Fachhochschule Wiener Neustadt
Wirtschaft · Technik · Gesundheit · Sicherheit · Sport

IT Service Management

Masterstudium "IT Management"
2. Semester, SS 2013

Dipl. BW (FH) Christian Philipp
Dipl. BW (FH) Marcus Römer

Fachhochschule Wiener Neustadt
Wirtschaft · Technik · Gesundheit · Sicherheit · Sport

Service Operation

Grundlagen und Modelle
Event Management
Incident Management
Request Fulfillment
Problem Management
Access Management

Service Operation: Management Summary

- Koordination und Ausführung der notwendigen Aktivitäten und Prozesse, um Services in der zugesagten Qualität an den Kunden und die Anwender zu liefern
- Fortwährendes Management der zur Service-Erbringung notwendigen Technologie: Monitoring, Messung, Sammeln von Daten
- Management der für die Service-Erbringung notwendigen Facilities (Rechenzentren und deren Infrastruktur)

Service Operation: Wert für das Business

- Aus Kundensicht ist "Service Operation" die Phase, in welcher der Wert für das Geschäft am deutlichsten sichtbar ist
- Durch effektives Event-, Incident- und Problem-Management können Design-Schwächen erkannt werden, ebenso durch die Auswertung der in der Service Operation Phase gesammelten Daten
- Die Kundenzufriedenheit wird durch zielgerichtetes, professionelles Request Fulfilment und Access Management hoch sein
- Die Betreuung der Anwender durch den Service Desk erleichtert den Anwendern die Kommunikation mit dem Service Provider und bietet schnellstmögliche Unterstützung bei Änderungswünschen oder ServiceUnterbrechungen

Erreichen von Balance in Service Operation

- Die interne Sicht vs. Externe Business Sicht

- Stabilität vs. Reaktionsfreudigkeit
- Service-Qualität vs. Service Kosten
- Reaktiv vs. proaktiv

Service Operation basierend auf ITILv3, van Haren Publishing, 2008

Operation → Service Bereitstellung

Alle Service Operation Mitarbeiter müssen sich dessen bewusst sein, dass sie einen Service für das Business bereitstellen!

→ Daher sollte man Mitarbeiter nicht nur in der Bereitstellung und der Unterstützung von IT Services trainieren, sondern auch ihre persönliche Einstellung, mit der sie diese Services bereitstellen.

Überblick

Event Management
Request Fulfillment
Incident Management
CMDB
Problem Management
Change Management
SACM

IT Betrieb - Operations

- **Die Operations Bridge**
  ist der zentrale Koordinationspunkt, der eine Reihe von Events und operativen Routineaktivitäten steuert; sie bemerkt Incidents und berichtet über den Performancestatus von Technologiekomponenten.
- **Job Scheduling**
  IT Operations führt die Standardroutinen, -anfragen oder -berichte durch, die die technischen Teams sowie die des Anwendungsmanagements als Teil des Service oder als Teil von täglichen Routinewartungsaufgaben an es übertragen haben.
- **Backup und Wiederherstellung**
  Backup und Wiederherstellung ist notwendigerweise eine Baustein gut geplanter Continuity. Das Service Design muss bei der Gewährleistung dessen, dass es für jeden Service gute Backup-Strategien gibt, unter-stützen

IT Operations führt die täglichen, operativen, für das Management der IT-Infrastruktur notwendigen Aktivitäten durch.

Andere operativen Tätigkeiten

- Mainframe Management
- Server Management und –Support
- Netzwerk Management
- Storage und Archivierung
- Datenbankmanagement
- Directory Services-Managment
- Desktop-Support
- Middleware Management
- Internet/Web-Management
- Facility- und Rechenzentrums-Management

9

Mainframe-Management

Mainframes bilden den zentralen Teil vieler Services. Ihre Leistungsfähigkeit sowohl für die Service-Leistung als auch für die Anwender- und Kundenerwartung Ausgangspunkt.

Server-Management und -Support

Die meisten Organisationen nutzen Server, um flexible und zugängliche Services zum Hosting von Anwendungen oder Datenbanken oder zur Durchführung von Client Server-Services, Storage, Druck- oder Dateimanagement anzubieten.

Netzwerk Management

Da die meisten IT Services von Konnektivität abhängen, ist Netzwerk Management für die Service-Bereitstellung entscheidend. Außerdem greifen Service OperationMitarbeiter über das Netzwerkmanagement auf wichtige Servicekomponenten zu.

Storage und Archivierung

Viele Services erfordern es, dass Daten für eine bestimmte Zeit gespeichert werden. Häufig müssen solche Daten, so sie nicht mehr regelmäßig benötigt werden, in einem Offline-Archiv verfügbar gemacht werden. Dies geschieht nicht nur im Sinne der Compliance mit externen Regularien und Gesetzen, sondern auch, weil Daten aus einer Vielzahl weiterer Gründe von unschätzbarem Wert für eine Organisation sind.

Datenbankmanagement

Das Datenbankmanagement muss eng mit wichtigen Teams oder Abteilungen des Anwendungsmanagements zusammenarbeiten. In einigen Organisationen können die Funktionen kombiniert oder in eine eigene Managementstruktur gebracht werden.

Directory Services-Management

Ein Directory Service ist eine spezielle Softwareanwendung, welche Informationen über die in einem Netzwerk verfügbaren Ressourcen und die Anwender, für welche diese im Zugriff sind, verwaltet. Sie bildet die Basis dafür, den Zugriff auf diese Ressourcen zu gewährleisten oder zu erkennen und zu verhindern, dass dieser unauthorisiert erfolgt.

Service Operation Team

Die Rolle eines Service Operation-Teams umfasst:

- **Grundsätze und Berichte**
- **Technische Unterstützung**
- **Operatives Sicherheitsmanagement**
- **Selektion und Sicherheitsüberprüfung**
- **Schulung und Bewusstsein**

10

Grundsätze und Berichte - operative Mitarbeiter überprüfen System-Journals, Logs, Meldungen der Event-Überwachung, Entdeckung von Hackern sowie tatsächliche oder mögliche Sicherheitsverletzungen. Um dies zu tun, arbeiten sie eng mit dem Management der Informationssicherheit zusammen. So beginnt ein System gegenseitiger Kontrolle, das erfolgreiche Erkennung und Steuerung von Sicherheitsfragestellungen gewährleistet.

Technische Unterstützung - manchmal benötigen IT-Sicherheitsmitarbeiter Unterstützung bei ihrer Untersuchung von sicherheitsrelevanten Incidents, für die Erstellung von Berichten oder die Zusammenstellung forensischer Beweise, die für Disziplinarmaßnahmen oder die Strafverfolgung verwendet werden

Operatives Sicherheitsmanagement - aus operativen Gründen benötigen Techniker Zugang zu wichtigen technischen Bereichen (Root-Systempasswörter, physischen Zugang zu Rechenzentren oder Kommunikationsräumen etc.); es ist wichtig, dass all diese Aktivitäten geprüft und dokumentiert werden, so dass sicherheitsrelevante Events entdeckt oder verhindert werden können

Selektion und Sicherheitsüberprüfung - zur Gewährleistung, dass jedes Mitglied der Service Operation-Belegschaft dem Sicherheitsniveau der Organisation entspricht, erfolgt eine Überprüfung des Hintergrunds eines jeden Mitarbeiters; auch der Hintergrund von Lieferanten und dritten Parteien kann einer Sicherheitsüberprüfung bedürfen

Schulung und Bewusstsein - Service Operation-Mitarbeiter müssen regelmäßig in den Sicherheitsgrundsätzen und -verfahren einer Organisation geschult werden; dies fördert das Sicherheitsbewusstsein. Darüber hinaus müssen diese Schulungen Details zu Disziplinarmaßnahmen enthalten.

Funktionen

Organisationseinheiten, die

- Spezialisiert sind auf die Ausführung bestimmter Aufgaben
- Für bestimmte Ergebnisse verantwortlich sind
- In sich geschlossene Einheiten mit Fähigkeiten und Ressourcen sind
- Über ihren eigenen Wissensgehalt (durch Erfahrung aufgebaut) verfügen
- Struktur und Stabilität der Organisation bilden
- Rollen und zugehörige Berechtigungen und Zuständigkeiten definieren

© Crown copyright 2007 Reproduced under license from OGC

Service Desk

Zentraler Service Desk

Lokaler Service Desk

Virtueller Service Desk

Follow-the-Sun

© Crown copyright 2007 Reproduced under licence from OGC

Technisches Management

Das technische Management unterstützt bei der Planung, Implementierung und Wartung einer stabilen technischen Infrastruktur zur Unterstützung der Geschäftsprozesse der Organisation durch:

- eine gut entworfene und kosteneffektive technische Architektur
- Einsatz angemessener technischer Fähigkeiten zur Beibehaltung des optimalen Zustands der technischen Infrastruktur
- Gute Ausnutzung technischer Fähigkeiten zur raschen Bestimmung und Behebung technischer Fehler

Zielsetzungen des IT Operations Management sind,

- Aufrechterhaltung der gegenwärtigen Situation zur Erreichung von Stabilität in den Prozessen und Aktivitäten der Organisation
- Kontinuierliche Untersuchungen und Verbesserung zur Erreichung besseren Services zu geringeren Kosten unter Beibehaltung der Stabilität
- Rasche Anwendung von operativen Fähigkeiten zur Analyse von Fehlern im Betrieb sowie zu deren Behebung

Application Management

Lebenszyklus des Application Management

Service Operation basierend auf ITILv3, van Haren Publishing, 2008

Jede Phase des Application Management-Lebenszyklus hat seine eigenen, spezifischen Zielsetzungen, Aktivitäten, Lieferergebnisse und Teams. Jede Phase hat außerdem eine klare Verantwortlichkeit für die Gewährleistung, dass ihr Output den spezifischen Zielsetzungen des Service Management-Lebenszyklus entspricht.

Event Management

Grundbegriffe

- Verschiedene Arten von Events:
  - Events, die regulären Betrieb bezeichnen
    →Anwender hat sich angemeldet um Anwendung zu verwenden
  - Events, die Ausnahmen bezeichnen
    → Anwender versucht sich mit falschem Passwort anzumelden
  - Events, die ungewöhnlichen, aber nicht außergewöhnlichen Betrieb kennzeichnen
    → Beendigungszeit der Transaktion ist 10% länger als normal

Event Management: Ziel

- Ermöglicht die Erkennung von Events, deren logische Einordnung und die Festlegung geeigneter Maßnahmen
- Bietet die Möglichkeit, tatsächliche Performance / Verhalten mit Design Standards bzw. SLAs zu vergleichen
- Grundlage für operatives Monitoring und operative Steuerung
- Operative Informationen:
  - Ausnahmen
  - Warnungen

Event Management

- stellt Einstiegspunkt für die Ausführung vieler Service Operation (Servicebetrieb) Prozesse und Aktivitäten zur Verfügung
- bietet einen Weg um aktuelle Performance und aktuelles Verhalten mit Design-Standards und SLAs zu vergleichen
- bietet eine Basis für Serviceversicherung und Berichterstattung; und Serviceverbesserung
- Verschiedene Arten von Events:
  - Events, die regulären Betrieb bezeichnen
  - Events, die Ausnahmen bezeichnen
  - Events, die ungewöhnlichen, aber nicht außergewöhnlichen Betrieb kennzeichnen

Funktionen in ihrer Eigenschaft als First oder Second Level Support führen Event Management aus (z.B. Service Desk).

Event: ist üblicherweise eine von einem IT Service, CI oder Monitoring Tool erstellte Benachrichtigung.

Alert: Zweck des Alert ist es, sicherzustellen, dass jene Person, die aufgrund ihrer Qualifikationen mit dem Event angemessen umgehen kann, benachrichtigt wird.

Der Alert wird alle Informationen, die für diese Person notwendig sind, um die angemessene Aktion festzulegen, enthalten - inklusive Referenzen zu allen benötigten Dokumentationen (z.B. Benutzerhandbuch).

Hauptaktivitäten des Event Managements

- Ein Event tritt auf
- Event Bericht
- Event Erkennung
- Event Filterung
- Event Klassifizierung
- Event Zuordnung
- Auslöser
- Reaktionsmöglichkeiten
- Bewertungsmaßnahmen
- Abschluss des Events

Event Filterung

Eine der wichtigsten Grundlagen des Eventmanagements ist das Erreichen der richtigen Grads der Filterung, um Management- und Kontrollmaßnahmen auf die wichtigen Events zu konzentrieren. Es gibt verschiedene Strategien, die eingesetzt werden können, um den richtigen Grad der Filterung zu erhalten.

- **Integration:** Integration in alle Event-Management-Service-Management-Prozesse, bei denen es machbar ist.
- **Design:** Design neuer Services mit Event-Management im Hinterkopf.
- **Trial and Error:** Es wird immer Klassen von Ereignissen geben, die nicht richtig gefiltert werden können.
- **Planning**: Die richtige Planung ist für den Einsatz von Event-Management-Software in der gesamten IT-Infrastruktur notwendig.

KPI

- Anzahl von Events pro Kategorie
- Anzahl wichtiger Events
- Anzahl und Prozentsatz von Events, die menschlichen Eingriff erfordern und in wie vielen Fällen dies geschehen ist

- Anzahl und Prozentsatz von Events, die zu Incidents und Changes führten
- Anzahl und Prozentsatz von jeder Event-Art pro Plattform oder Anwendung

Incident Management

Incident

Incident

Ein Incident ist eine ungeplante Unterbrechung eines IT Service oder Reduktion der Qualität eines IT Service. Der Ausfall eines CI, der sich noch auf keinen Service ausgewirkt hat, ist ebenfalls ein Incident.

ITIL

Beispiel: Ein Ausfall einer oder mehrerer Festplatten in einer gespiegelten Partition."

Incident Management: Ziel

- Das Hauptziel des Incident Management Prozesses ist es, den normalen Servicebetrieb (Service Operation) so schnell wie möglich wiederherzustellen und die nachteiligen Auswirkungen auf den Geschäftsbetrieb auf ein Minimum zu begrenzen, so dass Verfügbarkeit und Qualität des Services auf möglichst hohem Niveau erhalten bleiben

- 'Normaler Servicebetrieb' ist hier definiert als Servicebetrieb, bei dem die Vorgaben der SLA eingehalten werden

Incident Management

- Incident Management enthält jeden Event, der eine Unterbrechung des Services verursacht oder zu verursachen droht
- die Kommunikation kann erfolgen durch:
  - den Anwender direkt
  - den Service Desk
  - eine Schnittstelle vom Event Management
- Grundbegriffe:
  - Incident Modelle
  - Major Incidents

27

Umfang

- Incident Management enthält jeden Event, der eine Unterbrechung das Services verursacht oder zu verursachen droht
- die Kommunikation kann erfolgen durch
  - den Anwender direkt
  - den Service Desk
  - eine Schnittstelle vom Event Management

Grundbegriffe

- Incident Modelle (vordefinierte Workflows für Incidents abhängig von deren Klassifizierung)
- Major Incidents (Schwerwiegende Incidents, größere Dringlichkeit. Erfordern ein eigenes Incident Modell)
- Zeitskalen (Zeit von Erkennen bis zum Abschluss, Eskalationszeiten, ...)

Grundkonzepte

Die folgenden Elemente sollten beim Incident Management berücksichtigt werden:

- **Zeitlimits** – man vereinbart Zeitlimits für alle Phasen und verwendet sie als Ziele in OLAs und UCs.
- **Incident Modelle** – ein Incident Modell ist ein Weg zur Bestimmung der für die korrekte Durchführung eines Prozesses notwendigen Schritte. Dies bedeutet Standard-Incidents korrekt und innerhalb der vereinbarten Zeitrahmen gehandhabt werden.

- **Schwerwiegende Incidents** – für schwerwiegende Incidents (major incidents) ist ein separates Verfahren mit kürzeren Zeitlinien und größerer Dringlichkeit erforderlich.

Von diesem generellen Prozessfluss sind die Incident Modelle abzuleiten.

Derjenige der einen Incident eröffnet (Service Desk) ist und bleibt der Owner während des gesamten Lifecycle eines Incident.

Schritte des Incident Management

1. Identifizierung
2. Registrierung
3. Klassifizierung
4. Priorisierung
5. Diagnose
6. Eskalation
7. Untersuchung und Diagnose
8. Lösung und Wiederherstellung
9. Abschluss

Klassifizierung / Categorization

Impact, Urgency, Priority

- Impact (Auswirkung)

  Ein Maß für die Folgen eines Incident, Problems oder Change auf die Business-Prozesse. Die Auswirkung basiert häufig darauf, inwieweit Service Levels betroffen sind. Mithilfe der Auswirkung und der Dringlichkeit erfolgt die Zuweisung einer Priorität.

- Urgency (Dringlichkeit)

  Ein Wert, der wiedergibt, wie lange es dauert, bis ein Incident, Problem oder Change maßgebliche Auswirkungen auf das Business hat. Ein Incident mit erheblichen Auswirkungen kann beispielsweise von geringer Dringlichkeit sein, wenn die Auswirkungen das Business bis zum Ende des Geschäftsjahrs nicht beeinträchtigen. Auf der Grundlage der Auswirkung und Dringlichkeit werden Prioritäten zugewiesen.

- Priority (Priorität)

  Ist die relative Wichtigkeit eines Incident, Problems oder Change. Die Priorität basiert auf der Auswirkung und Dringlichkeit und wird eingesetzt, um den erforderlichen Zeitbedarf für die auszuführenden Aktionen zu ermitteln. Ein SLA kann beispielsweise angeben, dass Incidents der Priorität 2 innerhalb von 12 Stunden behoben werden müssen.

Beispiel einer Priority Matrix

URGENCY \ IMPACT	High	Mid	Low
High	1	2	3
Mid	2	3	4
Low	3	4	5

PRIORITY	Time to resolve [h]
1	2
2	8
3	24
4	36
5	160

Arten der Eskalation

Rollen im Incident Management

Incident Manager

- Verantwortung für Effizienz & Effiktivität, Management Berichte
- Monitoring
- Verwaltung der Support-Mitarbeiter
- Entwickeln & Pflegen der IM-Systeme und der Prozesse und Verfahren des IM
- Verwalten von Major Incidents

First-Level Support

- Service Desk, SPOC

Second-Level Support

- Technische Qualifikation & Zeit für Incident Diagnose und Lösung

Third-Level Support

- Interne Spezialisten und/oder externe Lieferanten

35

Rollen im Incident Management

- Incident Manager
  - Effizienz und Effektivität des Incident Management Prozesses verantworten
  - Erstellung von Management-Information
  - Monitoring (Überwachung) der Effektivität des Incident Managements und Empfehlungen zur Verbesserung
  - Verwaltung der Arbeit der Support-Mitarbeiter (First- und Second-Level)
  - Entwickeln und Pflegen der Systeme für das Incident Management
  - Verwalten der Major Incidents (Schwerwiegender Incidents)
  - Entwickeln und Pflegen der Prozesse und Verfahren des Incident Managements

- First-Level Support
  - Service Desk

- Second-Level Support
  - Personal mit besseren technischen Qualifikationen und Zeit, um sich der Incident Diagnose und Lösung zu widmen ohne durch Telefonunterbrechungen beeinträchtigt zu sein.

- Third-Level Support
  - interne Gruppen und/oder externe Lieferanten

Schnittstellen zu anderen Prozessen

- Problem Management
- Configuration Management
- Change Management
- Capacity Management
- Availability Management
- Service Level Management

36

- **Problem Management** - Incidents werden häufig durch zugrunde liegende Probleme verursacht, die zur Verhinderung des Wiederauftretens des Incidents gelöst werden müssen. Incident Management bietet einen Weg, um diese Probleme zu melden.

- **Configuration Management** - Configuration Management stellt die zur Identifizierung und Verfolgung von Incidents eingesetzten Daten zur Verfügung. Das Configuration Management System (CMS) wird unter anderem zur Identifizierung defekter Komponenten und zur Bestimmung der Auswirkung eines Incidents verwendet. Das CMS wird auch zur Identifizierung von Anwendern, welche von möglichen Problemen betroffen sind, eingesetzt.

- **Change Management** - Wenn ein Change zur Implementierung eines Workarounds oder einer Lösung notwendig ist, wird er als RFC registriert und durch das Change Management bearbeitet. Das Incident Management kann aus unangebrachten Changes resultierende Incidents verfolgen und lösen.

- **Capacity Management** - Incident Management löst die Überwachung der Leistungsfähigkeit aus, wenn ein Leistungsfähigkeitsproblem auftritt. Capacity Management kann Workarounds für Incidents anbieten.

- **Availability Management** - Availability Management verwendet Daten aus dem Incident Management zur Bestimmung der Verfügbarkeit von IT Services und stellt fest, an welchen Stellen der Incident-Lebenszyklus verbessert werden kann.

- **Service Level Management (SLM)** - SLM überwacht die den bereitzustellenden Support betreffenden Vereinbarungen mit Kunden. Das Incident Management berichtet an das SLM. Beispielsweise kann dieser Prozess SLAs objektiv und regelmäßig bewerten. SLM etabliert akzeptable Service Levels, innerhalb derer das Incident Management arbeiten muss.

KPI & CSF

- KPIs
  - Gesamtanzahl an Incidents (als Steuerungsmaß)
  - Aufschlüsselung von Incidents in jeder Phase [z.B. erfasst, in Arbeit (Work in Progress, WIP), geschlossen, etc.]

- CSFs
  - ein guter Service Desk ist der Schlüssel zu erfolgreichem Incident Management
  - klar definierte Ziele auf die hingearbeitet werden kann - wie in SLAs definiert

37

Herausforderung:

Fähigkeit, Incidents so früh wie möglich zu erkennen

Request Fulfilment

Request Fulfillment: Ziele

- Einen Weg für Anwender zur Verfügung zu stellen, um Standard Services für die ein vordefinierter Bewilligungs- und Qualifikationsprozess existiert, anzufordern und zu erhalten.
- Anwendern und Kunden Informationen über die Verfügbarkeit von Services sowie die Prozedur, wie diese zu erhalten sind zur Verfügung stellen.
- Komponenten angeforderter Standard Services (z.B. Lizenzen und Softwaremedien) beziehen und übergeben.
- Unterstützen bei allgemeinen Informationen, Beschwerden oder Anmerkungen.

39

Grundbegriffe

- Request Modelle
  - ähnliches Konzept wie bei Incident Modellen, angewandt auf Service Requests (Serviceanträge)

Request Fulfillment

- **Prozessaktivitäten**
  - Menüauswahl (Self-Help-Tool)
    - via Webinterface
    - vordefinierte Liste
  - finanzielle Bewilligung
  - andere Bewilligungen
  - Ausführung
  - Abschluss

40

Service Desk und Incident Management übernehmen folgende Aufgaben im Rahmen des Request Fulfilment:

Der Single Point of Contact (SPOC) für die Kommunikation zwischen Service Provider und Anwendern. Ein Service Desk bearbeitet in der Regel Incidents und Service Requests (Serviceanträge) und ist für die Kommunikation mit den Anwendern zuständig

Service Operation Teams / Abteilungen / ext. Supplier übernehmen in der Regel das Fulfilment von Service Requests

Beziehung zwischen Service, Service Request, Request Model und RFC

KPI

- Die Gesamtzahl der Serviceanfragen
- Das phasenweise Herunterbrechen der Serviceanfragen
- Das Ausmaß des gegenwärtigen Rückstands an noch ausstehenden Serviceanfragen

- Die durchschnittl. Zeit für die Handhabung jeder Art von Serviceanfrage
- Die durchschnittl. Kosten pro Art von Serviceanfrage
- Grad der Kundenzufriedenheit

Problem Management

Problem Management: Ziele

- Ursachen und daraus resultierende Incidents verhindern
- Wiederkehrende Incidents eliminieren
- Auswirkungen von Incidents, die nicht verhindert werden können, minimieren

Wichtige Definitionen

- **Problem:**
  - Die Ursache für einen oder mehrere Incidents
- **Workaround (Umgehungslösung):**
  - Die Reduzierung oder Beseitigung der Auswirkungen von Incidents oder Problemen, für die noch keine vollständige Lösung verfügbar sind
- **Known Error:**
  - Ein Problem, für das die zugrunde liegende Ursache und ein Workaround dokumentiert wurden
- **Known Error Data Base (KEDB)**
  - Eine Datenbank, die sämtliche Records bekannter Fehler enthält

45

Problem:

Zum Zeitpunkt der Erstellung eines Problem Record ist die Ursache in der Regel unbekannt. Für die weitere Untersuchung ist der Problem Management Prozess verantwortlich.

Workaround (Umgehungslösung):

Workarounds für Probleme werden in Known Error Records dokumentiert. Workarounds für Incidents, die nicht über zugeordnete Problem Records verfügen, werden in Incident Records dokumentiert.

Known Error:

Das Problem Management ist verantwortlich für die Erstellung und Verwaltung von bekannten Fehlern während ihres gesamten Lebenszyklus. Bekannte Fehler können auch von der Entwicklung oder den Lieferanten identifiziert werden.

Known Error Data Base (KEDB)

Diese Datenbank wird vom Problem Management erstellt und vom Incident und Problem Management eingesetzt. Die Known Error Database ist Teil des Service Knowledge Management Systems.

Die zentralen Arbeitsobjekte des PM

Problem

Unbekannte Ursache einer oder mehrerer (potentieller) Störungen

Known Error (Bekannter Fehler)

Problem, dessen Ursache festgestellt u. für das ein Workaround definiert wurde

Request for Change (RFC)

Auftrag zur Änderung, um den Known Error zu beseitigen

Problem Management

- **Prozessaktivitäten :**

  2 Hauptprozesse:

  - Reaktiv (Teil von Service Operation)
  - Proaktiv (Teil von Continual Service Improvement)

Aktivitäten des reaktiven Problem Mgt.

- Identifizierung
- Registrierung
- Klassifizierung
- Priorisierung
- Untersuchung und Diagnose
- Entschluss zu Workarounds
- Identifizierung von Known Errors
- Lösung
- Abschluss
- Review
- Korrektur gefundener Fehler

Der reaktive Problem Management Prozess

In diesem Diagramm ist der normale Prozessfluss abgebildet. In der Praxis können sich einige der Zustände wiederholen oder müssen modifiziert werden, um an bestimmte Situationen angepasst zu werden.

Schritte:

- Problemerkennung
- Problemkategorisierung
- Problempriorisierung
- Problemuntersuchung und -diagnose
- Workarounds
- Erstellen eines Known Error Record
- Problemlösung
- Problemabschluss
- Review nach schwerwiegenden Problemen

Untersuchung und Diagnose

Causes	Percentage of total	Computation	Cumulative
Network Controller	35	0+35%	35
File corruption	26	35%+26%	61
Addressing conflicts	19	61%+19%	80
Server OS	6	80%+6%	86
Scripting error	5	86%+5%	91
Untested change	3	91%+3%	94
Operator error	2	94%+2%	96
Backup failure	2	96%+2%	98
Intrusion attempts	1	98%+1%	99
Disk failure	1	99%+1%	100

50

Service Operation basierend auf ITILv3, van Haren Publishing, 2008

Der reaktive Problem Management Prozess

In diesem Diagramm ist der normale Prozessfluss abgebildet. In der Praxis können sich einige der Zustände wiederholen oder müssen modifiziert werden, um an bestimmte Situationen angepasst zu werden.

Schritte:

- Problemerkennung
- Problemkategorisierung
- Problempriorisierung
- Problemuntersuchung und -diagnose
- Workarounds
- Erstellen eines Known Error Record
- Problemlösung
- Problemabschluss
- Review nach schwerwiegenden Problemen

Change Management

- Problem Management stellt sicher: alle Lösungen od. Workarounds, die Change an CI erfordern werden über RFC bei Change Management eingereicht
- Change Management überwacht Fortschritt der Changes u. hält Problem Management auf dem Laufenden
- Problem Management hilft bei Verbesserung einer Situation, die durch fehlgeschlagene Changes verursacht wurde

Financial Management

- Financial Management hilft bei Bewertung der Auswirkungen vorgeschlagener Lösungen od. Workarounds u. bei der Schadenswertanalyse
- Problem Management stellt Management-Informationen über die bei Lösung und Vermeidung von Problemen anfallenden Kosten bereit → Input für Finanzplanungs- u. Kostenrechnungssysteme u. für Berechnungen der Total Cost of Ownership

KPIs & CSF

- Gesamtzahl der Probleme, die im Zeitraum registriert wurden
- Prozentsatz der Probleme, die innerhalb von SLA-Zielen gelöst wurden
- Der Rückstand an ausstehenden Problemen und der Trend

- Die durchschnittl. Kosten der Problembehandlung
- Die Anzahl der zur KEDB hinzugefügte Probleme
- Der Prozentsatz der Genauigkeit der KEDB

Problem Manager

Hauptaktivitäten:

- Zusammenarbeit mit allen Problemlösungsgruppen um eine rasche Lösung
- des Problems innerhalb der SLA Ziele sicherzustellen
- Verantwortung für die Known Error Datenbank (KEDB)
- Abschluss aller Problem Records
- Verwalten von Major Problems

53

Im Detail:

Problem Manager

- Zusammenarbeit mit allen Problemlösungsgruppen um eine rasche Lösung des Problems innerhalb der SLA Ziele sicherzustellen
- Verantwortung für die Known Error Datenbank (KEDB)
- Informationsregulator für die Einbeziehung aller Known Errors und Management von Suchalgorithmen
- formeller Abschluss aller Problem Records
- Zusammenarbeit mit Supplier, Auftragnehmern, etc. um sicherzustellen, dass Drittparteien ihre vertraglichen Verpflichtungen einhalten, besonders in Bezug auf die Bereinigung von Problemen und die Bereitstellung problembezogener Informationen und Daten
- Aufbauen, Betreiben, Dokumentieren und alle Nachfolgeaktivitäten in Bezug auf Major Problem Reviews

Weitere Rolle:

Problemlösungsteams

Access Management

Access Management

Ermöglicht den Anwendern das Recht, ein Service oder eine Gruppe von Services zu verwenden → Ausführung von Richtlinien und Aktionen, die im Security und Availability Management definiert sind

Grundbegriffe:

- Zugriff
- Identität
- Rechte
- Services und Service Gruppen
- Directory-Service

Prozess Aktivitäten im Detail:

- Zugriff anfordern
- Verifizierung
- Berechtigung erteilen
- Identitätsstatus überwachen
- Zugriff erfassen und verfolgen Berechtigung entfernen oder begrenzen

Beteiligte Funktionen:

- Service Desk
    - bestätigt die Anfrage
    - kommuniziert mit dem Anwender
    - erfasst und berichtet zugriffsbezogene Incidents
- Technical und Application Management
    - einige wichtige Rollen während Service Design, Transition und Operation
- IT Operations Management

Schnittstellen

Access Management wird durch eine Anfrage eines Anwenders nach Zugriff auf eine Service(gruppe) **ausgelöst**.

Eine solche Anfrage kann herrühren von:

- einem RFC
- einer Serviceanfrage
- einer Anfrage der Personalabteilung
- einer Anfrage von einem Manager oder einer Abteilung, der/die einer Personalmanagement-Rolle ausfüllt oder der/die eine Entscheidung zur erstmaligen Nutzung eines Services getroffen hat

KPIs & CSF

- Die Zahl der Zugriffsanfragen (Service-Anfragen) und RFCs
- Die Häufigkeit, mit der einem Service, einem Anwender oder einer Abteilung Zugriff gewährt wurde.
- Die Anzahl der zur Zurücksetzung von Zugriffsrechten notwendige Incident
- Die Anzahl von durch unrichtige Zugriffseinstellungen verursachte Incidents

Begriffe aus Service Operation

- Event
- Alert
- Incident
- Impact, Urgency, Priority
- Service Request
- Problem
- Workaround
- Known Error, Known Error Database (KEDB)

Begriffe sind wichtig für die ITIL®v3 Foundation Prüfung. Man sollte sie kennen/beschreiben können.