darf das Incident Management die Störung keinesfalls schließen, sondern vergibt einen entsprechenden Status wie „wait – problem ticket created". Dieses Problem-Ticket aktiviert den reaktiven Teil des Problem-Management-Prozesses (siehe Kapitel 4, *Problem Management*), der das Incident Management in der Störungsbehebung durch eine notwendige Ursachenanalyse und Fehleridentifizierung sowie Behebung durch einen Request for Change (RFC – siehe Kapitel 5, *Change Management*) unterstützt. Sobald das Problem-Ticket erfolgreich bearbeitet und geschlossen ist, erhält das Incident Management eine Mitteilung (automatisch bei einem guten Ticketing-System), und der Incident-Prozess läuft in der Störungsbearbeitung und -behebung normal weiter.

3.2 Schnittstellen zu anderen Prozessen

Die wichtigsten Schnittstellen des Incident Managements zu anderen ITIL-Prozessen sind:

- **Problem Management** – Das Problem Management stellt Information über Probleme, bekannte Fehler (Known Errors) und Workarounds zur Verfügung. Das Incident Management eröffnet bei Bedarf ein Problem-Ticket.
- **Change Management** – Incidents und Service Requests werden z.B. mittels Veränderungen unter Kontrolle des Change Managements behoben bzw. bearbeitet.
- **Configuration Management** – Informationen und Beziehungen über CIs aus der Configuration Management Database (CMDB) helfen, Incidents effizienter zu spezifizieren, zu bearbeiten und zu lösen (auch ohne ungewünschte Nebeneffekte).
- **Service-Level Management** – Informationen an das Service-Level Management (SLM) ermöglichen eine Qualitätsaussage über den Service. Das SLM stellt dem Incident Management wichtige SLA-Informationen wie beispielsweise Reaktions-, Lösungs- und Wiederherstellungszeit zur Verfügung.

3.3 Zusammenfassung

Ziele

- Eine schnelle Reaktion beim Eingang einer Störungsmeldung (sei es vom Kunden oder von diversen Monitoring- und Eskalationssystemen)
- Im Störungsfall die zügige Wiederherstellung des Services (gemäß den im SLA vereinbarten Leistungen)
- Die Beeinträchtigung der im SLA vereinbarten Leistungen im Störungsfall soweit wie möglich zu minimieren, beispielsweise durch das Anbieten von Workarounds
- Effizienter Einsatz von IT-Ressourcen (First-, Second- und Third-Level-Support-Einheiten)

Aufgaben

- Annahme, Registrierung, Klassifizierung, Priorisierung, Administration, Monitoring und Behebung und ggf. auch Eskalierung von Störungen
- Beheben und Schließen der gemeldeten Störungen (nach Absprache mit dem Kunden)
- Aktives Informationsmanagement – vor allem gegenüber den Kunden über den Verlauf ihrer Störungsbehebung
- Dokumentation von Anwender-, Störungs- und Lösungsinformationen
- Bereitstellung von vollständigen Informationen für das Problem- und Service-Level-Management

Key Performance Indikatoren

- Anzahl und das Verhältnis der gelösten Incidents innerhalb der in den SLA vereinbarten Zeiten zu den außerhalb liegenden, der „on time and on Budget“ zu den nicht „on time and on Budget“, wie im SLA vereinbart etc.
- Minimale, maximale und durchschnittliche Support-Kosten und -Zeit bezogen auf die Incidents
- Erstlösungsrate im Verhältnis zu den gesamten Incidents
- Verhältnis der richtig klassifizierten zu den falsch klassifizierten Incidents (Irrläufer)
- Und vieles mehr, je nach Bedarf …