# Basiswissen ITIL® 2011 Edition

Grundlagen und Know-how für das IT Service Management und die ITIL®-Foundation-Prüfung

von
Nadin Ebel

1. Auflage

dpunkt.verlag 2014

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 86490 147 8

Zu Inhaltsverzeichnis

# 15 Prozesse der Service Operation

Nachdem Sie im vorhergehenden Kapitel die Grundprinzipien der Service-Operation-Phase kennengelernt haben, sind die fünf Prozesse dieser Lifecycle-Phase und die Detailerläuterungen zu ihren Schlüsselelementen Gegenstand dieses Kapitels. Zu den Prozessen, die der Service-Operation-Phase angehören, aber auch andere Abschnitte des Service-Lebenszyklus unterstützen, gehören laut ITIL Event Management (Abschnitt 15.2), Incident Management (Abschnitt 15.3), Request Fulfilment (Abschnitt 15.4), Problem Management (Abschnitt 15.5) und Access Management (Abschnitt 15.6).

Sie enthalten Anleitungen für eine effektive und effiziente Erbringung der IT Services, ihren Support und ihre Pflege, um den definierten Wertbeitrag für den Kunden liefern zu können. Ich beschreibe in diesem Kapitel nach einer kurzen Einführung (Abschnitt 15.1) Zweck, Zielsetzungen und Umfang des jeweiligen Prozesses. Diese stehen in direkter Verbindung zu den strategischen Zielen des Serviceproviders und dem erwarteten Nutzen von Kundenseite, deren Realisierung letztendlich in der Service-Operation-Phase erfolgt.

Zu den Prozessen gehören Grundprinzipien sowie zentrale Begriffe, die im Zuge der Prozessumsetzung angewendet werden und die Ihnen für den jeweiligen Prozess bekannt sein sollten. Auch die Prozessaktivitäten mit Triggern, Inputs und Outputs des jeweiligen Prozesses, Rollen und Schnittstellen erläutere ich und gehe kurz auf einige beispielhafte Kennzahlen und Erfolgsfaktoren pro Prozess ein.

Dieses Kapitel beschäftigt sich nicht mit den Funktionen, die ITIL nennt. Sie sind Gegenstand des nächsten Kapitels.



## 15.1 Überblick über die Service-Operation-Prozesse

Die Prozesse in der Lifecycle-Phase Service Operation unterstützen das Management des Servicebetriebs. Das Ziel ist ein stabiler, möglichst fehlerfreier Servicebetrieb, der von einer Einhaltung der Service Level Agreements (SLAs) geprägt ist. Die Prozesse und die Funktionen (zu den Funktionen siehe Kap. 16) sind an diesen Service-Level-Zielen ausgerichtet. Zu diesen Prozessen gehören:

- Event Management:
  Identifizieren und Analysieren von Benachrichtigungen (Events), Erkennen von Ausnahmebedingungen und Ableiten von adäquaten Maßnahmen
- Incident Management:
  schnellstmögliche Wiederherstellung des normalen Servicebetriebs im Falle beeinträchtigter oder unterbrochener Services und die Minimierung der negativen Auswirkungen von Störungen auf den Geschäftsbetrieb
- Request Fulfilment:
  Bearbeiten von Anfragen der Anwender nach Information oder Standard-Serviceleistungen
- Problem Management:
  Ursachenanalyse zur Bestimmung und Beseitigung von Problemen und der aus ihnen resultierenden, immer wiederkehrenden Störungen sowie die Minimierung der Auswirkungen von nicht vermeidbaren Incidents
- Access Management:
  autorisierten Anwendern das Recht zur Nutzung eines Service zu gewähren und nichtautorisierten Anwendern den Zugriff verwehren

Da sowohl Prozesse als auch Funktionen für die Service Operation relevant sind, möchte ich Ihnen an dieser Stelle einen kurzen Überblick über die Funktionen geben (siehe Abb. 15–1). Sie werden in diesem Kapitel erwähnt, da sie an verschiedenen Prozessaktivitäten beteiligt sind, werden im Detail aber erst im nachfolgenden Kapitel erläutert. Funktionen stehen für organisationale Teilbereiche wie Teams, Gruppen oder Abteilungen.

Sie sind Teil der Aufbaustruktur eines Unternehmens, wohingegen Prozesse für die Ablauforganisation stehen und diese abbilden. ITIL nennt den Service Desk, das Technical und das Application Management sowie das IT Operations Management mit den zwei Unterfunktionen IT Operations Control und Facilities Management als Funktionen.

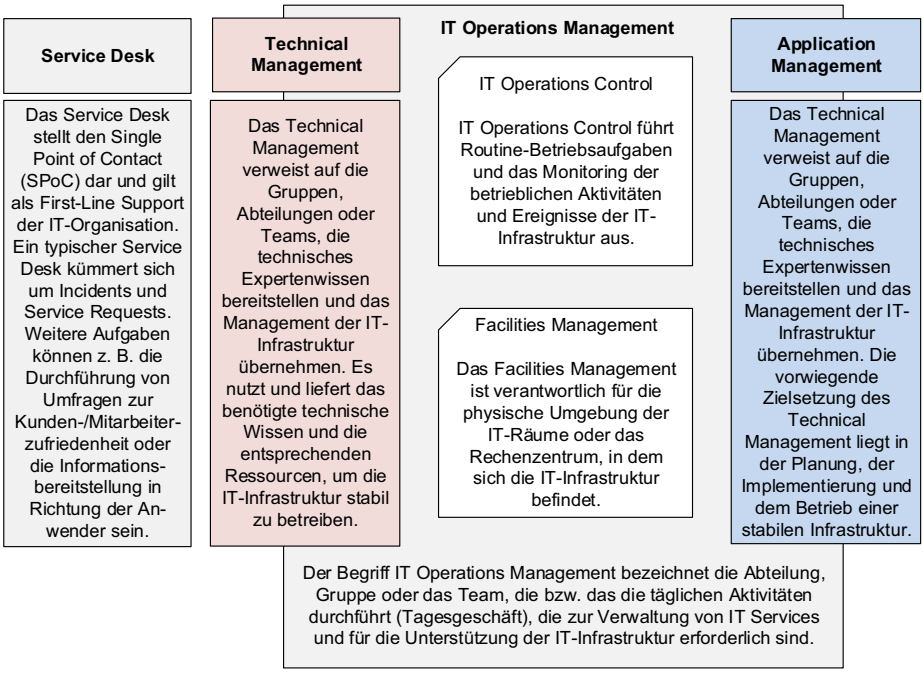


**Abb. 15–1** *Die Funktionen im Überblick*

## 15.2 Event Management

Für einen effektiven und effizienten Servicebetrieb wird der Status der Infrastrukturkomponenten und der Anwendungen als bekannt vorausgesetzt. Ist dieser Status nicht bekannt oder fehlt die Darstellung der Ist-Situation, sind diese Grundvoraussetzungen zu erarbeiten. Eine abgeschlossene Erhebung und Dokumentation des Ausgangszustandes ist notwendig, um den Zustand, der als funktionierend und »fehlerfrei« definiert wird, darzustellen. Abweichungen von einem fehler- und störungsfreien Zustand bzw. einem normalen oder erwarteten Betriebszustand werden im Event Management erkannt und an die relevanten Mitarbeiter oder Teams weitergeleitet.

Das Identifizieren und Analysieren von Events und das Ableiten von adäquaten Maßnahmen sind daher die Hauptaufgaben des Event Management. Als Events lassen sich alle Statusänderungen zusammenfassen, die für das Management eines Configuration Items (CI) oder die IT Services relevant sind. Events laufen typischerweise über Benachrichtigungen, die von einem IT Service, einer Komponente (CI) oder einem Monitoring-Tool erzeugt werden. Daher spielen die Tool-Auswahl und der Tool-Einsatz in Form von Monitoring- und Steuersystemen im Event Management eine wichtige Rolle. Dabei können zwei Arten von Tools Unterstützung leisten. Zum einen sind es Tools für aktives Monitoring, mit

denen die relevanten und definierten CIs abgefragt werden, um ihren Status und ihre Verfügbarkeit festzustellen. Alle Ausnahmen führen zu einem Alarm, der weitergeleitet und in adäquate Maßnahmen zu überführen ist. Zum anderen gibt es Tools für das passive Monitoring. Sie ermitteln und mappen operative Alarme oder die von CIs erzeugten Benachrichtigungen.

Das Event Management bietet die Möglichkeit, Incidents oder gar Probleme bzw. deren Ursachen frühzeitig zu entdecken. Es identifiziert Ansatzpunkte für Automatismen und zeigt so Optimierungspotenzial auf. Dies kann in eine Verringerung der Downtimes sowie Kosten- und Zeitersparnisse durch gezielte Hinweise auf Abweichungen münden.

### 15.2.1 Zweck und Zielsetzungen

Der Zweck des Prozesses besteht darin, die Steuerung und das Management der Events über ihren gesamten Lifecycle hinweg zu gewährleisten. Dieser Lebenszyklus reicht von der Entdeckung eines Events über die entsprechenden Schlussfolgerungen bis zur Auswahl der angemessenen Aktion. Daher steht die Entdeckung der relevanten Statusänderungen (als Events) genauso im Fokus wie die Auswahl der Maßnahmen, die Festlegung der passenden Steuerungsaktionen (z.B.: »Wie werden welche Schwellenwerte in Abstimmung mit wem definiert?« und »Wie gelangen die Informationen aus dem Event Management wohin?«) und die dazugehörige Kommunikation. Zudem stellt das Event Management eine Basis für das Service-Reporting dar.

Die Ziele des Event Management lassen sich folgendermaßen darstellen:

- Erkennen von relevanten Statusänderungen, die für das Management von CIs oder IT Services maßgeblich sind
- Identifizieren und Definieren geeigneter Maßnahmen für Events sowie Gewährleisten, dass diese Maßnahmen den entsprechenden Teams oder Mitarbeitern bekannt sind
- Anbieten von Ausgangs- und Ansatzpunkten für die Ausführung geeigneter Aktivitäten in den anderen Service-Operation-Prozessen. Sie sind durch den Anstoß über das Event Management in der Lage zu reagieren, um Servicebeeinträchtigungen zu beheben. Drei der fünf Prozesse in Service Operation sind diesbezüglich eng miteinander verzahnt: Event Management, Incident Management und Problem Management. Alle drei Prozesse beschäftigen sich mit dem Verarbeiten von vorwiegend ungeplant eingetretenen Vorfällen oder deren Ursachenforschung.
- Bereitstellen der Methoden und Verfahren zum Vergleich von Ist-Leistung und Soll-Leistung gemäß der SLA-Details. Daneben legt das Monitoring auch das unverzichtbare Faktenfundament für die Kapazitätsplanung und ermöglicht die professionelle Abrechnung von IT-Dienstleistungen auf der Grund-

lage von Service Level Agreements (SLA). Es spielt eine wichtige Rolle im Ressourcenmanagement und ist nicht wegzudenken beim Performance Tuning.
- Bieten einer Basis für die Servicezusicherung, das Service-Reporting und die Serviceverbesserung

### 15.2.2 Prinzipien und Begriffe

Das Event Management mit seinen vielfältigen Überwachungsaspekten und -optionen kann sich auf jeden Bereich des Service Management beziehen, der entsprechender Steuerung und Automatisierung bedarf. Beispiele hierfür sind z.B. CIs, die in Bezug auf Änderungen ihres Status überwacht werden, um Abweichungen rechtzeitig aufdecken zu können (z.B. ein fehlerfrei arbeitender Netzwerk-Switch, der in seinem »grünen« Zustand verbleiben soll, oder die Erreichbarkeit eines Servers über das Netzwerk), oder eine Umgebungsprüfung in einem Rechenzentrum (Brand- und Wasserschutz).

Dabei werden unterschiedliche Faktoren mit unterschiedlicher Zielsetzung abgefragt, was letztendlich dazu dient, Mechanismen für eine möglichst frühe Aufdeckung von Störungen bereitzustellen. Dies kann auch über Automatismen erfolgen. Je früher die Störung entdeckt wird, umso eher kann die Störungsbehebung aktiv werden, was letztendlich auch Auswirkungen auf die Servicequalität und Kundenzufriedenheit hat. Im besten Fall wird die Störung entdeckt und behoben, bevor der Anwender diese bemerkt.

#### Anwendungsbereiche und Umfang

Event Management kann in Bezug auf Steuerung und Automatisierung demzufolge für ganz unterschiedliche Aspekte des Service Management herangezogen werden. Events können allerdings nicht nur Fehler und Ausnahmen anzeigen, sondern auch belegen, dass Aktionen wie geplant und vorgesehen abgelaufen sind. Dementsprechend können sie auch ein Indiz dafür sein, dass eine Anwendung ganz normal läuft und verwendet wird, z.B. durch Einträge im Protokoll der Anwendung oder An- und Abmeldungen von Anwendern am System. Events können aber auch zeigen, dass Fehler am System auftreten, z.B. wenn ein Anwender wiederholt versucht, sich mit einem falschen Passwort anzumelden, oder ein Scan-Lauf zeigt, dass auf einem Arbeitsplatzrechner nicht autorisierte Software installiert wurde.

Demzufolge besitzt das Event Management einen recht großen Umfang. Dazu gehören sowohl CIs, die überwacht werden, weil sich ihr Zustand nicht ändern darf, oder CIs, die überwacht werden, weil sich ihr Status häufig ändern muss. Auch Umgebungsbedingungen (z.B. Feuer- und Raucherkennung) oder normale Aktivitäten können Teil des Event Management sein. Das Lizenz-Monitoring oder die (IT) Security können ebenfalls in das Event Management einbezogen werden.

Der Wertbeitrag des Event Management ist im Allgemeinen nicht direkt ersichtlich. Dadurch, dass über das Event Management die Möglichkeit besteht, Incidents frühzeitig zu entdecken, können sie der entsprechenden Gruppe zugewiesen und gelöst werden, bevor der verbundene Service beeinträchtigt wird. Event Management bietet Ansatzpunkte für Automatismen und schafft dadurch eine Verringerung der Downtimes, Kostenersparnisse und Zeit für das Betriebspersonal in Bezug auf andere Tätigkeiten. Eine Einbettung des Event Management in die anderen Prozesse im Service-Operation-Bereich und benachbarte Prozesse wie Availability oder Capacity Management aus der Service-Design-Phase ist zu empfehlen, um die Statusinformationen und sich abzeichnende Probleme frühzeitig abzufangen. Dies kann sich beispielsweise darauf beziehen, wenn die Speicherverwendung eines Servers (RAM) 7 % über dem akzeptablen Leistungslevel liegt oder eine Transaktion 12 % länger benötigt als normalerweise.

#### Richtlinien im Event Management

Für das Event Management ist eine Vielzahl von Richtlinien möglich. Über sie wird beispielsweise festgelegt, welche Event-Typen wohin berichtet werden. Benachrichtigungen sind nur zu den Verantwortlichen zu leiten, die für die weiteren Aktivitäten oder Entscheidungen zuständig sind. Zudem ist das Event Management und die entsprechende Unterstützung zentral anzusiedeln, um Konflikte bei der Erkennung und Behandlung zu vermeiden und klare Zuständigkeiten zu wahren. Dafür sind allgemeine Regelungen notwendig. Andernfalls kann es bspw. zu Verzögerungen bei der Entscheidungsfindung oder der Umsetzung kommen.

Automatismen werden, wo immer möglich und gerechtfertigt, eingesetzt, auch um u.a. eine konsistente Handhabung der notwendigen Schritte im Event Management umzusetzen. Dazu gehört auch ein standardisiertes Klassifizierungsschema (Eskalationsschritte, Einbindung des Incident und Problem Management etc.).

Ein weiteres Beispiel für eine Richtlinie im Event Management ist die Vorgabe, dass alle erkannten Events zu erfassen und zu protokollieren sind. Diese Daten- und Informationssammlung bietet Ansatzpunkte für die Untersuchung von Incidents, Problemen und Trends. Dafür ist es allerdings notwendig, einen entsprechenden Mechanismus mit ausreichend Ressourcen für die Erfassung und Aufbewahrung von Event-Informationen zu etablieren. Events werden möglichst einfach mit Incident und Problem Records verknüpft.

#### Event und Event-Typen

Ein Event (Ereignis) ist, wie bereits beschrieben, als Statusänderung definiert, die für ein CI oder einen IT Service signifikant ist. Events sind üblicherweise Benachrichtigungen, die für das Management eines IT Service, Configuration Item oder eines Monitoring Tools von Bedeutung sind und dementsprechend vorab über Schwellenwerte oder andere Trigger berücksichtigt wurden.

Es existieren unterschiedliche Klassifizierungsmöglichkeiten für Events, die nach einer entsprechenden Definition verlangen, um z. B. Routing- und Eskalationswege festzulegen (siehe Abb. 15–2). Die Wichtigkeit eines Events wird nach der ITIL 2011 Edition wie folgt festgelegt:

- Information:
  Dies gilt für ein Event, das keine Aktion benötigt und keine Störung darstellt (z. B. Anwenderanmeldung an einem System, Abschluss einer Installationsroutine, Mail-Zustellung).
- Warnung:
  Wenn ein CI oder Service einen Grenzwert erreicht, zeugt dies von einem unüblichen, aber nicht außergewöhnlichen (fehlerhaften) Verhalten. Warnungen weisen darauf hin, dass die Situation der Beobachtung bedarf, um die angemessenen Maßnahmen zu ergreifen und eine Störung zu verhindern (z. B. wenn Transaktionszeiten oder Bereinigungsläufe für Datenbanken länger als »üblich« dauern, Auffälligkeiten sich häufen). Es kann aber auch sein, dass sich der Fall von selbst erledigt. Die entsprechenden Regelungen sind in der Richtlinie zum Event Management zu finden.
- Ausnahme (Exception):
  Eine Ausnahme bedeutet, dass ein Service oder ein CI zurzeit nicht normal funktioniert. Beispiele für eine Exception sind z. B. ein ausgefallener Server oder zu lange Antwortzeiten einer Applikation. Derartige Ausnahme-Events werden ggf. zur Bearbeitung an das Incident Management weitergeleitet (siehe Abb. 15–5).

Das, was als normal, unnormal oder als eine Ausnahme anzusehen ist, muss individuell pro Service, Komponente und Unternehmen festgelegt werden. Für die entsprechenden Metriken gibt es keine pauschale Empfehlung.

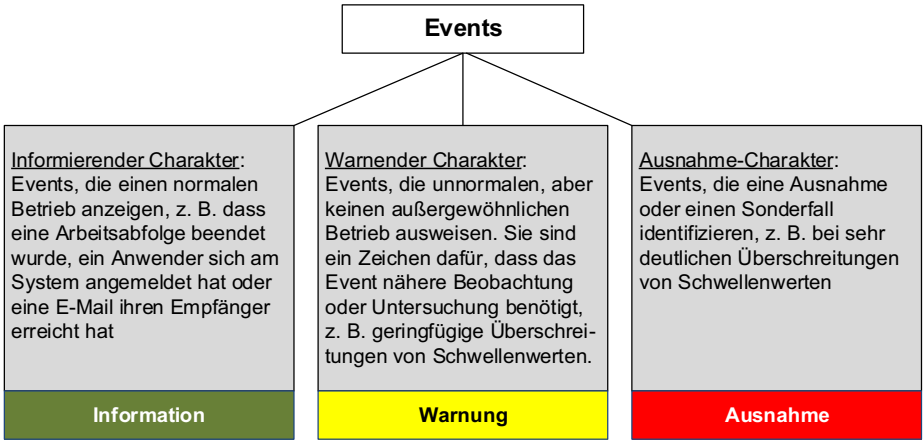


**Abb. 15–2** *Event-Typen*

Um der Fülle von Benachrichtigung Herr zu werden, ist es notwendig, die Events korrekt zu filtern, um die Ressourcen nur für die Maßnahmen für die Steuerung und das Management relevanter Events zu aktivieren.

### Alarm

Ein Alarm stellt eine Warnung dar, dass ein Grenzwert erreicht oder eine Änderung vorgenommen wurde bzw. dass ein Ausfall aufgetreten ist. Ein Alarm wird häufig über Systems-Management-Tools erstellt und gemanagt. Ein Alarm gewährleistet, dass über das Tool letztendlich eine Person über einen Event (z. B. das Erreichen eines Schwellenwertes) informiert wird. Die Festlegung, was einen solchen Alarm auslöst, erfolgt nach bestem Wissen durch einen Mitarbeiter des IT-Serviceproviders und richtet sich auch nach dem Detail- bzw. Informationsbedarf des IT-Serviceproviders insgesamt.

Einige Tools bringen bereits Empfehlungen für solche Definitionen mit oder nutzen voreingestellte Festlegungen. Diese sind zu verifizieren und bei Bedarf anzupassen. Nur wenn ein Grenzwert als Wert einer bestimmten Messgröße definiert und im System hinterlegt wurde, kann er einen Alarm auslösen (siehe Abb. 15–3). Beispiele für solche Grenzwerte sind zum Beispiel: »Incident mit Priorität 1 wurde nicht innerhalb von vier Stunden gelöst« oder »mehr als 5 Datenträgerfehler in einer Stunde«.

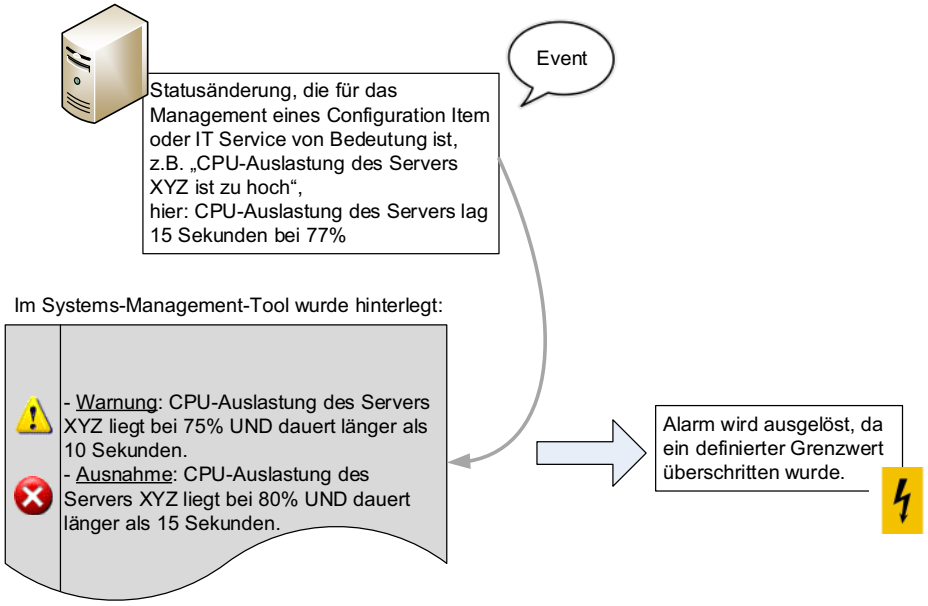


**Abb. 15–3** *Events können Alarme generieren.*

Der Alarm beinhaltet alle Informationen, um geeignete Maßnahmen einzuleiten. Um einen solchen Alarm zu generieren, ist es notwendig, dass ein entsprechendes Design diskutiert und abgestimmt wird, das über eine entsprechende Tool-Konfiguration hinterlegt wird.

### 15.2.3 Trigger und Input

Den Anstoß für den Prozess gibt eine Event-Meldung (Notification), die als Ausnahme, Warnung oder Information eingestuft wird (siehe Abb. 15–2). Somit könnte eine beliebige Statusänderung den Prozess anstoßen, wobei klar zu definieren ist, bei welcher Statusänderung Handlungsbedarf besteht.

Als Input dienen vorwiegend Ergebnisse aus dem Service Design und der Service Transition, z. B. SLR und Operational Level Requirements (OLAs) in Verbindung mit Events und den nachgelagerten Aktionen, Alarmen und Vorgaben für Schwellenwerte von Events sowie Korrelationstabellen, Regeln, Ereigniscodes oder automatisierte Lösungen. Auch Rollen und Verantwortlichkeiten für die Event-Bearbeitung und die Kommunikation dienen als Input. Aber auch Verfahren aus dem Betrieb in Bezug auf die Erkennung, Protokollierung, Eskalation oder die Kommunikation unterstützen die Aktivitäten des Prozesses.

### 15.2.4 Aktivitäten

Bevor der Prozess aktiv genutzt werden und seine Zielsetzungen erfüllen kann, ist es notwendig, das Design für das Event Management festzulegen. Dies erfolgt in der Regel in Zusammenarbeit von Prozess-Owner und Prozessmanager. Ist dies geschehen, kann der Prozess auf Basis des Designs ablaufen.

#### Design für das Event Management

Das Design für ein effektives Event Management erfolgt, bevor der Prozess aktiv wird. Dazu ist eine Vielzahl von Vorüberlegungen, Abwägungen, Abstimmungen und Festlegungen notwendig. Gibt es Verbesserungspotenzial für das Design, wenn der Prozess aktiv ist, können diese Verbesserungen über das Continual Service Improvement (CSI) erfolgen.

Die unterschiedlichen Teams und Abteilungen der Service Operation (Funktionen, siehe Kap. 16) wirken in der Regel am Design mit. Da das Event Management die Basis für das Monitoring der Service-Performance und -verfügbarkeit ist, sind die genauen Ziele und die Überwachungsverfahren zusammen mit dem Availability Management und Capacity Management abzustimmen und zu vereinbaren. Für das Event Management stellen die unterschiedliche Wünsche und Belange aus den anderen Prozessen in Bezug auf das Monitoring Anforderungen dar, die der Prozess abwägen und berücksichtigen muss. Im Zuge der Design-Dis-

kussion sind eine ganze Reihe von Fragen zu klären. Einige davon sind in Abbildung 15–4 dargestellt.

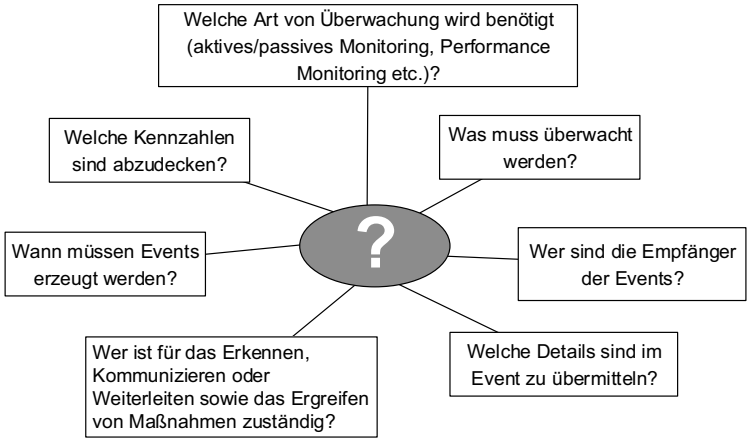


**Abb. 15–4** *Beispielhafte Fragen, die mindestens im Zuge des Prozessdesigns zu klären sind*

Das Design umfasst dann im Detail die folgenden Aspekte:

- Instrumentierung:
  Die Instrumentierung legt fest, auf welche Art und Weise IT Services überwacht und gesteuert werden. Diesbezüglich sind die entsprechenden Entscheidungen zu treffen und Mechanismen zu identifizieren, um diese Entscheidungen umsetzen zu können. Beispiele für Entscheidungen, die zu treffen sind, beziehen sich auf die Art und Weise, wie Events generiert und klassifiziert sowie kommuniziert und weitergeleitet werden. Zudem sind Fragen relevant, wie bspw. Events automatisch erzeugt und wo diese protokolliert und gespeichert werden.
- Generierung von Fehlermeldungen:
  Fehlermeldungen, die von Hardware und Software erzeugt werden, werden in aussagekräftiger Form an das Event Management übergeben.
- Event-Erkennung und Alarmmechanismen:
  Teil des Designs sind auch Festlegungen für Tools zum Filtern, Korrelieren und Weiterleiten von Events sowie die Eingabe weiterer Daten und Details in diese Tools. Für die Correlation Engine werden bspw. Regeln und Kriterien benötigt, um die Signifikanz von Events erkennen zu können und unterschiedliche Aktionen für die verschiedenen Event-Typen zu definieren. Um dies vornehmen zu können, sind bspw. Kenntnisse zu den Geschäftsprozessen, Service-Level, CIs und CI-Betrieb, Diagnose und den Kategorien sowie weiterer Details aus dem Incident-Management-Prozess notwendig. Aus diesem Grund ist es notwendig, dass die unterschiedlichen Teams mitwirken und ihr jeweiliges Fachwissen einbringen.

Die folgenden Aktivitäten sind Bestandteil des eigentlichen Event Management (siehe Abb. 15–5).

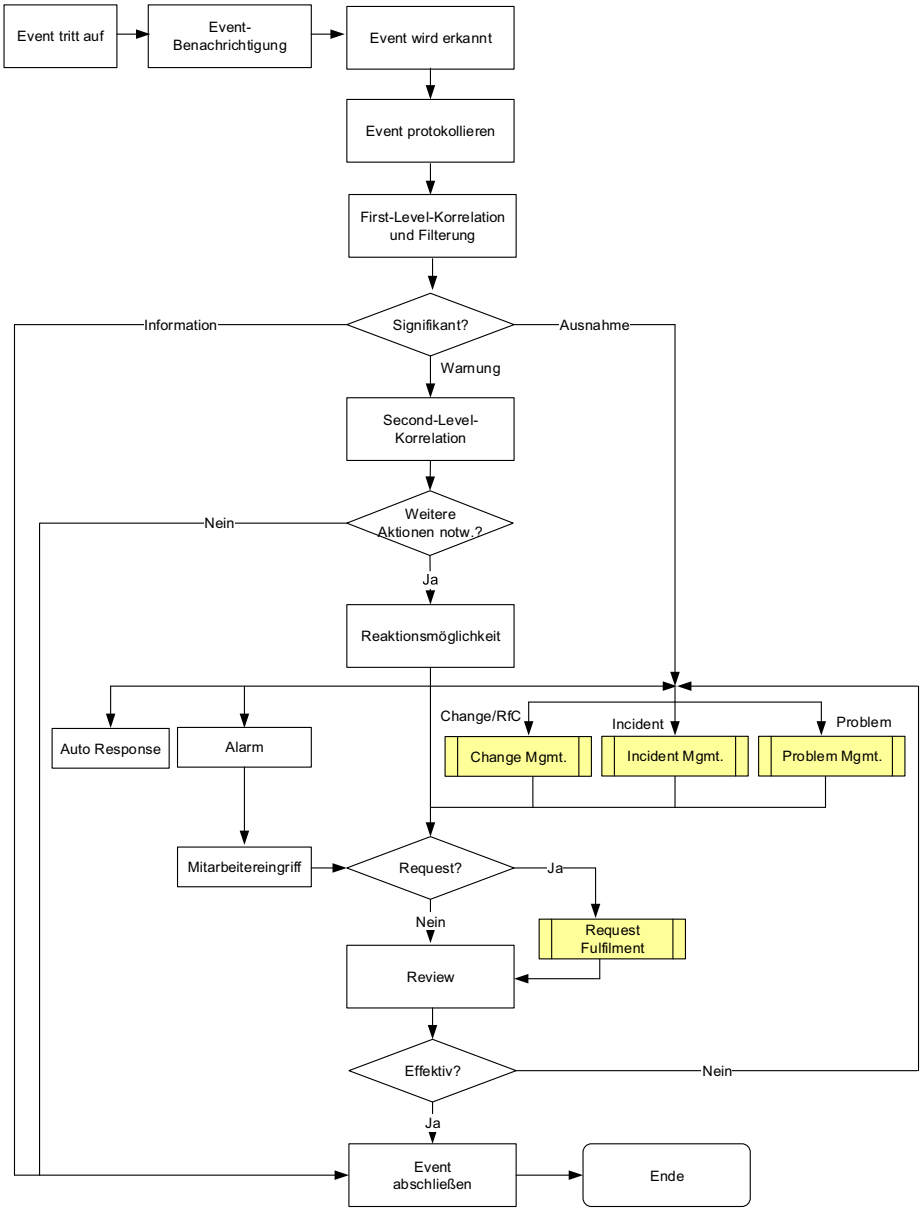


**Abb. 15–5** *Prozessdarstellung des Event Management (nach AXELOS-Material (ITIL®), Wiedergabe lizenziert von AXELOS)*

#### Eintreten eines Events

Events ereignen sich ständig. Nicht jedes Event ist für das Service Management relevant. Events können nicht nur bei Fehlern auftreten, sondern auch belegen, dass Aktionen wie geplant abgelaufen sind, z.B. durch Einträge im Protokoll einer Anwendung. Events können aber auch auf Fehler oder Probleme hindeuten, z.B. dann, wenn ein Scan zeigt, dass auf einem Client nicht autorisierte Software installiert wurde. Daher ist es besonders wichtig, dass alle an Design, Entwicklung, Management und Support der IT Services und der dafür genutzten IT-Infrastruktur beteiligten Mitarbeiter wissen und aufzeigen, welche Arten von Events erkannt und registriert werden müssen. Ohne diese Informationen, die bereits in das Design des Prozesses Eingang gefunden haben, kann das Event Management seine Ziele nicht erreichen und wäre weit entfernt von einem strukturierten und effektiven Vorgehen.

#### Event-Benachrichtung (Notification)

CIs oder Services können aktiv und/oder passiv in das Event Management eingebunden sein. Entweder geben sie selbst Meldungen ab, wenn sie definierte Schwellenwerte überschreiten, und/oder sie werden durch Tools oder Mechanismen regelmäßig hinsichtlich ihres Status abgefragt. Zudem können die Event-Benachrichtigungen aufgrund der eingesetzten herstellerspezifischen Tool-Auswahl proprietär sein, d.h., Tools anderer Hersteller können die entsprechenden Events nicht erkennen und registrieren. Daher ist in vielen Fällen die Verwendung eines offenen Standards zu empfehlen. SNMP (Simple Network Management Protocol) ist ein Beispiel für einen solchen Standard. Durch seine Einfachheit, Modularität und Vielseitigkeit hat sich SNMP zu einem Standard entwickelt, der von den meisten Managementprogrammen und Endgeräten unterstützt wird. Zur Überwachung werden sogenannte Agenten eingesetzt. Dabei handelt es sich um Programme, die direkt auf den überwachten Geräten laufen. Diese Programme sind in der Lage, den Zustand des Gerätes zu erfassen und auch selbst Einstellungen vorzunehmen oder Aktionen auszulösen. Mithilfe von SNMP ist es möglich, dass die zentrale Management-Station mit den Agenten über ein Netzwerk kommunizieren kann. Welche Formen und Typen der Event-Meldungen eingesetzt werden, ist meist abhängig von der eingesetzten Systems-Management-Lösung.

Auch für diese Aktivität ist ein gutes Design des Prozesses Voraussetzung. Idealerweise definieren die beteiligten Mitarbeiter bereits im Zuge der Service-Design-Phase, welche Events erzeugt werden und wie dies für den jeweiligen CI-Typ auszusehen hat. In der Praxis wird meist von einem Standard-Set des jeweiligen Systems-Management-Tool ausgegangen, das im Laufe der Zeit immer weiter angepasst wird, um z.B. neue Event-Typen hinzuzufügen oder andere Events auszuklammern. Im Allgemeinen sind in Bezug auf die Event-Meldungen vor allem die Inhalte und Daten relevant. Kodierte Meldungen verlangen (außer bei erfah-

renen Spezialisten) meist nach Rechercheaufwänden. Sprechende Meldungen sowie definierte Zuständigkeiten und Rollen werden während des Service Designs und der Service Transition formuliert und dokumentiert. Andernfalls kann es passieren, dass Arbeiten doppelt oder gar nicht umgesetzt werden.

#### Event-Erkennung (Detection)

Nach Generierung der Event-Benachrichtigung erfolgt die Erkennung durch den Agenten, der auf demselben System ausgeführt wird, oder die direkte Übergabe der Event-Meldung an den Prozess. Dies kann automatisiert z.B. über ein Management-Tool erfolgen.

#### Event-Protokollierung

Der notwendige Event Record kann z.B. als Eintrag im Event Management-Tool und die nachfolgenden Maßnahmen festgehalten und gepflegt werden. Später kann dieser Eintrag ggf. durch das Incident Management eingesehen oder bearbeitet werden. Voraussetzung dafür ist allerdings ein Tool, das eine solche Zusammenarbeit über Prozessgrenzen hinweg ermöglicht.

In diesem Zusammenhang sind durch die verantwortlichen Teams Maßgaben hinsichtlich der Frage zu entwickeln, wer auf die Events Zugriff hat und wie lange Events wo verbleiben, bevor sie archiviert und gelöscht werden. Steht kein integrierendes, umfassendes Tool zur Verfügung, bestünde auch die Möglichkeit, einen Eintrag im Systemprotokoll als Event Record zu verwenden, diesen regelmäßig zu prüfen und auf dieser Basis Maßnahmen zu entwickeln und umzusetzen, falls notwendig.

#### Erste Event-Einstufung und Filterung

Da die Menge der täglich zu erwartenden Meldungen nicht ohne weiteres zu bewältigen ist, werden die wichtigen Meldungen sorgfältig identifiziert. Dies erfolgt bereits frühzeitig durch die Filterung. Dabei wird festgelegt, ob das Event überhaupt an ein Management-Tool weitergegeben oder ignoriert wird. Erfolgt Letzteres, steht zwar ein Eintrag in einem Systemprotokoll, weitere Maßnahmen werden aber nicht ergriffen. Nicht immer ist es möglich, irrelevante Event-Benachrichtigungen im Vorfeld zu deaktivieren.

Im Zuge der Filterung erfolgt eine erste Einstufung des Events in die drei unterschiedlichen Event-Typen (Information, Warnung, Ausnahme), die üblicherweise toolgestützt über einen Agenten oder eine Correlation Engine erfolgt. Werden die Meldungen durch ein Korrelationsverfahren mit festgelegten Korrelationsregeln analysiert und verdichtet, können teilweise neue, qualifizierte Meldungen entstehen, während die als unbedeutend erkannten Meldungen ignoriert oder unterdrückt werden. Nicht immer ist eine solche Einstufung in die unter-

schiedlichen Event-Typen notwendig, da bei manchen CIs jedes Event von Bedeutung ist.

#### Kategorisierung von Events bezüglich deren Signifikanz

Jede Organisation wird ihre eigene Einstufung der Events nach ihrer Signifikanz und vornehmen, bspw. in Form dreier allgemeiner Kategorien wie Information, Warnung oder als Ausnahme (siehe Abb. 15–2). Bei Bedarf können weitere oder anders abgegrenzte Kategorien definiert werden, die die Bedeutung der Events berücksichtigen und anzeigen.

#### Zweite Event-Einstufung

Liegt eine Warnung vor, ist auf Basis einer Event-Analyse zu entscheiden, ob und welche Maßnahmen einzuleiten sind. Dies übernimmt die Correlation Engine, die üblicherweise Teil des Management-Tools ist. Sie vergleicht die Events mit verschiedenen Kriterien und Regeln. Dies dient auch zur Bestimmung, ob ein Zusammenhang zwischen Events, CIs und/oder Services vorliegt. Diese Kriterien werden auf Basis von Vorgaben des Service Design eingesetzt. Wird durch die Korrelation ein Event erkannt und identifiziert, sind entsprechende Aktionen als Antwortverhalten für das jeweilige Event notwendig.

Warum eine Korrelation wichtig ist, zeigt folgendes Beispiel: Ein erfolgloser Anmeldeversuch an einem System ist isoliert betrachtet nicht als hoch einzustufen. Wenn dieser Vorgang jedoch zeitgleich an unterschiedlichen Systemen passiert, dann könnte von einem gezielten Angriff ausgegangen werden. Erst die Betrachtung und Prüfung des Kontextes einer Statusmeldung bringt zusätzliche Aussagekraft. Die Signifikanz für den Betrieb steigt.

#### Abklärung der Notwendigkeit, weitere Maßnahmen zu ergreifen

Wurde im vorangegangenen Schritt ein relevantes Event ermittelt, geht es bei dieser Aktivität darum, zu entscheiden, ob weitere Maßnahmen erforderlich sind. Mögliche Reaktionen können sein:

- Erstellen eines Incident Records, falls eine Störung vorliegt oder eine Störung auftreten wird, falls keine Reaktion erfolgt. Auf diese Weise wird der Incident-Management-Prozess initiiert.
- Erstellen eines Request for Change (RfC), falls Fehlerursache und die dementsprechende Lösung bereits zweifelsfrei bekannt sind. Auf diese Weise wird der Change-Management-Prozess initiiert.
- Ausführen eines Skriptes, um bestimmte Aktionen auszuführen (Batch-Job starten, Dienst-Neustart, Admin-Tasks o.Ä.), für die keine Interaktion mit dem Change-Management-Prozess notwendig ist
- datenbankspezifische Maßnahmen

- Erstellen eines Tickets für das Problem Management zur Ursachenforschung bei einem aufgetretenen Problem. Auf diese Weise wird der Problem-Management-Prozess initiiert.

#### Auswahl der Reaktion

In Abhängigkeit vom Analyseergebnis sind unterschiedliche Reaktionen auf ein Event denkbar. Auch eine Kombination von Maßnahmen ist möglich. Eine automatische Reaktion (Auto Response) kann unter Umständen umgesetzt werden (System-Reboot, Service-Restart o. Ä.). Falls das Event über einen Alarm nach einem Eingriff eines Mitarbeiters verlangt, muss dies (funktional) eskaliert werden, um sicherzustellen, dass sich die richtige Person des Events annimmt.

Je nach Event kann es aber notwendig sein, dass das Incident, Problem oder Change Management ins Boot geholt wird. Dies bedeutet, dass das Event Management einen dieser Prozesse anstößt. Dies geschieht in der Regel, indem ein Incident oder Problem Record eröffnet oder ein Request for Change (RfC) erstellt wird. In der Regel allerdings nicht direkt ein Problem Record erstellt, sondern dieser wird über einen Incident Record, der so viele aussagekräftige Informationen wie möglich enthält, angelegt.

#### Review von Aktionen

Bei dieser Aktivität geht es um die Frage, ob bedeutende Events angemessen bearbeitet worden sind und geschlossen werden können. Da pro Tag Tausende von Events erzeugt und bearbeitet werden, kann nicht jedes Event einem formalen Review unterzogen werden. Nur signifikante Events und Ausnahmen werden einer Überprüfung unterzogen, um festzustellen, ob die Event-Ursache beseitigt werden kann, sich allgemein ähnliche Trends abzeichnen oder ob Nachbearbeitung notwendig erscheint. Ist das Event als RfC sowie als Record im Incident bzw. Problem Management vorhanden, muss sichergestellt werden, dass zum einen keine doppelten Reviews stattfinden und dass zum anderen die Schnittstellen zwischen den Prozessen und die Übergaben sauber funktionieren.

Die Ergebnisse des Reviews werden auch als Input für das Continual Service Improvement (CSI), als Basis für die Evaluation und das Audit des Event Management verwendet.

#### Review-Abschluss

Hier werden die Event Records und Logs nach Trends und Mustern analysiert und es werden gegebenenfalls korrigierende Maßnahmen zur Verbesserung der Event-Filterung und -Korrelation abgeleitet.

Manche Events bleiben offen, bis die entsprechenden Aktionen für den Abschluss des Events stattgefunden haben. Die meisten Events werden jedoch nicht explizit geöffnet oder geschlossen. Events mit Informationscharakter kön-

nen als Input für andere Prozesse dienen, z.B. für das Backup und Storage Management. Auto Response Events werden durch die Nachricht automatisch geschlossen, dass das System wie definiert arbeitet.

### 15.2.5 Output

Ergebnisse dieses Prozesses sind bspw. Events, die kommuniziert und an den zuständigen Mitarbeiter weitergeleitet wurden. Auch Event-Logs, die die Geschehnisse darstellen, zählen zu den Outputs des Prozesses. Dazu gehören z.B. auch Events, die eine SLA- oder OLA-Verletzung anzeigen, oder auf einen Incident hinweisen. Events und Alarme, die den Abschluss einer Aktivität anzeigen oder sonstige Supportaktivitäten signalisieren, werden vom Event Management als Output ausgegeben.

### 15.2.6 Schnittstellen

Das Event Management kann Schnittstellen zu jedem anderen Prozess aufweisen, der nach Input aus dem Bereich Monitoring und Steuerung verlangt, ohne auf Echtzeit-Monitoring angewiesen zu sein.

Die primären Beziehungen zeigen sich entsprechend der Aktivitätenbeschreibung in Richtung *Incident, Problem und Change Management*. Das *Availability und das Capacity Management* leisten wertvolle Unterstützungsleistung bei der Frage, welche Events signifikant sind, welche Schwellenwerte zu definieren sind und wie auf Überschreitungen zu reagieren ist. Umgekehrt kann das Event Management die Verfügbarkeit und Leistung eines Service durch rasche und richtige Reaktionen verbessern. Durch das entsprechende Berichtswesen in Richtung *Service Level Management* für aktuelle Events und Event-Muster (im Vergleich zu SLA-Zielen und Kennzahlen) könnten Aspekte des Infrastruktur-Designs oder des Betriebs aufgezeigt werden, die es zu verbessern gilt. Über das *Information Security Management* erfolgt eine Interaktion mit den Schnittstellen zu den Geschäftsanwendungen und/oder Geschäftsprozessen, um mögliche signifikante Geschäftsereignisse ausfindig zu machen und zu reagieren, z.B. bei möglichen Sicherheitsverstößen.

Das *Service Asset and Configuration Management* ist in der Lage, aufgrund der Event-Informationen den Status der CIs in der Infrastruktur zu bestimmen. Beim Vergleich der Events zu den CI-Baselines kann es auch möglich sein, unautorisierte Change-Aktivitäten aufzudecken. Das Asset Management kann das Event Management nutzen, um Statusinformationen als Events, z.B. nach Implementierung oder Umzug eines Assets, zu erhalten. Events können auch dem Knowledge Management als Input dienen, z.B. für zukünftige Design- und Strategieentscheidungen.

### 15.2.7 Rollen

Auch die generischen Rollen des Prozessmanagers und des Prozess-Owners sind an diesem Prozess beteiligt.

In den Zuständigkeitsbereich des Prozess-Owner im Prozess fallen das Ausführen der generischen Prozess-Owner-Rolle, die Planung und das Management für den Support von Event-Management-Tools und -Aktivitäten sowie die Zusammenarbeit mit den Prozess-Ownern der anderen Prozesse. Diese Kooperation dient der Sicherstellung eines umfassenden Ansatzes für das Design und die Implementierung von Event Management, Incident Management, Request Fulfilment, Access Management und Problem Management.

Der Prozessmanager kümmert sich um die generischen Aufgaben eines Prozessmanagers und die Koordination der Schnittstellen zwischen dem Event Management und den anderen Service-Management-Prozessen. Darüber hinaus können auch Service-Desk-Mitarbeiter oder Mitarbeiter der anderen Funktionsbereiche an diesem Prozess beteiligt sein (siehe Kap. 16).

### 15.2.8 Beispielhafte Kennzahlen und Erfolgsfaktoren

Beispiele für Kennzahlen des Event Management sind:

- Anzahl und Prozentsatz der Events, die einen Incident oder Problem Record nach sich ziehen (und die Veränderung dieser Kennzahl im Zeitverlauf)
- Anzahl der Incidents, die aufgetreten sind, ohne eine vorherige Identifikation durch das Event Management, oder das Verhältnis von Incidents und Events
- Anzahl der Events nach Kategorie und nach Signifikanz

Beispiele für Erfolgsfaktoren für den Prozess sind:

- Sicherstellen der Kommunikation zu den relevanten und definierten Funktionsbereichen hinsichtlich der für sie wichtigen Events
- erprobte und akzeptierte Richtlinien hinsichtlich der Korrelations- und Eskalationsverfahren sowie eine adäquate Umsetzung der Alarmkonfiguration



## 15.3 Incident Management

Das Incident Management registriert, prüft, kategorisiert, priorisiert und verfolgt alle Servicestörungen, um diese so schnell wie möglich mit minimalen Auswirkungen für die Anwender zu beheben. Der Prozess ist also für das Management des Lebenszyklus aller Incidents verantwortlich. Dabei werden erste Hilfestellungen geleistet, und gegebenenfalls wird die weitere Bearbeitung in den nachgelagerten Supporteinheiten koordiniert.

Ein solcher Incident (Störung) ist definiert als eine nicht geplante Unterbrechung eines IT Service oder eine Qualitätsminderung eines CI ggf. ohne bisherige