Service Operation Prozesse

Elia Griffo, Moritz Küttel

Abstract

In diesem Dokument betrachten wir die Service Operation Prozesse Incident Management, Request Fulfillment, Problem Management und Access Management wie in ITIL definiert. Jeder Dieser Prozesse ist in einem Kaptiel beschrieben.

Incident Management

Incident Management befasst sich mit allen Ereignissen, die einen Service stören oder beeinflussen können, und ist verantwortlich für den gesamten Lebenszyklus aller Incidents. Wichtige Begriffe und Rollen sind:

- **Incident**: Ungeplante Unterbrechung oder Reduktion der Qualität eines IT-Services. Zum Beispiel:
  - Fragen von Benutzern
  - Meldungen von IT-Mitarbeitern
  - Monitoring Events
  - Ausfall einer Hard-Disk im RAID (auch ohne Service Unterbruch)

  In der Praxis entspricht dies einem Ticket.

  Die Wiedereröffnung eines Tickets sollte grundsätzlich vermieden werden. Jedoch können Situationen in der Praxis auftreten, in denen dies sinnvoll ist. Es benötigt jedoch klare Regeln, wann ein Incident wiedereröffnet wird und wann es sich um einen neuen Incident handelt.
- **Major Incident**: Im Gegensatz zu einfachen Incidents haben Major Incidents besonders grosse Auswirkungen auf die Geschäftsprozesse und bedingen besondere Massnahmen bei der Service-Wiederherstellung.
- **Workaround**: Massnahme zur Reduzierung der Auswirkungen eines Incidents, solange keine endgültige Lösung verfügbar ist.
- **Timescales**: Anhand des SLAs werden für die einzelnen Aktivitäten eines Incidents Zeiten vereinbart, welche im OLA festgehalten werden.
- **Incident Models**: Vordefinierte Vorgehensweise für eine bestimmte Art von ähnlichen oder auch gleichen Incidents.
- **Incident Manager** Der Incident Manager ist verantwortlich für die Erstellung und Weiterentwicklung des Incident Management Prozesses. Weitere Aufgaben beinhalten:
  - Überwachung der Effektiviät des Prozesses, und kontinuierliche Verbesserung
  - Steuerung der Support Teams und Auswahl und Integration der benötigten Werkzeuge
  - Hierarchische Eskalationsinstanz und Steuerung der Durchführung von Major Incidents
  - Management Reporting
- **Service Desk / 1st Line Support** : Nimmt Anrufe entgegen und bearbeitet Meldungen, nach den unten definierten Aktivitäten.
- **2st Line Support** Sind Spezialisten die über ausgeprägte Fachkenntnisse über ein bestimmtes Thema verfügen. Incidents werden vom Service Desk zuerst hierher eskaliert.
- **3rd Line Support** Ist die nächste Stufe der Eskalation, wenn der 2nd Line Support ein Incident weiterleitet. Es handelt sich hier um noch weiter spezialisierte Teams. Es kann aber auch ein externer Dienstleister oder der Hersteller eines Produkts sein.

Abgrenzung zum Problem Management

Ein Incident bleibt immer ein Incident, auch ein Major Incident. Es werden nur Symptome und Auswirkungen mittels eines Workarounds behoben. Sie werden höchstens zu einem Problem zugewiesen, welches die grundlegende Ursache für ein oder mehrere Incidents ist.

Jedoch ist es sehr wichtig für einen funktionierenden Incident Management Prozess, dass Informationen wie Errors und Workarounds aus dem Problem Management Prozess zur Verfügung stehen, um aus vergangenen Incidents zu lernen und sinnvolle Workarounds einzusetzen.

Aktivitäten

Die Aktivitäten können sich grundsätzlich je nach Unternehmen und Umständen unterscheiden. Folgende Aktivitäten bieten aber einen guten Rahmen für die Gestaltung eines Incident Management Prozesses:

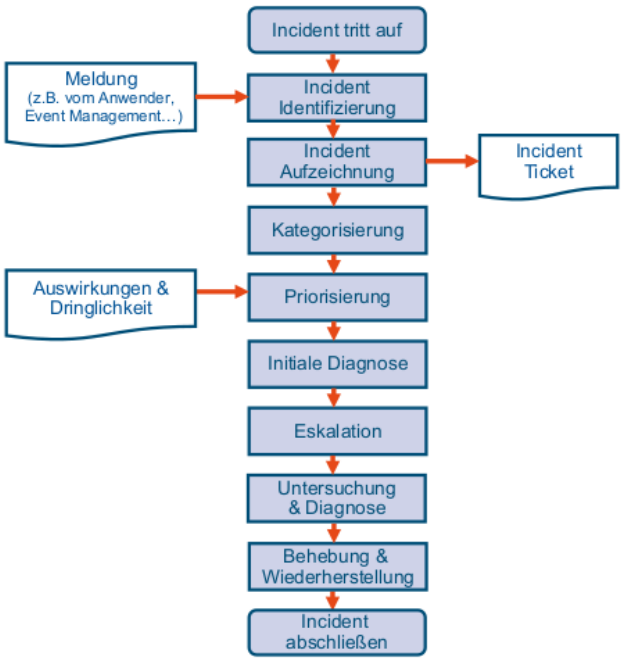

Figure 1: Incident Management Prozesse

1. **Incident tritt auf**: Wenn ein Incident auftritt, heisst nicht unbedingt, dass dieser direkt auch identifiziert wird.
2. **Incident identifizierung**: Entweder durch auftreten, oder durch eine Meldung vom Anwender oder des Monitorings. Je früher man Fehler entdecken kann, desto schneller können Fehler beseitigt werden. Der Anwender bekommt dies im besten Fall nicht einmal mit.
3. **Incident Aufzeichnung**: Alle Incidents sollen aufgezeichnet werden, da dies wichtig ist für den ganzen Prozess wie auch zur Messung der Prozess-Performance. Dies soll beinhalten:
    - Zeit/Datum der Erfassung & Abschluss
    - Eindeutige ID
    - Status
    - Kategorie / Kategorie bei Abschluss
    - Dringlichkeit & Ausirkung
    - Name des Erfassers und Kommunkationsart
    - Name des Benutzers und Kommunkationsart

- Betroffene Configuration Items
- Verlinkte Problems / Known Errors
- Durchgeführte Massnahmen zur Behebung
- Personen/Rolle welcher Incident bearbeitet

4. **Statusverfolgung**: Der Status soll gepflegt werden & vereinfacht die Handhabung. Typische Stati sind:
   Offen: Noch nicht zugeordnet
   In Arbeit Der Incident wird bearbeitet.
   Gelöst: Incident wurde behoben, Lösung jedoch nicht bestätigt.
   Solved: Incident ist abgeschlossen & Lösung wurde durch Anwender bestätigt.

5. **Kategorisierung**: Eine Kategorisierung wird vorgenommen, damit der Incident von den dafür zuständigen Mitarbeitern direkt verarbeitet werden kann. Keine Kategorisierung oder eine Fehlkategorisierung kann zu Mehraufwand, z.B. durch mehrfaches weiterleiten führen.

6. **Priorisierung**: Incidents werden Priorisiert nach *Auswirkung* auf das Business des Kunden und nach *Dinglichkeit* wie schnell der Service wieder hergestellt werden muss (nach SLA). Es braucht hier klare Richtlinien und Praxisbeispiele für die Mitarbeiter, um die Priorisierung korrekt vorzunehmen. Die Priorisierung legt lediglich die Reihenfolge der Abarbeitung fest.

7. **Initiale Diagnose**: Nach dem Erfassen des Incidents und dessen Symptome, wird direkt versucht eine schnelle Lösung zu finden. Dies ist der Job des Service Desks, der z.B. noch direkt am Telefon mit dem Kunden versucht durch z.B. Fragebäume oder Wissensdatenbanken oder der Known Error Database das Problem zu lösen. Im besten Fall, wenn der Anwender die Lösung akzeptiert, kann der Incident direkt abgeschlossen werden.

8. **Eskalation**: Bei des Eskalation handelt es sich um die Weitergabe des Incidents an eine andere Instanz, um dort jeweils weitere Aktivitäten durchzuführen. Es wird hier grundsätzlich zwischen zwei Arten unterschieden.
   Funktionale Eskalation: Weitergabe z.B. aufgrund von fehlendem Wissen, Fähigkeiten oder Experitise. Aber auch anhand der Zuständigkeit der zugewiesenen Kategorie. Dies ist z.B. eine Weiterleitung des Service Desk an den 2nd Line Support. Die Verwantwortung zur Bearbeitung des Incidents bleibt hier aber bei der Instanz die ihn weitergeleitet hat.
   Hierarchische Eskalation: Hier handelt es sich um eine Weitergabe an den übergeordneten Manager (Oft zuerst der Incident Manager). Dies kann im Falle eines Major Incidents sein, um den Manager zu informieren. In anderen Fällen, wie der Überschreitung der vorgesehenen Lösungszeit, wird dies getan, um weitere Massnahmen einzuleiten.

9. **Untersuchung und Diagnose**: Hier werden alle Informationen bewertet und Ereignisse identifiziert, welche den Incident ausgelöst haben könnten. Dies kann dazu führen, dass die Priorisierung des Incidents angepasst werden muss, da der Grad der Auswirkungen hier neu bewertet wird.

10. **Behebung und Wiederherstellung**: In dieser Aktivität werden die Massnahmen zur Wiederherstellung des Services durchgeführt, nachdem eine potenzielle Lösung identifiziert wurde. Dies kann durch den Anwender selbst, durch den Service-Desk, ein internes Support-Team oder auch durch externe Lieferanten geschehen.

11. **Incident abschliessen** Hier wird durch den Service Desk sichergestellt, dass der Fehler wirklich behoben wurde und der Anwender die Lösung akzeptiert (Kann auch durch *nicht antworten* auf ein geschlossenes Ticket geschehen). Ausserdem ist es wichtig, die Vollständigkeit der Dokumentation zu überprüfen, evtl. die Kategorie zu korrigieren. Zudem muss bei Bedarf das Problem Management informiert werden, über die Notwendigkeit präventiver Massnahmen. Es kann auch die Anwenderzufriedenheit abgefragt werden, jedoch gut dosiert, da man sonst auf Unmut stossen könnte.

Key Performance Indikatoren (KPI)

Mögliche Kennzahlen zur Messung der Performance des Incident Management Prozesses sind:

- Incidents pro Status
- Durchschnittliche Kosten pro Incident
- Anzahl Major Incidents im Verhältnis zur Anzahl Incidents
- Anteil der innerhalb der SLAs behobenen Störungen

- Anteil der Incidents, die wiedereröffnet wurden
- Anteil falsch kategorisierter oder falsch zugewiesener Incidents
- Erstlösungsrate

Request Fulfilment

Das Request Fulfilment setzt sich mit Anwenderanfragen verschiedenster Natur auseinander. Beispiele dafür sind:

- Umzüge von Anwendersystemen oder Anfragen bezüglich zusätzlicher Informationen
- Passwort zurücksetzen
- Unterstützung bei der Nutzung von Services

Ziele

- Kanal für Bestellung und Bezug von «Standardleistungen» bereitstellen
- Informationen zu beziehbaren Leistungen und deren Bezugsweg verfügbar machen
- Beschwerden entgegennehmen und verarbeiten
- Angebotene Standardleistungen haben definierte Genehmigungswege und Prozesse
- Andere Prozesse wie Incident- oder Change-Management entlasten

Begriffe

- **Service Request**
  - Anfrage eines Anwenders nach Informationen, Beratung, Support, Standard-Change oder nach Zugriff auf IT-Service
  - Meist direkt am Service Desk bearbeitet
  - Oft sehr einfache, risikoarme und schnell zu bearbeitende Anfragen
- **Menüauswahl (Menue selection)**
  - Abrufmöglichkeit der gewünschten Leistungen anhand definierter Menüauswahl
  - Kann innerhalb des Servicemanagement-Tools abgebildet werden
  - Bei Fehlen eines solchen Tools kann ein Katalog oder eine Anforderung beim Service Desk Abhilfe schaffen
- **Statusüberwachung (request status tracking)**
  - Zuverlässige Überwachung der Request-Status
  - Mögliche Status Codes: Draft, In Review, Abgelehnt, Fertiggestellt etc.
- **Koordination der Ausführung (coordination of fulfilment activities)**
  - Tatsächliche Ausführung abhängig von der Art der Anfrage
  - Häufig direkt durch Service-Desk-Mitarbeiter, aber es können auch weitere Personen und Rollen miteinbezogen werden (z.B. Facility Mgmt. für Umzüge)

Aktivitäten

Der Prozess besteht aus den folgenden Aktivitäten:

- **Request annehmen (receive request)**
  - Arbeiten erst beginnen, wenn die formale Anfrage beim Service Provider eingeht
  - Vordefinierte Templates nutzen falls möglich, um Aufwand gering zu halten
  - Beurteilung, ob es tatsächlich ein Request ist und nicht etwa ein Incident
- **Logging und Validierung (request logging and validation)**
  - Requests müssen vollständig erfasst und mit Zeitstempel versehen werden
  - Wichtige Informationen sind: Kategorie, Zeitstempel, Anwender, Dringlichkeit, Priorität, Status, Beschreibung etc.
- **Kategorisierung (request categorization)**
  - Beschreibt, um welche Art von Request es sich handelt

  - Wichtig für spätere Reports zur Nutzung der Services und Planung der Ressourcen
  - Beispiele: Nach Service, nach Aktivitäten, nach CI Typ
- **Priorisierung (request priorization)**
  - Legt die Reihenfolge der Abarbeitung der Requests fest
  - Setzt sich zusammen aus der Auswirkung auf das Business und der Dringlichkeit
- **Autorisierung (request authorization)**
  - Jeder Request braucht vor der Ausführung eine Autorisierung
  - Kann je nach Fall unterschiedlich ablaufen
  - Falls keine Autorisierung möglich ist, folgt eine Begründung an den Anwender
- **Review (request review)**
  - Überprüfung, welche Funktion für die Durchführung verantwortlich ist
  - Requests, die nicht direkt im Service Desk bearbeitet werden können, werden weitergeleitet und überwacht
- **Durchführung (request model execution)**
  - Die Durchführung erfolgt durch die zugewiesene Funktion anhand vorgegebener Request Models – so wird die Wiederholbarkeit und Konsistenz gewährleistet
- **Abschluss (request closure)**
  - Nach Beendigung der Aktivitäten wird der Request über den Service Desk abgeschlossen
  - Anwender werden informiert und die Aktivitäten dokumentiert

Rollen

- **Service-Desk-Mitarbeiter**
  - Nehmen die initiale Bearbeitung vor
  - Führen einfache Service Requests direkt aus
- **Service-Operation-Teams und externe Lieferanten**
  - Erfordern Service Requests weitere Aktivitäten werden diese von internen Teams oder Dienstleistern ausgeführt
- **Facility Management, Einkauf und weiter Abteilungen**
  - Sind bei der Erfüllung der Requests eingebunden und unterstützen bei Bedarf (Übernahme von Aktivitäten oder Freigaben)
- **Dedizierte Support-Teams**
  - Für Ausnahmefälle zuständig: Grosse Zahl von Reqeusts oder kritische Anfrage müssen abgearbeitet werden

Key-Performance-Indikatoren (KPI)

Folgendes sind Beispiele für mögliche Kennzahlen, an denen sich die Prozessqualität messen lassen:

- Gesamtzahl der Service Requests
- Anteil offener Requests, die auf Bearbeitung warten
- Durchschnittliche Zeit für die Bearbeitung
- Anteil Requests, die in vorgesehener Zeit abgeschlossen wurden
- Durchschnittliche Kosten für die Durchführung

Herausforderungen

Für einen erfolgreichen Prozess muss gewährleistet werden, dass alle Anfragen tatsächlich zu diesem Prozess zuzuordnen sind. Es braucht klare Kriterien bei der Kategorisierung von Incidents und Service Requests. Bei Anforderungen neuer Komponenten oder deren Umzug gibt es oft verschiedenste Lösungen, welche identifiziert und durch die Prozesse des Request Fulfilment ersetzt werden sollten.

Problem Management

Ziel des Problem Management ist die Vermeidung von Incidents. Z.B. Das die gleichen Incidents nicht mehrmals auftreten, oder gar nicht auftreten können.

Begriffe

- **Problem**: Unbekannte Ursache eines oder mehrerer Incidents.
- **Workaround**: Massnahme zur Reduzierung der Auswirkungen eines Incidents, solange keine endgültige Lösung verfügbar ist.
- **Known Error**
  - Problem, dessen Ursache identifiziert wurde und ein Workaround existiert
  - Speicherung in der Known-Error-Datenbank
- **Known Error Database**: Beinhaltet alle dokumentierten Known Errors und dazugehörige Workarounds.

Aktivitäten

Das Problem Management besteht grundsätzlich aus zwei wesentlichen Prozessbereichen:

Proaktives Problem Management, befasst sich mit der Identifikation von Schwachstellen und der Vermeidung möglicher zukünftiger Probleme und Störungen.
Reaktives Problem Management, befasst sich mit der Identifikation, Analyse und Beseitigung von Problemen.

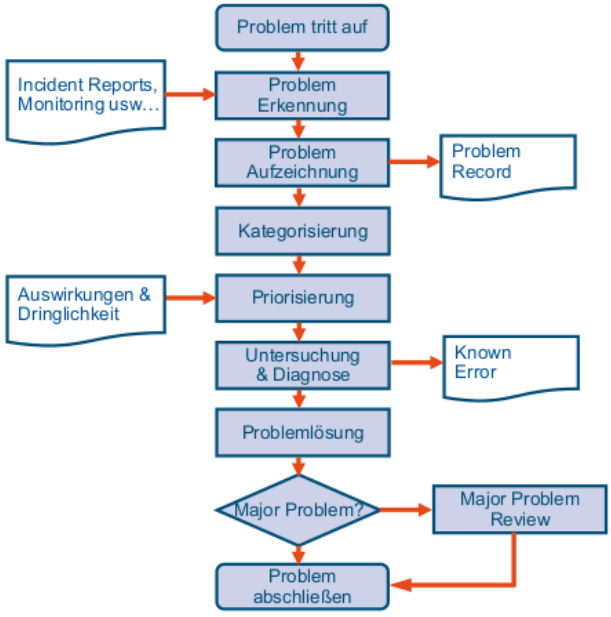

Figure 2: Incident Management Prozesse

- **Problem-Erkennung (Problem detection)**
  - Für einen erfolgreichen Prozess müssen die Probleme zuerst als solche erkannt werden
  - Es gibt verschiedenste Wege zur Erkennung. Beispiele sind: Erfahrung des Service Desks, nachgelagerte Analysen von Incidents, Überwachung des automatisierten Monitorings
- **Problem-Aufzeichnung (Problem logging)**: Für die Bearbeitung relevante Daten werden im Problem Record erfasst und fortlaufend aktualisiert

- **Kategorisierung**: Damit eine effektive Bearbeitung gewährleistet werden kann, muss wie beim Incident Management eine Einteilung stattfinden
- **Priorisierung**: Problems werden priorisiert, um die Reihenfolge und Geschwindigkeit der Bearbeitung den erwarteten Auswirkungen und der Dringlichkeit anzupassen
- **Untersuchung und Diagnose (Investigation and diagnosis)**: Es werden Ressourcen entsprechend der Priorisierung und Kategorisierung zusammengestellt und die Ursache diagnostiziert
- **Known Error dokumentieren (raising a known error)**: Entdeckte Workarounds werden in der Known Error Database dokumentiert und stehen anderen Prozessen zur Verfügung
- **Problemlösung**
  - Identifizierte Ursachen werden bewertet – passende Lösungen werden gesucht
  - Festgelegte Lösungen können nun implementiert werden, sofern kein anderer Service beeinträchtig wird und Ressourcen zur Verfügung stehen
  - Angestrebte Lösung sollte deshalb mit einem RFC genehmigt werden
- **Problem abschliessen**
  - Problem Record wird aktualisiert und formal abgeschlossen
  - Known Error Record wird geupdatet
  - Verlinkte Incident Tickets werden ebenfalls geschlossen

Rollen

- **Problem Manager**
  - Verantwortlich für einen funktionierenden Prozess, Effektivität und Effizienz
  - Weitere Aufgaben: Management Reporting, Pflege der Known Error Database, Formaler Abschluss der Problem Records etc.
- **Problem Solving Groups**
  - Werden in Bezug zum jeweiligen Problem vom Problem Manager zusammengestellt und führen Diagnose und Lösungssuche durch
  - Bestehen aus internen und externen Spezialisten

Key-Performance Indikatoren (KPI)

Beispiele für mögliche Kennzahlen sind:

- Anzahl der identifizierten Problems
- Anteil der in der vorgesehenen Zeit gelösten Problems
- Anteil offener Problem Records, die auf Bearbeitung warten
- Durchschnittliche Kosten je Problem (ggf. auch je Kategorie)
- Reduzierung der Anzahl der Incidents
- Anteil der Problems, für die ein Known Error dokumentiert wurde

Herausforderungen

Es ist unerlässlich, dass die Schnittstelle zwischen Incident- und Problem-Management definiert sind und funktionieren. Dies ist vor allem für die Identifizierung von Problems und Bereitstellung von Workarounds bedeutend. Tools sollten gemeinsam genutzt werden können. Zudem sollten Kategorien und Priorisierungen auf beide Prozesse abgestimmt sein und gleich verwendet werden.

Access Management

Das Access Management ist Verantwortlich für die Verwaltung der Zugriffsrechte. Ziel ist es, das Anwender Services oder Servicegruppen nutzen können, falls diese dazu berechtigt sind, unter Berücksichtigung der Information Security wie auch dem Availability Management.

Der Service-Desk nimmt die Anfragen des Access Managements entgegen. Er entscheidet selber nicht über die Gewährung von Berechtigungen, sondern setzt lediglich die Vorgaben aus der Service Strategy und des Service Designs um, basierend auf den Anforderungen des Unternehmens.

Identität

Das Access Management setzt voraus, dass die Anwender korrekt identifiziert werden können und der Status innerhalb der Organisation verifiziert werden kann.

Aktivitäten

- **Verifikation der Identität**: Um Rechte vergeben zu können, muss erst die Identität des Benutzers verifiziert werden.
  - Ist der Anwender derjenige der er vorgibt zu sein? Es wird zum Beispiel überprüft über Benutzername/Passwort, oder SmartCards
  - Darf er die Angeforderten Berechtigungen erhalten?
- **Überwachung des Identiätsstatus**: Die Rolle eines Mitarbeiters innerhalb einer Organisation kann sich ändern oder der Mitarbeiter kann auch die Organisation verlassen. Auf solche Veränderungen muss auch reagiert werden und dementsprechend Zugriff entfernt, oder die Rechte angepasst werden.

Zugriff

Der Zugriff beschreibt, das komplette Ausmass an Rechten eines Benutzer an einem Service oder Daten hat.

Aktivitäten

- **Zugriff anfordern**: Zugriff kann von Benutzern z.B. durch eine Service Request an das Requestfulfilment angefordert werden.
- **Protokollieren und Überwachen**: Die Vergebenen Rechte und deren Nutzung wird aktiv überwacht, um Missbrauch oder Veränderungen in der Organisation, sollen die Berechtigungen dementsprechend entzogen oder angepasst werden.

Rechte

Die Rechte sind die effektiven Berechtigungen die ein Benutzer oder Gruppe auf bestimmte Services oder Daten *im Detail* hat. (z.B. lesen, schreiben, löschen, ausführen) Hat der Benutzer keinen Zugriff, können auch keine Rechte vergeben werden.

Aktivitäten

- **Rechte vergeben**: Autorisierten Benutzern wird die Berechtigung auf spezifische Services oder Daten *im Detail* gewährt.
- **Rechte entfernen oder einschränken**: Rechte sollen auch wieder entfernt oder eingeschränkt werden werden, z.B. auf Anfragen von Benutzern oder aufgrund der Überwachung des Identitätsstatus (siehe oben)

Key Performance Indikatoren (KPI)

Beispiele für mögliche Kennzahlen sind:

- Anzahl der Anfragen zur Vergabe von Rechten
- Anzahl der Anpassungen aufgrund identifizierter Rollenänderungen
- Anzahl der Incidents aufgrund veränderter Berechtigungen