Fazit

Der digitale Wandel ist nicht aufzuhalten: Nach einer Bitkom-Untersuchung ist er für 72 Prozent der Unternehmen aktuell die größte Aufgabe – nach der Sicherstellung des Fachkräftebedarfs (73 Prozent). Und 40 Prozent der befragten Geschäftsführer und Vorstände sind überzeugt, „dass ihnen Wettbewerber voraus sind, die frühzeitig auf die Digitalisierung gesetzt haben" (Bitkom 2016). CIOs und andere ICT-Verantwortliche müssen daher den Spagat schaffen: einerseits einen zuverlässigen IT-Betrieb sicherstellen, andererseits die Digitalisierung des eigenen Unternehmens vorantreiben und innovative Lösungen entwickeln. Beides gleichzeitig kann nur gelingen, wenn Qualität oberstes Gebot ist.

Denn Qualität ist heute viel mehr als ein Hygienefaktor. Qualität ist der „Klebstoff" der Digitalisierung, der alles zusammenhält. Erst eine zuverlässige Informations- und Telekommunikationstechnik ist die Grundlage für eine erfolgreiche digitale Transformation. Die Geschäftsfähigkeit und damit die gesamte Existenz von Unternehmen hängen heutzutage davon ab. Doch Qualität fällt nicht vom Himmel. Qualität in der ICT sicherzustellen, ist eine aufwendige Managementaufgabe. Unzählige Komponenten müssen jederzeit reibungslos zusammenspielen, damit etwa Produktion oder Vertrieb störungsfrei arbeiten können.

Doch wie ist diese Komplexität zu lösen? Wie können IT-Verantwortliche für einen stabilen und zuverlässigen ICT-Betrieb sorgen? Die Antwort: mit Standardisierung auf allen Ebenen. Für größtmögliche Qualität und Ausfallsicherheit in der ICT werden klare Standards benötigt – für die Prozesse, für die technischen Plattformen und für die Ausbildung des Personals. Diese müssen nicht nur eingeführt und umgesetzt, sondern auch konsequent nachgehalten werden. Eine zentrale Governance ist daher unabdingbar. Nur so kann die Komplexität in der ICT – bei der hohen Geschwindigkeit neuer Entwicklungen und schnell wechselnden Anforderungen – wirkungsvoll reduziert werden.

Qualität ist jedoch nicht nur eine Frage von klaren Standards, sondern immer auch eine Frage der inneren Haltung. Denn menschliches Fehlverhalten ist und bleibt die häufigste Ursache für IT-Störungen. Und es nützen die besten Schulungen nichts, wenn die Mitarbeiter der Qualitätssicherung keine ausreichende Beachtung schenken. Hier hilft nur

S. Kasulke, J. Bensch, *Zero Outage*, DOI 10.1007/978-3-658-14222-3,

ein ganzheitlicher Ansatz, der die Belegschaft des Unternehmens systematisch für das Thema Qualität sensibilisiert und der sicherstellt, dass sich – vom Auszubildenden bis zum Topmanager – jeder Mitarbeiter einer Null-Fehler-Kultur verpflichtet fühlt. Eine starke Qualitätsorganisation, die in die operativen Prozesse aktiv eingebunden ist, muss dieses Zero-Outage-Credo mit Konsequenz und Beharrlichkeit auf allen Unternehmensebenen treiben.

Und das Qualitätsdenken darf an den Unternehmensgrenzen nicht haltmachen. Kein Produkt wird heutzutage ausschließlich von einem Hersteller entwickelt. Unternehmen jeder Größenordnung arbeiten industrieübergreifend zusammen. Damit gibt es immer mehr Schnittstellen und immer mehr Reibungspunkte. Wenn nicht jeder dasselbe hohe Qualitätsverständnis hat und nachhält, drohen fehlerhafte Produkte und Ausfälle. Zudem setzt erst ein Höchstmaß an Qualität Innovationen wie medizinische Eingriffe mithilfe von Robotern oder das selbst fahrende Auto in Gang.

Eine reibungslose Zusammenarbeit kann daher nur funktionieren, wenn nicht jeder sein eigenes Süppchen kocht, sondern wenn es einen gemeinsamen Qualitätsstandard gibt. Die ICT-Branche braucht ein Netzwerk an Partnern, das sich dem Null-Fehler-Prinzip verpflichtet und gemeinsame Regeln für das Qualitätsmanagement verfolgt: Nach welchen Vorgaben wollen wir ausfallsichere Produkte entwickeln? Wie hoch muss der Reifegrad für neue Komponenten in kritischen Systemen sein? Und auf welche Reaktionszeiten bei Störungen wollen wir uns verpflichten? Wenn wir diese und andere Punkte gemeinsam festlegen, profitieren künftig Kunden weltweit von „Zero Outage“, einer ausfallsicheren ICT. Und wir schaffen die Voraussetzungen für eine erfolgreiche, nachhaltige Digitalisierung der gesamten Industrie.

Anhang zu Kapitel 3: ISO, ITIL & Co. – Basis und Orientierung schaffen

Definierte Standards

International Organization for Standardization (ISO)

Die ISO zertifiziert das Verhalten einer Organisation und die Einhaltung der in der jeweiligen Norm definierten Vorgänge. Sie ist branchenunabhängig, länderübergreifend und anerkannt.

Die Vorteile einer ISO-Zertifizierung sind:

- „nachhaltige Qualitätssicherung
- Aufspüren von Verbesserungs- und Einsparungspotenzialen
- höhere Zufriedenheit von Kunden und Mitarbeitern
- Imageaufwertung
- Risikominimierung
- höhere Wirtschaftlichkeit durch Prozessverbesserung
- Verbesserung der Wettbewerbsfähigkeit
- Erfüllung spezifischer Kundenanforderungen“ (TÜV NORD GROUP 2014).

ISO 9000

Diese Norm ist die Anleitung dafür, welche Normen im Bereich „Qualitätsmanagement und Qualitätssicherungs-Nachweisstufen“ für ein Unternehmen wie angewandt werden sollen. Somit ist die ISO 9000 keine Zertifizierungsmöglichkeit, sondern hilft den Unternehmen dabei, die für sie richtige ISO von 9001 bis 9003 zu identifizieren. Sie dient daher als begrifflicher und inhaltlicher Leitfaden (vgl. Glaap 1993).

S. Kasulke, J. Bensch, *Zero Outage*, DOI 10.1007/978-3-658-14222-3,

ISO 9001

Diese Norm zertifiziert das Qualitätsmanagement in Unternehmen. Sie ist die am weitesten verbreitete Norm – national wie international – und somit von großer Bedeutung, wenn ein Unternehmen seine hohen Qualitätsstandards nach außen präsentieren und gleichzeitig seine eigene Effizienz steigern möchte. ISO 9001 ist branchenunabhängig und der Grundstein für jedes Unternehmen, um seine Qualitätsmanagementsysteme dauerhaft zu verbessern. Die Vorteile für Unternehmen, die sich nach dieser Norm zertifizieren lassen möchten, sind:

- Transparenz innerbetrieblicher Abläufe nach außen
- Steigerung der Kundenzufriedenheit
- Senkung der Fehlerquote und die daraus resultierende Kostensenkung

Die ISO 9001 fußt dabei auf acht Grundsätzen des Qualitätsmanagement (QM) (vgl. TÜV 2015):

- **Kundenorientierung:** Das Unternehmen muss sorgfältig die Kundenwünsche beziehungsweise die Anforderungen des Marktes erfassen, prüfen, inwieweit diese intern erfüllt werden können, die Leistung gemäß den Spezifikationen erbringen und schließlich die Kundenzufriedenheit ermitteln.
- **Führung:** Ein QM-System nach ISO 9001 ist ein Steuerungsinstrument der Geschäftsführung. Es ist Führungsaufgabe, dieses System vorzuhalten und weiterzuentwickeln. Die oberste Unternehmensleitung muss selbst aktiv werden und dies durch klar definierte Visionen, Leitbilder und Ziele nachweisen.
- **Einbeziehung der Mitarbeiter:** Auf allen Ebenen formen die Mitarbeiter das Wesen eines Unternehmens. Nur wenn diese in die Abläufe mit einbezogen werden, können sie ihre Fähigkeiten im Sinne des Unternehmens richtig entfalten, wobei auch die Motivation, das Engagement und die Kreativität gesteigert werden.
- **Prozessorientierter Ansatz:** Das QM-System nach ISO 9001 soll die tatsächlichen optimierten betrieblichen Abläufe abbilden. Um die gewünschten Ergebnisse zu erhalten, sollten alle Tätigkeiten und die dazugehörigen Ressourcen als Prozess definiert und effizient gesteuert werden.
- **Systemorientierter Management-Ansatz:** Ein System besteht aus einem Geflecht von Prozessen, die miteinander in unterschiedlichen Wechselbeziehungen stehen. Nur wenn diese Zusammenhänge verstanden, geleitet und gemanagt werden, kann ein Unternehmen seine Ziele wirksam und effizient erreichen. Der systemorientierte Management-Ansatz führt zur Strukturierung der Prozesse und deckt die wechselseitigen Abhängigkeiten zwischen diesen auf.
- **Ständige Verbesserung:** Die ständige Verbesserung im Rahmen der ISO 9001 ist für eine gesunde Unternehmensentwicklung essenziell. Erfolgreiche Unternehmen reagieren auf die Markt- und Kundenerwartungen und optimieren ihre Produkte/Dienstleistungen und Prozesse kontinuierlich. Eine konsequent und unternehmensweit umgesetzte Verbesserungskultur kann das Leistungspotenzial des Unternehmens steigern und den Wettbewerbsvorsprung sichern.

- **Sachbezogener Ansatz zur Entscheidungsfindung:** Wirksame Entscheidungen beruhen auf der Analyse von Daten und Informationen. Dieser Grundsatz ermöglicht sachlich fundierte Entscheidungen, die auf einer verlässlichen Datenbasis beruhen. Anhand von Zahlen, Daten und Fakten können Meinungen und Entscheidungen verglichen oder bewertet werden. Die Aufzeichnungen von Entscheidungsgrundlagen lassen außerdem eine rückblickende Bewertung der Wirksamkeit bestimmter Maßnahmen zu. Ein Beispiel: Wenn ein Unternehmen im letzten Jahr eine Anzahl von x IT-Ausfällen hatte und durch Qualitätsmaßnahmen eine Besserung um y erwartet, aber y nicht annähernd erreichen konnte, müssen andere Maßnahmen gefunden werden, die fruchten könnten.
- **Lieferantenbeziehung beidseitig nutzen:** Ein Unternehmen ist von seinen Lieferanten abhängig – und umgekehrt. Umso wichtiger ist es, eine Win-win-Situation herbeizuführen, um die Wertschöpfungsfähigkeit auf beiden Seiten zu erhöhen. Dieser QM-Grundsatz stärkt das Vertrauen zwischen Unternehmen und Lieferanten, woraus sich eine langfristige, partnerschaftliche Zusammenarbeit (zum Beispiel langfristige Lieferantenverträge) entwickeln kann.

ISO 20000

Während ISO 9001 ein branchenunabhängiges Zertifikat für alle Unternehmen darstellt, geht ISO 20000 spezifisch auf die IT-Branche ein und liefert Vorgaben für ein effizientes IT Service Management (vgl. itwnet 2016). ISO 20000 baut auf ISO 9000 auf, ist stellenweise redundant, aber dennoch spezifisch auf IT-Unternehmen ausgerichtet. ISO 20000 zeigt hierzu die dazugehörigen Mindestanforderungen für eine Zertifizierung auf. Die grundlegenden Prinzipien wie Kundenorientierung, Führung etc. (siehe ISO 9001) werden nicht nochmals genannt.

ISO 20000 besteht aus fünf Teilen (vgl. Beims 2012):

- Part 1 „Service Management System Requirements“: Beinhaltet alle Shall-Anforderungen, die für eine Zertifizierung notwendig sind.
- Part 2 „Code of Practice“: Beinhaltet die Should-Anforderungen und darüber hinaus eine Anleitung, um die Methoden aus Part 1 umzusetzen.
- Part 3 „Guidance on Scope Definition and Applicability of ISO/IEC 20000-1“: Beinhaltet Ergänzungen zu Part 2 und fokussiert die Implementierung eines Service Management Systems (SMS).
- Part 4 „Process Reference Model“: Beinhaltet ein Prozessreferenzmodell für Service Management Prozesse und berät beim Aufbau eines Prozessbewertungsmodells.
- Part 5 „Exemplar Implementation Plan for ISO/IEC 20000-1“: Enthält einen Leitfaden zur Implementierung eines zertifizierbaren Service Management.

ISO 27001

Diese Norm regelt die IT-Sicherheit und deren Einsatz in Unternehmen, Behörden und Non-Profit-Organisationen.

„Diese Norm dient damit

- zur Formulierung von Anforderungen und Zielsetzungen an die IT-Sicherheit,
- zum kosteneffizienten Management von Sicherheitsrisiken,
- zur Definition von Managementtätigkeiten rund um die Informationstechnik,
- zur Sicherstellung von spezifischen Zielen zur Informationssicherheit.

Die […] Norm […] beinhaltet:

- Beschreibung der Anforderungen an das Management (Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung)
- Berücksichtigung aller Organisationen (zum Beispiel Handelsunternehmen, staatliche Organisationen, Non-Profit-Organisationen)
- Implementierung von geeigneten Sicherheitsmechanismen durch spezifizierte Anforderungen“ (TÜV NORD AUSTRIA 2016).

IT Infrastructure Library (ITIL)

Servicestrategie (Service Strategy)

Es ist wichtig zu verstehen, dass der IT-Dienstleister sich innerhalb des Unternehmens emanzipieren muss. Entscheidungen, Strategien und Portfolioanalysen lassen den Dienstleister zum Unternehmen im Unternehmen werden – und das ist auch so gewollt. Er muss selbst Entscheidungen treffen und sollte die entsprechenden Rechte hierfür eingeräumt bekommen.

Die Servicestrategie sieht vor, dass der IT-Dienstleister immer darauf vorbereitet sein muss, dass es günstigere und/oder effizientere Anbieter geben wird, die ihm seinen Platz streitig machen. Somit muss er seine eigene Konkurrenzfähigkeit kontinuierlich steigern und seine eigene Leistung permanent kritisch hinterfragen. Das ist dringend zu empfehlen, unabhängig davon, ob externe Kunden beliefert werden sollen oder „nur“ das eigene Unternehmen. Denn auch intern werden irgendwann externe Anbieter auftreten, die ihre Produkte als die effizientere Lösung verkaufen wollen.

Somit müssen sich die IT-Dienstleister grundsätzliche Fragen stellen: Welche Leistungen sollen und können angeboten werden? Was kann kosteneffizient produziert werden und bei welchen Produkten ist man der Konkurrenz voraus? Dabei muss das Unternehmen auch in die Rolle des Kunden schlüpfen. Als Unterstützung formuliert ITIL 21 verschiedene Produktnutzen, die der IT zum besseren Verständnis der Kundenperspektive verhelfen. Auf diese Weise verändert sich der Kern einer solchen Zusammenarbeit grundlegend: Die IT wartet nicht mehr auf den Auftrag vom Kunden und führt ihn dann aus. Der Dienstleister lernt vielmehr die Prozesse des Kunden in- und auswendig, hin-

terfragt durchgängig sein Angebot und geht von sich aus auf den Kunden zu (vgl. van Bon et al. 2010).

Serviceentwicklung (Service Design)

Im Service Design wird es nun konkreter. Es geht nicht mehr um alle Produkte generell, sondern vielmehr um die dem Kunden spezifisch angebotenen Lösungen, also um das Produktportfolio einzelner Auftraggeber. Im Service Design muss dabei aber zwingend beachtet werden, dass es sich lediglich um die Produkte handelt, die auch in der Servicestrategie festgelegt wurden.

Ein weiterer Bestandteil des Service Design ist die Nutzung der Service Level Agreements (SLA) (vgl. van Bon et al. 2010). Darauf wird in Kap. 10 gesondert eingegangen.

Serviceinbetriebnahme (Service Transition)

Veränderungen in der IT-Infrastruktur oder beispielsweise der Rollout neuer Software gehen bei Unternehmen in der Regel nur unter großem Aufwand vonstatten und bergen zudem die Gefahr, dass die Produktivität des Unternehmens während dieser Zeit – insbesondere bei Fehlern oder unvorhersehbaren Ausfällen – massiv leidet. Und mehr noch: Der Kunde verliert im Zweifel bares Geld, wenn die Geschäftsfähigkeit nicht aufrechterhalten werden kann. Das wird selbst bei kleineren Veränderungen schnell zum Hemmschuh, und Kunden stimmen neuer Software oder Softwareupdates oft nicht zu, auch wenn das wichtig für ihren Geschäftserfolg wäre. Und auch für den Dienstleister sind selbst kleinere Softwareupdates erfolgsentscheidend, da er im Sinne der Zukunftsfähigkeit des Kunden immer dafür Sorge tragen muss, dass die Unternehmens-IT auf dem neuesten Stand ist. Das zahlt auch auf die Kundenbindung ein und ist ein wichtiger Baustein dafür, dass die Konkurrenz nicht als innovativer wahrgenommen wird und die Kunden zu ihr abwandern. Außerdem ist es ein wichtiges Signal dafür, dass der IT-Partner selbstständig seine Leistung verbessert und sich der Kunde auf den Dienstleister verlassen kann. Deshalb muss die Transition auch ein eigener Bereich sein, damit dieser Prozess kontinuierlich optimiert wird und Best Practices erreicht werden.

Service Transition ist in ITIL in unterschiedliche Bereiche unterteilt:

- Service Asset und Configuration Management (inklusive Configuration Management System, CMS),
- die Configuration Management Data Base (CMDB), in der die Configuration Items (CI) dokumentiert werden,
- Knowledge Management (KM).

Zielsetzungen dieser Bereiche in der Service Transition sind ein hoher Spezialisierungsgrad, die Dokumentation allen Wissens sowie das kritische Hinterfragen der eigenen Arbeit durch Erhebung von KPIs und Audits. Darüber hinaus misst ITIL Schulungen nach Softwareänderungen oder der Einführung einer neuen Software eine hohe Bedeutung bei. So soll erreicht werden, dass nicht nur hinterfragt wird, wie wichtig die Updates sind, sondern auch, ob die Sichtweise der Kunden ausreichend Berücksichtigung findet: Was halten die

Mitarbeiter von der Software und wie kann man die Kolleginnen und Kollegen schnellstmöglich mit der neuen Lösung vertraut machen? (vgl. van Bon et al. 2010)

Servicebetrieb (Service Operation)

Service Operation widmet sich dem reibungslosen Ablauf nach der Softwareeinführung. Das beinhaltet unter anderem den Umgang mit Kundenanfragen, Störungen, Back-ups etc. Nennenswert ist hier die Differenzierung bei Störungen. Während sich das Incident Management um eine schnellstmögliche Behebung bestehender Incidents kümmern soll, übernimmt das Problem Management die Analyse von Incidents und wiederkehrenden Incidents. Es soll im Sinne der Prävention nicht nur auf die Behebung einer Störung ausgerichtet sein, sondern den Ursprung herausfinden, um ihn dauerhaft zu beseitigen (vgl. van Bon et al. 2010).

Kontinuierliche Serviceverbesserung (Continual Service Improvement)

Dieses ITIL-Buch will das Bewusstsein schärfen, Produkte, Serviceleistung, Qualität und Prozesse permanent zu verbessern – wobei festgehalten werden sollte, dass CSI nicht als eigene Phase am Ende einer Wertschöpfungskette gesehen werden sollte, sondern dauerhaft in jeder einzelnen ITIL-Phase durchgeführt werden muss.

Dieses Buch behandelt:

- Prozesse (Wie gehe ich an einen Verbesserungsprozess heran? Was ist bei Service Reporting, Service-Level-Entwicklung, Service Measurement zu beachten?)
- Organisation (Wie sind die entsprechenden Positionen wie Projektmanager, Service Manager, CSI Manager etc. zu besetzen?)
- Methoden und Hilfsmittel (Assessment, Benchmark, Balanced Score Card etc.)
- Durchführung im Betrieb (Was muss vorhanden sein, um CSI zu implementieren?) (vgl. van Bon et al. 2010)

Die Version von 2011 basiert auf ITIL V3. Darin sind 34 Prozesse und acht bis neun Funktionen definiert, die den Lebenszyklus von IT regeln sollen. Die Inhalte sind sehr umfangreich und es gilt für das eigene Unternehmen auch hier, die jeweils passenden und notwendigen Prozesse für sich zu definieren und an die individuelle Situation der Organisation anzupassen.

Folgende Prozesse werden „gelebt“; in etwa dieser Reihenfolge/Verbreitung/Reifegrad:

1. Incident Management
2. Request Fulfillment
3. Event Management
4. Access Management
5. Service Level Management
6. Change Management
7. Problem Management
8. Configuration Management

Und der Service Desk gilt als gelebte Funktion.

Projektstandards

PRINCE2

Die sieben Prozesse von PRINCE2:

1. Starting up a Project (SU):

Dieser Prozess beinhaltet die Projektvorbereitung. Der Projektmanager und der Kunde/Auftraggeber stimmen sich miteinander ab. Grundlage dieser Änderung ist meistens ein Business Case. Darüber hinaus werden in dieser vorbereitenden Phase konkrete Ziele (und Nicht-Ziele zur Abgrenzung zu anderen Projekten) gesetzt, das Team zusammengestellt und der Lenkungsausschuss gebildet. Der Lenkungsausschuss besteht in der Regel aus den Stakeholdern des Projektes.

Die To-do-Liste besteht in dieser Phase aus folgenden Punkten:

- SU1: Ernennung Projektauftraggeber und Projektmanager
- SU2: Definition Projektmanagementteam
- SU3: Verpflichtung Projektmanagementteam
- SU4: Vorbereitung Projektbeschreibung
- SU5: Definition Projektlösungsansatz
- SU6: Planung Initiierungsphase

2. Directing a Project (DP):

Dieser Prozess läuft während des gesamten Projekts parallel mit und soll die Arbeitsqualität maximieren und eine hohe Erfolgschance garantieren. Dahinter verbirgt sich die Kontrolle des Projekts und jeder einzelnen Phase.

To-do-Liste:

- DP1: Projektinitiierung freigeben
- DP2: Projekt freigeben
- DP3: Phasen- oder Ausnahmeplan freigeben
- DP4: Ad-hoc-Anweisungen geben
- DP5: Projektabschluss bestätigen

3. Initiating a Project (IP):

Das Projekt beginnt, Projektmanagementprozesse werden definiert und eine detaillierte Planung erfolgt. Hierbei muss auch ein Ergebnis definiert werden. Das zentrale Managementprodukt ist die Projektleitdokumentation, die in dieser Phase entsteht. Output ist hierbei:

- Der Qualitätsplan
- Der Konfigurationsmanagementplan
- Der Projektplan

- Der Kommunikationsplan

Auf der To-do-Liste dieser Projektphase steht:

- IP1: Qualität planen
- IP2: Projekt planen
- IP3: Business Case und Risiken verfeinern
- IP4: Projektsteuerungsmittel einrichten
- IP5: Projektablagestruktur einrichten
- IP6: Projektleitdokument zusammenstellen

4. Controlling a Stage (CS):

Hier wird das Tagesgeschäft des Projektmanagers erklärt, also die Steuerung, Planung und Kontrolle des Projekts. Arbeitsaufträge werden Arbeitspakete genannt. Der Status dieser Pakete (erledigt/nicht erledigt) gibt Aufschluss über den Gesamtstatus des Projekts. Wichtig ist es, messbare Ziele für die Arbeitspakete vorzugeben und somit den Status des Projekts zu abstrahieren, da sonst eine Messbarkeit erschwert ist. Die To-do-Liste für diese Phase lautet:

- CS1: Arbeitspaket freigeben
- CS2: Fortschritt überwachen
- CS3: Offene Punkte aufnehmen
- CS4: Offene Punkte prüfen
- CS5: Phasenstatus prüfen
- CS6: Über Projektstatus berichten
- CS7: Korrekturmaßnahmen einleiten
- CS8: Offene Punkte eskalieren
- CS9: Abgeschlossenes Arbeitspaket entgegennehmen

5. Managing Product Delivery (MP)

PRINCE2 definiert die durch Projekte erzeugten Produkte als Managementprodukte. „Dieser Prozess erzeugt die Produkte des Projekts, hier wird der größte Teil der Projektressourcen eingesetzt“ (Ebel 2011).

Hier werden die in Arbeitspakete geschnürten Arbeitsaufträge ausgeführt, nachdem sie in (der) vorherigen Prozessphase(n) beschlossen und freigegeben wurden.

To-do-Liste:

- MP1: Arbeitspaket annehmen
- MP2: Arbeitspaket ausführen
- MP3: Arbeitspaket abliefern

6. Managing Stage Boundaries (SB)

In dieser Phase besteht die Aufgabe darin, dem Lenkungsausschuss sozusagen das erste und das letzte Wort zu den unterschiedlichen Prozessen zu geben. Am Ende eines Prozesses wird der Lenkungsausschuss kritisch hinterfragen, was der ursprüngliche Plan war und was tatsächlich davon umgesetzt wurde. Ausgehend vom Business Case muss das Ergebnis mit den Anforderungen verglichen werden und zur Not – und das ist in der Praxis nicht selten – der Business Case angepasst und nachverhandelt werden. So können die Risiken in den laufenden Prozessen erkannt werden, die dann in das Risikoprotokoll aufgenommen werden und deren Auswirkungen auf den Business Case ermittelt werden müssen. Die „Idee" hinter dem Projekt: Der Lenkungsausschuss und das Management erhalten in dieser Phase einen Überblick sowie ein Gefühl dafür, „wo sie stehen" und was in der kommenden Phase zu unternehmen ist. So wird eine bessere Planung der bevorstehenden Phase möglich.
To-dos in dieser Phase:

- SB1: Phase planen
- SB2: Projektplan aktualisieren
- SB3: Business Case aktualisieren
- SB4: Risikoprotokoll aktualisieren
- SB5: Phasenabschluss berichten

7. Closing a Project (CP)

PRINCE2 schreibt sich ein koordiniertes Projektende auf die Fahne. Das umfasst sowohl das Beenden des Projektes sowie die Auflösung der (unternehmerischen) Projektstrukturen als auch die Analyse, inwieweit das Projekt nach Plan durchgeführt wurde, welche Abweichungen aufgetreten sind und wie sich diese auf die Einführung und den täglichen Workflow der Veränderung auswirken. Das bedeutet, die Veränderung im Regelprozess im Betrieb muss nach folgenden Kriterien geprüft werden: Ist sie effektiv und effizient? Bietet sie einen tatsächlichen Mehrwert? Welche Auswirkung hat sie auf die Organisation und auf welche Resonanz stößt sie bei der Belegschaft?
To-do-Liste für diese Phase:

- CP1: Projekt auflösen
- CP2: Folgeaktionen identifizieren
- CP3: Projekt bewerten (vgl. Beims et al. 2015)

Six Sigma

Entscheidet sich ein Unternehmen dazu, Six Sigma als Prozessoptimierungsansatz zu nutzen, ist der Weg dorthin tatsächlich auf einer „Testebene" durchführbar. Zunächst werden einige wenige Führungskräfte durch anerkannte Experten geschult. Diese müssen während der Schulungen einen definierten Prozess in ihrem Unternehmen mit der Six-Sigma-Methodik optimieren, um sich zu qualifizieren. So kann frühzeitig und effizient festgestellt werden, ob für das Unternehmen grundsätzlich ein Mehrwert durch dieses Verfahren ge-

schaffen werden kann. Das Verfahren ist über den Return on Investment eindeutig quantifizierbar, was die Frage klärt, ob der Gewinn durch die Optimierung das Investment übersteigt. Somit können anschließend die Erfolge auf alle Bereiche im Unternehmen übertragen werden.

Six Sigma kann auf unterschiedliche Verantwortlichkeiten zugeschnitten werden; denn Abteilungsleiter, Manager oder Sachbearbeiter haben im Unternehmen unterschiedliche Funktionen inne, für die es dann jeweils perfekt passende „Belts" gibt.

Viele werden sich nun fragen, ob Six Sigma vielleicht zu komplex oder kompliziert ist, um es in einem Unternehmen anzuwenden. Doch das Gegenteil ist der Fall. Denn Six Sigma bietet viele unterschiedliche Möglichkeiten an, um an Problemstellungen heranzutreten. Möchte man beispielsweise auf der einen Produktionslinie die Durchlaufzeit von 24 Stunden bei einem Produkt auf 12 Stunden reduzieren, ist Six Sigma die richtige Methodik. Six Sigma selbst ist nur dann komplex, wenn der Prozess kompliziert ist. Arbeitet das Unternehmen bereits vor der Optimierung nach ISO oder ITIL, ist dies sogar förderlich, denn dann existieren bereits Standards in den Prozessen und müssen nicht erst gebildet werden. So kann sehr schnell und einfach durch die Prozessbeschreibung analysiert und optimiert werden. Dafür wird zunächst untersucht, ob ein Verbesserungspotenzial besteht, was im Prinzip eine rein mathematische Arbeit ist; anschließend wird die Optimierung anhand der gelernten Methoden problemlos umgesetzt.

Darüber hinaus ist noch eine weitere Form von Six Sigma verfügbar: das sogenannte Lean Six Sigma. Der Hauptunterschied: Six Sigma verbessert einzelne Prozesse. Das Lean Six Sigma muss hingegen eher als eine das Unternehmen verschlankende Methodik statt als eine Art Umstrukturierung und Strategieänderung gesehen werden. Dazu werden die Abteilungen, Prozesse und Strukturen von Unternehmen mit bekannten Mitteln verschlankt und optimiert.

Anwendungsfelder von Six Sigma kann man nicht spezifisch nennen, weil das Spektrum unbegrenzt ist. Überall, wo Prozesse im Einsatz sind, die optimiert werden können, kann Six Sigma zur Anwendung kommen. Beispielsweise können „Problembereiche in der Supply Chain erkannt sowie Ursachen ermittelt und behoben werden" (Gestmann 2008b), oder es können „mithilfe der statistischen Instrumente von Six Sigma Wirkzusammenhänge erkannt und wichtige Einfluss- und Erfolgsfaktoren für den Vermittlungserfolg [eines Personaldienstleisters, d. V.] identifiziert werden […]. Wenn Personaldienstleister den Vermittlungserfolg ihrer Mitarbeiter erhöhen wollen, schulen sie meist zunächst ihr Personal. Wenn jedoch die Ablauforganisation und die Geschäftsprozesse im Rahmen eines Six-Sigma-Projekts optimal auf die Ziele des Personaldienstleisters ausgerichtet werden, lassen sich Vermittlungserfolge signifikant steigern. Dies belegt ein unlängst durchgeführtes Six-Sigma-Projekt bei einem bundesweit aktiven Personaldienstleister" (Business Wissen 2009). Weiter half die Methodik auch, „Probleme in der Lieferkette zu erkennen und Fehler abzustellen. […] Der zahlengetriebene Ansatz wendet statistische Methoden von Six Sigma auf die Leistungsmessgrößen des sogenannten SCOR-Modells an. SCOR, kurz für Supply Chain Operation Reference, ist ein standardisiertes Modell, um Geschäftsprozesse zu beschreiben. ‚Dieses Instrument, das wir SCMAnalytics nennen, ermöglicht es,

fundierte Aussagen zur Performance der jeweiligen Supply Chain zu machen‘, erklärt Dipl.-Ing. Michael Ferger von Six Sigma Deutschland. Insgesamt werden 55 Leistungsmessgrößen erhoben, mit den statistischen Methoden von Six Sigma ausgewertet und abschließend das Ergebnis interpretiert. ‚Jede einzelne Aussage zur Wertschöpfungskette wird qualifiziert sowie mit Zahlen, Daten und Fakten abgesichert‘, so Ferger weiter. Anschließend werden die den Leistungsmessgrößen bereits zugeordneten potenziellen Problemursachen analysiert und gewichtet. ‚So können Leistungshemmnisse sofort identifiziert und behoben werden‘, ergänzt Professor Schmieder, der an der Toolentwicklung beteiligt war.“ (Gestmann 2008a) In der Mitte und am Ende der 1990er-Jahre liefen zwei Wellen von den Vereinigten Staaten nach Europa. Six Sigma schaffte nach seiner Einführung bei Motorola 1987 den Durchbruch, sodass die Methode in zahlreichen US-Tochtergesellschaften in Europa angewendet wird – darunter beispielsweise Kodak, Allied Signal und General Electric (vgl. Töpfer 2007).

Anhang zu Kapitel 7: Qualität im Betrieb: Zero Outage sorgt für Ausfallsicherheit und Nachhaltigkeit

Beispielhafte Checkliste aus den Zero Outage Compliance Audits

INCIDENT MANAGEMENT

- Für alle schwerwiegenden und kritischen Incidents wird ein vollständiger Incident Report erstellt.
- Es ist sichergestellt, dass Supplier Tickets geöffnet werden, bevor ein Fall an das RedPhone übergeben wird.
- Es wird eine Prüfung der Changes der letzten Tage durchgeführt und jeder schwerwiegende Incident in der Change-Liste markiert.
- Cross Checks/Fire Drills (Simulationen von Störungen) werden zeitnah geplant und durchgeführt.
- Im Falle eines potenziellen critical oder critical Incident wird das RedPhone innerhalb von 45 Minuten miteinbezogen.
- Für critical/high Incidents wird die Known Error Datenbank genutzt.
- Der Customer Business Impact ist verifiziert, bevor ein Fall an das RedPhone übergeben wird.
- Die Teilnahme an den 4-wöchentlichen Incident Management Community Meetings ist für alle Zeitzonen (Americas, EMEA/APAC) sichergestellt.
- Teilnahme an den RedPhone und Global Problem Management Handover Calls an allen Wochentagen frühmorgens, um schwerwiegende Fälle zu melden und zu übergeben, die zuvor in der Service Line/im Account/in der Local Business Unit gehandhabt wurden.
- Bei schwerwiegenden oder potenziell kritischen Incidents wird das Yellow Local Phone innerhalb von 20 Minuten eingesetzt (lokale Lead Incident Manager oder MoDs).

S. Kasulke, J. Bensch, *Zero Outage*, DOI 10.1007/978-3-658-14222-3,

PROBLEM MANAGEMENT

- Die Standard- (oder kundenbasierte) Vorlage für die Root Cause Analyse wird in vollem Umfang genutzt.
- Eine übergreifende Root Cause Datenbank ist im Einsatz und steht bei Major Incidents und Early Warnings auch auf Englisch zur Verfügung.
- Das Problem Maßnahmen Tracking (Zeitplan & Inhalte) für Major Incidents/Early Warnings/On-Demand-Fälle/schwerwiegende Incidents ist vorhanden.
- Für die wichtigsten von Incidents betroffenen Technologien (zum Beispiel Storage Boxes/ SAN, Cloud/Appcom; Data Center Network; Datenbanken; Middleware; Betriebssysteme) werden Einträge in der Known Error Datenbank erstellt.
- Es werden vierteljährliche Trendanalysen durchgeführt.
- Sign off Calls für schwerwiegende Fälle (High Incidents) sind festgelegt (Fälle, die nicht zentral vom Global Problem Management verwaltet werden).
- Maßnahmen für überfällige Root Causes sind definiert und implementiert, um eine Reduzierung des Backlogs zu gewährleisten.
- Es ist ein proaktives Problem Management vorhanden, wiederkehrende Ereignisanalysen werden regelmäßig durchgeführt, und es sind entsprechende Maßnahmen definiert, um die Root Causes nachhaltig zu beseitigen.
- Dedizierte Lead Problem Manager (LPRM) nehmen bei größeren Incidents/Early Warnings/schwerwiegenden und speziellen Fällen an „Get the day started"-Übergabe-Calls teil.
- Dedizierte LPRM nehmen an lokalen/globalen Lessons Learned Sessions teil.
- Kontinuierliche Verbesserungen/Qualitätsinitiativen auf Grundlage der Root-Cause-Analysen finden statt.
- Fire Drills (Simulationen von Incidents unter Echtbedingungen) sind aufgeplant – falls die Alarmierungskette (intern/extern) Schwächen zeigt.
- Maßnahmen zu Erkenntnissen oder Schwachstellen aus Fire Drills sind definiert und werden zeitgerecht umgesetzt.
- Die Critical Landscapes und alle enthaltenen Serviceketten werden regelmäßig aktualisiert, um Informationen auf dem neuesten Stand zu halten (letzte bestätigte Überprüfung durch Service Delivery und Operations Manager nicht älter als vier Wochen).
- Root Causes enthalten eine schriftliche und bestätigte Root Cause von Zero-Outage-zertifizierten Lieferanten im Fall von Incidents, die als „Lieferantenfehler" bewertet werden.
- Maßnahmen zur nachhaltigen Problemlösung enthalten auch einen vom Lieferanten geführten Health Check der kompletten Installationsbasis seiner Produkte und Services.
- Überarbeitete Einträge in der Known Error Datenbank sind geprüft und gegebenenfalls auch von zertifizierten Lieferanten genehmigt.
- Problem Tickets werden aktiv eröffnet, wenn ein monatlicher SLA eines relevanten Kunden ROT markiert ist.

CHANGE MANAGEMENT

- Für jeden Kunden ist ein Lead Change Manager übergreifend verantwortlich.
- Die Teilnahme an globalen „Lessons Learned Sessions“ (monatlich) ist gewährleistet.
- Alle Major und Significant Changes wurden mit Genehmigung des Central Change Advisory Board (CCAB) implementiert (in den letzten drei Monaten).
- Das lokale CAB hat Change-Modelle für wiederkehrende Changes genehmigt.
- Der Input in den globalen Change-Kalender erfolgt auf regelmäßiger Basis.
- Relevante Projekte (Kategorie A, B) sind Teil des Change-Kalenders.
- Hoch-Risiko-Changes und Special Focus Changes (zum Beispiel Risiko „sehr hoch“, sehr komplexe und kritische Changes) sind mindestens 40 Tage vor Umsetzungsdatum bekannt, Teil des Change-Kalenders und werden im CCAB und mit dem Topmanagement besprochen.
- Für alle rückabgewickelten Hoch-Risiko-Changes und Special Focus Changes (zum Beispiel Risiko „sehr hoch“, sehr komplexe und wichtige Changes) ist ein Review nach Durchführung erfolgt.
- Die Anzahl der benötigten Safeguarding Calls für Hoch-Risiko und Special Focus Changes ist aufgrund sauberer Planung nicht höher als drei (inklusive des letzten finalen Safeguarding Calls).
- Die Change-Bewertung „rechtzeitige Change Implementierung“ (Ziele: 95 % für alle und 90 % für Change-Typen „Major“ und „Significant“) ist erreicht.
- Für jeden Change, der nicht rechtzeitig implementiert wurde (60 Minuten über dem Change Window) wird der Grund für die Zeitüberschreitung geprüft.
- Die Change-Bewertung „erfolgreiche Change-Durchführung“ (Ziel: 98 % für alle Change-Typen) ist erreicht.
- Für jeden nicht erfolgreichen Change wird der Grund geprüft.
- Die relevanten CCAB/CAB-Mitglieder sind im Falle von Change-bezogenen Incidents beteiligt, um die Ursache herauszufinden (Was lief beim Change falsch?).

CONFIGURATION MANAGEMENT

- Eine Critical Landscape (für alle kritischen Serviceketten) ist beschrieben und in der CMDB Ende zu Ende abgebildet.
- Für jedes Configuration Item (und jede Servicekette) ist die korrekte Kritikalität in der CMDB gespeichert.
- Alle kritischen Serviceketten haben einen SLA von mindestens xx,x %.
- Die Datenqualität wird regelmäßig mithilfe der Standard KPIs und Berichte geprüft.

Glossar

3P: Zusammenfassung der drei zentralen Faktoren zur langfristigen Qualitätssicherung – bestmöglich ausgebildetes Personal (**P**eople), einfache, standardisierte Prozesse (**P**rocesses) und einheitliche, hochperformante Plattformen (**P**latforms).

Agile Vorgehensmodelle: Flexible Herangehensweise an Projekte insbesondere in der Softwareentwicklung. Agilität beinhaltet den raschen Beginn mit der eigentlichen Programmierung, die ständige Abstimmung mit dem späteren Nutzer, laufende Tests und die kontinuierliche Weiterentwicklung der Architektur.

Appliance: Designansatz für ein kombiniertes System aus Hardware und speziell darauf optimierter Software. Appliance dient überwiegend einer einzigen oder wenigen Anwendungen.

Aufbauorganisation: Das hierarchische Gerüst eines Unternehmens. Die Aufbauorganisation beschreibt, welche Aufgaben von welchen Ressourcen (Menschen und Arbeitsmitteln) erledigt werden. Darüber hinaus hat jedes Unternehmen eine Ablauforganisation, die die Prozesse darstellt.

Bebauungsplan: Einzigartige Methode innerhalb von Zero Outage, um alle qualitätsrelevanten Risiken bei T-Systems nach einer fest definierten Struktur zu managen. Dazu werden knapp 280 identifizierte Einzelrisiken in 40 Kategorien zusammengefasst. Die daraus abgeleiteten Karten des Bebauungsplans definieren Initiativen und Maßnahmen, um die Risiken nachhaltig zu eliminieren. Die drei wichtigsten Komponenten hierbei sind qualitätszertifizierte Mitarbeiter, standardisierte Prozesse sowie moderne, hochverfügbare Plattformen.

S. Kasulke, J. Bensch, *Zero Outage*, DOI 10.1007/978-3-658-14222-3,

Capability Maturity Management Model (CMMI): Modell zur Entwicklung von Produkten und Prozessen, indem diese in unterschiedliche Capability Level eingeteilt werden, die den jeweiligen Reifegrad beschreiben.

Central Change Advisory Board (CCAB): Prüft als genehmigende Instanz und als Teil des globalen De-Escalation Management alle wichtigen und kritischen Changes in der IT-Landschaft und überwacht deren Durchführung.

Change Management: Beschreibt im Rahmen von ITIL einen Prozess, der das Ziel hat, alle Anpassungen an der IT-Infrastruktur kontrolliert, effizient und unter Minimierung von Risiken für den Betrieb bestehender Business-Services durchzuführen.

Claim Management: Kommt es zu Abweichungen von einem vereinbarten Vertragsumfang, werden im Rahmen des Claim Management Maßnahmen eingefordert und die Verrechnung von Zusatzaufwendungen initiiert. Ein Claim ist die Forderung eines Partners, die sich aufgrund einer Abweichung ergibt.

Cloud Computing: IT-Infrastrukturen und -Anwendungen (wie Software oder Speicherkapazität) aus einem Netzwerk, meist betrieben von einem Service-Provider. Die Daten werden somit nicht mehr auf den eigenen Speichermedien des Unternehmens vorgehalten, sondern im Rechenzentrum des Providers. Anwender erhalten damit dynamische und skalierbare IT-Ressourcen, die dem jeweiligen Bedarf flexibel angepasst werden können. Die Abrechnung erfolgt in der Regel nach genutzten Dienstleistungen.

Commodity Business: Zunehmend austauschbares Leistungsangebot von Anbietern am Markt.

Configuration Items (CIs): Nach ITIL (IT Infrastructure Library) sämtliche an den Geschäftsprozessen beteiligten Betriebsmittel. Beispiele sind: PC, Netzwerkkomponenten, Applikationen, Server, Software.

Configuration Management Data Base (CMDB): Datenbank für die Verwaltung von Informationen zur IT-Infrastruktur und -Konfiguration innerhalb des Configuration Management. Hilft Unternehmen dabei, Risiken und Auswirkungen zu bewerten und damit Störungen zu reduzieren.

Continuous-Improvement-Programm: Programm, das die systematische, dauerhafte und objektive Messung der Kundenbedürfnisse einerseits sowie Maßnahmen zur Sicherstellung der Kundenzufriedenheit andererseits beinhaltet.

Critical Landscape: Übersicht der geschäftskritischen IT-Systeme des Kunden. Unter anderem relevant für das Incident Management (siehe auch Major Incidents).

Customer Business Impact (CBI): Auswirkung eines Changes oder Incidents auf die Geschäftsprozesse des Kunden.

De-Escalation Management: De-Escalation Management umfasst das Central Change Advisory Board, das Global Incident Management und das zentrale Problem Management. Die Aufgabe des De-Escalation Management besteht darin, bei Störungen schnellstmöglich den normalen Betrieb wiederherzustellen und die Ursache zu identifizieren, um vorbeugende Maßnahmen ergreifen zu können.

Ende zu Ende (E2E): Die Bereitstellung eines IT-Services wird in den meisten Fällen durch die Zusammenarbeit von verschiedenen Organisationseinheiten innerhalb eines IT-Service-Providers sowie von externen Suppliern und Partnern realisiert. Eine Ende-zu-Ende(E2E)-Perspektive berücksichtigt alle Beteiligten.

Failover Test: Ein Failover ist der ungeplante Wechsel von einer technischen Komponente auf eine andere während eines einseitigen Ausfalls. Der Failover Test prüft, ob dieser Wechsel funktioniert und damit Hochverfügbarkeit sichergestellt ist.

Firedrill: In der IT die Simulation von Systemausfällen zwecks Training der Störungsbehebung.

GxP-Richtlinien: Die verschiedenen („x“) Richtlinien für eine gute Arbeitspraxis, insbesondere in den Bereichen Medizin, Pharmazie und pharmazeutische Chemie. Beispiele: GMP (Good Manufacturing Practice) und GCP (Good Clinical Practice).

Health Check: Die regelmäßige Überprüfung beispielsweise von Systemen, Applikationen oder Projekten mithilfe von standardisierten, aber auch spezialisierten Fragebögen bei T-Systems.

ICT: Kurzform für „Information and Communications Technology“ (Informations- und Kommunikationstechnologie). Beschreibt die Zusammenführung von Informationstechnik (IT) und Telekommunikation (TK).

Incident Management: Beschreibt im Rahmen von ITIL (IT Infrastructure Library) einen Prozess, der das Ziel hat, Störungen (Incidents) des IT-Betriebs zu beseitigen.

Intensive Care: Standardisierter Analyse- und Verbesserungsansatz bei T-Systems zur Lösung von Qualitätsproblemen bei Topkunden.

ISAE 3402: Kurzform für „International Standard on Assurance Engagements“. Zertifiziert das Kontrollsystem eines Service-Providers. ISAE 3402 hat den US-Standardauditreport SAS-70 abgelöst und dient als Grundlage eines ganzheitlichen Kontrollsystems.

IT Infrastructure Library (ITIL): Sammlung von Best Practices für IT-Prozesse. ITIL wurde erstmals 1989 durch das Office of Government Commerce (OGC) veröffentlicht und wird in unterschiedlichen Ausprägungen weiterentwickelt.

Key Performance Indicator (KPI): Eine Leistungskennzahl, die dazu dient, die Erreichung definierter Zielwerte zu messen.

Kritikalität: Drückt in der IT aus, welche Bedeutung ihrem Fehlverhalten beigemessen wird. Sie wird in Stufen bewertet, wobei die Einstufung umso höher ist, je gravierender die erwarteten Auswirkungen bei Fehlverhalten sind.

Lean Management: Maßnahmen zur Optimierung beziehungsweise „Verschlankung" von Prozessen.

Major Incident (MI): Schwerwiegende Störung – beispielsweise ein Ausfall eines IT-Systems, in dessen Folge ein wichtiger Geschäftsprozess eines Unternehmens gestört wird, sodass mit einem erheblichen Schaden (Reputationsverlust oder finanziellem Schaden) zu rechnen ist.

Manager on Duty (MoD): Repräsentant aus dem Management der Betriebseinheiten innerhalb des IT-Service-Providers. Er wird in Eskalationen und bei Notfällen aktiviert. Seine Hauptaufgaben sind Koordination von Krisengesprächen, Entscheidung über Ressourcen, Unterstützung bei der Eskalation zu Dritten und Organisation der Bestätigungen für Emergency Changes.

Mean Time to Repair (MTTR): Durchschnittliche Zeit, die nach einem Systemausfall zur Wiederherstellung der IT-Systeme benötigt wird.

Nearshore: Verlagerung von Leistungen in Nachbarländer (siehe auch Offshore beziehungsweise Onshore).

Offshore: Verlagerung von Dienstleistungen ins (Übersee-)Ausland (siehe auch Nearshore beziehungsweise Onshore).

Onshore: Auslagerung von Leistungen innerhalb des eigenen Landes (siehe auch Nearshore beziehungsweise Offshore).

Onsite: Auslagerung von Leistungen an andere Mitarbeiter innerhalb des eigenen Standorts (siehe auch Onshore).

Outsourcing: Auslagerung von Leistungen oder Bereichen an Dritte.

Problem Management: Beschreibt im Rahmen von ITIL einen Prozess, der das Ziel hat, die Ursachen für Störungen (Incidents) herauszufinden und für die Zukunft zu beheben. Ergebnisse können entweder Known Errors oder Workarounds sein – sie werden dem Incident Management zur Verfügung gestellt, um eine Wiederholung der Störung zu vermeiden.

Quality Academy: Konzernweite Weiterbildungsakademie von T-Systems mit einem modularen, auf Jobprofile ausgerichteten Selbsttrainingsansatz sowie einem durchgängigen Zertifizierungssystem. Der Inhalt der Trainings und verfügbaren Zertifizierungen besteht aus Qualitätsthemen – mit dem Ziel, Qualität in die DNA der Mitarbeiter zu integrieren.

Root Cause: Ursache für einen Incident (Störung).

Root Cause Rate/Root Cause Rate in Time: Kennzahl, die misst, ob die Ursache für einen Incident schnell beziehungsweise innerhalb der vorgegebenen Zeit ausfindig gemacht wurde.

Service Delivery Manager: Schnittstelle zum Kunden. Verantwortet Kundenanforderungen, den Vertrag, finanzielle Planung, operative Eskalationen, regelmäßige Reviews und das SLA Reporting.

Service Improvement Program (SIP): Definiert Maßnahmen zur Verbesserung von Prozessen und Services in einem vereinbarten Zeitraum sowie mit messbaren Fortschritts- und Ergebniskennzahlen. Baut beispielsweise auf den Ergebnissen eines Service Review auf und hat zum Ziel, die identifizierten Lücken zu schließen.

Service Level Agreement (SLA): Vereinbarung zwischen dem Kunden und dem Provider, in der die Qualität einer Leistung messbar festgehalten wird (beispielsweise Bandbreite, Verfügbarkeiten etc.).

Standardisierung: In der IT eine Vereinheitlichung von Prozessen, Produkten und Services, basierend auf Erfahrungswerten, um Abläufe effizienter (im Sinne von Kosten und Produktivität) zu gestalten und Kunden eine höchstmögliche Qualität und Wirtschaftlichkeit von Leistungen zu bieten.

Supply Chain: Stellt die komplette Wertschöpfungs- und Lieferkette von Einzelteilen/-services bis hin zum Endprodukt (oder Service) dar.

WAN: Wide Area Network ist ein Rechnernetz, das sich über Länder oder Kontinente erstreckt und an das eine unbegrenzte Anzahl an Rechnern angeschlossen werden kann.

Zero Outage: Holistisches Qualitätsprogramm von T-Systems mit Standards in den Bereichen People, Process und Platform (siehe auch 3Ps) mit dem Ziel, einen so weit wie möglich fehlerfreien IT-Betrieb und Zuverlässigkeit in Projekten für die Kunden sicherzustellen.

Literaturverzeichnis

Beims, Martin (2012): IT-Service Management in der Praxis mit ITIL (3. Auflage. München: Carl Hanser Verlag, S. 225f.

Beims, Martin; Ziegenbein, Michael (2015): IT-Service Management in der Praxis mit ITIL (4. Auflage). München: Carl Hanser Verlag München, S. 310–325.

Bitkom (2016): Digitalisierung der Wirtschaft nimmt Fahrt auf. https://www.bitkom.org/Presse/Presseinformation/Digitalisierung-der-Wirtschaft-nimmt-Fahrt-auf.html. Zugegriffen: 27.06.2016.

Bon, Jan van; Jong, Arjen de; Kolthof, Axel; Pieper, Mike; Tjassing, Ruby; van der Veen, Annelies; Verheijen, Tienke (2010): ITIL V – Das Taschenbuch. Zaltbommel: Van Haren Publishing, S. 25–64.

Business Wissen (2009): Six-Sigma-Projekt schafft Grundlage für höhere Vermittlungserfolge. http://www.business-wissen.de/artikel/personalvermittlung-six-sigma-projekt-schafft-grundlage-fuer-hoehere-vermittlungserfolge/. Zugegriffen: 14.06.2016.

Capgemini (2015): Studie IT-Trends 2015 – Digitalisierung gibt Zusammenarbeit zwischen Business und IT eine neue Qualität. https://www.de.capgemini.com/resource-file-access/resource/pdf/it-trends-studie-2015.pdf. Zugegriffen: 09.06.2016.

DeMarco, Tom; Lister, Tim (2003): Bärentango, Mit Risikomanagement Projekte zum Erfolg führen. Carl Hanser Verlag GmbH & Co. KG.

Ebel, Nadin (2011): PRINCE2:2009 – für Projektmanagement mit Methode. München: Addison-Wesley, S. 103–111.

Fröhlich, Martin; Glasner, Kurt (2007): IT-Governance. Wiesbaden: Betriebswirtschaftlicher Verlag Dr. Th. Gabler; GWV Fachverlage GmbH, S. 6.

Gestmann, Michael (2008a): Auf Fehlersuche in der Lieferkette. In: Industrieanzeiger Online. http://www.industrieanzeiger.de/home/-/article/12503/11824006/Auf+Fehlersuche+in+der+Lieferkette/art_co_INSTANCE_0000/. Zugegriffen: 14.06.2016.

Gestmann, Michael (2008b): Six Sigma: Probleme in der Lieferkette erkennen und abstellen. http://www.business-wissen.de/artikel/six-sigma-probleme-in-der-lieferkette-erkennen-und-abstellen/. Zugegriffen: 28.06.2016.

Glaap, Winfried (1993): ISO 9000 leichtgemacht. München, Wien: Carl Hanser Verlag München Wien.

Gorecki, Pawel; Pautsch, Peter R. (2014): Praxisbuch Lean Management – Der Weg zur operativen Excellence (2. Auflage). München: Carl Hanser Verlag München, S. 3–27.

Görgen, Peter (2015): Das Problemkind „Problem Management“, in: Materna Monitor (2015) Nr. 2, S. 33–35.

S. Kasulke, J. Bensch, *Zero Outage*, DOI 10.1007/978-3-658-14222-3,

International Organization for Standardization (2015): Quality management principles. http://www.iso.org/iso/pub100080.pdf. Zugegriffen: 21.06.2016.
ISG (2015): ISG Studie. https://www.t-systems.com/de/de/ueber-uns/unternehmen/newsroom/news/news/isg-studie-bestaetigt-t-systems-strategie-221890. Zugegriffen: 04.07.2016.
ITSM Group (2015): Wachsender Fokus auf die IT-Servicequalität. https://www.itsm-consulting.de/news-events/news-feed/wachsender-fokus-auf-die-it-servicequalitaet. Zugegriffen: 06.06.2016.
Itwnet (2016): ISO 9001:2000 and ISO/IEC 20000:2005 Comparison. http://www.itwnet.com/system/files/ISO9001_20000_Cross-reference.pdf. Zugegriffen: 28.06.2016.
Kaspersky (2013): Security Bulletin 2013 / 2014. http://media.kaspersky.com/de/business-security/Kaspersky Security Bulletin 2013_2014_ebook_deutsch.pdf. Zugegriffen: 10.06.2016.
Kasulke, Stephan (2013a): Maßnahmen zur kurzfristigen Qualitätsverbesserung. In: Abolhassan, Ferri (Hrsg.): Der Weg zur modernen IT-Fabrik. Industrialisierung – Automatisierung – Optimierung. Wiesbaden: Springer Gabler, S. 71–78.
Kasulke, Stephan (2013b): Maßnahmen zur mittel- und langfristigen Qualitätsverbesserung. Erschienen in: Der Weg zur modernen IT-Fabrik. Hrsg. v. F. Abolhassan, Springer Fachmedien Wiesbaden 2014, S. 109–113.
Kasulke, Stephan (2014): Continuous Improvement – Qualität optimieren und Kundenzufriedenheit garantieren. In: Abolhassan, Ferri (Hrsg.): Kundenzufriedenheit mit IT-Outsourcing. Das Optimum realisieren. Wiesbaden: Springer Gabler, S. 41–52.
Kayenta (2015): PMP Zertifizierung – Project Management Professional PMP nach PMI. http://web.archive.org/web/20151014233229/http://www.kayenta.de/seminar-training/projektmanagement/pmp-zertifizierung-project-management-professional-pmp-nach-pmi.html. Zugegriffen: 14.06.2016.
PMI (2014): Project Management Institute. http://h10076.www1.hpe.com/education/standards_faq_brand.pdf. Zugegriffen: 14.06.2016.
PwC (2012): IT-Sourcing-Studie 2012 – Aktuelle IT-Sourcing-Perspektiven erkennen und nutzen. http://www.pwc.at/presse/2012/pdf/studie-it-sourcing-2012.pdf. Zugegriffen: 09.06.2016.
PwC (2015): IT-Sourcing-Studie – Die Perspektive der Anbieter. http://www.conect.at/uploads/tx_posseminar/20150319_ITSM_PwC_IT_Sourcing_v1.0_2_.pdf. Zugegriffen: 09.06.2016.
Schiefer, Helmut; Schitterer, Erik (2008): Prozesse optimieren mit ITIL (2. Auflage). Wiesbaden: GWV Fachverlage GmbH, S. 12.
SixSigma (2015): http://www.six-sigma.de/
Stych, Christof; Zeppenfeld, Klaus (2008): ITIL. Berlin: Springer-Verlag Berlin Heidelberg, S. 15.
T-Online (2014): Hacker durch Zufall: Jugendliche knacken Bankautomaten. http://www.t-online.de/computer/sicherheit/id_69792478/14-jaehrige-knacken-bankautomaten-mit-handbuch-aus-dem-internet.html. Zugegriffen: 10.06.2016.
Töpfer, Armin (2007): Six Sigma: Konzeption und Erfolgsbeispiele für praktizierte Null-Fehler-Qualität (4. Auflage). Springer Berlin, Heidelberg, New York.
TÜV (2015): ISO 9001 – Qualität mit System. http://www.tuev-sued.de/management-systeme/iso-9001. Zugegriffen: 14.06.2016.
TÜV NORD AUSTRIA (2016): Informationen – ein kostbares Gut. https://www.tuv-nord.com/at/de/informations-technologie/iso-27001-616.htm. Zugegriffen: 14.06.2016.
TÜV NORD GROUP (2014): TÜV NORD CERT – Zertifizierung von Qualitätsmanagementsystemen nach DIN EN ISO 9001. https://www.tuev-nord.de/fileadmin/Content/Global/TUEV_NORD_Archiv/pdf/pdb-iso-9001.pdf. Zugegriffen: 14.06.2016.
ZDNet (2015): Apple: iTunes Store, App Store outage cased by 'internal' error. http://www.zdnet.com/article/apples-itunes-store-app-store-experiencing-outages/. Zugegriffen: 27.06.2016.

Danksagung

Wir möchten uns bei allen Beteiligten für ihr Engagement herzlich bedanken.

Unser besonderer Dank für die Mitwirkung bei der Erstellung und Umsetzung dieses Buches sowie die wesentliche Unterstützung der Autoren gilt den folgenden Personen:

Heike Bayerl ist seit 2012 Vice President für Security Compliance und Quality Management bei der T-Systems International GmbH. In dieser Funktion verantwortet sie weltweit die Quality Akademie. Darüber hinaus steuert und auditiert sie maßgeblich Themen für den IT-Betrieb des internen Sicherheits- und Qualitätsmanagements. Heike Bayerl absolvierte ihr Studium zur Diplom-Ingenieurin (FH) der Nachrichtentechnik an der Fachhochschule Offenburg (Hochschule für Technik, Wirtschaft und Medien). Zudem ist sie zertifizierter Six Sigma BlackBelt.

Dr. Jürgen Herczeg ist seit 2013 Vice President Process & Quality Management bei der T-Systems International GmbH. Er ist seit 20 Jahren im Bereich der Entwicklung, Beratung, Qualitätssicherung und Management von Software-Projekten tätig. Seit Ende 2005 erarbeitet er in einem Team von Software-Architekten die unternehmensweiten Standards und Entwicklungsprogramme der T-Systems für Software Engineering & Architecture. Dr. Jürgen Herczeg studierte Informatik an der Universität Stuttgart und promovierte im Jahr 1995.

S. Kasulke, J. Bensch, *Zero Outage*, DOI 10.1007/978-3-658-14222-3,

Ines-Maria Böckl ist seit 2006 als Projektleiterin bei der T-Systems International GmbH tätig und steuert Projekte verschiedener Organisationen und Landesgesellschaften. Sie begleitete den Aufbau von strategischen Produktionsstandorten und wirkte an der Erstellung eines Hardware- und Kapazitätsmanagements mit. Zudem gestaltete sie das Ressourcenmanagement für drei Landesgesellschaften. 2016 wechselte sie in das Line Office Quality bei T-Systems. Kommunikation und Erwachsenenbildung waren bereits in ihrem Studium zur Dipl.-Religionspädagogin (FH) Schwerpunktthemen. Später absolvierte sie mit Fokus auf interkulturelles Lernen, Arbeiten und Steuern zusätzlich den MBA an der University of Louisville.

Nadine Schmidt entwickelt seit 2013 als Communications Expert bei der T-Systems International GmbH interne und externe Kommunikationskonzepte zu Zero Outage und sorgt für deren zielgruppengerechte Umsetzung. Im Jahr 2000 begann sie ihre Karriere im Konzern, nachdem sie International Business Studies an der Fachhochschule Dortmund sowie der University of Abertay Dundee, Schottland studiert hatte. Sie hält ein Diplom für Betriebswirtschaft und ist Bachelor of Arts with First Class Honours. 2008 absolvierte sie ein berufsbegleitendes Studium zur PR-Beraterin.

Christian Braunsteiner ist seit über 15 Jahren in der ICT-Branche tätig. Nach Ende seiner kaufmännischen Ausbildung mit dem Schwerpunkt Wirtschaftsinformatik trat er 2000 dem Mobilfunkanbieter max.mobil (heute T-Mobile Austria) in den Bereichen Service und Systembetrieb bei. Seit 2008 ist er bei der T-Systems International GmbH im Bereich Quality beschäftigt. Christian Braunsteiner absolvierte ein Bachelor-Studium am Internationalen Management Center in Krems sowie ein Master-Studium an der Donau-Universität Krems.

Zudem bedanken wir uns herzlich bei folgenden Kolleginnen und Kollegen, die inhaltlich und in der Koordination wertvolle Impulse geliefert haben: Doris Reitter, Björn Petersen, Sascha Lisson, Joachim Bausch, Falk Reckert und Bernd Najewitz. Und last but not least bei der Agentur PSM&W (hier im Speziellen Birgit Wölker und Dominique-Silvia Kemp).

Zero Outage

Das Fachbuch zeigt, wie die Zero-Outage-Methode zu mehr Stabilität im Betrieb, mehr Zuverlässigkeit in Projekten und letztlich zu einer höheren Kundenzufriedenheit führt. Es verdeutlicht, weshalb klare Standards bei Plattformen, Prozessen und Personal unverzichtbar sind, um eine hohe ICT-Qualität von Ende zu Ende sicherzustellen und worauf es bei Changes – den häufigsten Ursachen für IT-Ausfälle – ankommt. Zudem erfahren die Leser, wie man Störungen schnellstmöglich behebt und dauerhaft abstellt und warum die industrieweite Zusammenarbeit künftig nur mit einem gemeinsamen Qualitätsstandard gelingen kann. So dient dieses Buch als praxisnahe Anleitung, die eigene ICT-Welt noch ausfallsicherer und leistungsfähiger zu machen. Dazu teilen die Autoren ihre wichtigsten Erkenntnisse im Qualitätsmanagement und geben einen exklusiven Einblick in ihr – über viele Jahre erprobtes und kontinuierlich weiterentwickeltes – Erfolgsrezept: den Zero-Outage-Ansatz.

Der Inhalt

- Qualität im Betrieb: Zero Outage im Change, Incident und Problem Management
- Der Zero-Outage-Bebauungsplan: Ausfallrisiken erkennen und proaktiv managen
- Qualität in Projekten: Pain Points, Frühwarnsysteme, De-Escalation
- Compliance und Security: gesetzliche Anforderungen meistern
- Von der Kundenwahrnehmung zur Kundenzufriedenheit
- Ende-zu-Ende-Qualität gelingt nur im Verbund mit Partnern und Suppliern
- „Null Fehler"-Denken: Zero Outage in der Unternehmenskultur verankern

Mit einem Grußwort von **Dr. Ferri Abolhassan**, Geschäftsführer von T-Systems, verantwortlich für die IT Division und Telekom Security und Initiator von Zero Outage.

Die Autoren

Stephan Kasulke ist seit 2012 Senior Vice President Quality von T-Systems. Er leitet in dieser Funktion das weltweite Zero-Outage-Programm zur Verbesserung der Betriebs- und Projektqualität.
Jasmin Bensch ist Executive Consultant ITIL und Leiterin des Stabs Quality von T-Systems. Sie hat langjährige Erfahrung im Prozessdesign und der Prozessoptimierung im IT-Outsourcing.

ISBN 978-3-658-14221-6
9 783658 142216
► springer-gabler.de