

Referenzprofil

# *Network Administrator*

Stefan Grunwald

Thoralf Freitag

Dieses Referenzprofil wurde im Rahmen des bmb+f geförderten Projekts  
„Arbeitsprozessorientierte Weiterbildung in der IT-Branche“ erarbeitet von:



**Fraunhofer ISST**



Deutsche Telekom AG  
**Bildungspartner**



Deutsche Telekom AG  
**Unternehmenspartner**

## Danksagung

---

Diese Umsetzungsempfehlung entstand mit freundlicher Unterstützung der Deutschen Telekom AG. Besonderer Dank gilt den Fachexperten Markus Zielonka und Stefan Jäckel, die mit großem Einsatz die Entwicklung dieses Dokuments unterstützt haben.

# Inhalt

---

<b>1</b>	<b>EINFÜHRUNG: REFERENZPROZESSE ALS CURRICULA .....</b>	<b>5</b>
1.1	EREIGNIS-PROZESS-KETTEN: SYMBOLIK .....	6
1.2	REFERENZPROZESS UND TEILPROZESSE .....	7
<b>2</b>	<b>PROFILBESCHREIBUNG.....</b>	<b>10</b>
2.1	TÄTIGKEITSBESCHREIBUNG.....	10
2.2	PROFILTYPISCHE ARBEITSPROZESSE .....	11
2.3	PROFILPRÄGENDE KOMPETENZFELDER.....	12
2.4	QUALIFIKATIONSERFORDERNISSE.....	13
2.5	EINORDNUNG INS SYSTEM UND KARRIEREPFADE .....	13
<b>3</b>	<b>REFERENZPROZESSE NETWORK ADMINISTRATOR .....</b>	<b>14</b>
3.1	CHANGEMANAGEMENT .....	14
3.1.1	Referenzprozess Changemanagement.....	15
3.1.2	Prozesskompass Changemanagement.....	17
3.1.3	Teilprozesse Changemanagement.....	18
3.1.3.1	Analysieren der Anforderung.....	18
3.1.3.2	Ausarbeiten eines Angebots .....	20
3.1.3.3	Planen der Abwicklung .....	21
3.1.3.4	Beschaffen der erforderlichen Komponenten.....	22
3.1.3.5	Installieren der Komponenten .....	23
3.1.3.6	Konfigurieren nach Anforderung .....	25
3.1.3.7	Überprüfen der durchgeführten Änderungen .....	26
3.1.3.8	Durchführen der Übergabe.....	28
3.1.3.9	Informieren betroffener Personen/Stellen .....	29
3.1.3.10	Erstellen einer Prozessdokumentation.....	30
3.1.4	Beispiel Changemanagement.....	32
3.1.4.1	Auftrag (Analyse der Anforderung, Ausarbeiten eines Angebots) .....	32
3.1.4.2	Genehmigung (Durchführbarkeitsprüfung).....	32
3.1.4.3	Planung (Durchführbarkeitsprüfung, Planen der Abwicklung, Zuweisen der Ressourcen) .....	32
3.1.4.4	Beschaffung (Beschaffen der Komponenten) .....	33
3.1.4.5	Installation (Zusammenfügen der Komponenten) .....	33
3.1.4.6	Konfiguration (Konfigurieren nach Anforderung).....	34
3.1.4.7	Test und Fehlerbehebung (Prüfen der durchgeführten Änderungen).....	34
3.1.4.8	Bereitstellung (Bereitstellen des Systems).....	35
3.1.4.9	Einweisung (Durchführen von Kommunikationsmaßnahmen).....	35
3.1.4.10	Übergabe (Durchführen der Übergabe) .....	35
3.1.4.11	Schulung (Informieren betroffener Personen/Stellen).....	35
3.1.4.12	Dokumentation (Erstellen einer Prozessdokumentation).....	35
3.2	FAULTMANAGEMENT .....	37
3.2.1	Referenzprozess Faultmanagement .....	38
3.2.2	Prozesskompass Faultmanagement .....	40
3.2.3	Teilprozesse Faultmanagement .....	41
3.2.3.1	Durchführen der initialen Bereitstellung .....	41
3.2.3.2	Durchführen kontinuierlicher Überwachung .....	43
3.2.3.3	Wahrnehmen der Störung .....	45
3.2.3.4	Lokalisieren der Störung.....	47
3.2.3.5	Eingrenzen der Fehlerart.....	49
3.2.3.6	Planen der Abwicklung.....	51
3.2.3.7	Ausführen der Arbeiten nach Plan .....	52
3.2.3.8	Durchführen von Tests (im Fehlerumfeld).....	53
3.2.3.9	Informieren betroffener Personen/Stellen .....	55
3.2.3.10	Erstellen einer Prozessdokumentation.....	55
3.2.4	Beispiel Faultmanagement .....	56
3.3	PERFORMANCEMANAGEMENT.....	57
3.3.1	Referenzprozess Performancemanagement.....	58

3.3.2	Prozesskompass Performancemanagement.....	60
3.3.3	Teilprozesse Performancemanagement.....	61
3.3.3.1	Durchführen der initialen Bereitstellung .....	61
3.3.3.2	Durchführen kontinuierlicher Messungen.....	63
3.3.3.3	Analysieren der Schwellwertüberschreitung .....	65
3.3.3.4	Lokalisieren des Engpasses.....	66
3.3.3.5	Erstellen von Handlungsalternativen .....	68
3.3.3.6	Ausführen Changemanagement .....	70
3.3.3.7	Informieren betroffener Personen/Stellen .....	70
3.3.3.8	Erstellen einer Prozessdokumentation .....	70
3.3.4	Beispiel Performancemanagement .....	71
3.4	SECURITYMANAGEMENT .....	72
3.4.1	Referenzprozess Securitymanagement .....	73
3.4.2	Prozesskompass Securitymanagement .....	75
3.4.3	Teilprozesse Securitymanagement .....	76
3.4.3.1	Umsetzen der Richtlinien auf Netzwerkebene .....	76
3.4.3.2	Durchführen kontinuierlicher Kontrollen .....	78
3.4.3.3	Umfassendes Informieren .....	80
3.4.3.4	Analysieren des Vorkommnis .....	81
3.4.3.5	Untersuchen der Auswirkungen .....	82
3.4.3.6	Reaktives Entwickeln von ad-hoc-Lösungen.....	83
3.4.3.7	Aktives Entwickeln von Umsetzungsmöglichkeiten.....	84
3.4.3.8	Ausführen Changemanagement .....	86
3.4.3.9	Ausführen Sicherheitscheck .....	86
3.4.3.10	Informieren betroffener Personen/Stellen .....	88
3.4.3.11	Erstellen einer Prozessdokumentation .....	88
3.5	ORGANISATION UND BERATUNG .....	89
3.5.1	Referenzprozess Organisation und Beratung .....	90
3.5.2	Prozesskompass Organisation und Beratung .....	91
3.5.3	Teilprozesse Organisation und Beratung .....	92
3.5.3.1	Erstellen eines Vorschlags für Servicestrukturen.....	92
3.5.3.2	Durchführen von Service .....	94
3.5.3.3	Beraten von nicht-fachlichen Projektleitern .....	95
3.5.3.4	Bereitstellen von Netzwerkressourcen .....	96
3.6	WERKZEUGE .....	98

# 1 Einführung: Referenzprozesse als Curricula

---

Das Referenzprojekt des Network Administrator verdeutlicht paradigmatisch die diesem Tätigkeitsfeld zu Grunde liegenden Arbeitsprozesse, die mit ihnen verbundenen Ansprüche sowie die daraus resultierenden Anforderungen an Inhalt und Durchführung einer qualitativ hochwertigen Weiterbildung.

Das Referenzprojekt erfüllt mehrere Funktionen:

## **Aus der Praxis für die Praxis:**

Als Abstraktion tatsächlich stattgefundener Projekte und Prozesse bieten die Referenzprozesse eine realistische und leicht nachvollziehbare Abbildung dessen, was die Tätigkeiten eines Network Administrator sind.

## **Prozessorientierung als innovatives „Curriculum“:**

Als vollständige Darstellung aller wichtigen Arbeitsprozesse sowie der dazugehörigen Qualifikationen, Tätigkeiten und Werkzeuge bieten die Referenzprozesse die Grundlage für die Weiterbildung zum Network Administrator. Alle diese Prozesse müssen - entsprechend den Vorgaben - einmal oder mehrfach durchlaufen werden und ermöglichen dadurch den Weiterzubildenden den arbeitsplatznahen, integrativen Erwerb von relevanten Kompetenzen. Durch den Verbleib im Arbeitsprozess wird nicht nur für die Weiterzubildenden eine hohe Motivation (Arbeit an echten Projekten/Aufgaben) und Nachhaltigkeit erreicht, sondern auch - aus Sicht des Unternehmens - die Kontinuität und Qualität der laufenden Arbeiten gesichert (keine Ausfallzeit durch Seminartage, kein mühsamer Transfer).

## **Qualitätsstandard für die Weiterbildung:**

Als Referenz bieten insbesondere die Teilprozesse und die mit ihnen verbundenen Tätigkeits- und Qualifikationsziele einen Qualitätsmaßstab für die arbeitsprozessorientierte Weiterbildung und die resultierenden Abschlüsse. Vollständige Transparenz und klare Zielvorgaben ermöglichen die qualitativ hochwertige Absicherung auch komplexer Kompetenzen sowie den systematischen Erwerb des notwendigen Erfahrungswissens.

## **Transferprozesse:**

Die Generalisierung des Referenzprojekts aus der Praxis und seine didaktische Anreicherung ermöglichen eine leichte Auswahl angemessener Transferprozesse, deren Bearbeitung die Grundlage der Weiterbildung ist. Transferprozesse sind reale Prozesse, die Referenzprojekte in einer lernförderlichen Umgebung abbilden. Abgeschlossene Transferprozesse auf Basis der hier dargestellten Anforderungen und Qualitätsmaßstäbe sind nicht nur Qualifikationsnachweis des Einzelnen, sondern bilden auch die Basis eines angemessenen und zielgerichteteren Umgangs mit Geschäfts- und Arbeitsprozessen im Unternehmen.

## 1.1 Ereignis-Prozess-Ketten: Symbolik

Die Darstellung der Referenzprozesse in Form von Ereignis-Prozess-Ketten<sup>1</sup> ermöglicht einen schnellen Überblick. Vollständigkeit kann leicht überprüft werden, Anpassungen und Modifikationen in Hinblick auf das eigene Unternehmen sind problemlos möglich und Anknüpfungspunkte an andere Prozesse, aber auch zu weiterführenden Informationen ergeben sich automatisch.

Die bei der Darstellung der Referenz- und Teilprozesse verwendete Modellierungssprache stellt eine Anpassung und Weiterentwicklung der klassischen EPK-Modellierung dar:

- Referenz- wie Teilprozesse sind aus der Sicht des jeweiligen Spezialisten, also als Arbeitsprozesse einer Person dargestellt.
- Referenz- wie Teilprozesse stellen in der Regel keinen Geschäftsprozess dar.

Die EPK-Symbole werden hier wie folgt verwendet:

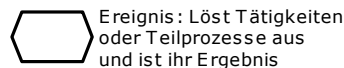
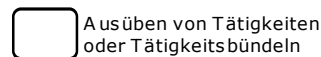
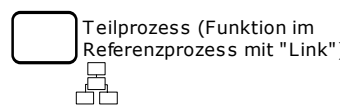


Abbildung A: Grundlegende Symbole der Referenz- und Teilprozessmodelle

Die wichtigsten Symbole sind:

die Tätigkeiten bzw. Tätigkeitsbündel oder Teilprozesse, die mit dem Funktionssymbol dargestellt werden;

die Ereignisse, die Tätigkeiten bzw. Teilprozesse auslösen und Ergebnisse von Teilprozessen sind.

Grundsätzlich gilt: Auf ein Ereignis folgt immer ein Teilprozess bzw. eine Tätigkeit.

Ergebnisse von Tätigkeiten sind sehr oft Dokumente, diese werden dann zusätzlich durch das Dokument-Symbol dargestellt.

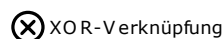
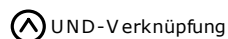


Abbildung B: Konnektoren

<sup>1</sup> vgl. A.-W. Scheer, Wirtschaftsinformatik, Springer 1998

Wenn Alternativ-Möglichkeiten bestehen, werden Ereignisse und Teilprozesse/Tätigkeiten über Konnektoren (AND, OR, XOR) verbunden. Dabei steht AND für ein verbindendes „und“, OR für ein „oder“, das alle Möglichkeiten offen lässt und XOR für ein „ausschließendes oder“, welches nur einen der angegebenen Pfade ermöglicht.

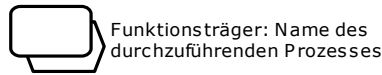


Abbildung C: Schnittstelle

Da die Prozesse aus der Sicht des jeweiligen Spezialisten formuliert werden, sind Schnittstellen zu Prozessen anderer Spezialisten oder zu Entscheidungsprozessen auf höherer Ebene notwendig. Dazu wird das Schnittstellensymbol verwendet. Es steht für Prozesse, die der Spezialist nicht selber durchführt, auf deren Durchführung er aber angewiesen ist. Parallel zu jeder Schnittstelle wird die Tätigkeit dargestellt, die der Spezialist selbst in diesem Zusammenhang ausübt, wie „Beraten bei ...“, „Unterstützen bei ...“ oder „Informieren des ...“.

Alle Prozesse werden durch die Verwendung dieser Symbole klar und einfach strukturiert dargestellt und sind offen für die Übertragung in konkrete Transferprozesse.

## 1.2 Referenzprozess und Teilprozesse

---

Der hier vorgestellte Referenzprozess und seine Teilprozesse stellen das Curriculum des Spezialistenprofils Network Administrator dar.

Der Referenzprozess erhebt nicht den Anspruch eines Vorgehensmodells, sondern bildet beispielhaft den möglichen Arbeitsprozess und Verlauf eines Projekts auf Spezialistenebene ab.

Er bildet die Grundlage für Weiterbildungen und damit einen Qualitäts-, Niveau- und Komplexitätsmaßstab. Die zugehörigen Teilprozesse sind hier beispielhaft modelliert und stellen eine Möglichkeit der Durchführung dar. Einzelheiten zu den unverzichtbaren Prozessen und Kompetenzfeldern sind hier im Referenzprojekt festgelegt. Die Reihenfolge und die Inhalte der Teilprozesse sind abhängig vom jeweils auszuwählenden Transferprojekt und werden in diesem Zusammenhang festgelegt.

Die Darstellung der Prozesse erfolgt systematisch:

Jeder Prozess wird mit Hilfe von Ereignis-Prozess-Ketten dargestellt. Einem auslösenden Ereignis folgt eine Funktion, die wiederum ein oder mehrere Ereignisse als Ergebnis hat. Ereignisse und Funktionen können mit AND, OR oder XOR, den Konnektoren, verbunden sein.

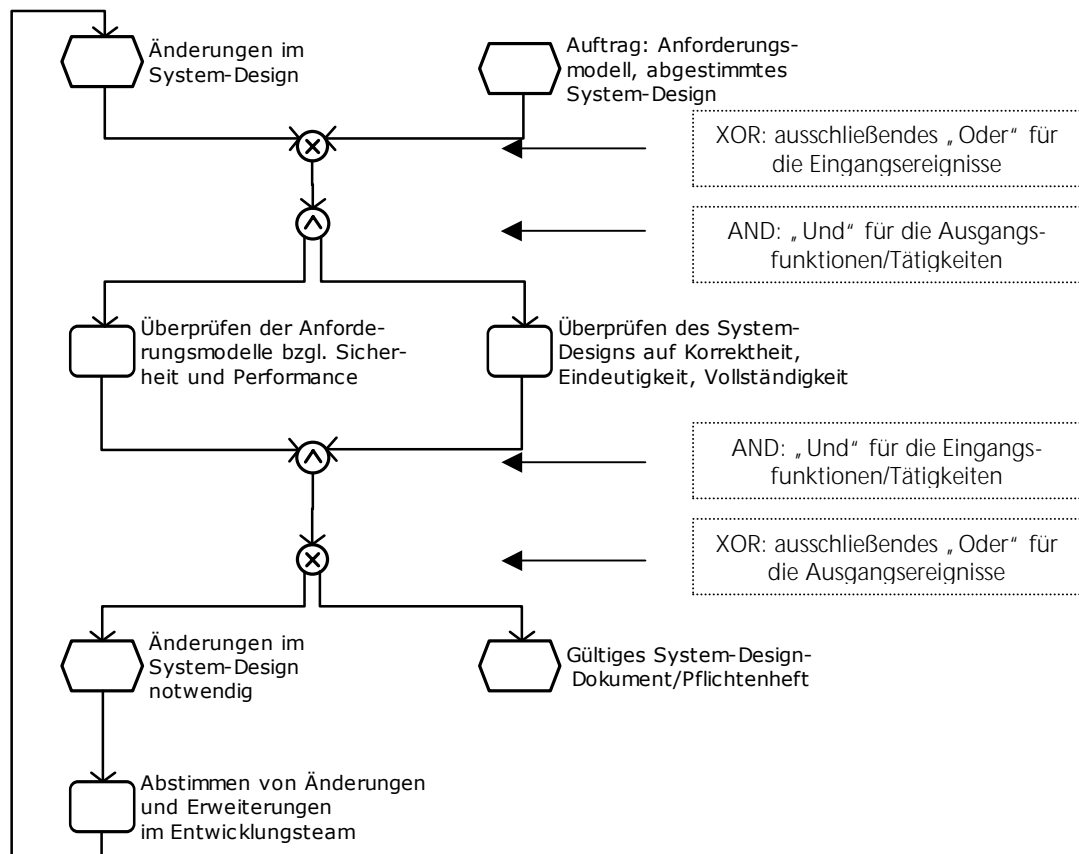


Abbildung D: Beispielprozess (Teilprozess "Überprüfen des Systemdesigns") mit unterschiedlicher Verwendung von Konnektoren

Die Verbindung von Referenzprozess und Teilprozessen erfolgt über die Funktionen des Referenzprozesses:

Jede Funktion im Referenzprozess steht für einen Teilprozess.

Ereignisse, die dem jeweiligen Teilprozess direkt vor oder nachgeordnet sind, sind Anfangs- und Endereignisse der jeweiligen Teilprozesse. Damit stellen die Teilprozesse die Funktionen des Referenzprozesses ausführlich dar und ein Hin- und Herbewegen zwischen Referenz- und Teilprozessen ist jederzeit problemlos möglich.





## 2 Profilbeschreibung

---

Network Administrator<sup>2</sup> betreiben Netzwerke. Sie analysieren und bewerten den internen und externen Datenverkehr, kontrollieren und analysieren Datendurchsatz und Fehlerrate. Sie organisieren den Netzbetrieb, einschließlich des Benutzersupports. Sie analysieren Probleme beim Netzbetrieb, isolieren und beheben fehlerhafte Zustände in Netzwerken und erarbeiten Richtlinien für den Netzbetrieb. Sie erarbeiten neue technische Konzepte für den Netzbetrieb und entwickeln Netze unter Beachtung der Auswirkungen der Veränderungen bedarfsgerecht und wirtschaftlich weiter. Network Administratoren planen und überprüfen Sicherheitsmaßnahmen gegen Angriffe von außen und von innen.

Network Administrator administrieren aktive und passive Komponenten und unterstützen Systemdienste mit Netzwerk- und Systemmanagementsystemen.

### 2.1 Tätigkeitsbeschreibung

---

Die zentrale Tätigkeit des Network Administrator ist das Betreiben eines oder mehrerer Netzwerke. Network Administrator befassen sich mit der Analyse und Bewertung des internen und externen Datenverkehrs. Einen Teil des Tagesgeschäftes eines Network Administrators macht die Problembehebung aus, also die Überwachung bzw. Funktionskontrolle des Netzes sowie die Analyse und Beseitigung von auftretenden Problemen und Fehlern. Außerdem erarbeitet der Network Administrator Richtlinien für den Netzbetrieb. Er gewährleistet das Management der Systemfunktionen, und zwar:

- das Changemanagement, also die bedarfsgerechte Weiterentwicklung des Netzes unter Beachtung sowohl prozessorientierter als auch sozialer Auswirkungen der Veränderungen
- das Faultmanagement, also das Erkennen (Monitoring), Isolieren und Beheben fehlerhafter Zustände im Netzwerk
- das Performancemanagement, also die Kontrolle und Analyse des Datendurchsatzes und der Fehlerrate, d.h. das Sicherstellen der geforderten „Quality of Services“ - Parameter
- das Securitymanagement, also die Planung und Überprüfung von Sicherheitsmaßnahmen sowohl gegen Angriffe von außen als auch von innen

und führt diese durch. Zudem ist er verantwortlich für die Organisation und Beratung im Netzwerkumfeld. Dazu gehört z. B.:

- das Verwalten der Netzwerkprotokolle (z.B. die Verwaltung der Netzwerkadressen)
- das Auswählen und Integrieren von Netzwerk-, Hard- und Software-Produkten für das Netzwerk und seinen Betrieb sowie deren Konfiguration
- Planen und Analysieren der Hardware- und Netzwerkkapazitäten
- die Entwicklung und Einrichtung von Netzwerk- und Sicherheitsstandards
- die Anpassung von Funktionen in der Netzwerkmanagementplattform
- die Erstellung von kleinen Werkzeugen.

---

<sup>2</sup> Das Kapitel 2: „Das Profil: Network Administrator“ gibt - mit Ausnahme des Abschnitts 2.1 „Tätigkeitsbeschreibung“ - den offiziellen Text der „Vereinbarung über die Spezialistenprofile im Rahmen des Verfahrens zur Ordnung der IT-Weiterbildung“ vom 25.05.2002 (Bundesanzeiger 105, ausgegeben am 12.06.2002) wieder.

Darüber hinaus muss der Network Administrator z.B. im Bereich Aus- und Weiterbildung von Mitarbeitern auch Führungsaufgaben wahrnehmen. Hier hat er Fachkräfte für die Betreuung der Auszubildenden auszuwählen. Daneben muss der Network Administrator Fachkräfte im Arbeitsprozess beim Kenntnis- und Fähigkeitserwerb unterstützen.

Außerdem beschäftigt er sich mit der Entscheidungsvorbereitung für seinen Vorgesetzten (Professional).

## **2.2 Profiltypische Arbeitsprozesse**

---

Die im Folgenden beschriebenen Referenz- und Teilprozesse dokumentieren die profiltypischen Arbeitsprozesse des Network Administrator in ihrer Gesamtheit. Die Beherrschung dieser Arbeitsprozesse in Verbindung mit den Kompetenzen in den jeweiligen Kompetenzfeldern und der Berufserfahrung bilden die Grundlage für die berufliche Handlungskompetenz.

### **Changemanagement**

1. Analysieren der Anforderung, Prüfen des Änderungsbedarfs aus technischer Sicht, Durchführen von Evaluierungen und Variantenvergleichen, Durchführen von Wirtschaftlichkeitsbetrachtungen.
2. Erstellen und Weiterentwickeln von Betriebskonzepten, Planen der Änderungen.
3. Ausarbeiten von Angeboten, Führen und Begleiten von Vertragsverhandlungen.
4. Beschaffen von erforderlichen Komponenten.
5. Installieren der Komponenten.
6. Konfigurieren der Anwendungen nach Anforderung und Systemvorgaben.
7. Prüfen der durchgeführten Änderungen. Integrieren des Systems/Teilnetzes in die bestehende Infrastruktur.
8. Durchführen der Übergabe an Kunden. Durchführen von Einweisungen und Schulungen der Kunden in neue und geänderte Systeme.
9. Erstellen von Prozessdokumentationen.

### **Fault-, Performance- und Securitymanagement**

1. Durchführen der initialen Bereitstellung. Umsetzen des Sicherheitskonzepts.
2. Durchführen kontinuierlicher Überwachungen, Messungen und Kontrollen.
3. Wahrnehmen von Störungen, Analysieren von Schwellwertüberschreitungen, Vorkommnissen und ihres Bedrohungspotentials.
4. Lokalisieren von Störungen oder Engpässen.
5. Eingrenzen der Fehlerart. Gegebenenfalls Prüfen der Aktivitäten eines Angreifers und Feststellen von Schädigungen.
6. Reaktives Entwickeln von Ad-hoc-Lösungen falls notwendig.
7. Planen der Problembeseitigung, Spezifizieren der Parameter für Ressourcenplanungen sowie Vergleichen und Auswählen von Handlungsalternativen.
8. Beseitigung von Fehlern bzw. Ausführen von Changemanagementprozessen. Testen der erfolgten Änderung.
9. Informieren betroffener Personen und Stellen. Durchführen von Einweisungen und Schulungen in geänderte oder neue Systeme.
10. Erstellen von Prozessdokumentationen.

## Organisation und Beratung

1. Verwalten von Nutzern und Rechten, Betreiben von Verzeichnisdiensten.
2. Technisches Beraten von nicht-fachlichen Projektleitern bei Projektplanung und Projektmanagement im Netzwerkbereich.
3. Durchführen Support für (interne) Kunden zur Gewährleistung der Kundenzufriedenheit.

## 2.3 Profilprägende Kompetenzfelder

---

Die Beherrschung der profiltypischen Arbeitsprozesse setzt Kompetenzen unterschiedlicher Reichweite in den nachstehend aufgeführten beruflichen Kompetenzfeldern<sup>3</sup> voraus. Den Kompetenzfeldern sind Wissen und Fähigkeiten sowie typische Methoden und Werkzeuge unterschiedlicher Breite und Tiefe zugeordnet.

Grundlegend zu beherrschende, gemeinsame Kompetenzfelder<sup>4</sup>:

- Unternehmensziele und Kundeninteressen,
- Problemanalyse, -lösung,
- Kommunikation, Präsentation,
- Konflikterkennung, -lösung,
- Fremdsprachliche Kommunikation (englisch),
- Projektorganisation, -kooperation,
- Zeitmanagement, Aufgabenplanung und -priorisierung,
- Wirtschaftliches Handeln,
- Selbstlernen, Lernorganisation,
- Innovationspotenziale,
- Datenschutz, -sicherheit,
- Dokumentation, -standards,
- Qualitätssicherung.

Fundiert zu beherrschende, gruppenspezifische Kompetenzfelder:

- Datenbanken, Netzwerke, Betriebssysteme
- Datensicherungskonzepte,
- Sicherheitskonzepte und -überwachung,
- Statistik und Datenvisualisierung,
- Wirtschaftlichkeitsanalysen,
- Marktüberblick,
- Unternehmensorganisation,
- Nutzerorientierte Problemanalyse, -lösung.

Routiniert zu beherrschende, profilspezifische Kompetenzfelder:

- Netzwerke, Netzwerkprotokolle, -dimensionen, -topologien,
- Netzwerkkomponenten, -organisation,
- Übertragungsmedien, -systeme, -techniken,
- Übertragungsprotokolle,
- Schnittstellen,
- Netzwerkmanagementsysteme, Netzwerkanalysewerkzeuge.

---

<sup>3</sup> Die Kompetenzfelder werden in der nachfolgenden Auflistung jeweils durch ein zusammenfassendes Stichwort benannt. Da die Weiterbildung zum Spezialisten auf die erfolgreiche Bewältigung zunehmend offener beruflicher Handlungssituationen sowie ganzheitlichen Kompetenzerwerb abzielt, bildet der Kompetenzerwerb einen integralen Bestandteil der Arbeits- und Weiterbildungsprozesse und lässt sich nur im Zusammenhang mit diesen operationalisieren (vgl. dazu die Abschnitte „Kompetenzfelder“ in Kapitel 3.1.4 ff).

<sup>4</sup> Jeder Spezialist muss in den in diesem Abschnitt genannten Kompetenzfeldern wie „Kommunikation, Präsentation“, „Konflikt-erkennung, -lösung“ usw. ein Niveau erreichen, dass über dem einer Fachkraft liegt. D. h. er muss auch in diesen Feldern zu eigenständigem Handeln in der Lage sein und zum Erreichen des Ziels in dem jeweiligen Feld gegebenenfalls über den Rahmen bekannter Verfahren und Lösungen hinaus gehen können.

## 2.4 Qualifikationserfordernisse

---

Es wird ein hinreichendes Qualifikationsniveau auf der Basis einschlägiger Berufsausbildung oder Berufserfahrung vorausgesetzt.

## 2.5 Einordnung ins System und Karrierepfade

---

Das neue IT-Weiterbildungssystem gibt auf Basis der vier neuen IT-Ausbildungsberufe drei Ebenen für die Weiterqualifizierung vor: Spezialisten, wie auch der Network Administrator einer ist, operative und strategische Professionals. Auf der Ebene der Spezialisten existieren eine Reihe verwandter Profile und selbstverständlich kann sich auch der Datenbankentwickler zu einem Professional weiterqualifizieren.

### **Verwandte Profile**

Die Tätigkeiten des Network Administrators decken die Bereiche des Netzaufbaus, des Betriebs und der Wartung von Netzwerken und ihrer Hard- und Software-Komponenten ab. Der Schwerpunkt liegt allerdings in der Wartung eines Netzwerks.

Ähnliche Profile auf diesem Gebiet sind vor allem der Network Developer und der IT Systems Administrator, deren Tätigkeitsschwerpunkte sich in Teilen überschneiden.

### **IT Systems Administrator:**

Ähnlich wie der Network Administrator, jedoch mit stärkerer Fokussierung auf Hard- und Software-Systeme, die nicht unbedingt Netz(werk)komponenten sein müssen.

### **Network Developer:**

Ähnliches Tätigkeitsfeld wie der Network Administrator, jedoch mit ausschließlicher Ausrichtung auf Netzplanung.

### **Aufstiegsqualifizierung**

Das Tätigkeitsfeld des Network Administrator ist eine ideale Grundlage für Aufstiegsqualifizierungen, insbesondere zum IT Engineer, mit dem Schwerpunkt technisch optimale und marktgerechte Lösungen für komplexe Projekte zu erstellen und zum IT Manager, mit dem Schwerpunkt Koordinieren, Steuern und Unterstützen von Projekten und Prozessen zur Absicherung der jeweiligen Projekt- und Prozessziele.

## 3 Referenzprozesse Network Administrator

---

Im folgenden Abschnitt werden die Referenzprozesse des Network Administrator beschrieben. Dazu wurden die vier nun folgenden Netzmanagementbereiche identifiziert:

- Changemanagement
- Faultmanagement
- Performancemanagement
- Securitymanagement und
- Organisation und Beratung.

Im Folgenden werden diese Prozesse immer weiter differenziert: Während die Referenzprozesse die jeweiligen Netzwerkmanagementprozesse auf hohem Abstraktionsniveau wiedergeben und so einen Überblick ermöglichen, wird mit den dazugehörigen Teilprozessen in die Referenzprozesse hineinge'zoomt'. Die Teilprozesse entsprechen damit der Abbildung von Arbeitsprozessen, sie stellen einen konkreten Tätigkeitsverlauf, einschließlich auslösendem Ereignis und Ergebnis dar. Die zur Durchführung der Teilprozesse notwendigen Tätigkeiten, Qualifikationen werden jeweils in einem separaten Abschnitt aufgelistet. Als Beispiel zur Konkretisierung und Veranschaulichung dienen Abschnitte aus dem Praxisprojekt. Das Praxisprojekt ist ein echtes, bereits durchgeführtes Projekt, welches die Grundlage für die Referenz- und Teilprozesse darstellt.

In Abschnitt 3.5 werden die für den Network Administrator relevanten Werkzeuge aufgelistet.

### 3.1 Changemanagement

---

In diesem Abschnitt wird das Changemanagement in Form

- eines Referenzprozesses
- einer detaillierteren Darstellung der einzelnen Teilprozesse
- einer beispielhaften Ausgestaltung des Prozesses Changemanagement

dargestellt.

Dabei wird jeweils der gesamte Prozess dargestellt, um mögliche Aufgaben neben den Kernaufgabenfeldern aufzuzeigen.

### 3.1.1 Referenzprozess Changemanagement

Das folgende Ablaufdiagramm zeigt allgemein den Prozess des Changemanagements. Eine konkrete Ausgestaltung dieses Prozesses sollte in der Weiterbildung daran orientiert werden.

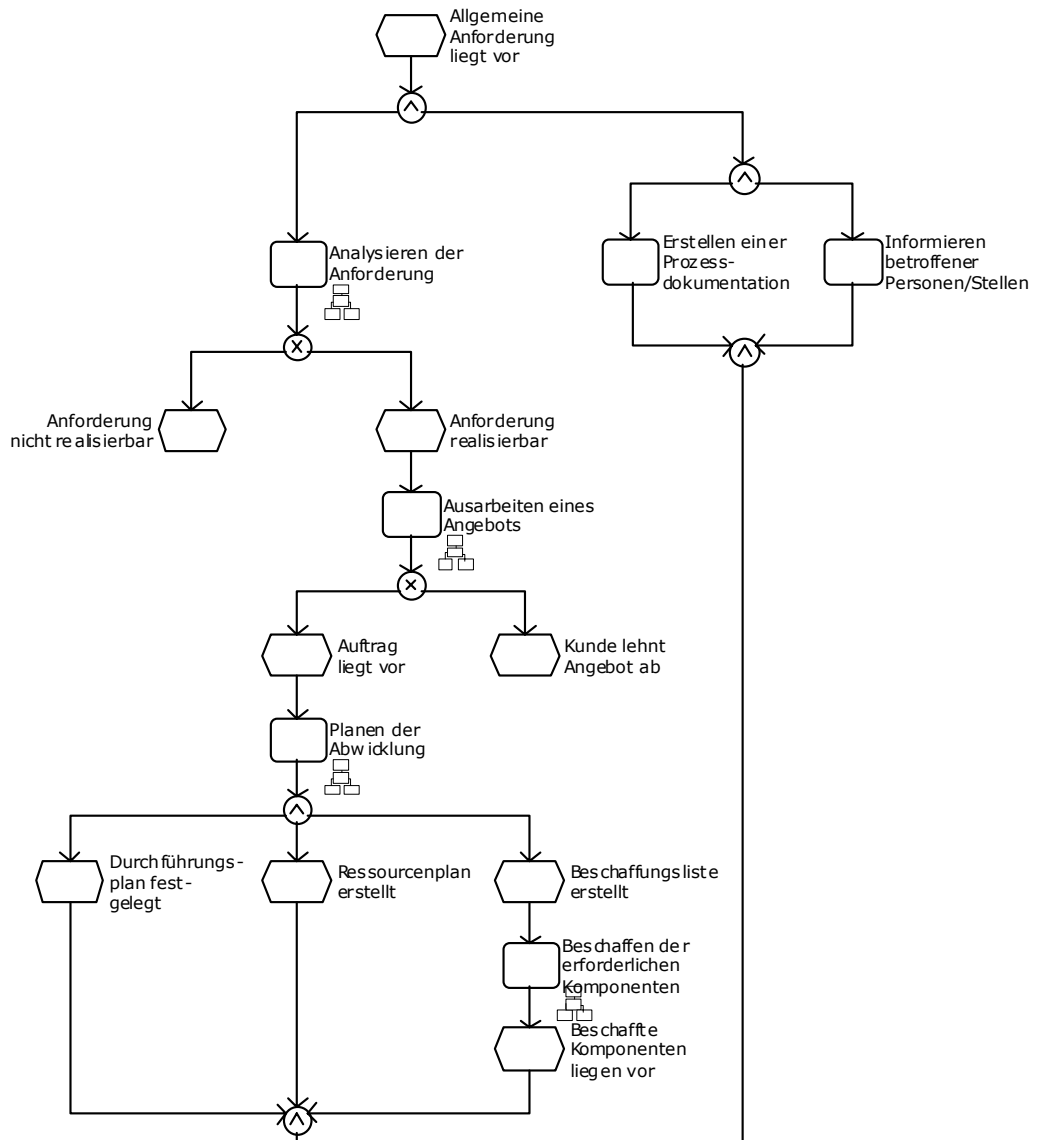


Abbildung: Referenzprozess 1: Changemanagement, Teil 1

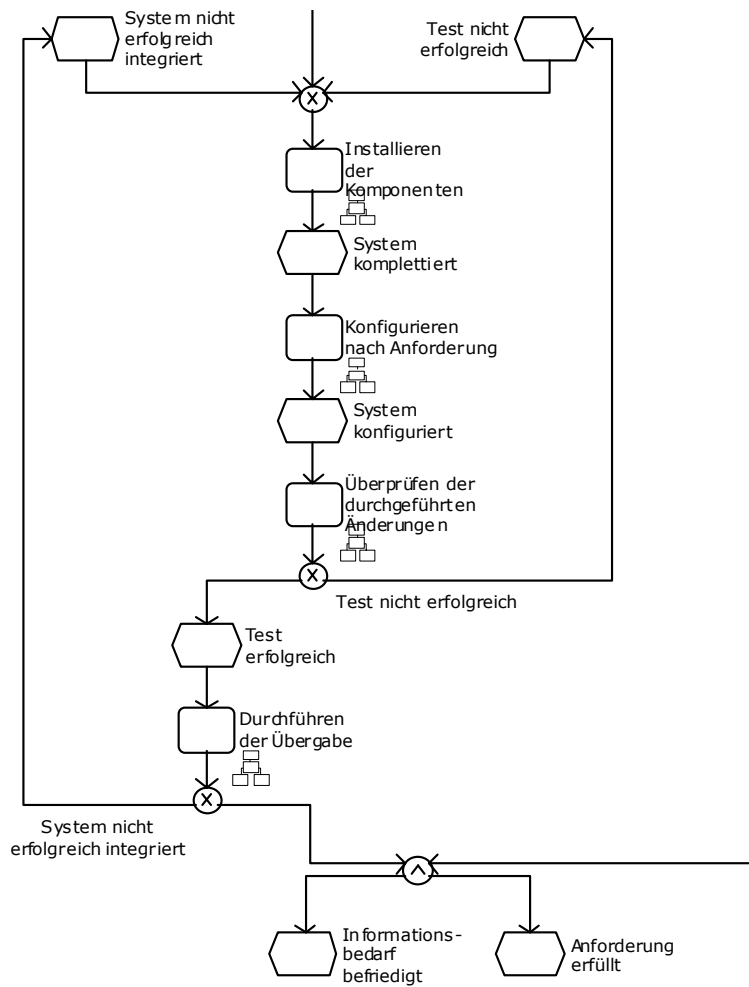


Abbildung: Referenzprozess 1: Changemanagement, Teil 2



### **3.1.2 Prozesskompass Changemanagement**

1. Analysieren der Anforderung
2. Erstellen einer Prozessdokumentation
3. Informieren betroffener Personen/Stellen
4. Ausarbeiten eines Angebots
5. Planen der Abwicklung
6. Beschaffen der erforderlichen Komponenten
7. Installieren der Komponenten
8. Konfigurieren nach Anforderung
9. Überprüfen der durchgeführten Änderungen
10. Durchführen der Übergabe

### 3.1.3 Teilprozesse Changemanagement

Im nun folgenden Abschnitt werden die Teilprozesse des Changemanagements dargestellt.

#### 3.1.3.1 Analysieren der Anforderung

Jeder Changemanagementprozess beginnt mit einer Analyse der Anforderung. Hier ist zu prüfen, welche Anforderungen aus technischer Sicht hinsichtlich des Änderungsbedarfs bestehen. Danach ist zu prüfen, welche technischen Voraussetzungen vorhanden sein müssen, um den Änderungsbedarf zu befriedigen, bzw. ob man die Voraussetzungen schaffen kann. Das Ergebnis ist eine technische Bewertung der Anforderung.

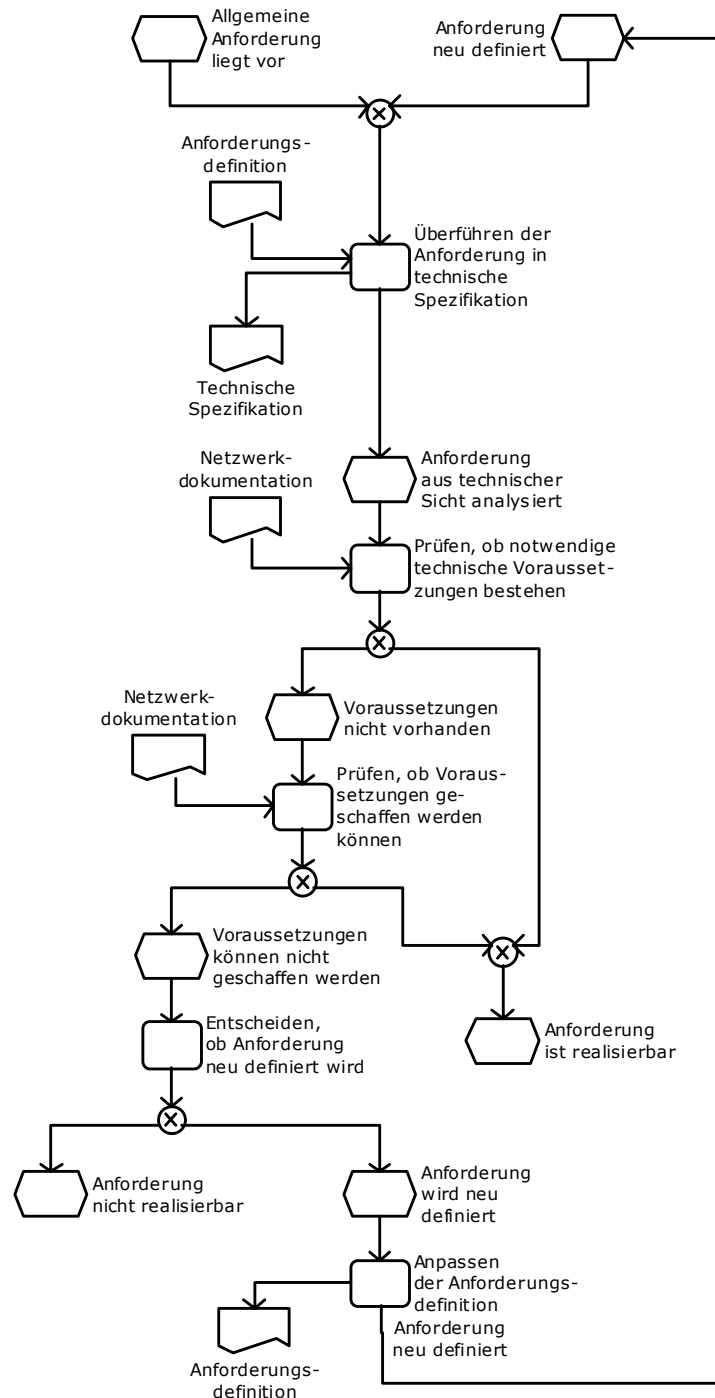


Abbildung 1: Analysieren der Anforderung

#### **3.1.3.1.1 Tätigkeiten: Analysieren der Anforderung**

- Überführen der Anforderungen in technische Spezifikation
- Prüfen, ob notwendige technische Voraussetzungen bestehen
- Prüfen, ob Voraussetzungen geschaffen werden können

Falls Voraussetzungen nicht geschaffen werden können

- Entscheiden, ob Anforderung neu definiert wird

Falls Anforderung neu definiert wird

- Anpassen der Anforderungsdefinition

#### **3.1.3.1.2 Kompetenzfelder: Analysieren der Anforderung**

Fähigkeiten/Fertigkeiten

- Spezielle Anforderung verstehen können
- Anforderungen in technische Spezifikation überführen können
- Technische Voraussetzungen prüfen können
- Nachträgliche Schaffung der Voraussetzungen prüfen können
- Entscheiden können
- Anforderungsdefinition anpassen können
- Dokumentieren können

Wissen

- Netzwerkdimensionen
- Netzwerkorganisation
- Kommunikationsarchitektur
- Betriebsarten
- Sitzungscharakterisierung
- Aktive Komponenten
- Passive Komponenten
- Topologien
- Strukturierte Verkabelung
- Standards
- Schnittstellen
- Übertragungssysteme, -techniken
- Übertragungsmedien
- Protokolle
- Referenzmodelle
- Prozess- und Organisationskenntnisse
- Spezielle Anforderung
- Dokumentationsstandards

### 3.1.3.2 Ausarbeiten eines Angebots

Nach dem die Durchführbarkeit geprüft worden ist, kann (dem Kunden) ein konkretes Angebot unterbreitet werden, das in einen Auftrag seitens des Kunden führen sollte.

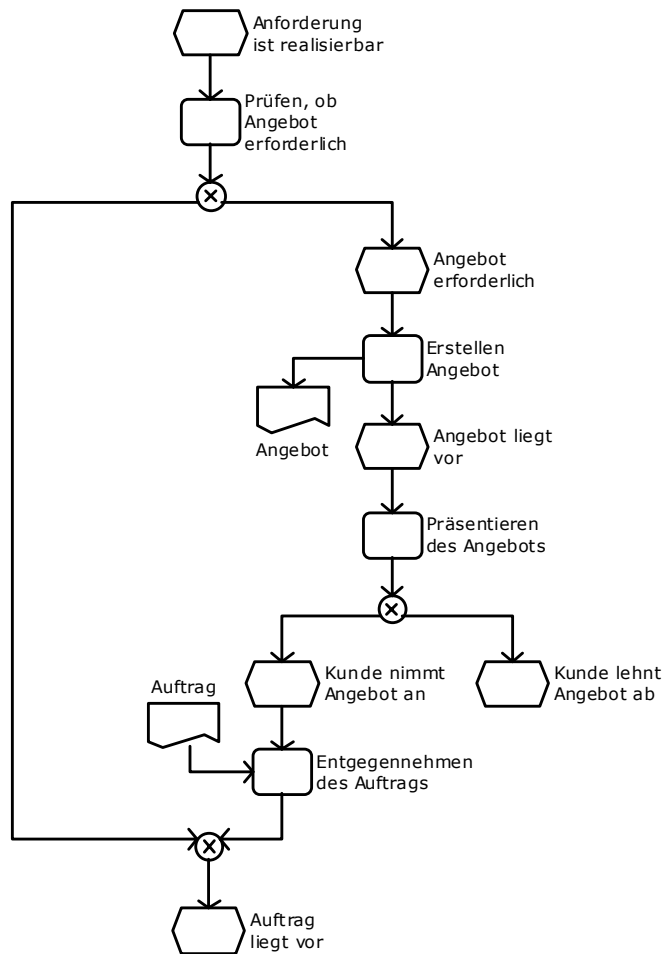


Abbildung 2: Ausarbeiten eines Angebots

#### 3.1.3.2.1 Tätigkeiten: Ausarbeiten eines Angebots

- Prüfen, ob ein Angebot erforderlich ist

Falls ein Angebot erforderlich ist

- Erstellen eines Angebots
- Präsentieren des Angebots

Falls der Kunde das Angebot annimmt

- Entgegennehmen des Auftrags

#### 3.1.3.2.2 Kompetenzfelder: Ausarbeiten eines Angebots

Fähigkeiten/Fertigkeiten

- Erforderlichkeit eines Angebots beurteilen können
- Entscheiden können
- Angebot erstellen können
- Angebot präsentieren können
- Dokumentieren können

Wissen

- Kaufmännische Grundkenntnisse
- Prozess- und Organisationskenntnisse
- Dokumentationsstandards

### 3.1.3.3 Planen der Abwicklung

Hat der Kunde das Angebot akzeptiert, liegt der endgültige Auftrag vor. Hier sind die Parameter spezifiziert, die in die Planung einfließen. Das Ergebnis dieses Prozesses ist eine Durchführungs- und Ressourcenplanung sowie eine Beschaffungsliste, über die zu beschaffenden Komponenten.

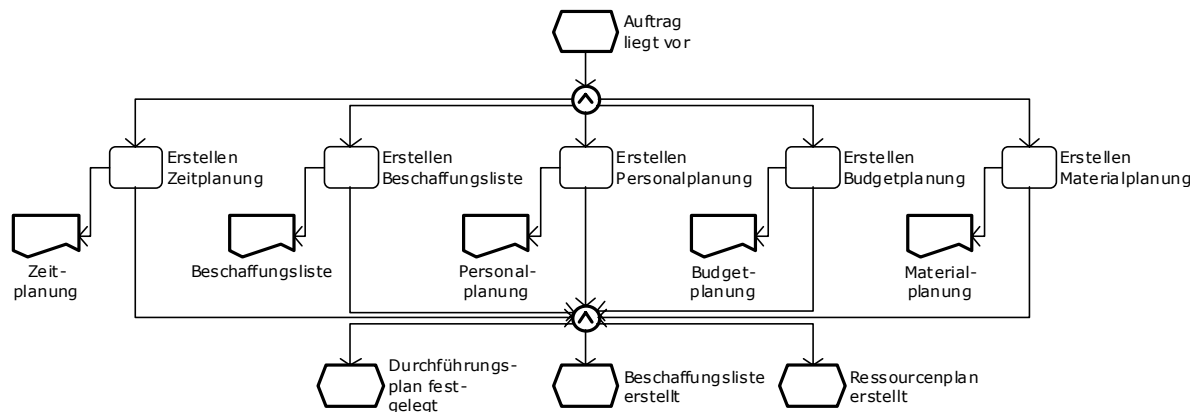


Abbildung 3: Planen der Abwicklung

#### 3.1.3.3.1 Tätigkeiten: Planen der Abwicklung

- Erstellen einer Zeitplanung
- Erstellen einer Beschaffungsliste
- Erstellen einer Personalplanung
- Erstellen einer Budgetplanung
- Erstellen einer Materialplanung

#### 3.1.3.3.2 Kompetenzfelder: Planen der Abwicklung

Fähigkeiten/Fertigkeiten

- Planen können
- Zeitplanung erstellen können
- Beschaffungsliste erstellen können
- Sich selbst (evtl. Mitarbeiter) beurteilen/einschätzen können
- Personalplanung erstellen können
- Budgetplanung erstellen können
- Materialplanung erstellen können
- Dokumentieren können

Wissen

- Spezielle Anforderung
- Prozess- und Organisationskenntnisse
- Technisches Englisch
- Dokumentationsstandards

### 3.1.3.4 Beschaffen der erforderlichen Komponenten

Anhand der vorher erstellten Spezifikation erfolgt nun ein Beschaffungsvorgang. Hier müssen Angebote über die zu beschaffenden Komponenten und Geräte eingeholt und verglichen werden. Ist ein attraktives Angebot identifiziert, wird eine Bestellung ausgelöst. Ist die Lieferung erfolgt, wird sie mit der Bestellung verglichen und auf Lieferschäden kontrolliert. Sofern diese Kontrolle ohne Probleme verlaufen ist, wird die gesamte Lieferung an die Komponentenmontage übergeben.

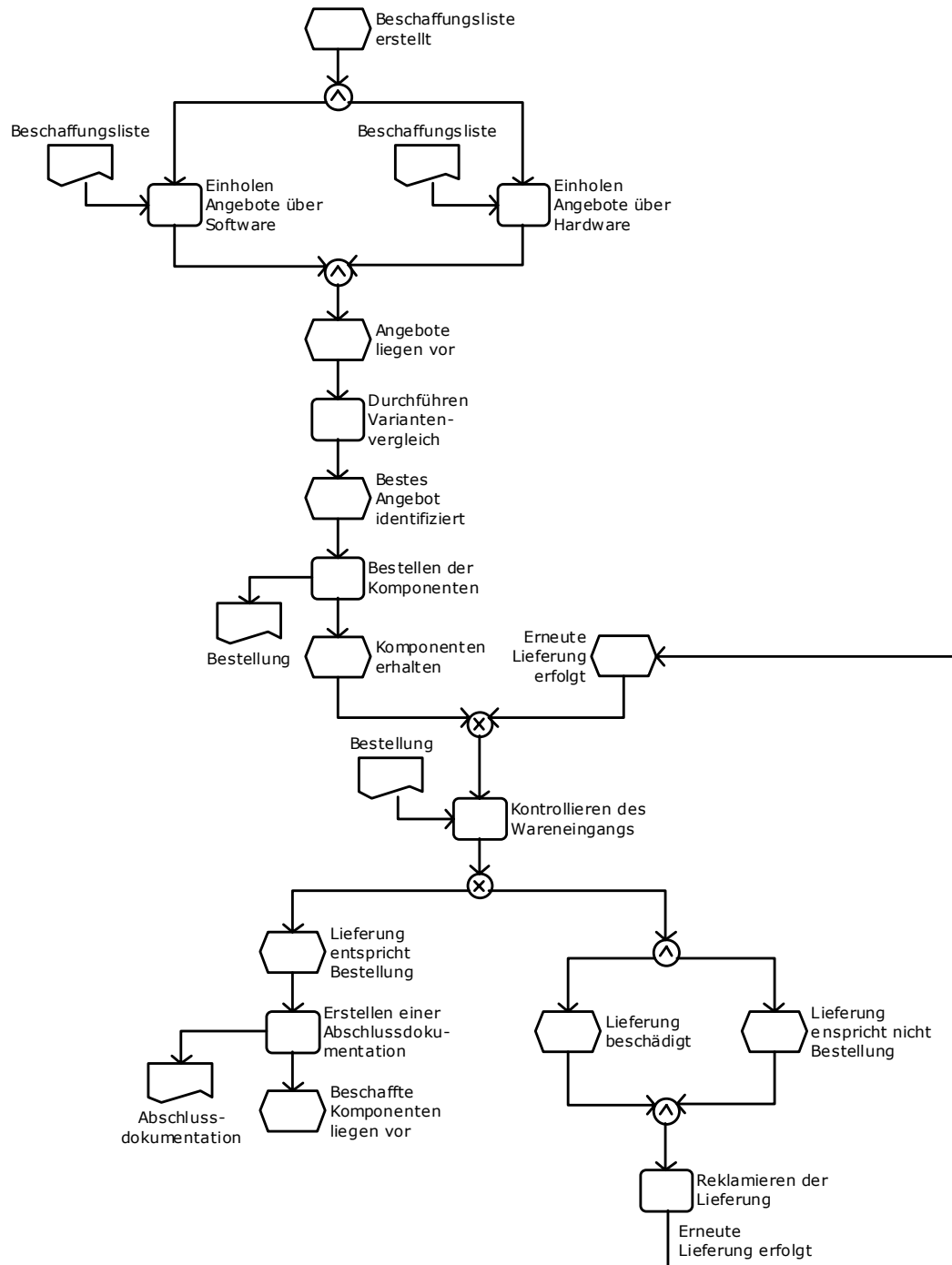


Abbildung 4: Beschaffen der erforderlichen Komponenten

#### 3.1.3.4.1 Tätigkeiten: Beschaffen der erforderlichen Komponenten

- Einholen von Angeboten über Software
- Einholen von Angeboten über Hardware

- Durchführen eines Variantenvergleichs
- Bestellen der Komponenten
- Kontrollieren des Wareneingangs

Falls Lieferung defekt ist oder nicht der Bestellung entspricht

- Reklamieren der Lieferung

In jedem Fall

- Erstellen einer Abschlussdokumentation

#### **3.1.3.4.2 Kompetenzfelder: Beschaffen der erforderlichen Komponenten**

Fähigkeiten/Fertigkeiten

- Angebote einholen können
- Angebote analysieren und bewerten/beurteilen können
- Entscheiden
- Komponenten bestellen können
- Wareneingang kontrollieren können
- Dokumentieren können

Wissen

- Aktive Komponenten
- Passive Komponenten
- Hardware
- Übertragungsmedien
- Kaufmännische Grundkenntnisse
- Dokumentationsstandards
- Technisches Englisch

#### **3.1.3.5 Installieren der Komponenten**

Zur Installation der Komponenten werden Beschreibungen und Handbücher der Hersteller herangezogen. Nachdem die Hardwarekomponenten zu einem Gesamtsystem komplettiert worden sind, erfolgt die Softwareinstallation. Parallel dazu werden die erforderlichen Leitungen und Schnittstellen installiert. Als Ergebnis erhält man das fertiggestellte Gesamtsystem.

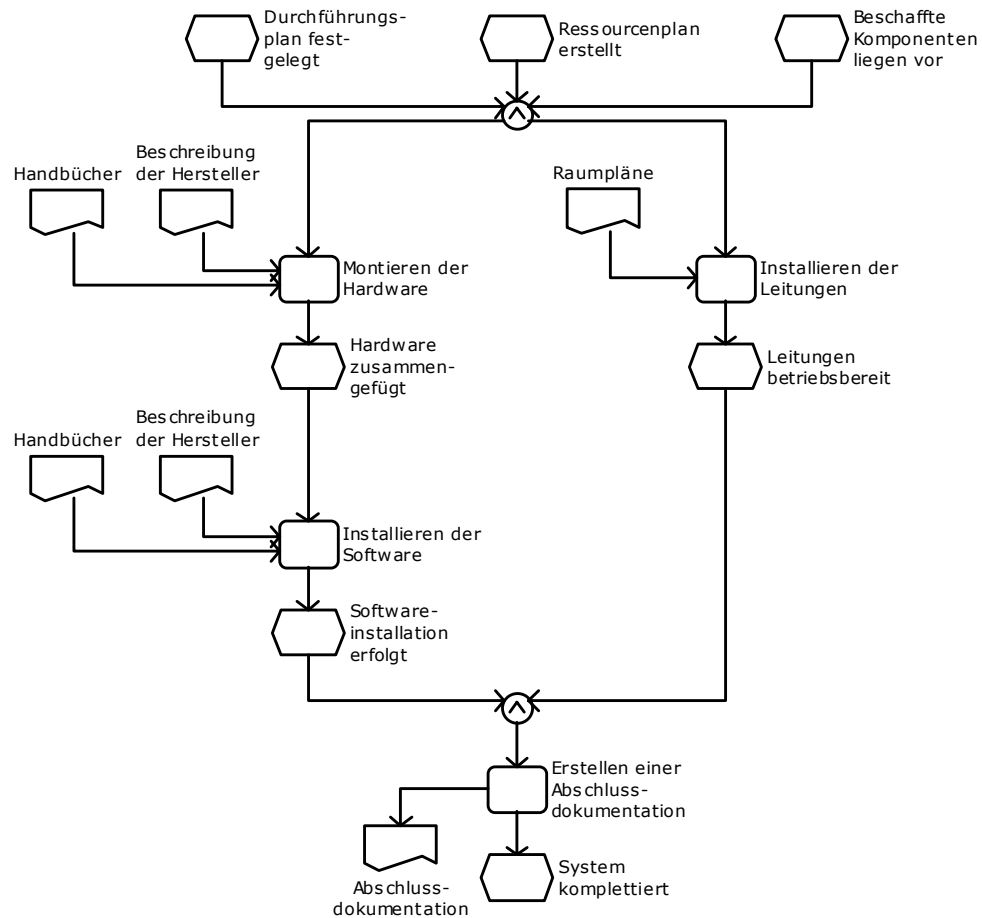


Abbildung 5: Installieren der Komponenten

#### 3.1.3.5.1 Tätigkeiten: Installieren der Komponenten

- Montieren der Hardware
- Installieren der Software
- Installieren der Leitungen
- Erstellen einer Abschlussdokumentation

#### 3.1.3.5.2 Kompetenzfelder: Installieren der Komponenten

Fähigkeiten/Fertigkeiten

- Hardware montieren können
- Software installieren können
- Leitungen installieren können
- Dokumentieren können

Wissen

- Hardware
- Systemsoftware/Betriebssysteme
- Übertragungsmedien
- Standards
- Schnittstellen
- Erfahrungswissen



- Elektrotechnik
- EGB (elektrostatische gefährdete Bauelemente/-gruppen)
- Dokumentationsstandards
- Technisches Englisch

### 3.1.3.6 Konfigurieren nach Anforderung

Das komplettierte System muss nun konfiguriert werden. Dazu werden die Systemvorgaben auf die Verkabelung, die Netzwerkkomponenten und die Firewall angewendet. Im Anschluss daran werden, wiederum ausgehend von den Systemvorgaben (der Hersteller), die Netzwerkeinstellungen, die Systemeinstellungen und die Benutzereinstellungen konfiguriert. Die passiven Netzwerkkomponenten (Leitungen) werden in der Regel nicht konfiguriert. Als Ergebnis erhält man das konfigurierte System.

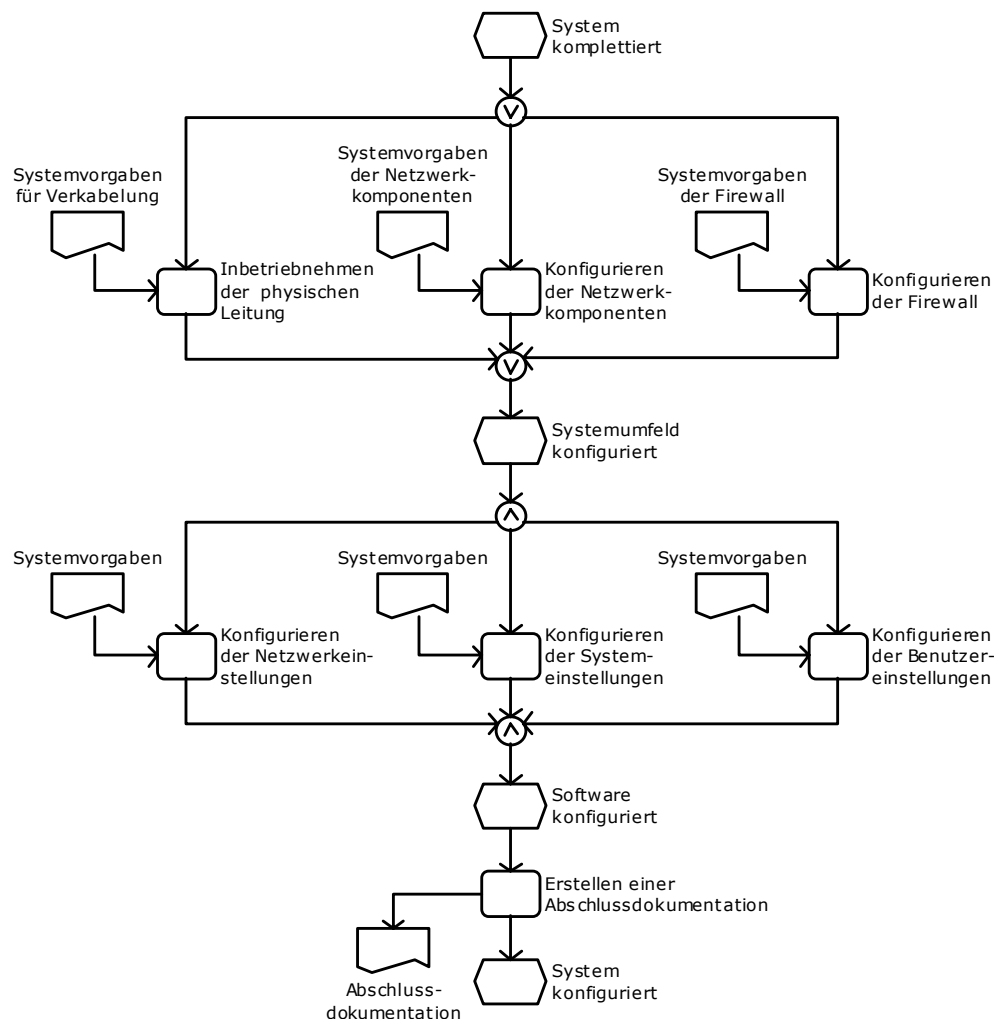


Abbildung 6: Konfigurieren nach Anforderung

#### 3.1.3.6.1 Tätigkeiten: Konfigurieren nach Anforderung

- In Betrieb nehmen der physischen Leitungen
- Konfigurieren der Netzwerkkomponenten
- Konfigurieren der Firewall
- Konfigurieren der Netzwerkeinstellungen

- Konfigurieren der Systemeinstellungen
- Konfigurieren der Benutzereinstellungen
- Erstellen einer Abschlussdokumentation

#### **3.1.3.6.2 Kompetenzfelder: Konfigurieren nach Anforderung**

Fähigkeiten/Fertigkeiten

- Leitungen in Betrieb nehmen können
- Netzwerkkomponenten konfigurieren können
- Firewall konfigurieren können
- Netzwerkeinstellungen konfigurieren können
- Systemeinstellungen konfigurieren können
- Benutzereinstellungen konfigurieren können
- Dokumentieren können

Wissen

- Netzwerkdimensionen
- Netzwerkorganisation
- Kommunikationsarchitektur
- Betriebsarten
- Sitzungscharakterisierung
- Topologien
- Hardware
- Systemsoftware
- Aktive Komponenten
- Passive Komponenten
- Erfahrungswissen
- Dokumentationsstandards
- Technisches Englisch

#### **3.1.3.7 Überprüfen der durchgeführten Änderungen**

Ist das Gesamtsystem installiert und konfiguriert, wird es zu Testzwecken erstmals in Betrieb genommen. Dazu werden zunächst die Verkabelung, die Netzwerkkomponenten sowie die Firewall auf einwandfreie Funktion überprüft. Ist dieser Schritt mit positivem Ergebnis abgeschlossen worden, werden die Netzwerk-, die System- und die Benutzereinstellungen getestet. Sollte es hier zu Fehlermeldungen oder Fehl Abläufen kommen, wird eine Überprüfung der und ggf. Anpassung an die Systemvorgaben des Herstellers vorgenommen. Führt das zum gewünschten Testergebnis bzw. war dieses in Ordnung, ist das System betriebsbereit.

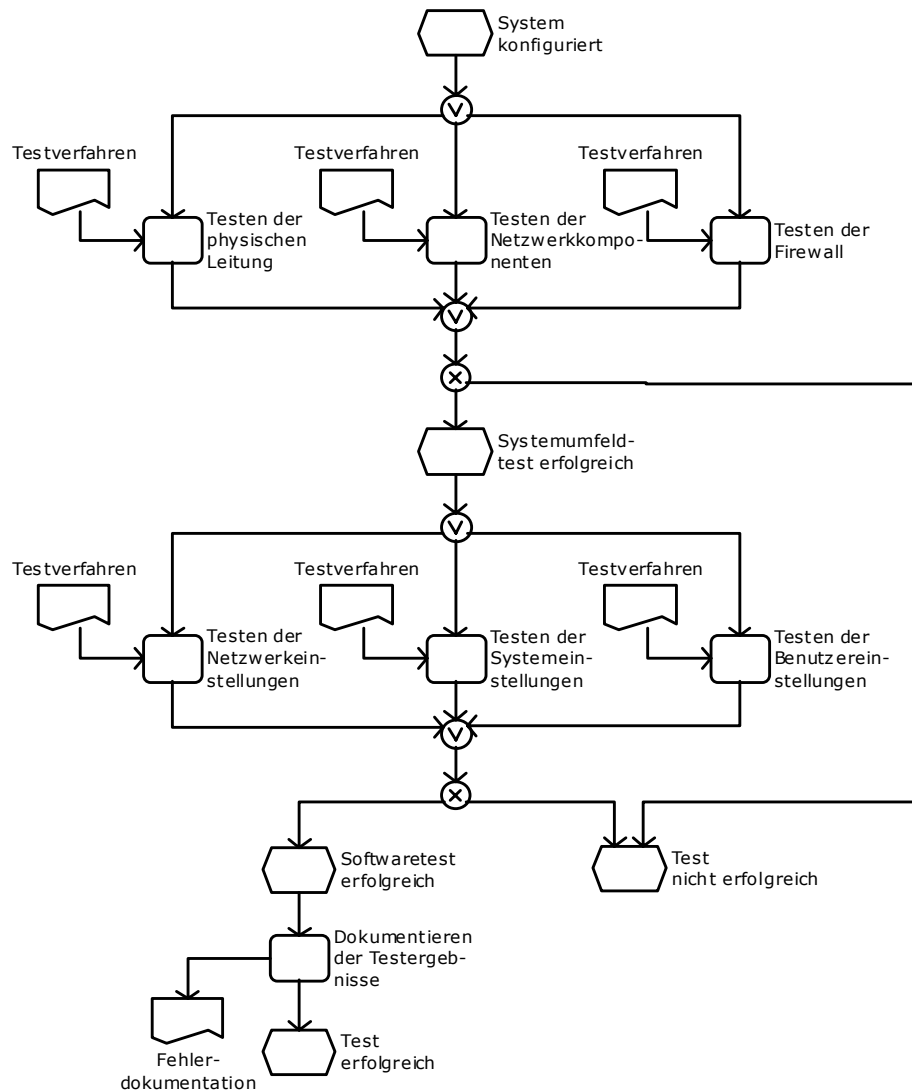


Abbildung 7: Überprüfen der durchgeführten Änderungen

### 3.1.3.7.1 Tätigkeiten: Überprüfen der durchgeführten Änderungen

- Testen der physischen Leitungen
- Testen der Netzwerkkomponenten
- Testen der Firewall

Wenn Test erfolgreich

- Testen der Netzwerkeinstellungen
- Testen der Systemeinstellungen
- Testen der Benutzereinstellungen

Wenn Test erfolgreich

- Dokumentieren der Testergebnisse

### 3.1.3.7.2 Kompetenzfelder: Überprüfen der durchgeführten Änderungen

Fähigkeiten/Fertigkeiten

- physische Leitungen testen können
- Netzwerkkomponenten testen können

- Firewall testen können
- Netzwerkeinstellungen testen können
- Systemeinstellungen testen können
- Benutzereinstellungen testen können
- Dokumentieren können

#### Wissen

- Netzwerkdimension
- Netzwerkorganisation
- Kommunikationsarchitektur
- Betriebsarten
- Sitzungscharakterisierung
- Hardware
- Aktive Komponenten
- Passive Komponenten
- Topologien
- Strukturierte Verkabelung
- Protokolle
- Referenzmodelle
- Standards
- Schnittstellen
- Übertragungssysteme, -techniken
- Übertragungsmedien
- Elektrotechnik
- Systemsoftware/Betriebssysteme
- Dokumentationsstandards
- Technisches Englisch

#### **3.1.3.8 Durchführen der Übergabe**

Sind die Tests vollständig abgeschlossen und alle (System-)Komponenten in Ordnung, erfolgt die Integration in das Wirknetz des Kunden (sofern diese nicht bereits erfolgt ist). Auch hier erfolgt noch einmal eine Überprüfung aller Funktionen des Systems. Sollten sich hier Fehler zeigen, wird nach dem Prozess „Test“ weiter verfahren. Ähnliches gilt auch für die installierten Leitungen. Außerdem erfolgt die formale Übergabe an den Kunden. Als Ergebnis wird die Anforderung erfüllt.

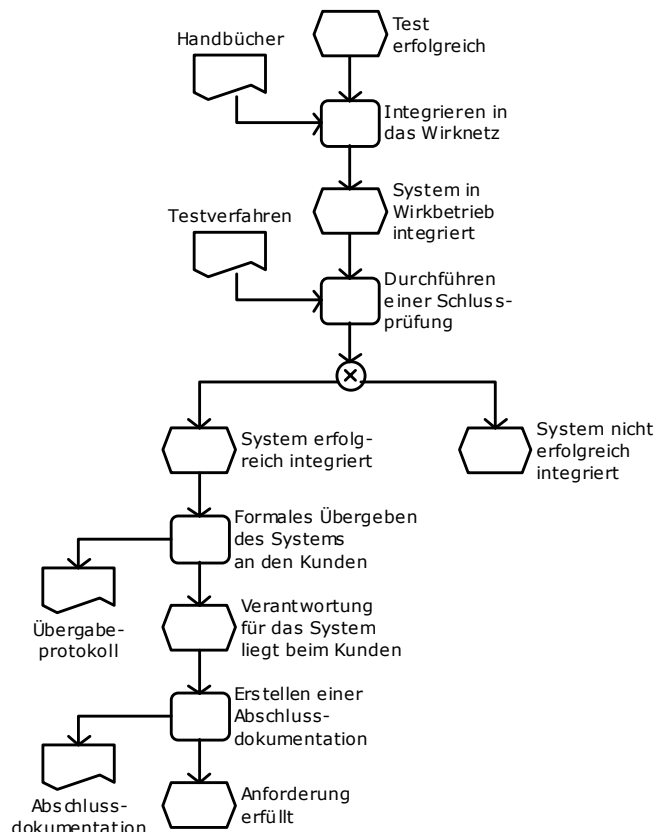


Abbildung 8: Durchführen der Übergabe

#### 3.1.3.8.1 Tätigkeiten: Durchführen der Übergabe

- Integration in das Wirknetz
- Durchführen einer Schlussprüfung
- Formales Übergeben des Systems an den Kunden
- Erstellen einer Abschlussdokumentation

#### 3.1.3.8.2 Kompetenzfelder: Durchführen der Übergabe

Fähigkeiten/Fertigkeiten

- System in das Wirknetz integrieren können
- Schlussprüfung durchführen können
- System an Kunden (formal) übergeben können
- Dokumentieren können

Wissen

- Grundbegriffe
- Dokumentationsstandards
- Technisches Englisch

#### 3.1.3.9 Informieren betroffener Personen/Stellen

In diesem Abschnitt werden die Kommunikationsmaßnahmen als kontinuierliche, den gesamten Prozess begleitende Teilprozesse beschrieben.

Solche Ad-hoc-Kommunikationsmaßnahmen werden durchgeführt, wenn bestimmte Personen oder Stellen über den aktuellen Stand der Bearbeitung informiert werden müssen. Dazu zählen aber auch die Einweisung der Nutzer nach erfolgreich durchgeführtem Änderungsprozess sowie ausführlichere Nutzerschulungen zu neu installierten Systemen.

#### ***Ad-hoc-Kommunikationsmaßnahme: Einweisung***

Falls nötig, findet eine Einweisung in das System durch den Network Administrator statt. Hier werden dem Kunden alle Funktionen der Anwendung und des Systems sowie Verhaltensrichtlinien für den Störfall erklärt.

Da diese Arbeit parallel und eng verknüpft mit dem Gesamtprozess verläuft und oben verbal beschrieben wurde, was der Inhalt dieses Prozesses ist, bedarf es hier keiner Prozessabbildung.

##### **3.1.3.9.1 Tätigkeiten: Informieren betroffener Personen/Stellen**

- Erklären grundlegender Dinge im Umgang mit dem System
- Erstellen einer Abschlussdokumentation

##### **3.1.3.9.2 Kompetenzfelder: Informieren betroffener Personen/Stellen**

Fähigkeiten/Fertigkeiten

- Erklären können
- Dokumentieren können

Wissen

- Je nach Informationsbedarf

#### ***Ad-hoc-Kommunikationsmaßnahme: Schulung***

Sollten die Erklärungen bei der Einweisung den Informationsbedarf des Kunden nicht decken, kann dieser seinen Bedarf anmelden. Darauf hin wird ein auf den Bedarf des Kunden zugeschnittener Schulungsplan ausgearbeitet und die Schulung durchgeführt.

##### **3.1.3.9.3 Tätigkeiten: Ad-hoc-Kommunikationsmaßnahme: Schulung**

- Erstellen eines Schulungsplans
- Durchführen der Schulung

##### **3.1.3.9.4 Kompetenzfelder: Ad-hoc-Kommunikationsmaßnahme: Schulung**

Fähigkeiten/Fertigkeiten

- Schulungsplan erstellen können
- Schulung durchführen können

Wissen

- Je nach Anforderung

##### **3.1.3.10 Erstellen einer Prozessdokumentation**

Der Teilprozess „Erstellen einer Prozessdokumentation“ setzt sich aus einer kontinuierlichen Prozessdokumentation und Dokumentationen zu einzelnen Teilprozessen zusammen. Es ist sowohl das Vorgehen, als auch die technischen Einstellwerte zu dokumentieren. Hier fällt auch die Tätigkeit „Erstellen einer Abschlussdokumentation“ hinein.

Ziel dieses Prozesses ist es, dass der Teilnehmer der arbeitsprozessorientierten Weiterbildung zum Network Administrator belegt, dass er Dokumentationen anwendergerecht anfertigen, zusammenstellen und modifizieren kann. Somit ist dieser Teilprozess auch Bestandteil der angestrebten Zertifizierung.

Darüber hinaus verfolgt die kontinuierliche Dokumentation auch den Zweck, dass einmal erarbeitete Prozessschritte mit der Dokumentation für Dritte nachvollziehbar werden und nicht erneut erarbeitet werden müssen, was die Effizienz im betrieblichen Alltag steigert.

Da diese Arbeit parallel und eng verknüpft mit dem Gesamtprozess verläuft und oben verbal beschrieben wurde, was der Inhalt dieses Prozesses ist, bedarf es hier keiner Prozessabbildung.

#### **3.1.3.10.1 Tätigkeiten: Erstellen einer Prozessdokumentation**

- Dokumentieren des gesamten Prozesses (parallel zur Abarbeitung)

#### **3.1.3.10.2 Kompetenzfelder: Erstellen einer Prozessdokumentation**

Fähigkeiten/Fertigkeiten

- Dokumentieren können
- „Schreiben können“

Wissen

- Dokumentationsstandards
- Technisches Englisch

### 3.1.4 Beispiel Changemanagement

Im nun folgenden Abschnitt werden die Teilprozesse des Changemanagements als konkrete Ausgestaltung aus der Praxis dargestellt, wie sie bei der Deutschen Telekom durchgeführt worden sind. Das konkrete Objekt des hier beschriebenen Changemanagementprozesses ist eine „Sichtstation“.

Die Deutsche Telekom AG betreibt u.a. weltweite Kommunikationsnetze. Diese Netze werden von unterschiedlichen Abteilungen und Gruppen an verschiedenen Standorten betreut. Das Ressort SSZ (Sonderaufgaben Servicezentrum) der TNL (Technik Niederlassung) Bochum betreut ein weltweites Telekom-Netz. Um dieses Netz effektiv zu betreuen, werden entsprechende Verfahren eingesetzt. Operatoren administrieren und verwalten das Netz mit Hilfe von Sichtstationen. Diese Sichtstationen sind (PC-)Clients mit einem Unix-Derivat als Betriebssystem. Über einen lokalen X-Server greift die Sichtstation auf einen Customer- oder Auxility-Server zu. Mit der Server Anwendung 46020, die als X-View auf den Sichtstationen erscheint, werden VPN Netze des Kunden auf Betriebssicherheit hin überwacht. In diesen Views wird das Teil- oder Gesamtnetz im aktuellen Betriebszustand dargestellt. Von diesen Sichtstationen werden nicht nur administrative Aufgaben ausgeführt, sondern auch das Monitoring und die Ressourcenverwaltung und -optimierung. Einem Kunden dient die Sichtstation dazu, sein bei der Deutschen Telekom AG gemietetes Netz einzusehen und für seine Zwecke auszuwerten.

Wer ist Kunde? - Das Ressort SSZ unterscheidet interne und externe Kunden. Der Mitarbeiter als Kunde im eigenen Haus bekommt seine Sichtstation nach den aktuellen Bedarfsanforderungen. Der interne Kunde stellt sich gegenüber dem Ressort SSZ als Mitarbeiter aus den Tochtergesellschaften oder der Mutter der Deutschen Telekom AG dar. Externe Kunden haben einen Ansprechpartner (one face to the customer). Diese Kundenschnittstellen sind der Vertrieb Großkunden und die Tochtergesellschaft DeTeSystems.

#### 3.1.4.1 Auftrag (Analyse der Anforderung, Ausarbeiten eines Angebots)

Gibt der Kunde eine Sichtstation in Auftrag, wird dieser Auftrag vom Vertrieb entgegengenommen. Der Vertrieb erstellt einen Telekom Designed Network Vertrag (TDN-Vertrag). In diesem Vertrag wird das Angebot eines PCs oder einer SUN Workstation mit einbezogen, das heißt, alle Hardware Komponenten des PCs oder der Sun Workstation und die Netzwerkkomponenten werden hier aufgeführt. Die Installations- und Konfigurationsarbeiten werden vertraglich aufgelistet. Der Vertrieb leitet diesen Vertrag an den Zentralbereich Netzinfrastruktur Darmstadt weiter. Der Zentralbereich Netzinfrastruktur Darmstadt prüft, ob die neue Sichtstation beim Kunden aufgebaut werden kann. Wenn der Auftrag genehmigt worden ist, werden an die einzelnen Gruppen und Ressorts die auszuführenden Aufgaben verteilt. Der Zentralbereich Netzinfrastruktur beauftragt das Ressort BBN (Bezirksbüro Netze), die Leitung termingerecht zu installieren. Das Ressort SSZ wird beauftragt, die Sichtstation und die weiteren Komponenten zu installieren und zu konfigurieren. Zu beachten ist hier, dass die Software 46020 nur eine begrenzte Anzahl an Sichtstationen aufnehmen kann.

#### 3.1.4.2 Genehmigung (Durchführbarkeitsprüfung)

Sind die im Vorfeld beschriebenen Details im Auftrag geklärt, wird die Genehmigung eingeleitet. Hier muss jeder Auftrag in jedem Fall formal auf Durchführbarkeit geprüft werden. Ist diese Entscheidung positiv ausgefallen, wird ein interner Auftrag an die jeweiligen Ressorts (einmal für den Teil der Verkabelung (BBN) und einmal für den Teil der Installation und Konfiguration der Hard- und Software (SSZ)) weitergeleitet.

#### 3.1.4.3 Planung (Durchführbarkeitsprüfung, Planen der Abwicklung, Zuweisen der Ressourcen)

Ist die Sichtstation für den Kunden genehmigt worden, wird die Planung vorgenommen. Alle Personen und Gruppen müssen in diese Planung mit einbezogen werden. Ebenfalls muss ein Zeitplan aufgestellt werden. Um die Planung sehr genau auszuführen, werden mit dem



Kunden die Örtlichkeiten besprochen. Bei Bedarf wird auch eine Ortsbegehung vorgenommen. In der Planung für die Örtlichkeiten sind folgende Punkte zu beachten:

- Raumklima
- Brandschutz
- Stromversorgung
- Schließsysteme / Zugangsberechtigung
- Komponentenentfernungen

Diese Angaben werden benötigt, um bei der Beschaffung z.B. die richtigen Kabellängen zu bestellen. Die personelle Ressourcenplan wird im Team erstellt.

#### **3.1.4.4 Beschaffung (Beschaffen der Komponenten)**

Die Beschaffung der Hardware - Komponenten für die Sichtstation setzt sich aus drei Bereichen zusammen:

- die Beschaffung der Hardware für einen PC
- die Beschaffung der Software für einen PC und
- die Beschaffung der sonstigen Hardware.

Der Kunde kann für seine künftige Sichtstation auch ein Angebot vom Ressort SSZ erarbeiten lassen. Dieses Angebot holt das Ressort SSZ bei örtlichen Computer-Fachhändlern ein. Hier wird, wenn nötig, ein Angebotsvergleich durchgeführt. Hat der Kunde sich für das Angebot entschieden, bestellt auf Wunsch das SSZ oder er selbst die Hardware.

Die Beschaffung einer Sichtstation für das eigene Ressort SSZ wird von der Zentralen Systembetreuung durchgeführt. Die Beschaffung von Ersatzteilen und Erweiterungen wird im PC-Bereich über örtliche Händler abgewickelt. Ersatzteile und Erweiterungen für die SUN Workstations können nur über die Firma SUN bezogen werden. Der Kunde hat auch die Möglichkeit sich nach den Vorgaben des Ressort SSZ ein Hardwaresystem selber zu beschaffen. Der Kunde bestellt in seinem Auftrag für eine Sichtstation auch die entsprechende Software und die dazugehörigen Lizenzen für das System. Diese Software setzt sich aus der Lizenz für die 46020 Softwareanwendung und aus der Linux SuSE Distribution zusammen. Die Beschaffung der weiteren Software wird durch das Ressort SSZ vorgenommen. Alle Komponenten, die vom Kunden oder durch das Ressort SSZ bestellt worden sind, werden an den Standort des SSZ geliefert.

#### **3.1.4.5 Installation (Zusammenfügen der Komponenten)**

Nach Lieferung der Sichtstationskomponenten erfolgt die Installation. Diese Komponenten wie Festplatte, Grafikkarte, Netzwerkkarte, Prozessor, Speicher, CD-ROM, Floppy, Motherboard, Tastatur, Maus, Gehäuse und Monitor werden dann in den Räumlichkeiten des SSZ zusammengebaut. Hier sind die von den Herstellern mitgelieferten Beschreibungen und Handbücher zu beachten. Sind die Komponenten ordnungsgemäß zusammengebaut, wird das Betriebssystem installiert. Bei späteren Hardware-Erweiterungen können durch die Mitarbeiter des Ressort SSZ noch zusätzliche Komponenten eingebaut und ausgetauscht werden. Softwareupdates oder das Installieren von zusätzlichen Anwendungen werden vor Ort durch die Mitarbeiter ausgeführt. Da die Hauptanwendung, die 46020, auf dem Server am Standort installiert ist und der Kunde sich nur seine View (sein Display) über das Netzwerk holt, können zentrale Änderungen auf dem Server eingestellt werden. Für die Anbindung der Sichtstation an das Telekom Netz der Deutschen Telekom AG muss gegebenenfalls in dem Kundenknoten eine entsprechende Schnittstellenkarte eingebaut werden. Die benötigte Zugangsleitung, die den Kunden mit dem Telekom Netz verbindet, wird durch das Ressort BBN installiert.

#### **3.1.4.6 Konfiguration (Konfigurieren nach Anforderung)**

Bei der Installation des PC-Systems muss in bestimmten Fällen eine Konfiguration im BIOS vorgenommen werden. Das BIOS wird dann mit der entsprechenden Tastaturkombination aufgerufen und in den Menüeinstellungen werden die Daten geändert. Weitere Software-Konfigurationen im Betriebssystem werden nach den Kundenanforderungen eingestellt. Allgemeine Konfigurationen wie Benutzer, Netzwerkeinstellungen und die Grafikeinstellungen werden nach den Systemvorgaben der 46020 gemacht. Ist das System installiert und konfiguriert, muss es in die Sichtstation mit ihren Daten in den Server eingebunden werden. Hier ist die Authentifizierung des Benutzers sehr wichtig, da er sich auf der Sichtstation lokal mit einem Benutzer und Passwort anmeldet und sich damit auch gleichzeitig auf dem Server in der Anwendung anmeldet. Ist der User im Server als Profil eingerichtet, bekommt er hier seine Rechte eingestellt, die er dann in seinem Netz hat. Zur Konfiguration der 46020 Serveranwendung stehen die Betriebshandbücher im Ressort zu Verfügung. Sind die Konfigurationen am PC und Server abgeschlossen, wird die Firewall konfiguriert.

Durch das Ressort SSZ wird die vom Ressort BBN physisch installierte Leitung mit der 46020 Anwendung verbunden. Die Leitung ist jetzt bis auf die Schnittstellenkarte im Kundenknoten geschaltet. Der Router wird nach Kundenanforderung konfiguriert. Sind alle Geräte, Komponenten und Anwendungen konfiguriert, werden sie getestet und geprüft.

#### **3.1.4.7 Test und Fehlerbehebung (Prüfen der durchgeführten Änderungen)**

Im Gesamtprozess: "Einrichten einer Sichtstation" gibt es verschiedene Test- und Prüfverfahren. Die Tests und Prüfungen werden in den einzelnen Abschnitten entsprechend aufgeführt. Die erste Prüfung findet bei der Warenannahme also der Lieferung statt. Hier werden Bestellung und Auslieferung verglichen. Bei der Sichtkontrolle werden alle Komponenten auf Lieferschäden hin geprüft. Sollten Schäden festgestellt werden, geht die Ware an den Hersteller zurück, und es wird Ersatz angefordert. Der erste Test prüft die Funktionen der PC-Hardware. Im zweiten Test wird eine Überprüfung des Linux Betriebssystems durchgeführt. Nach diesen Tests wird das System an die Referenzanlage angeschlossen. In dieser Referenzanlage können alle Situationen, die im Wirknetz entstehen, simuliert werden. Die Konfigurationen des PCs werden mit einfacher Prüfroutine getestet. Bei Fehlern, die während der Konfiguration und Installation auftreten, werden diese mit Hilfe von Installationshandbüchern, den Erfahrungswerten von Teamkollegen oder besonderen Anweisungen der Hersteller gelöst und behoben. Beispielsweise können Netzwerkeinstellungen mit Hilfe eines einfachen Befehls „ping“ geprüft werden. Der vorkonfigurierte Router wird jetzt mit in das System eingebunden und getestet. Kann sich ein Benutzer am System über das Netzwerk und den Router anmelden, ist die Verbindung in Ordnung. Ist der User auf dem Linux System angemeldet, baut er eine Verbindung über den lokalen X-Server auf den Customer Server auf. Hier sieht der User jetzt das Teil- oder Gesamtnetz des Kunden. Jetzt wird das Zugriffsverfahren getestet, ob der User eingeschränkte Rechte besitzt und sein Netz sieht. Sind alle diese Tests und Prüfungen erfolgreich gewesen, wird die Sichtstation im Wirknetz eingebunden. Diese Einbindung findet am Standort des SSZ statt. In diesem Test wird die Firewall mit einbezogen, und es wird noch einmal ein Gesamttest durchgeführt. Nach der Bereitstellung des Systems beim Kunden wird es vor Ort geprüft. Sollten hier Störungen oder Fehler auftreten, werden diese behoben. In der Softwareanwendung werden gegebenenfalls nötige Änderungen vorgenommen. Die Zugangsleitung für den Kunden wird durch die Mitarbeiter des Ressort BBN geprüft. Sie messen und testen die Leitung 24 Stunden ein. Wenn der Kunde eine Störung an seiner Sichtstation wahrnimmt, kann er sich telefonisch, per Fax oder Email im Ressort SSZ melden. Hier schildert der Kunde seine Störung dem Mitarbeiter, der diese Störung dann analysiert. Nach der Analyse des Fehlers hat der Mitarbeiter die verantwortliche Aufgabe das Problem entweder selbst zu lösen oder es an die entsprechende Stelle weiterzuleiten, damit der Fehler schnellstmöglich und ordnungsgemäß behoben wird. Sollte der Fehler nicht von den Mitarbeitern und den entsprechenden Ressorts und Gruppen gelöst werden können, werden die Systemhersteller mit einbezogen. Bei Störungen von Komponenten wie zum Beispiel Cisco Routern, werden diese per Fernadministration entstört oder im Hardwaredefekt ausgetauscht. Bei Modulkomponenten werden nur die Module getauscht. Bei Störungen der Leitungen wird der Fehler in der Softwareanwendung 46020

erkannt und mit einem entsprechendem Fehlercode als Trouble-Ticket ausgegeben. Diese Tickets werden dann von den Mitarbeitern bearbeitet.

#### **3.1.4.8 Bereitstellung (Bereitstellen des Systems)**

Das geprüfte System wird dann durch Mitarbeiter des Ressort SSZ oder vom Ressort ausgewählte Personen an den Kunden geliefert. Hier installieren sie das System mit allen dazugehörigen Komponenten. Der PC wird in den Örtlichkeiten des Kunden aufgebaut und an das Stromnetz angeschlossen. In einigen Fällen hat der Kunde eine USV, die dann mit einbezogen wird. Dann werden die Verbindungen zwischen dem Knoten und der Sichtstation hergestellt. Dabei gibt es verschiedene Anschlussvarianten. Je nach Knotenart 3600, 3645 und 3600+ wird vom Knoten mit einer entsprechenden Schnittstellenkarte die Verbindung zum Cisco Router herausgeführt. Der vorkonfigurierte Cisco Router wird nun mit der Schnittstelle am Knoten verbunden. Die Verbindung zwischen Router und PC basiert auf einer LAN Verbindung. Ist die physikalische Verbindung mit dem System hergestellt, wird die Sichtstation eingeschaltet. Nach der Anmeldung mit Benutzername und Passwort bekommt er seine View angezeigt. Hiermit ist das System für den Kunden betriebsbereit. Sollte das Netz des Kunden sich vergrößern, werden die Softwareanpassungen in der 46020 neu an die Gegebenheiten angepasst. Diese Anpassungen sieht der Kunde dann über seine View auf der Sichtstation. Bekommt der Kunde neue Hardware für eine Erweiterung, werden einzelne Schnittstellenkarten oder ein neuer Knoten bereitgestellt. Regelmäßige Änderungen wie das Einspielen einer neuen Firmware in den Knoten werden durch das Netzmanagement Center vorgenommen.

#### **3.1.4.9 Einweisung (Durchführen von Kommunikationsmaßnahmen)**

Nach der Bereitstellung des Systems vor Ort bekommt der Kunde eine Einweisung zu den bei ihm installierten Komponenten. Das sind je nach Auftrag unterschiedliche Komponenten wie Modems, Cisco Router, Verbindungskabel, PC-System oder spezielle Geräte (Netzteil 60V). Nach der Erläuterung der Hardwarekomponenten bekommt der Kunde Informationen zu seinem View auf seiner Sichtstation. Hier sieht der Kunde nur sein Teil- oder sein Gesamtnetz. Die Einweisung vermittelt dem Kunden grundlegendes Wissen. Das ist das An- und Abmelden an der Sichtstation, das Arbeiten und das Verhalten im Störfall.

#### **3.1.4.10 Übergabe (Durchführen der Übergabe)**

Das Produkt, also die Sichtstation und die dazugehörigen Komponenten, werden nach der Bereitstellung und der Einweisung dem Kunden betriebsbereit übergeben. Dieser unterschreibt die Verpflichtungserklärung, dass er die in der Einweisung erhaltenen Regeln und Sicherheitshinweise beachtet. Die Sicherheitshinweise sagen aus, dass nur das Ressort SSZ oder von ihm ausgewählte Personen an der PC-Hard- und Software und den Komponenten Störungsbeseitigungen oder Updates ausführen dürfen. Der Kunde darf keine von ihm bereitgestellten Komponenten wie z.B. Drucker oder andere Monitore an das System anschließen. Sollte es zu widerrechtlichen Handlungen kommen, wird dem Kunden das System abgeschaltet und deinstalliert.

#### **3.1.4.11 Schulung (Informieren betroffener Personen/Stellen)**

Wenn der Kunde nach der Einweisung noch eine ausführlichere und tiefergehende Schulung haben möchte, kann er beim Ressort SSZ der TNL Bochum seinen Bedarf anmelden. Das Ressort SSZ stellt dann einen Schulungsplan auf, in dem Inhalte, Zeiten und Teilnehmer festgelegt werden. Im Ressort achtet man aber auf die Wirtschaftlichkeit, so dass beispielsweise keine Schulung mit nur zwei Personen stattfindet.

#### **3.1.4.12 Dokumentation (Erstellen einer Prozessdokumentation)**

Die Dokumentation setzt sich aus einer stetigen Projektdokumentation und Teildokumentationen zusammen. Für das Erstellen und Verwalten von Dokumentationen besitzt die Deutsche Telekom AG eine integrierte Management-Verfahrensanweisung. In dieser Anweisung wird das Erstellen und Verwalten von Dokumenten nach Anforderungen des

Qualitätsmanagements beschrieben. Die wichtigsten Punkte dieser Anweisung sind die Aufbewahrung, Erstellung, Aktualisierung und die Änderung von Dokumenten. Teildokumentationen, wie zum Beispiel Konfigurationseinstellungen einer Komponente, werden in Papier oder elektronischer Form in den Teams aufbewahrt. Bei sensiblen, vertraulichen und geheimen Dokumentationen, wie der Firewall-Konfiguration, müssen diese Dokumente verschlossen oder in elektronischer Form verschlüsselt und mit Passwort versehen werden. Eine der Dokumentationen bezieht sich auf das lokale Betriebssystem und seine Anwendungen sowie auf die Server. Hier werden Benutzerkonten mit den dazugehörigen Passwörtern, Netzwerkeinstellungen wie IP-Adresse und MAC-Adresse dokumentiert. Komplexe Konfigurationen werden teilweise durch Systemausdrucke dokumentiert. Die Dokumentation der Installation der Leitungen wird durch das Ressort BBN erstellt und den Unterlagen beigelegt. In dieser Dokumentation sind die physikalischen Schaltwege dokumentiert. Die Router-Konfiguration der IP-Adresse, IP-Helperadresse, Zugangsnummern und Passwörter wird dokumentiert und in dem entsprechenden Team aufbewahrt. Dokumente zu Netzknoten und anderen Komponenten werden systembezogen aufbewahrt. Es ist bei allen Dokumenten darauf zu achten, dass bei Veränderungen an Systemen und Komponenten die Dokumente aktualisiert und korrigiert werden.

## 3.2 Faultmanagement

---

In diesem Abschnitt wird das Faultmanagement in Form

- eines Referenzprozesses
- einer detaillierteren Darstellung der einzelnen Teilprozesse
- einer beispielhaften Ausgestaltung des Prozesses Faultmanagement

dargestellt.

Dabei wird jeweils der gesamte Prozess dargestellt, um mögliche Aufgaben neben den Kernaufgabenfeldern aufzuzeigen.

### 3.2.1 Referenzprozess Faultmanagement

Das folgende Ablaufdiagramm zeigt allgemein den Prozess des Faultmanagements. Eine konkrete Ausgestaltung dieses Prozesses sollte in der Weiterbildung daran orientiert werden.

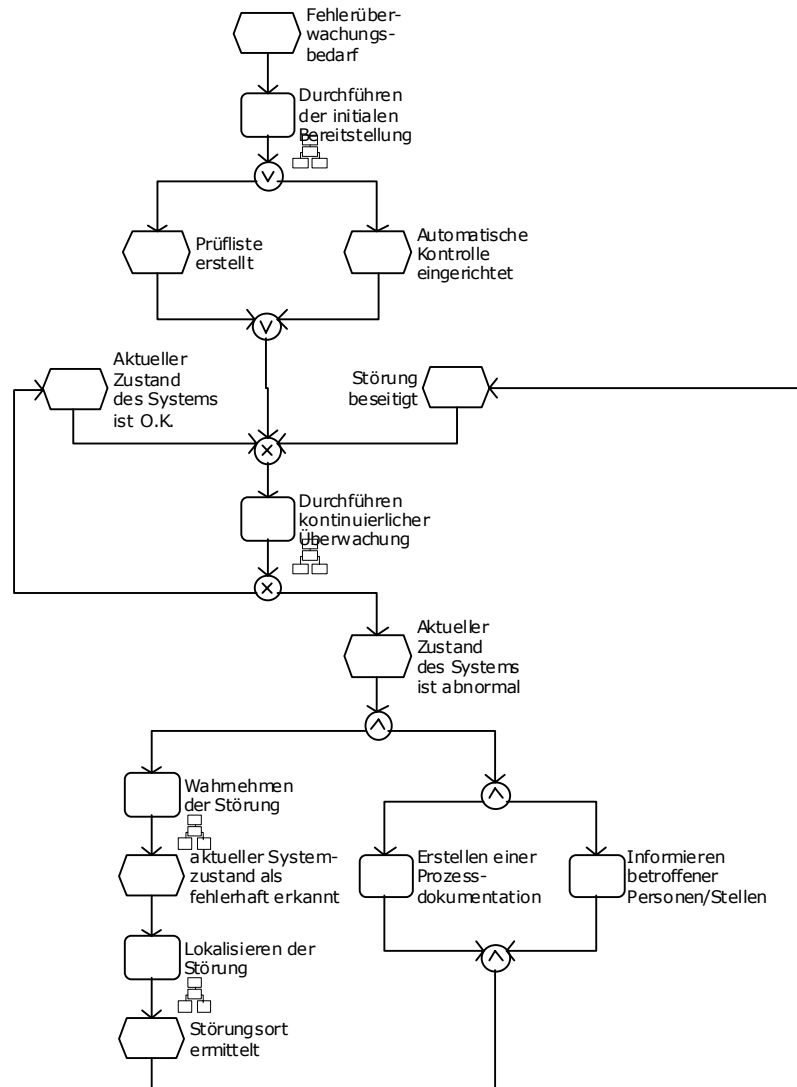


Abbildung: Referenzprozess 2: Faultmanagement, Teil 1

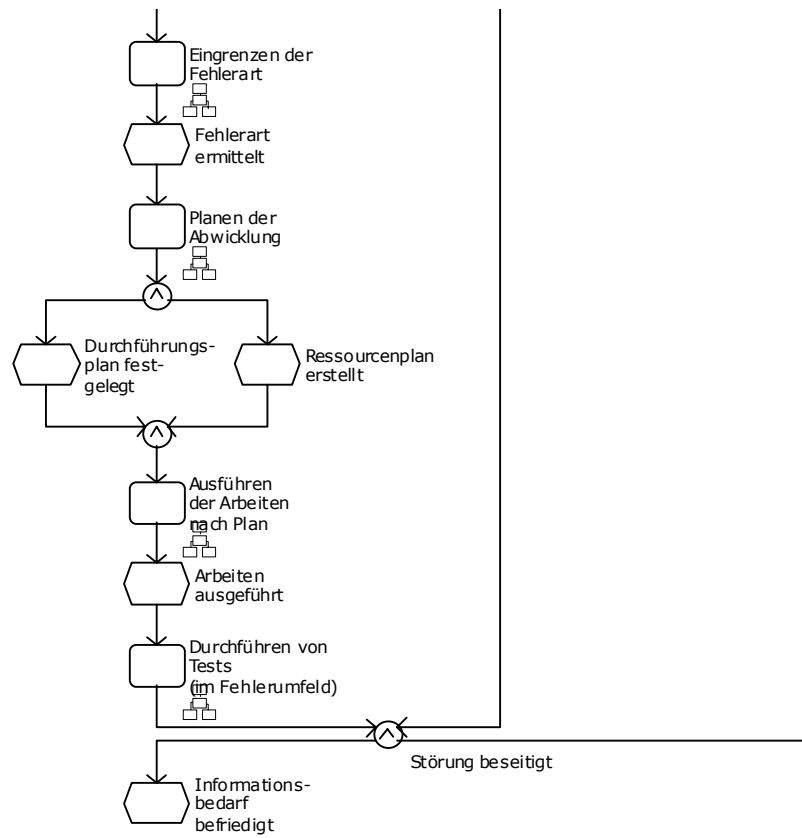


Abbildung: Referenzprozess 2: Faultmanagement, Teil 2

### **3.2.2 Prozesskompass Faultmanagement**

1. Durchführen der initialen Bereitstellung
2. Durchführen kontinuierlicher Überwachung
3. Wahrnehmen der Störung
4. Erstellen der Prozessdokumentation
5. Informieren betroffener Personen/Stellen
6. Lokalisieren der Störung
7. Eingrenzen der Fehlerart
8. Planen der Abwicklung
9. Ausführen der Arbeiten nach Plan
10. Durchführen von Tests (im Fehlerumfeld)



### 3.2.3 Teilprozesse Faultmanagement

Im nun folgenden Abschnitt werden die Teilprozesse des Faultmanagements dargestellt.

#### 3.2.3.1 Durchführen der initialen Bereitstellung

Um ein Faultmanagement durchführen zu können, muss erst einmal festgelegt werden, welche Komponenten und Dienste überwacht werden sollen und wie man evtl. den Überwachungsvorgang automatisieren kann. Als Ergebnis erhält man eine Prüfliste und es wird eine automatische Kontrolle eingerichtet.

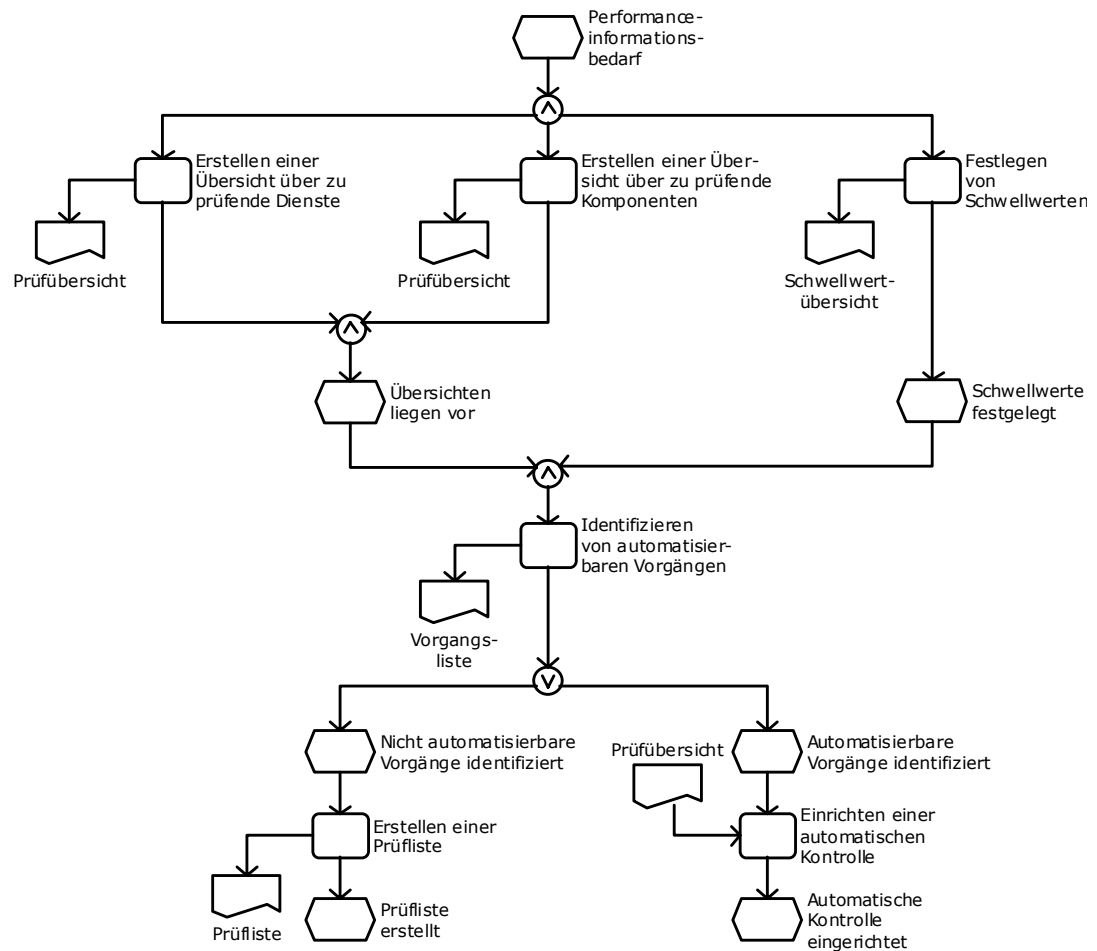


Abbildung 9: Durchführen der initialen Bereitstellung

##### 3.2.3.1.1 Tätigkeiten: Durchführen der initialen Bereitstellung

- Erstellen einer Übersicht über zu prüfende Dienste
- Erstellen einer Übersicht über zu prüfende Komponenten
- Identifizieren von automatisierbaren Vorgängen
- Einrichten einer automatischen Kontrolle
- Erstellen einer Prüfliste

##### 3.2.3.1.2 Kompetenzfelder: Durchführen der initialen Bereitstellung

Fähigkeiten/Fertigkeiten

- Übersicht über zu prüfende Dienste erstellen können
- Übersicht über zu prüfende Komponenten erstellen können

- Automatisierbare Vorgänge identifizieren können
- Automatische Kontrollen einrichten können
- Prüfliste erstellen können
- Dokumentieren können

#### Wissen

- Netzwerkdimension
- Netzwerkorganisation
- Kommunikationsarchitektur
- Betriebsarten
- Sitzungscharakterisierung
- Hardware
- Aktive Komponenten
- Passive Komponenten
- Topologien
- Strukturierte Verkabelung
- Protokolle
- Referenzmodelle
- Standards
- Schnittstellen
- Übertragungssysteme, -techniken
- Übertragungsmedien
- Elektrotechnik
- Systemsoftware/Betriebssysteme
- Prozess- und Organisationskenntnisse
- Dokumentationsstandards
- Technisches Englisch

### 3.2.3.2 Durchführen kontinuierlicher Überwachung

Hat man sich Gedanken darüber gemacht, was man mit welcher Vorgehensweise überwachen will, kann man die kontinuierliche Überwachung durchführen. Hier werden die Ausgaben der zuvor erstellten bzw. eingerichteten automatischen Kontrolle und die Ressourcenverfügbarkeit überwacht und ausgewertet. Diese Auswertung kann einen abnormalen Zustand des Systems ergeben.

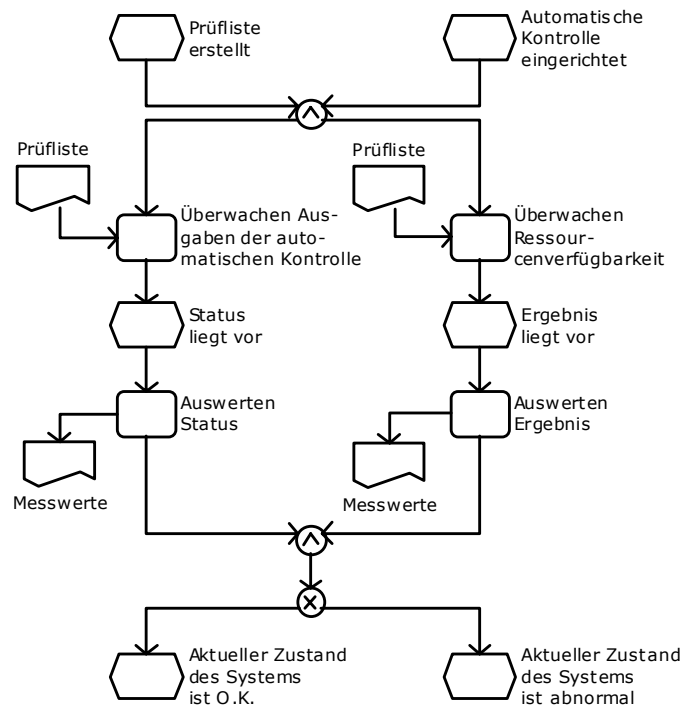


Abbildung 10: Durchführen kontinuierlicher Überwachung

#### 3.2.3.2.1 Tätigkeiten: Durchführen kontinuierlicher Überwachung

- Überwachen der Ausgaben der automatischen Kontrolle
- Auswerten des Status
- Überwachen der Ressourcenverfügbarkeit
- Auswerten des Ergebnisses

#### 3.2.3.2.2 Kompetenzfelder: Durchführen kontinuierlicher Überwachung

Fähigkeiten/Fertigkeiten

- Ausgaben der automatischen Kontrolle auswerten können
- Status auswerten/interpretieren können
- Ressourcenverfügbarkeit überwachen können
- Ergebnisse (der Überwachung) auswerten/interpretieren können
- Dokumentieren können

Wissen

- Netzwerkdimension
- Netzwerkorganisation
- Kommunikationsarchitektur
- Betriebsarten
- Sitzungscharakterisierung

- Hardware
- Aktive Komponenten
- Passive Komponenten
- Protokolle
- Standards
- Schnittstellen
- Übertragungssysteme, -techniken
- Übertragungsmedien
- Systemsoftware/Betriebssysteme
- Prozess- und Organisationskenntnisse
- Netzwerkmanagementsysteme
- Messverfahren
- Fernzugriffsverfahren
- Dokumentationsstandards
- Technisches Englisch

### 3.2.3.3 Wahrnehmen der Störung

Ergibt die kontinuierliche Überwachung, dass der aktuelle Systemzustand abnormal ist, kann eine genauere Information zum Störungsbeistand z.B. über ein Troubleticket und/oder durch eine Meldung von Benutzern beschrieben werden. Möglich ist hier auch, dass der Network Administrator eine Störung selbst erkennt. Im Anschluss müssen die Störungsmeldungen mit dem Ergebnis interpretiert werden, dass der aktuelle Systemzustand als fehlerhaft erkannt wird.

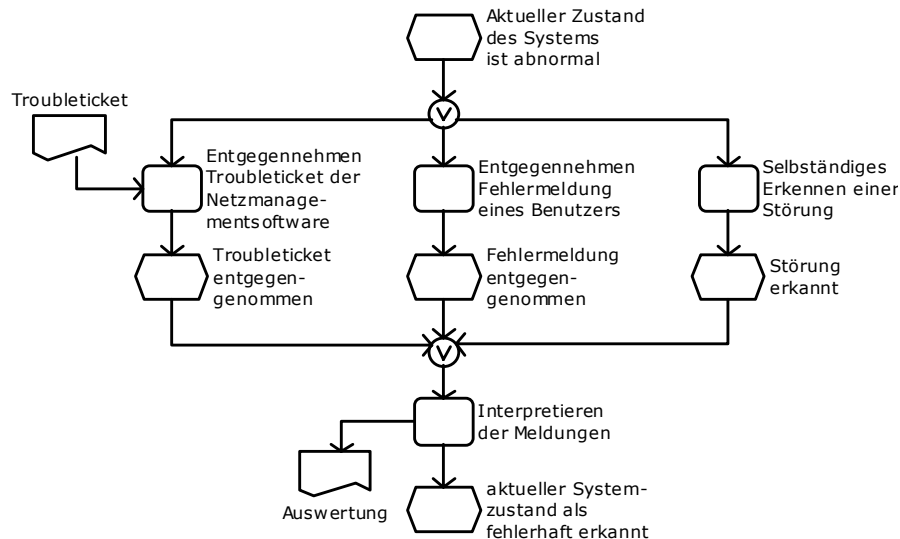


Abbildung 11: Wahrnehmen der Störung

#### 3.2.3.3.1 Tätigkeiten: Wahrnehmen der Störung

- Entgegennehmen eines Troubletickets der Netzmanagementsoftware
- Entgegennehmen einer Fehlermeldung eines Benutzers
- Selbständiges Erkennen einer Störung
- Interpretieren der Meldungen

#### 3.2.3.3.2 Kompetenzfelder: Wahrnehmen der Störung

Fähigkeiten/Fertigkeiten

- Troubleticket aus der Netzmanagementsoftware abrufen können
- Fehlermeldung eines Benutzers entgegennehmen können (Benutzer verstehen)
- Störung selbstständig erkennen können
- Meldungen/erkannte Störungen interpretieren können
- Dokumentieren können

Wissen

- Netzwerkdimension
- Netzwerkorganisation
- Hardware
- Aktive Komponenten
- Passive Komponenten
- Topologien
- Strukturierte Verkabelung

- Protokolle
- Schnittstellen
- Übertragungssysteme, -techniken
- Übertragungsmedien
- Systemsoftware/Betriebssysteme
- Prozess- und Organisationskenntnisse
- Netzwerkmanagementsysteme
- Messverfahren
- Fernzugriffsverfahren
- Dokumentationsstandards
- Technisches Englisch

### 3.2.3.4 Lokalisieren der Störung

Wurde der aktuelle Systemzustand als fehlerhaft erkannt, werden die Leitungswege getestet. Sind die Leitungswege schadhaf, muss das entsprechende defekte Teilstück analysiert werden. Sind die Leitungswege in Ordnung, werden die Übertragungskomponenten geprüft. Sind auch diese in Ordnung, ist es möglich, dass ein Dienst ausgefallen ist, was u.U. die Koordination der weiteren Arbeiten mit dem IT Systems Administrator erforderlich macht. Liegt es an den aktiven Komponenten, müssen diese identifiziert werden. Ergebnis dieses Prozesses ist die Ermittlung des Störungsorts.

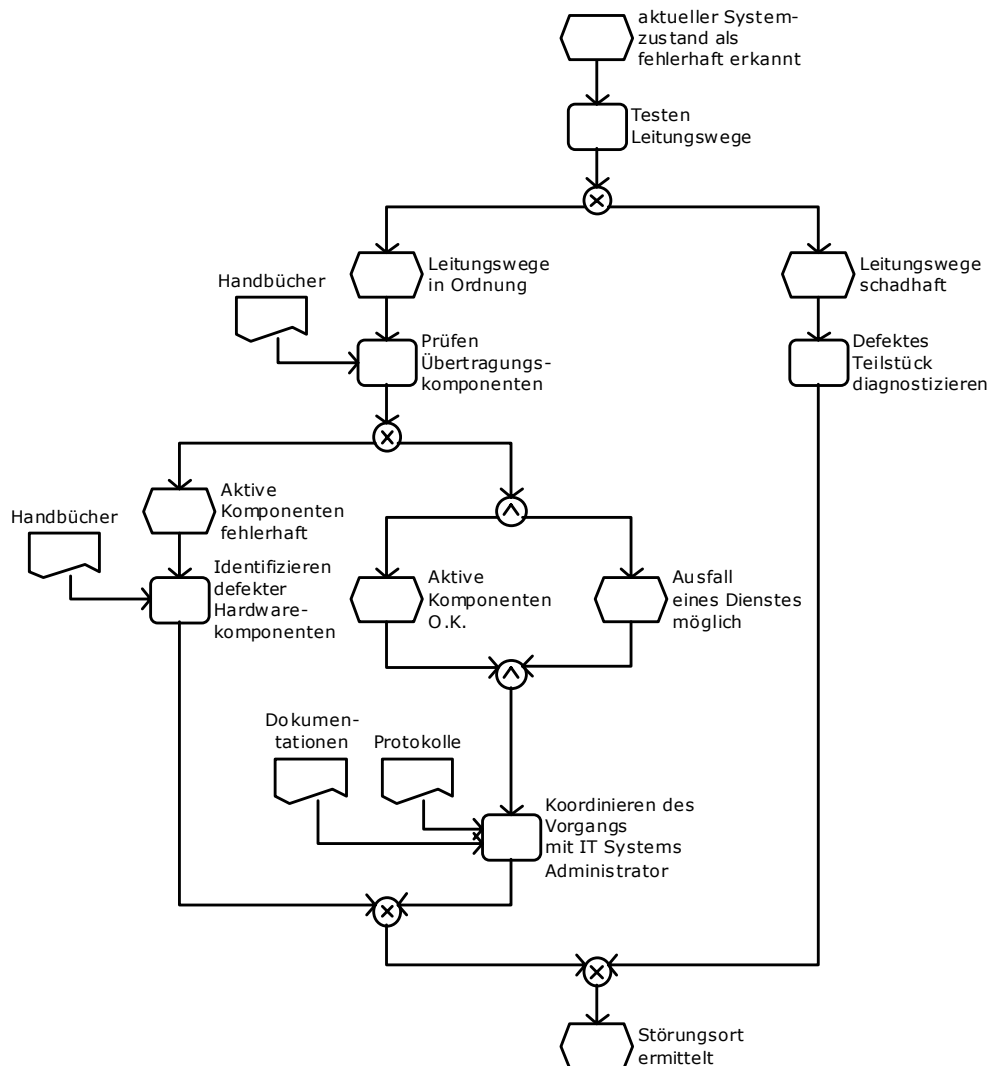


Abbildung 12: Lokalisieren der Störung

#### 3.2.3.4.1 Tätigkeiten: Lokalisieren der Störung

- Testen der Leitungswege
- Falls Leitungswege schadhaf
- Diagnostizieren defekter Teilstücke
- Falls Leitungswege in Ordnung
- Prüfen der Übertragungskomponenten
- Falls aktive Komponenten fehlerhaft
- Identifizieren defekter Hardwarekomponenten

Falls aktive Komponenten in Ordnung und möglicherweise ein Ausfall eines Dienstes vorliegt

- Koordinieren des Vorgangs mit IT Systems Administrator

Falls Leitungswege in Ordnung

- Prüfen der Übertragungskomponenten

#### **3.2.3.4.2 Kompetenzfelder: Lokalisieren der Störung**

Fähigkeiten/Fertigkeiten

- Leitungswege testen können
- Defekte Teilstücke diagnostizieren können
- Übertragungskomponenten prüfen können
- Defekte Hardwarekomponenten identifizieren können
- Vorgänge koordinieren können
- Übertragungskomponenten prüfen können
- Dokumentieren können

Wissen

- Hardware
- Aktive Komponenten
- Passive Komponenten
- Protokolle
- Standards
- Schnittstellen
- Übertragungssysteme, -techniken
- Übertragungsmedien
- Systemsoftware/Betriebssysteme
- Prozess- und Organisationskenntnisse
- Messverfahren
- Dokumentationsstandards
- Technisches Englisch



### 3.2.3.5 Eingrenzen der Fehlerart

Ist der Störungsort ermittelt, wird geprüft, ob ein Totalausfall der betreffenden Komponente/Dienst/Leitung vorliegt. Liegt kein Totalausfall vor, wird auf zeitweisen Totalausfall geprüft. Handelt es sich um einen zeitweisen Totalausfall (Teilausfall), werden diese ermittelt. In jedem Fall erfolgt noch die Ermittlung defekter Teile. Ergebnis dieses Teilprozesses ist die Ermittlung der Fehlerart.

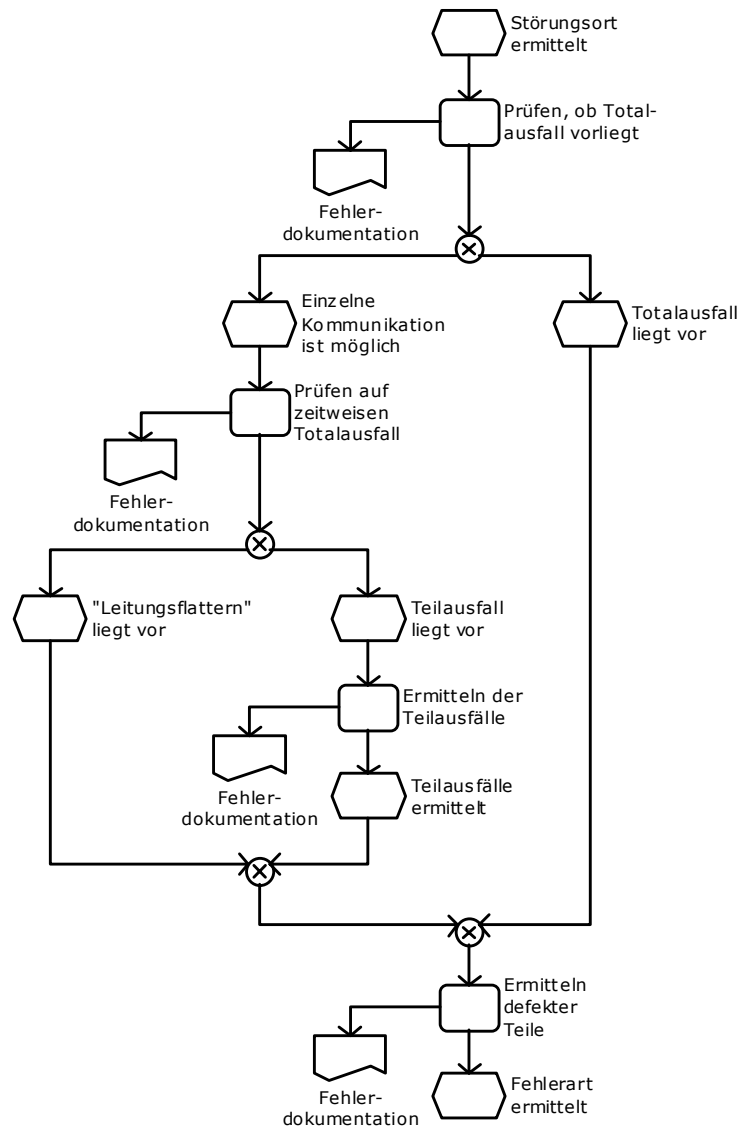


Abbildung 13: Eingrenzen der Fehlerart

#### 3.2.3.5.1 Tätigkeiten: Eingrenzen der Fehlerart

- Prüfen, ob Totalausfall vorliegt

Falls einzelne Kommunikation möglich ist

- Prüfen auf zeitweisen Totalausfall

Falls ein Teilausfall vorliegt

- Ermitteln der Teilausfälle

Falls Teilausfälle ermittelt sind oder ein „Leitungsflattern“ oder ein Totalausfall vorliegt

- Ermitteln defekter Teile

#### **3.2.3.5.2 Kompetenzfelder: Eingrenzen der Fehlerart**

Fähigkeiten/Fertigkeiten

- Netzwerk auf Totalausfall prüfen können
- Auf zeitweisen Totalausfall prüfen können
- Teilausfälle ermitteln können
- Defekte Teile ermitteln können
- Dokumentieren können

Wissen

- Netzwerkorganisation
- Kommunikationsarchitektur
- Hardware
- Aktive Komponenten
- Passive Komponenten
- Übertragungssysteme, -techniken
- Übertragungsmedien
- Messverfahren
- Dokumentationsstandards
- Technisches Englisch

### 3.2.3.6 Planen der Abwicklung

Ist die Fehlerart ermittelt, werden die Ressourcen und das Vorgehen geplant. Es wird daran anschließend ein Ressourcen- und ein Durchführungsplan und eine Beschaffungsliste erstellt.

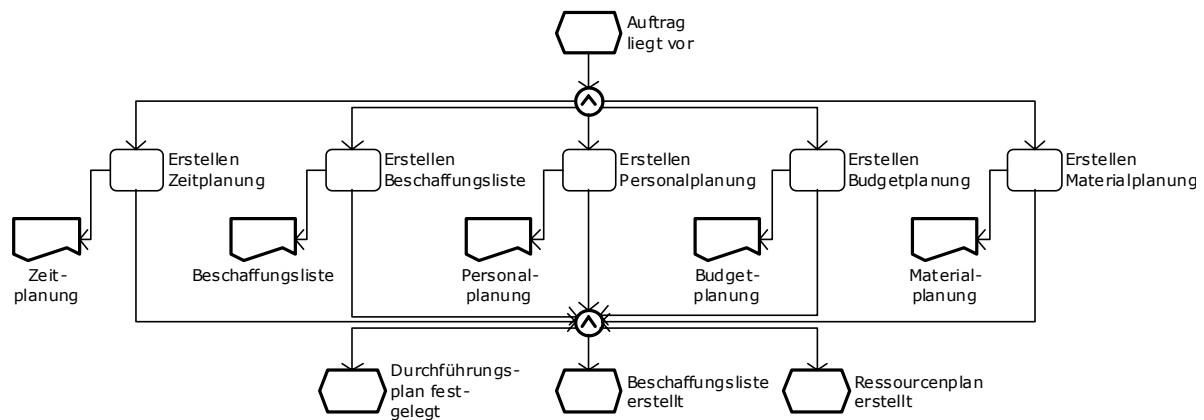


Abbildung 14: Planen der Abwicklung

#### 3.2.3.6.1 Tätigkeiten: Planen der Abwicklung

- Erstellen einer Zeitplanung
- Erstellen einer Personalplanung
- Erstellen einer Budgetplanung
- Erstellen einer Materialplanung

#### 3.2.3.6.2 Kompetenzfelder: Planen der Abwicklung

Fähigkeiten/Fertigkeiten

- Planen können
- Zeitplanung erstellen können
- Sich selbst (evtl. Mitarbeiter) beurteilen/einschätzen können
- Personalplanung erstellen können
- Budgetplanung erstellen können
- Materialplanung erstellen können
- Dokumentieren können

Wissen

- Konkreter Fehler
- Prozess- und Organisationskenntnisse
- Dokumentationsstandards
- Technisches Englisch

### 3.2.3.7 Ausführen der Arbeiten nach Plan

Steht der Ablaufplan fest und ist der Ressourcenplan erstellt, wird die Fehlerbeseitigung durchgeführt. Abhängig von der zu beseitigenden Störung wird die Beseitigung des Fehlers selbst übernommen oder an externe Dienstleister (z.B. Hersteller, Supporter) vergeben. Der Teilprozess ist beendet, wenn die Arbeiten ausgeführt worden sind.

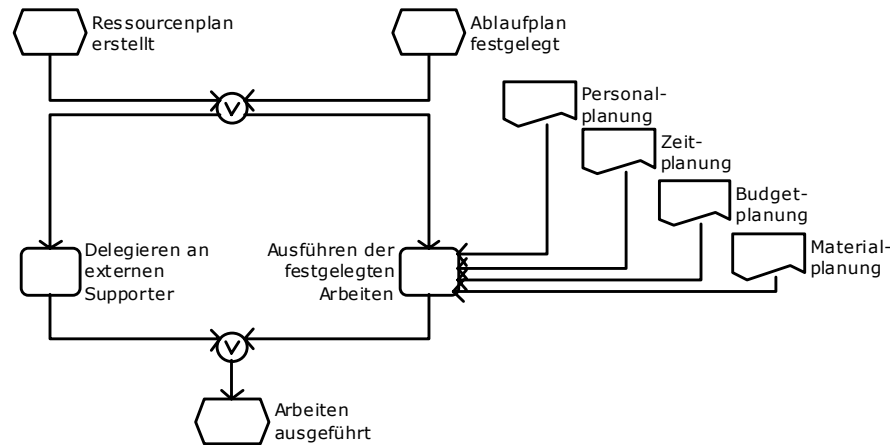


Abbildung 15: Ausführen der Arbeiten nach Plan

#### 3.2.3.7.1 Tätigkeiten: Ausführen der Arbeiten nach Plan

Falls der Ressourcenplan und/oder der Ablaufplan erstellt sind

- Delegieren an externen Supporter und/oder
- Ausführen der festgelegten Arbeiten

#### 3.2.3.7.2 Kompetenzfelder: Ausführen der Arbeiten nach Plan

Fähigkeiten/Fertigkeiten

- Delegieren können
- Koordinieren können
- (selbst) ausführen können
- Dokumentieren können

Wissen

- Konkreter Fehler
- Prozess- und Organisationskenntnisse
- Dokumentationsstandards
- Technisches Englisch

### 3.2.3.8 Durchführen von Tests (im Fehlerumfeld)

Nachdem die erforderlichen Arbeiten ausgeführt worden sind, wird getestet, ob der Fehler damit beseitigt worden ist, bzw. ob die Arbeiten erfolgreich ausgeführt wurden. Dazu wird die instandgesetzte Komponente separat getestet. Sollte die instandgesetzte Komponente nicht funktionstüchtig sein, muss diese nochmals geprüft und ggf. instandgesetzt werden. Ist sie funktionstüchtig, wird das gesamte System (im Fehlerumfeld) geprüft. Treten hier Fehler auf, müssen evtl. Einstellungen an die Systemvorgaben angepasst werden. Als Ergebnis sollte das System wieder betriebsbereit sein.

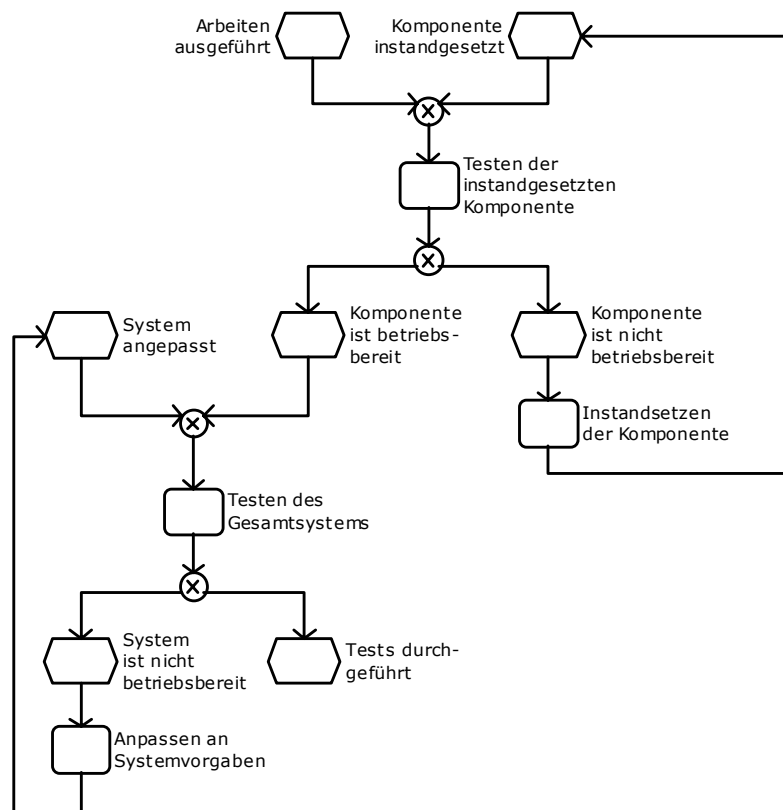


Abbildung 16: Durchführen von Tests (im Fehlerumfeld)

#### 3.2.3.8.1 Tätigkeiten: Durchführen von Tests (im Fehlerumfeld)

- Testen der instandgesetzten Komponente

Falls Komponente nicht betriebsbereit ist

- Instandsetzen der Komponente

Falls die Komponente betriebsbereit ist

- Testen des Gesamtsystems

Falls System nicht betriebsbereit ist

- Anpassen an Systemvorgaben

#### 3.2.3.8.2 Kompetenzfelder: Durchführen von Tests (im Fehlerumfeld)

Fähigkeiten/Fertigkeiten

- Testen können
- Instandgesetzte Komponente testen können
- Komponenten instandsetzen können
- Gesamtsystem testen können

- System an Systemvorgaben anpassen können
- Dokumentieren können

#### Wissen

- Netzwerkdimension
- Netzwerkorganisation
- Kommunikationsarchitektur
- Betriebsarten
- Sitzungscharakterisierung
- Hardware
- Aktive Komponenten
- Passive Komponenten
- Topologien
- Strukturierte Verkabelung
- Protokolle
- Referenzmodelle
- Standards
- Schnittstellen
- Übertragungssysteme, -techniken
- Übertragungsmedien
- Elektrotechnik
- Systemsoftware/Betriebssysteme
- Netzwerkmanagementsysteme
- Messverfahren
- Fernzugriffsverfahren
- Prozess- und Organisationskenntnisse
- Dokumentationsstandards
- Technisches Englisch

#### **3.2.3.9 Informieren betroffener Personen/Stellen**

Für dieses Kapitel gilt das Gleiche, was bereits im Kapitel 3.1.2.9 gesagt wurde. Eine Schulung bzw. Einweisung ist hier u.U. aber gar nicht notwendig.

#### **3.2.3.10 Erstellen einer Prozessdokumentation**

Für dieses Kapitel gilt das Gleiche, was bereits im Kapitel 3.1.2.10 gesagt wurde. Der Prozess „Erstellen einer Abschlussdokumentation“ fällt unter diesen Punkt.

### 3.2.4 Beispiel Faultmanagement

Das folgende Beispiel schildert das Vorgehen bei einem ganz bestimmten Fehler. Das Beheben **eines** Fehlers reicht in der Weiterbildung zur Erlangung des Titels „Network Administrator“ jedoch **nicht** aus.

Der Kunde erkennt eine Störung. Er meldet sich telefonisch bei einem Mitarbeiter und schildert ihm die Störung. Der Mitarbeiter analysiert die Störung. Er schaut sich mit Hilfe der 46020 die Kundensichtstation an. In der visuellen Darstellung ist die Verbindung bis zum Router in Ordnung. Mit Hilfe des Befehls „ping“ ist dies überprüft worden. Mit dem Befehl Telnet verbindet sich der Mitarbeiter mit dem Router und überprüft die Schnittstelle eth0. Bei der Nachfrage beim Kunden, ob die Leitung physisch verbunden ist, stellt sich heraus, dass die Ethernet-Leitung nicht in der Schnittstelle steckt. Der Kunde steckt die Leitung in den Router und meldet sich an seiner Sichtstation an. Es funktioniert wieder alles. Die Störung ist somit behoben.



### 3.3 Performancemanagement

---

In diesem Abschnitt wird das Performancemanagement in Form

- eines Referenzprozesses
- einer detaillierteren Darstellung der einzelnen Teilprozesse
- einer beispielhaften Ausgestaltung des Prozesses Performancemanagement

dargestellt.

Dabei wird jeweils der gesamte Prozess dargestellt, um mögliche Aufgaben neben den Kernaufgabenfeldern aufzuzeigen.

### **3.3.1 Referenzprozess Performancemanagement**

In diesem Abschnitt wird der Referenzprozess Performancemanagement abgebildet. Eine konkrete Ausgestaltung dieses Prozesses sollte in der Weiterbildung daran orientiert werden.

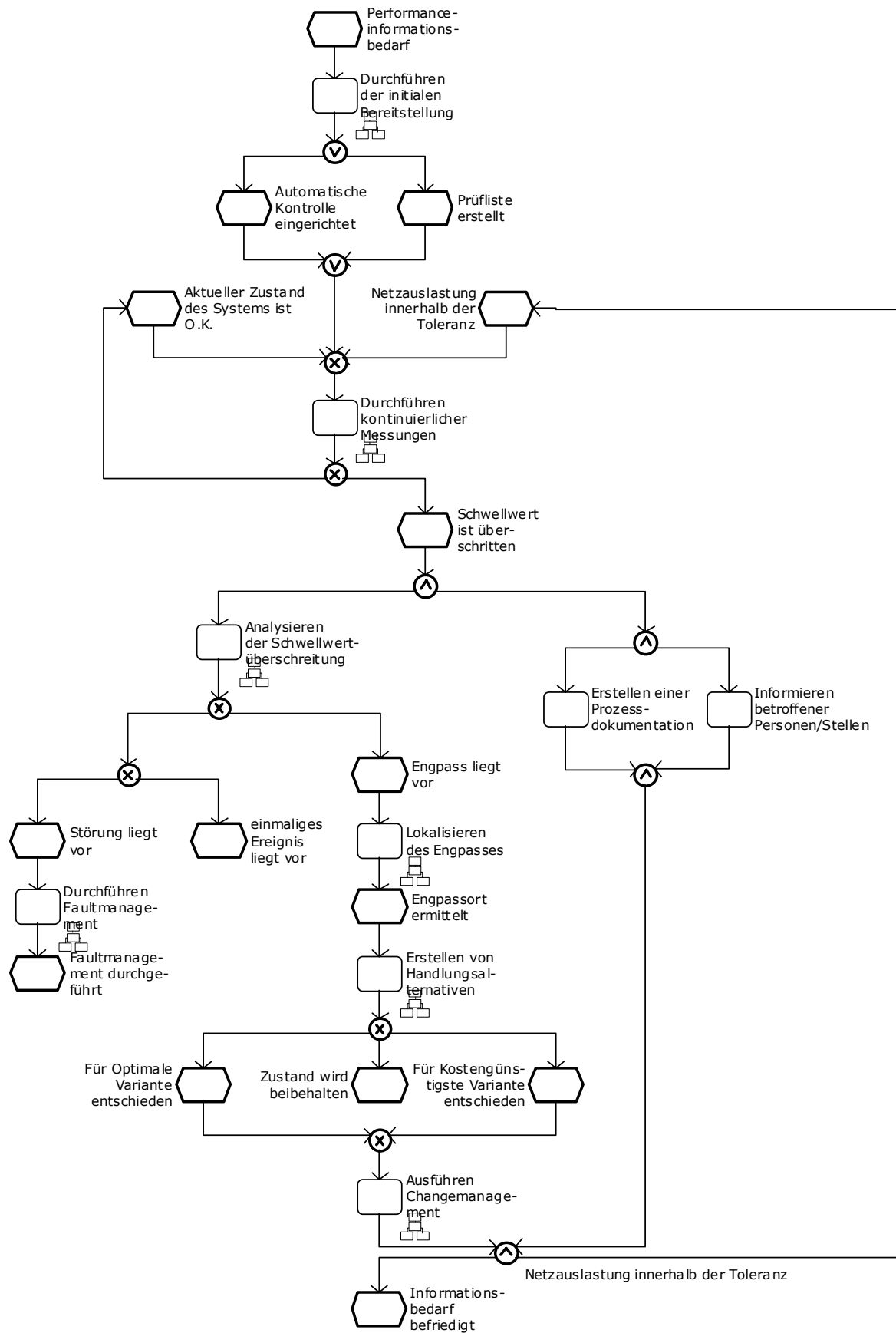


Abbildung 17: Referenzprozess 3: Performancemanagement

### **3.3.2 Prozesskompass Performancemanagement**

1. Durchführen der initialen Bereitstellung
2. Durchführen kontinuierlicher Messungen
3. Erstellen einer Prozessdokumentation
4. Informieren betroffener Personen/Stellen
5. Analysieren der Schwellwertüberschreitung
6. Lokalisieren des Engpasses
7. Erstellen von Handlungsalternativen
8. Ausführen Changemanagement

### 3.3.3 Teilprozesse Performancemanagement

In diesem Abschnitt werden die Teilprozesse des Performancemanagements abgebildet.

#### 3.3.3.1 Durchführen der initialen Bereitstellung

Um ein Performancemanagement durchführen zu können, muss erst einmal festgelegt werden, welche Komponenten und Dienste überwacht werden sollen und wie man evtl. den Überwachungsvorgang automatisieren kann. Außerdem müssen Schwellwerte festgelegt werden, deren Überschreitung eine Abnormität des Systems signalisieren. Als Ergebnis erhält man eine Prüfliste und es wird eine automatische Kontrolle eingerichtet.

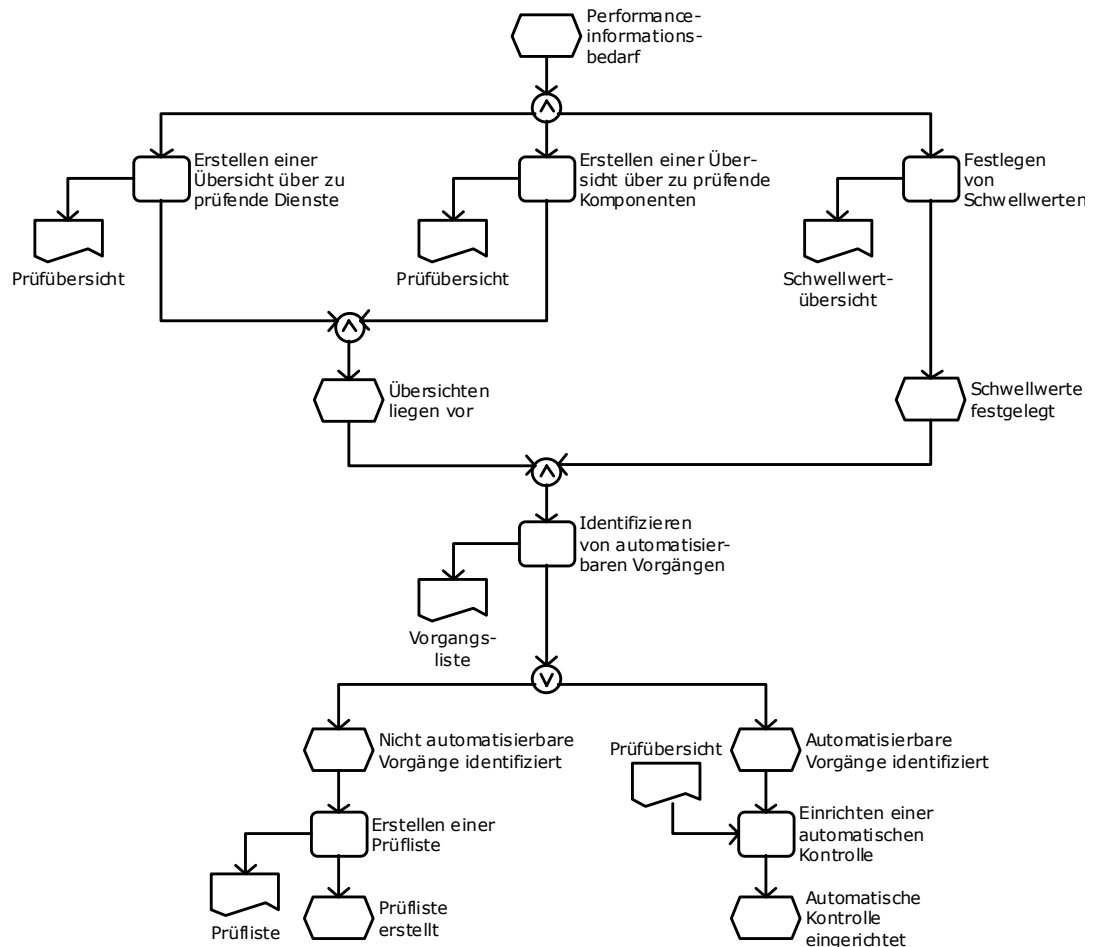


Abbildung 18: Durchführen der initialen Bereitstellung

##### 3.3.3.1.1 Tätigkeiten: Durchführen der initialen Bereitstellung

- Erstellen einer Übersicht über zu prüfende Dienste
- Erstellen einer Übersicht über zu prüfende Komponenten
- Festlegen von Schwellwerten
- Identifizieren von automatisierbaren Vorgängen

Wenn automatisierbare und nicht automatisierbare Vorgänge identifiziert sind

- Erstellen einer Prüfliste
- Einrichten einer automatischen Kontrolle

### **3.3.3.1.2 Kompetenzfelder: Durchführen der initialen Bereitstellung**

Fähigkeiten/Fertigkeiten

- Übersichten erstellen können
- Übersicht über zu prüfende Dienste erstellen können
- Übersicht über zu prüfende Komponenten erstellen können
- Schwellwerte festlegen können
- Automatisierbare Vorgänge identifizieren können
- Prüflisten erstellen können
- Automatische Kontrollen einrichten können
- Dokumentieren können

Wissen

- Netzwerkdimension
- Netzwerkorganisation
- Kommunikationsarchitektur
- Betriebsarten
- Sitzungscharakterisierung
- Hardware
- Aktive Komponenten
- Passive Komponenten
- Topologien
- Strukturierte Verkabelung
- Protokolle
- Referenzmodelle
- Standards
- Schnittstellen
- Übertragungssysteme, -techniken
- Übertragungsmedien
- Elektrotechnik
- Systemsoftware/Betriebssysteme
- Prozess- und Organisationskenntnisse
- Dokumentationsstandards
- Technisches Englisch

### 3.3.3.2 Durchführen kontinuierlicher Messungen

Hat man sich Gedanken darüber gemacht, was man mit welcher Vorgehensweise überwachen will, kann man kontinuierliche Messungen durchführen. Hier werden die Ausgaben der zuvor erstellten bzw. eingerichteten automatischen Kontrolle und die Ressourcenverfügbarkeit überwacht und ausgewertet. Diese Auswertung kann einen abnormalen Zustand des Systems in Form einer Schwellwertüberschreitung ergeben.

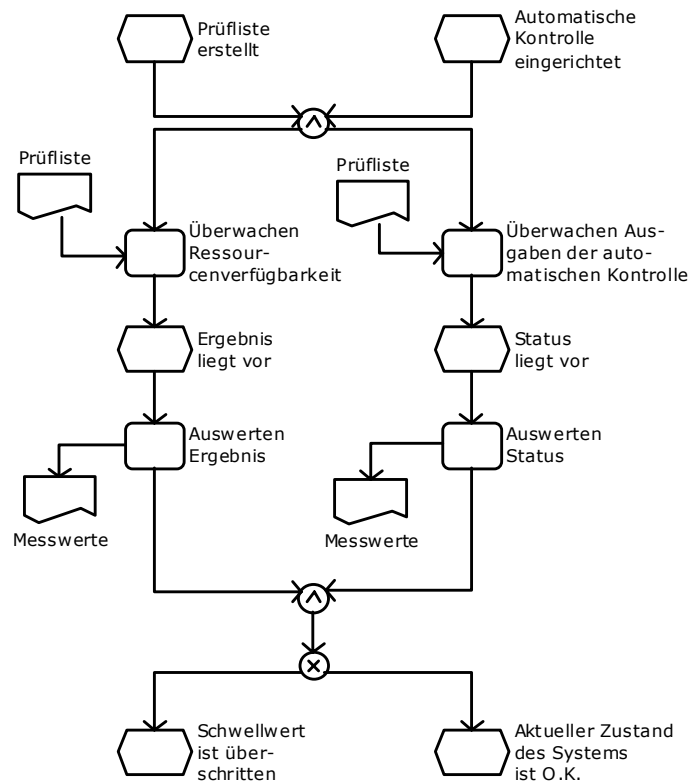


Abbildung 19: Durchführen kontinuierlicher Messungen

#### 3.3.3.2.1 Tätigkeiten: Durchführen kontinuierlicher Messungen

- Überwachen der Ressourcenverfügbarkeit
- Auswerten der Ergebnisse
- Überwachen der Ausgaben der automatischen Kontrolle
- Status auswerten

#### 3.3.3.2.2 Kompetenzfelder: Durchführen kontinuierlicher Messungen

Fähigkeiten/Fertigkeiten

- Ausgaben der automatischen Kontrolle auswerten können
- Status auswerten/interpretieren können
- Ressourcenverfügbarkeit überwachen können
- Ergebnisse (der Überwachung) auswerten/interpretieren können
- Dokumentieren können

Wissen

- Netzwerkdimension
- Netzwerkorganisation
- Kommunikationsarchitektur

- Betriebsarten
- Sitzungscharakterisierung
- Hardware
- Aktive Komponenten
- Passive Komponenten
- Protokolle
- Standards
- Schnittstellen
- Übertragungssysteme, -techniken
- Übertragungsmedien
- Systemsoftware/Betriebssysteme
- Prozess- und Organisationskenntnisse
- Netzwerkmanagementsysteme
- Messverfahren
- Fernzugriffsverfahren
- Dokumentationsstandards
- Technisches Englisch



### 3.3.3.3 Analysieren der Schwellwertüberschreitung

Ergibt die kontinuierliche Überwachung, dass ein Schwellwert überschritten wurde, kann eine genauere Information zum Grund für die Schwellwertüberschreitung notwendig sein. Dazu ist zu prüfen, ob ein Ausfall (eine Störung) vorliegt oder nicht. Liegt ein Ausfall vor, ist zu prüfen, ob die Störung reproduzierbar ist. Wenn dem so sein sollte, wird der Faultmanagementprozess angestoßen, andernfalls ist keine Handlung nötig. Liegt gar keine Störung vor, handelt es sich tatsächlich um einen Engpass.

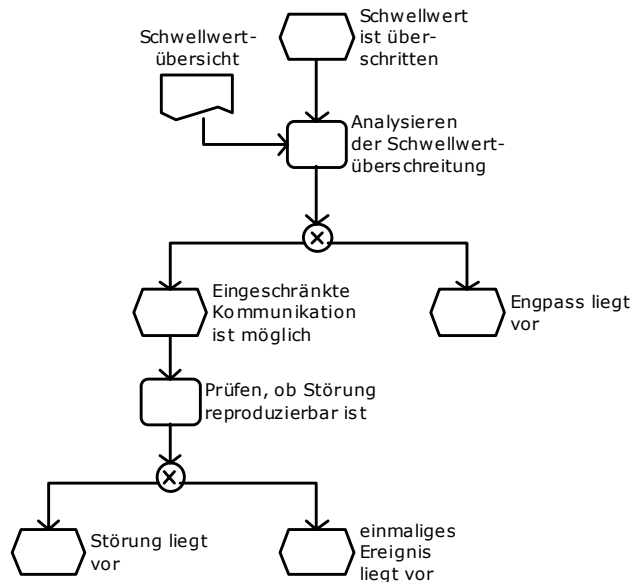


Abbildung 20: Analysieren der Schwellwertüberschreitung

#### 3.3.3.3.1 Tätigkeiten: Analysieren der Schwellwertüberschreitung

- Analysieren der Schwellwertüberschreitung
- Prüfen, ob Störung reproduzierbar ist

#### 3.3.3.3.2 Kompetenzfelder: Analysieren der Schwellwertüberschreitung

Fähigkeiten/Fertigkeiten

- Schwellwertüberschreitung analysieren können
- Reproduzierbarkeit einer Störung prüfen können
- Dokumentieren können

Wissen

- Spezielle Schwellwerte
- Netzwerkmanagementsysteme
- Dokumentationsstandards
- Technisches Englisch

### 3.3.3.4 Lokalisieren des Engpasses

Wurde ein Engpass erkannt, werden die Leitungswege getestet. Sind die Leitungswege nicht ausreichend performant, muss das entsprechende Teilstück analysiert werden. Sind die Leitungswege in Ordnung, werden die Übertragungskomponenten geprüft. Sind auch diese in Ordnung, ist es möglich, dass ein Dienst ausgefallen ist, was u.U. die Koordination der weiteren Arbeiten mit dem IT Systems Administrator erforderlich macht. Das Ergebnis dieses Teilprozesses ist der ermittelte Engpassort.

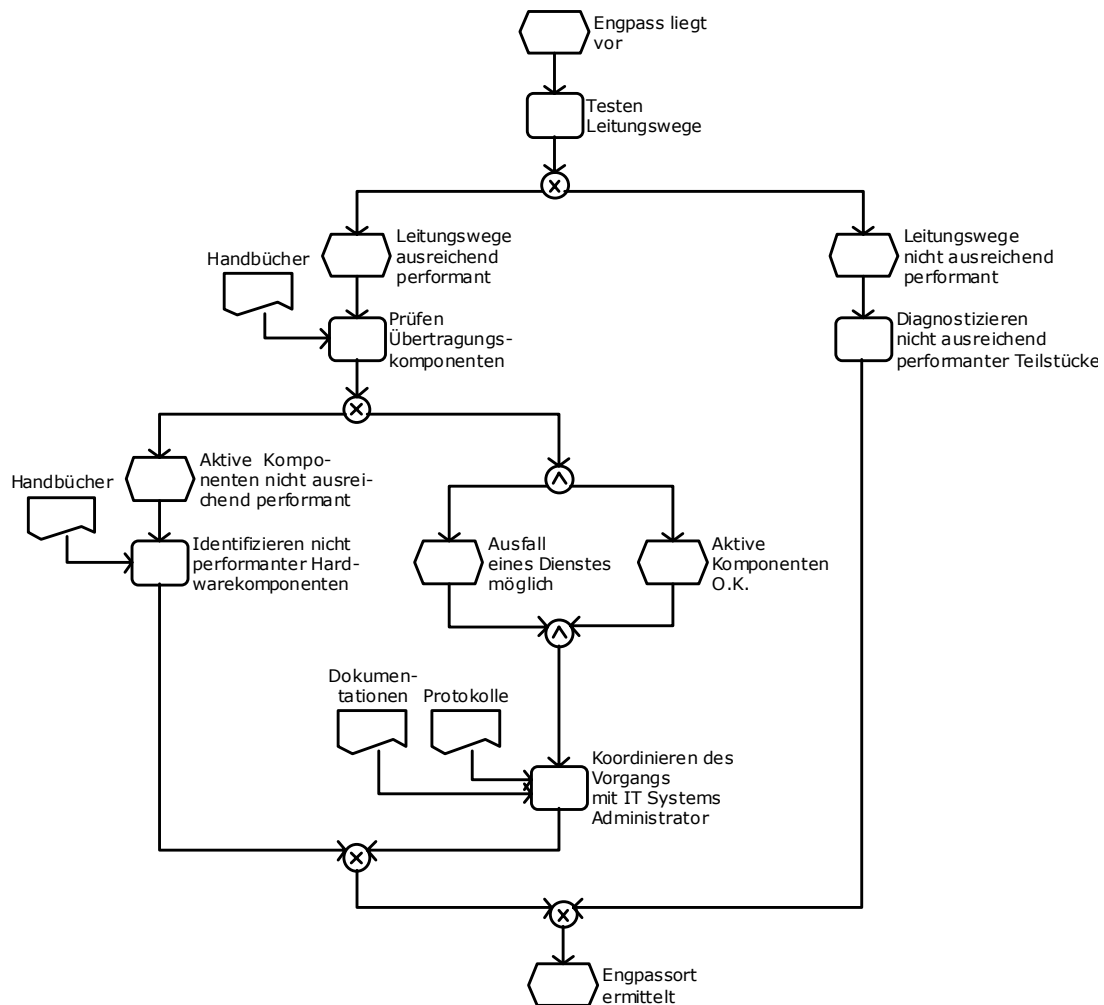


Abbildung 21: Lokalisieren des Engpasses

#### 3.3.3.4.1 Tätigkeiten: Lokalisieren des Engpasses

- Testen der Leitungswege
- Falls Leitungswege nicht ausreichend performant
- Diagnostizieren nicht ausreichend performanter Teilstücke
- Falls Leitungswege ausreichend performant
- Prüfen der Übertragungskomponenten
- Falls aktive Komponenten nicht ausreichend performant
- Identifizieren nicht performanter Hardwarekomponenten
- Falls aktive Komponenten in Ordnung und möglicherweise ein Ausfall eines Dienstes vorliegt
- Koordinieren des Vorgangs mit IT Systems Administrator

#### **3.3.3.4.2 Kompetenzfelder: Lokalisieren des Engpasses**

Fähigkeiten/Fertigkeiten

- Leitungswege hinsichtlich ihrer Performanz testen können
- Nicht ausreichend performante Teilstücke diagnostizieren können
- Übertragungskomponenten hinsichtlich ihrer Performanz prüfen können
- Nicht performante Hardwarekomponenten identifizieren können
- Vorgänge koordinieren können
- Dokumentieren können

Wissen

- Hardware
- Aktive Komponenten
- Passive Komponenten
- Protokolle
- Standards
- Schnittstellen
- Übertragungssysteme, -techniken
- Übertragungsmedien
- Systemsoftware/Betriebssysteme
- Prozess- und Organisationskenntnisse
- Messverfahren
- Dokumentationsstandards
- Technisches Englisch

### 3.3.3.5 Erstellen von Handlungsalternativen

Ist der Engpassort ermittelt, wird ein Variantenvergleich unter den möglichen Handlungsalternativen durchgeführt. Hier wird unterschieden zwischen der kostengünstigsten und der wirksamsten, der optimalen Variante. Sind diese ermittelt, erfolgt (sofern nötig) die Abstimmung mit dem Entscheidungsträger. Entschieden wird, welche Variante durchgeführt wird, bzw. ob überhaupt etwas an der bisherigen Situation geändert wird, wenn das Netzwerk im Prinzip weiterhin arbeitsfähig wäre.

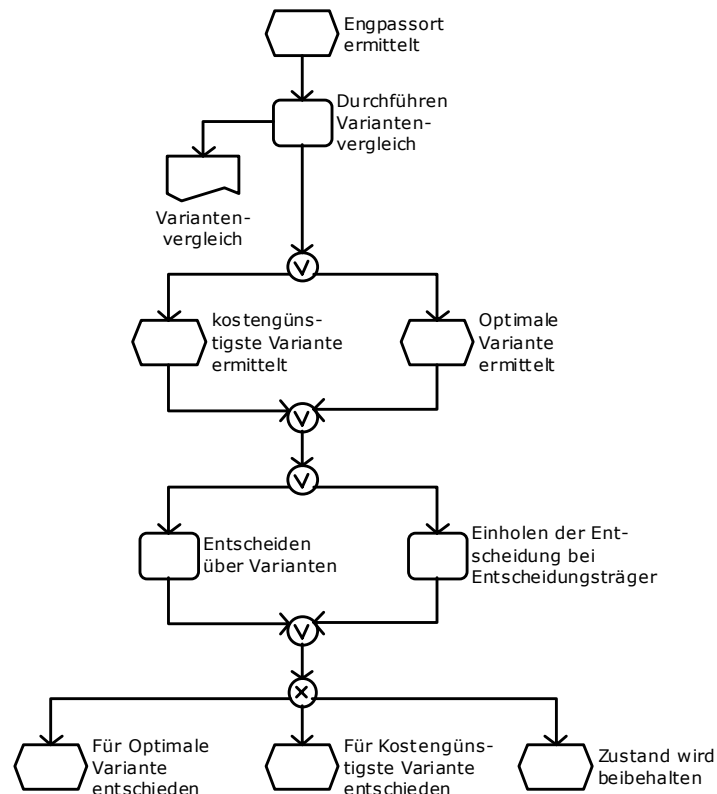


Abbildung 22: Erstellen von Handlungsalternativen

#### 3.3.3.5.1 Tätigkeiten: Erstellen von Handlungsalternativen

- Durchführen eines Variantenvergleichs
- Entscheiden über Varianten
- Einholen der Entscheidung beim Entscheidungsträger

#### 3.3.3.5.2 Kompetenzfelder: Erstellen von Handlungsalternativen

Fähigkeiten/Fertigkeiten

- Variantenvergleich durchführen können
- Wirtschaftlichkeitsbetrachtung durchführen können
- Entscheiden können
- Dokumentieren können

Wissen

- Aktive Komponenten
- Passive Komponenten
- Hardware
- Übertragungsmedien

- Kaufmännische Grundkenntnisse
- Dokumentationsstandards
- Technisches Englisch

#### **3.3.3.6 Ausführen Changemanagement**

Dieser Prozess entspricht dem unter 3.1.1ff. Gesagtem und wird deshalb an dieser Stelle nicht ausgeführt.

#### **3.3.3.7 Informieren betroffener Personen/Stellen**

Für dieses Kapitel gilt das Gleiche, was bereits im Kapitel 3.1.2.9 gesagt wurde. Eine Schulung bzw. Einweisung ist hier u.U. aber gar nicht notwendig.

#### **3.3.3.8 Erstellen einer Prozessdokumentation**

Für dieses Kapitel gilt das Gleiche, was bereits im Kapitel 3.1.2.10 gesagt wurde. Der Prozess „Erstellen einer Abschlussdokumentation“ fällt unter diesen Punkt.

### 3.3.4 Beispiel Performancemanagement

Das folgende Beispiel schildert das Vorgehen in einer ganz bestimmten Engpasssituation. Das Beheben **eines** Engpasses reicht in der Weiterbildung zur Erlangung des Titels „Network Administrator“ jedoch **nicht** aus.

Bedarf oder Auslöser für das Performancemanagement ergeben sich durch regelmäßiges Monitoring sowie in Bedarfsfällen. Das Performancemanagement wird mit Hilfe der Anwendung 46020 ausgeführt. Der Network Administrator kann mit seinen Administrationsrechten alle Messungen durchführen. Die erste Performancemessung ist das lokale Auslesen der cpu, swap, interrupts und errors. Dies bezieht sich auf die lokale Sichtstation und mit den entsprechenden Rechten auch auf die Server. Bei jeder Performancemessung muss sich der Network Administrator an der Sichtstation mit einem Benutzernamen und Passwort anmelden. Hier ruft er ein Menü auf, dass z.B. die Leitungsauslastung darstellt. Ein Diagramm erscheint und man kann hier z.B. die TX und RX Bytes sehen.

### 3.4 Securitymanagement

---

In diesem Abschnitt wird das Securitymanagement in Form

- eines Referenzprozesses
- einer detaillierteren Darstellung der einzelnen Teilprozesse
- einer beispielhaften Ausgestaltung des Prozesses Securitymanagement

dargestellt.

Dabei wird jeweils der gesamte Prozess dargestellt, um mögliche Aufgaben neben den Kernaufgabenfeldern aufzuzeigen.



### 3.4.1 Referenzprozess Securitymanagement

Das folgende Ablaufdiagramm zeigt allgemein den Prozess des Securitymanagements. Eine konkrete Ausgestaltung dieses Prozesses sollte in der Weiterbildung daran orientiert werden.

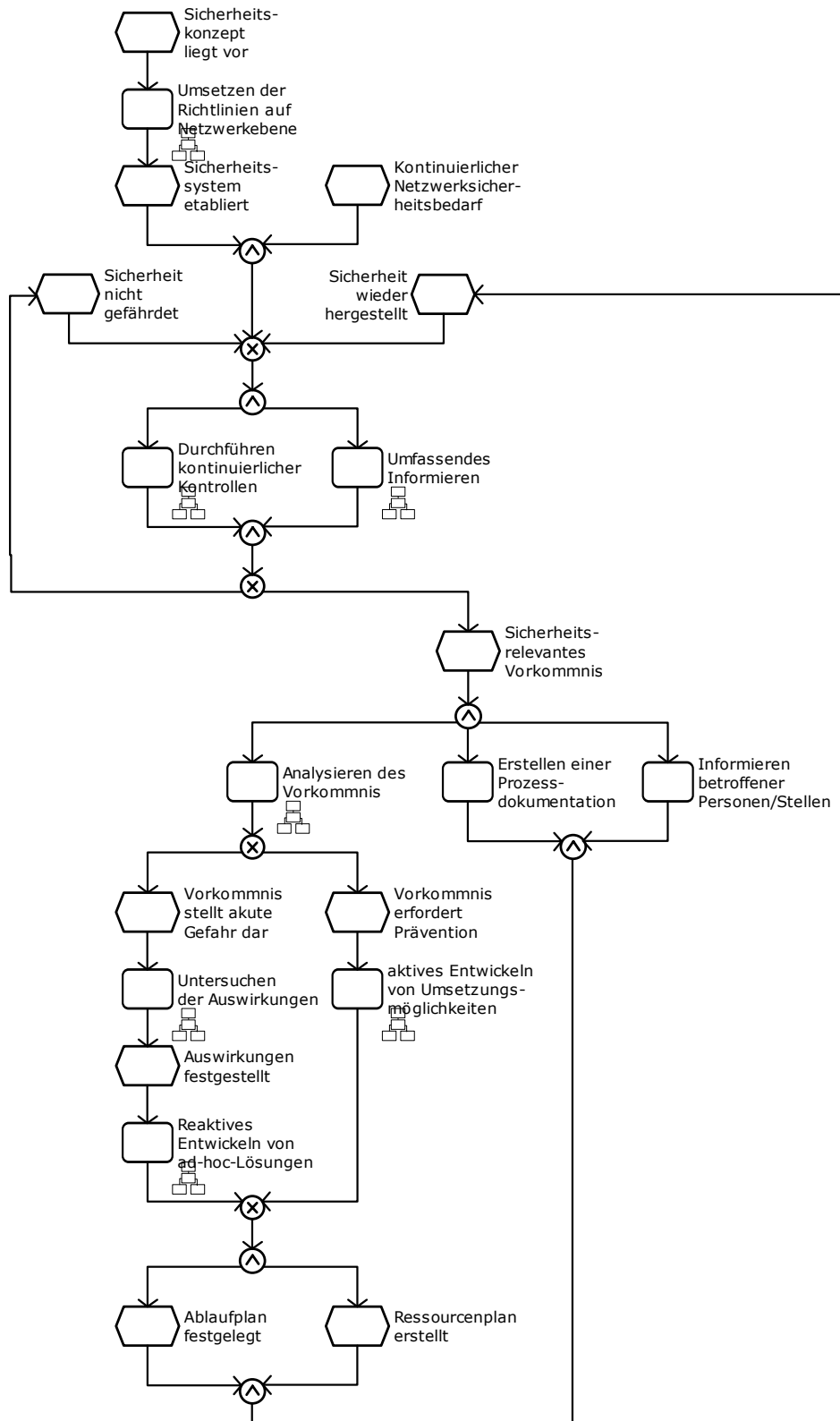


Abbildung: Referenzprozess 4: Securitymanagement, Teil 1



### **3.4.2 Prozesskompass Securitymanagement**

1. Umsetzen der Richtlinien auf Netzwerkebene
2. Durchführen kontinuierlicher Kontrollen
3. Umfassendes Informieren
4. Analysieren des Vorkommnisses
5. Erstellen einer Prozessdokumentation
6. Informieren betroffener Personen/Stellen
7. Untersuchen der Auswirkungen
8. Aktives Entwickeln von Umsetzungsmöglichkeiten
9. Reaktives Entwickeln von Ad-hoc-Lösungen
10. Ausführen Changemanagement
11. Ausführen Sicherheitscheck

### 3.4.3 Teilprozesse Securitymanagement

In diesem Abschnitt werden die Teilprozesse des Securitymanagements abgebildet.

#### 3.4.3.1 Umsetzen der Richtlinien auf Netzwerkebene

Eine jede Organisation stellt Richtlinien auf, die den Umgang mit sicherheitsrelevanten Daten und Objekten regeln. Diese Richtlinien müssen auf Netzwerkebene (so wie in jedem anderen Bereich auch) umgesetzt werden. Dazu müssen betroffene Netzwerkkomponenten ermittelt werden und für diese Komponenten eine entsprechende Konfiguration aus dem allgemeinen Sicherheitskonzept abgeleitet werden. Um das umzusetzen, bedient man sich des Changemanagements. Letztendlich erhält man ein den Richtlinien entsprechendes Sicherheitssystem.

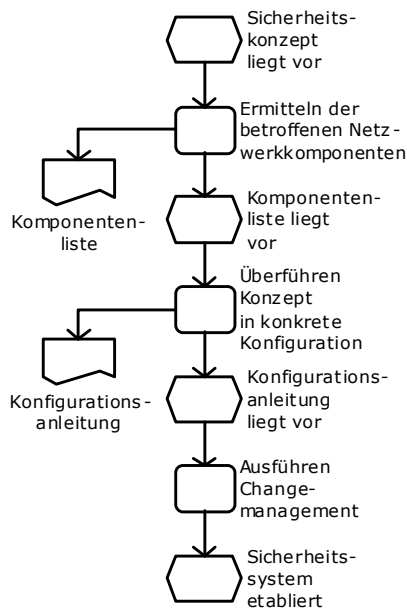


Abbildung 23: Umsetzen der Richtlinien auf Netzwerkebene

##### 3.4.3.1.1 Tätigkeiten: Umsetzen der Richtlinien auf Netzwerkebene

- Ermitteln der (von den Richtlinien) betroffenen Netzwerkkomponenten
- Überführen des Konzepts in konkrete Konfiguration
- Ausführen Changemanagement

##### 3.4.3.1.2 Kompetenzfelder: Umsetzen der Richtlinien auf Netzwerkebene

Fähigkeiten/Fertigkeiten

- Betroffene Netzwerkkomponenten ermitteln können
- Konzept in konkrete Konfiguration überführen können
- Changemanagement ausführen können
- Dokumentieren können

Wissen

- Netzwerkdimension
- Netzwerkorganisation
- Kommunikationsarchitektur
- Betriebsarten

- Sitzungscharakterisierung
- Hardware
- Aktive Komponenten
- Passive Komponenten
- Topologien
- Strukturierte Verkabelung
- Protokolle
- Referenzmodelle
- Standards
- Schnittstellen
- Übertragungssysteme, -techniken
- Übertragungsmedien
- Elektrotechnik
- Systemsoftware/Betriebssysteme
- Prozess- und Organisationskenntnisse
- Dokumentationsstandards
- Technisches Englisch

### 3.4.3.2 Durchführen kontinuierlicher Kontrollen

Verfügt man über das Sicherheitssystem und hat man einen entsprechenden Bedarf an Netzwerksicherheit, dann kann man eine kontinuierliche Kontrolle des Netzwerks anstreben. Dazu überwacht der Network Administrator die Ausgaben der Sicherheitseinrichtungen bzw. prüft manuell auf ungewöhnliche Vorkommnisse. Die Ergebnisse der Prüfung bzw. der Ausgabe werden dann ausgewertet und auf ihre Relevanz hin geprüft. Diese Überprüfung ergibt, ob es sich um ein sicherheitsgefährdendes Ereignis handelt oder nicht.

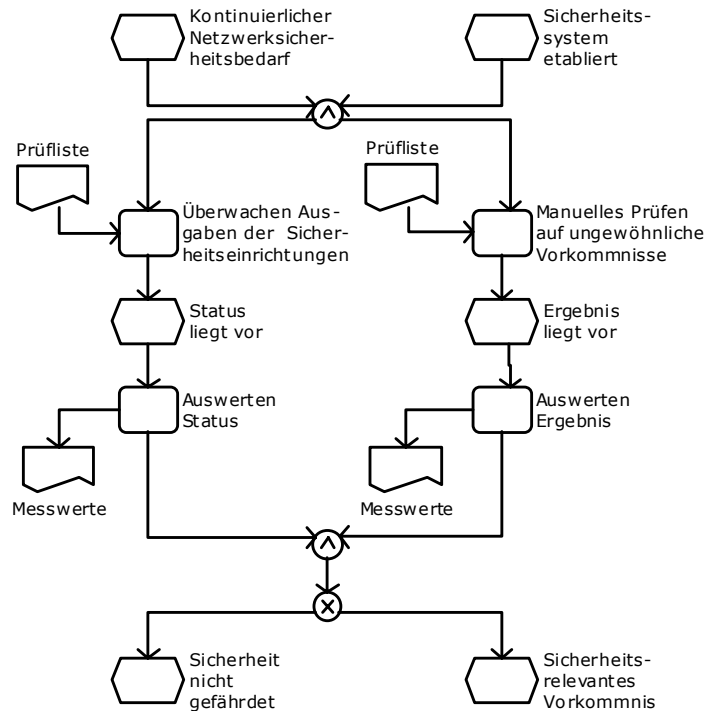


Abbildung 24: Durchführen kontinuierlicher Kontrollen

#### 3.4.3.2.1 Tätigkeiten: Durchführen kontinuierlicher Kontrollen

- Manuelles Prüfen auf ungewöhnliche Vorkommnisse
- Auswerten Ergebnisse
- Überwachen der Ausgaben der Sicherheitseinrichtungen
- Status auswerten

#### 3.4.3.2.2 Kompetenzfelder: Durchführen kontinuierlicher Kontrollen

Fähigkeiten/Fertigkeiten

- Auf ungewöhnliche Vorkommnisse (manuell) prüfen können
- Ergebnisse (der Prüfung) auswerten/interpretieren können
- Ausgaben der Sicherheitseinrichtungen überwachen können
- Status auswerten/interpretieren können
- Dokumentieren können

Wissen

- Netzwerkdimension
- Netzwerkorganisation
- Kommunikationsarchitektur
- Betriebsarten

- Sitzungscharakterisierung
- Hardware
- Aktive Komponenten
- Passive Komponenten
- Protokolle
- Standards
- Schnittstellen
- Übertragungssysteme, -techniken
- Übertragungsmedien
- Systemsoftware/Betriebssysteme
- Prozess- und Organisationskenntnisse
- Netzwerkmanagementsysteme
- Messverfahren
- Fernzugriffsverfahren
- Dokumentationsstandards
- Technisches Englisch

### 3.4.3.3 Umfassendes Informieren

Parallel zu den kontinuierlichen Kontrollen werden einschlägige Informationsquellen nach aktuellen Sicherheitsbedenken abgefragt. Die Bedeutung dieser Ergebnisse muss der Network Administrator dann auf die Bedeutung für das eigene Netzwerk hin überprüfen. Diese Überprüfung ergibt, ob es sich um ein sicherheitsgefährdendes Ereignis handelt oder nicht.

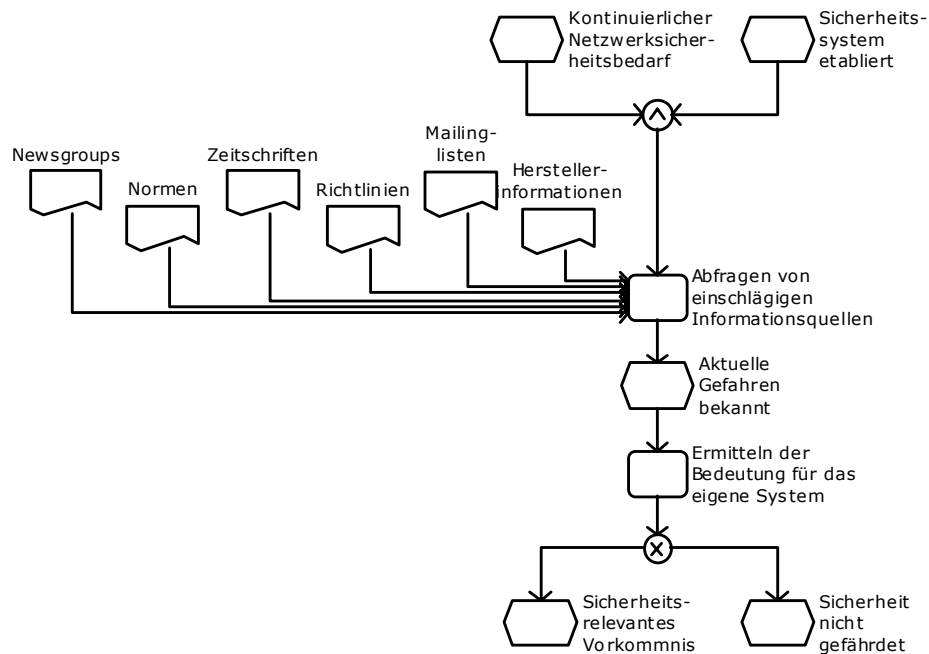


Abbildung 25: Umfassendes Informieren

#### 3.4.3.3.1 Tätigkeiten: Umfassendes Informieren

- Abfragen von einschlägigen Informationsquellen
- Ermitteln der Bedeutung für das eigene System

#### 3.4.3.3.2 Kompetenzfelder: Umfassendes Informieren

Fähigkeiten/Fertigkeiten

- Informationsquellen (selbst) recherchieren können
- Informationsquellen (themenspezifisch) abfragen können
- Informationen analysieren können
- Bedeutung für das eigene System ermitteln können
- Dokumentieren können

Wissen

- Informationsquellen
- Dokumentationsstandards



#### 3.4.3.4 Analysieren des Vorkommnisses

Ergibt die Kontrolle bzw. das Informieren ein sicherheitsrelevantes Vorkommnis für das Netzwerk, werden zuerst die betroffenen Knoten ermittelt. Sind diese bekannt, muss der Network Administrator das Bedrohungspotential abschätzen. Hier muss er entscheiden, ob es sich um eine akute Gefährdung handelt oder ob dem Vorkommnis präventiv begegnet werden muss.

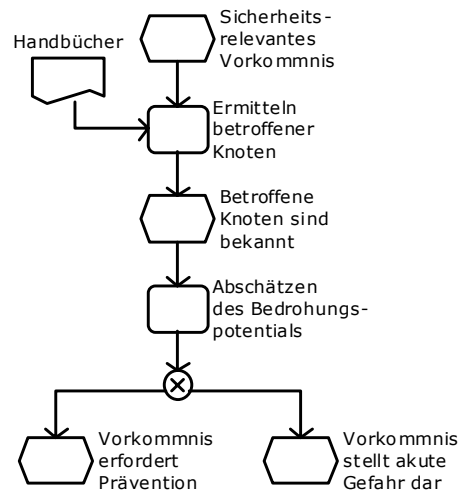


Abbildung 26: Analysieren des Vorkommnisses

##### 3.4.3.4.1 Tätigkeiten: Analysieren des Vorkommnisses

- Ermitteln betroffener Knoten
- Abschätzen des Bedrohungspotentials

##### 3.4.3.4.2 Kompetenzfelder: Analysieren des Vorkommnisses

Fähigkeiten/Fertigkeiten

- Betroffene Knoten ermitteln können
- Bedrohungspotential (für das eigene Netzwerk) abschätzen können
- Dokumentieren können

Wissen

- Netzwerkdimension
- Netzwerkorganisation
- Aktive Komponenten
- Passive Komponenten
- Übertragungssysteme, -techniken
- Übertragungsmedien
- Prozess- und Organisationskenntnisse
- Netzwerkmanagementsysteme
- Messverfahren
- Fernzugriffsverfahren
- Dokumentationsstandards

### 3.4.3.5 Untersuchen der Auswirkungen

Geht von dem Vorkommnis eine akute Gefährdung aus, so muss der Network Administrator prüfen, ob der Angreifer (sofern es einen gibt) noch aktiv ist, die Schädigungen feststellen und ermitteln, ob es zu Informationsübertragungen gekommen ist. Als Ergebnis werden die Auswirkungen des Vorkommnisses festgestellt.

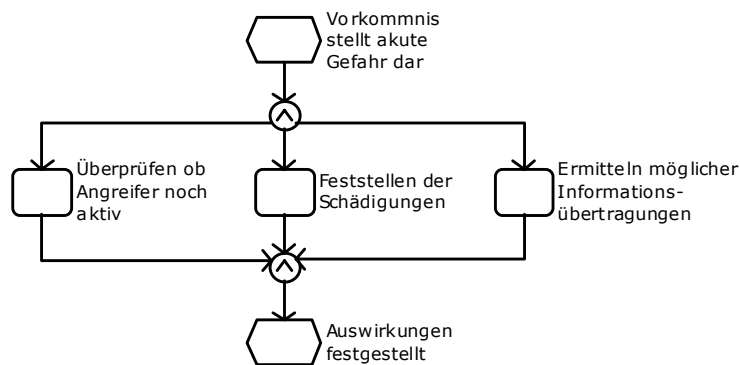


Abbildung 27: Untersuchen der Auswirkungen

#### 3.4.3.5.1 Tätigkeiten: Untersuchen der Auswirkungen

- Überprüfen, ob Angreifer noch aktiv ist
- Feststellen der Schädigungen
- Ermitteln möglicher Informationsübertragungen

#### 3.4.3.5.2 Kompetenzfelder: Untersuchen der Auswirkungen

Fähigkeiten/Fertigkeiten

- Aktivitäten von Angreifern überprüfen können
- Schädigungen feststellen können
- Mögliche Informationsübertragungen ermitteln können
- Dokumentieren können

Wissen

- Netzwerkdimension
- Netzwerkorganisation
- Kommunikationsarchitektur
- Sitzungscharakterisierung
- Standards
- Schnittstellen
- Netzwerkmanagementsysteme
- Messverfahren
- Fernzugriffsverfahren
- Dokumentationsstandards

### 3.4.3.6 Reaktives Entwickeln von ad-hoc-Lösungen

Sind die Auswirkungen festgestellt, müssen (alternative) Lösungswege (inkl. Ressourcen- und Ablaufplan) gefunden werden, über deren Verwirklichung der Network Administrator dann entscheiden muss. Das Ergebnis ist ein erstellter Ressourcenplan und ein festgelegter Ablaufplan.

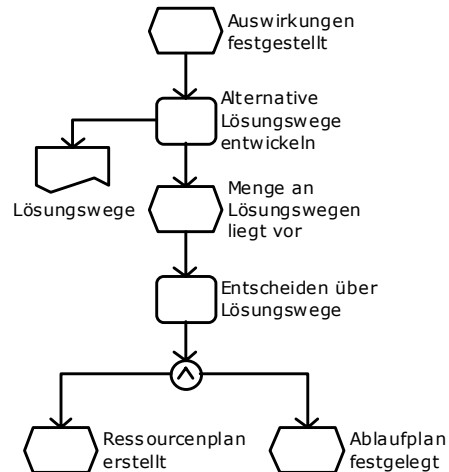


Abbildung 28: Reaktives Entwickeln von ad-hoc-Lösungen

#### 3.4.3.6.1 Tätigkeiten: Reaktives Entwickeln von ad-hoc-Lösungen

- Entwickeln alternativer Lösungswege
- Entscheiden über Lösungswege

#### 3.4.3.6.2 Kompetenzfelder: Reaktives Entwickeln von ad-hoc-Lösungen

Fähigkeiten/Fertigkeiten

- Alternative Lösungswege entwickeln können
- Über Lösungswege entscheiden können
- Dokumentieren können

Wissen

- Konkrete Sicherheitslücke
- Prozess- und Organisationskenntnisse
- Dokumentationsstandards
- Technisches Englisch

### 3.4.3.7 Aktives Entwickeln von Umsetzungsmöglichkeiten

Sollte dem Vorkommnis präventiv begegnet werden, muss der Network Administrator alle betroffenen Systeme ermitteln. Sind diese bekannt, muss er Umsetzungsstrategien zur Prävention entwickeln. Ergebnis dieser Handlung sind wiederum ein Ressourcen- und ein Ablaufplan.

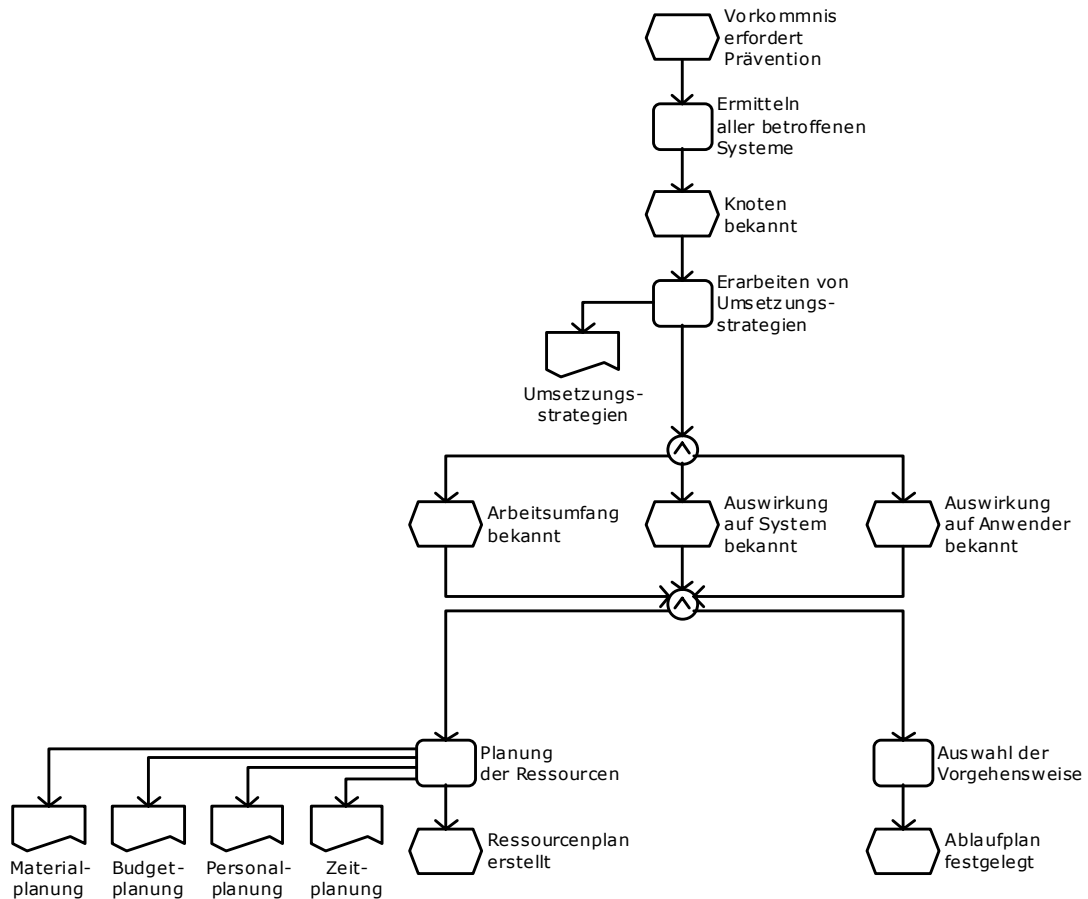


Abbildung 29: Aktives Entwickeln von Umsetzungsmöglichkeiten

#### 3.4.3.7.1 Tätigkeiten: Aktives Entwickeln von Umsetzungsmöglichkeiten

- Ermitteln aller betroffenen Systeme
- Erarbeiten von Umsetzungsstrategien
- Planen der Ressourcen
- Auswählen der Vorgehensweise
- Entscheiden über Lösungswege

#### 3.4.3.7.2 Kompetenzen: Aktives Entwickeln von Umsetzungsmöglichkeiten

Fähigkeiten/Fertigkeiten

- Alle betroffenen Systeme ermitteln können
- Umsetzungsstrategien erarbeiten können
- Ressourcen planen können
- Vorgehensweise auswählen können
- Über Lösungswege entscheiden können
- Dokumentieren können

## Wissen

- Potentielle Sicherheitslücke
- Prozess- und Organisationskenntnisse
- Dokumentationsstandards
- Technisches Englisch

### 3.4.3.8 Ausführen Changelogmanagement

Stehen der Ressourcen- und der Ablaufplan fest, bedient man sich zur Umsetzung des Changelogmanagements, das bereits in Abschnitt 3.1.1 beschrieben wurde.

### 3.4.3.9 Ausführen Sicherheitscheck

Ist das Changelogmanagement vollzogen, führt man einen abschließenden Sicherheitscheck durch, um sicherzugehen, dass die Sicherheitslücke tatsächlich geschlossen worden ist. Dazu prüft der Network Administrator die konkrete Sicherheitslücke sowie auf mögliche Seiteneffekte. Außerdem muss geprüft werden, ob nach der Veränderung des Netzwerks nach dem Changelogmanagement die Richtlinien noch eingehalten werden oder ob diese angepasst werden müssen. Sind die Richtlinien nicht eingehalten worden, so müssen entweder die Richtlinien angepasst werden (sofern dies möglich ist) oder das System (also das Netzwerk) muss auf die Richtlinien abgestimmt werden, was einen erneuten Changelogmanagement-Prozess nach sich zieht. Ergebnis dieses Teilprozesses ist die wiederhergestellte Netzwerksicherheit.

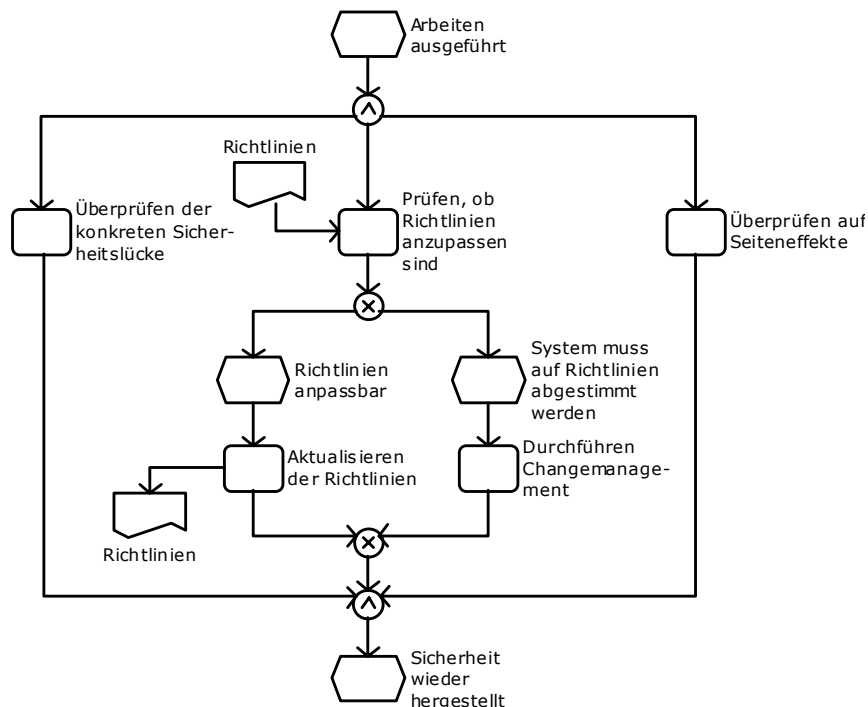


Abbildung 30: Ausführen Sicherheitscheck

#### 3.4.3.9.1 Tätigkeiten: Ausführen Sicherheitscheck

- Überprüfen der konkreten Sicherheitslücke
- Überprüfen auf Seiteneffekte
- Prüfen, ob Richtlinien anzupassen sind

Falls Richtlinien anpassbar sind

- Aktualisieren der Richtlinien

Falls System auf Richtlinien abgestimmt werden muss

- Ausführen Changelogmanagement

#### 3.4.3.9.2 Kompetenzfelder: Ausführen Sicherheitscheck

Fähigkeiten/Fertigkeiten

- Beseitigung der konkreten Sicherheitslücke überprüfen können

- Mögliche Seiteneffekte identifizieren können
- Mögliche Seiteneffekte überprüfen können
- Notwendigkeit zur Anpassung von Richtlinien prüfen können
- Richtlinien aktualisieren können
- Changemanagement ausführen können
- Dokumentieren können

#### Wissen

- Netzwerkdimension
- Netzwerkorganisation
- Kommunikationsarchitektur
- Betriebsarten
- Sitzungscharakterisierung
- Hardware
- Aktive Komponenten
- Passive Komponenten
- Topologien
- Strukturierte Verkabelung
- Protokolle
- Referenzmodelle
- Standards
- Schnittstellen
- Übertragungssysteme, -techniken
- Übertragungsmedien
- Elektrotechnik
- Systemsoftware/Betriebssysteme
- Konkrete Sicherheitslücke
- Dokumentationsstandards
- Technisches Englisch

#### **3.4.3.10 Informieren betroffener Personen/Stellen**

Für dieses Kapitel gilt das Gleiche, was bereits im Kapitel 3.1.2.9 gesagt wurde. Eine Schulung bzw. Einweisung ist hier u.U. aber gar nicht notwendig.

#### **3.4.3.11 Erstellen einer Prozessdokumentation**

Für dieses Kapitel gilt das Gleiche, was bereits im Kapitel 3.1.2.10 gesagt wurde. Der Prozess „Erstellen einer Abschlussdokumentation“ fällt unter diesen Punkt.



### **3.5 Organisation und Beratung**

---

In diesem Abschnitt wird der Prozess Organisation und Beratung in Form

- eines Referenzprozesses
- einer detaillierteren Darstellung der einzelnen Teilprozesse
- einer beispielhaften Ausgestaltung des Prozesses Securitymanagement

dargestellt.

Dabei wird jeweils der gesamte Prozess dargestellt, um mögliche Aufgaben neben den Kernaufgabenfeldern aufzuzeigen.

### 3.5.1 Referenzprozess Organisation und Beratung

Das folgende Ablaufdiagramm zeigt allgemein den Prozess Organisation und Beratung. Eine konkrete Ausgestaltung dieses Prozesses sollte in der Weiterbildung daran orientiert werden.

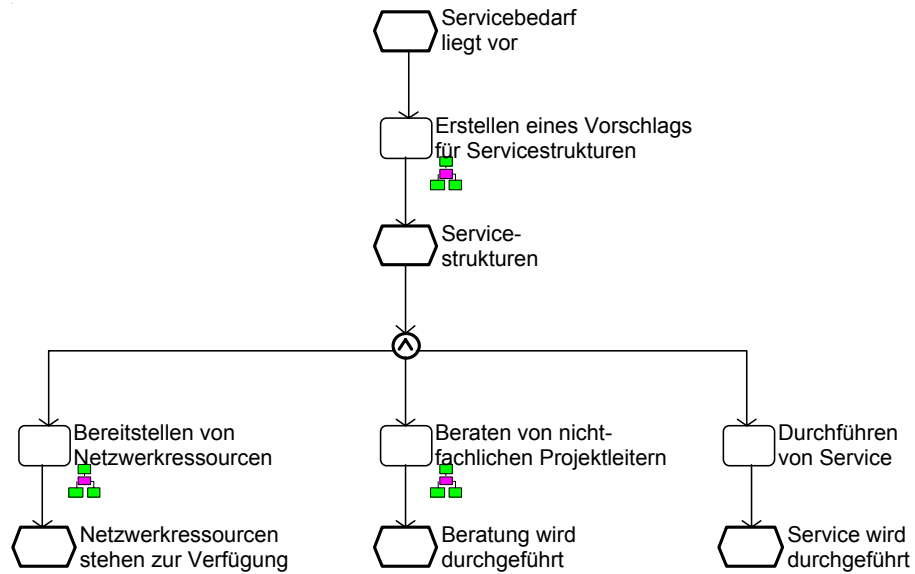


Abbildung: Referenzprozess 5: Organisation und Beratung

### **3.5.2 Prozesskompass Organisation und Beratung**

1. Erstellen eines Vorschlags für Servicestrukturen
2. Durchführen von Service
3. Beraten von nicht-fachlichen Projektleitern
4. Bereitstellen von Netzwerkressourcen

### 3.5.3 Teilprozesse Organisation und Beratung

In diesem Abschnitt werden die Teilprozesse des Prozesses Organisation und Beratung abgebildet.

#### 3.5.3.1 Erstellen eines Vorschlags für Servicestrukturen

Jeder Prozess der Organisation und Benutzerberatung beginnt mit der Erstellung eines Vorschlags für Einrichtung von Servicestrukturen. Dazu müssen die Zuständigkeiten für den Netzwerkservice geklärt werden. In Zusammenarbeit mit dem IT Service Advisor wird der Umfang des zu leistenden Services festgelegt. Nachdem diese Festlegung erfolgt ist, wird der Vorschlag für die Servicestrukturen den Entscheidern präsentiert. Im Ergebnis ist die Struktur festgelegt.

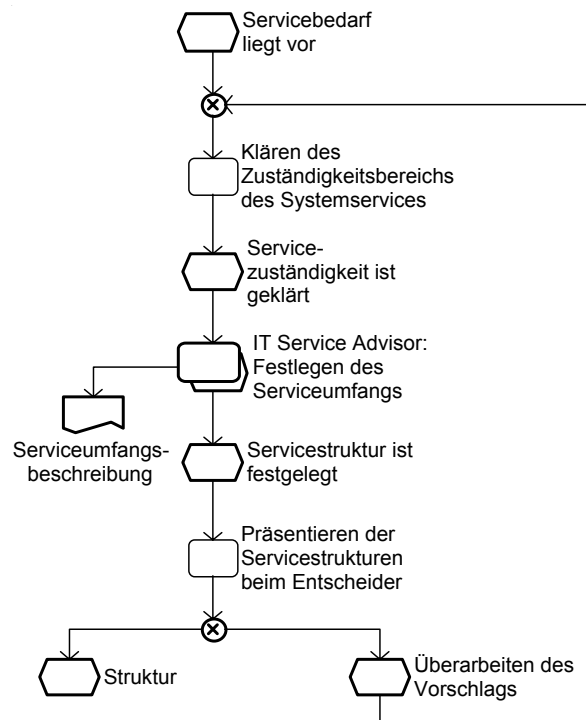


Abbildung 31: Erstellen eines Vorschlags für Servicestrukturen

##### 3.5.3.1.1 Tätigkeiten: Erstellen eines Vorschlags für Servicestrukturen

Um einen Vorschlag für die Servicestrukturen zu erstellen, muss der Network Administrator folgende Tätigkeiten durchführen:

- Klären des Zuständigkeitsbereichs des Netzwerkservices
- Zusammen mit dem IT Service Advisor: festlegen des Serviceumfangs
- Präsentieren der Servicestrukturen beim Entscheider

##### 3.5.3.1.2 Kompetenzfelder: Erstellen eines Vorschlags für Servicestrukturen

Fähigkeiten/Fertigkeiten

- Zuständigkeitsbereich des Netzwerkservice klären können
- Serviceumfang (im Team) festlegen können
- Servicestrukturen beim Entscheider präsentieren können

Wissen

- Prozess- und Organisationskenntnisse
- Dokumentationsstandards



### **3.5.3.2 Durchführen von Service**

Nachdem die Strukturen für den Service festgelegt sind, werden diese in konkrete Handlungen umgesetzt. Da die konkreten Handlungen kontextabhängig sind, können diese nicht näher spezifiziert werden.

#### **3.5.3.2.1 Tätigkeiten: Durchführen von Service**

- Je nach Servicebedarf

#### **3.5.3.2.2 Kompetenzfelder: Durchführen von Service**

Fähigkeiten/Fertigkeiten

- Servicebedarf erkennen
- Benutzeranliegen verstehen können
- Service durchführen können
- Dokumentieren können

Wissen

- Je nach Servicebedarf alle Themen, die den Service betreffen.

### 3.5.3.3 Beraten von nicht-fachlichen Projektleitern

Für dieses Kapitel gilt das Gleiche, was bereits im Kapitel 3.1.3.9 gesagt wurde.

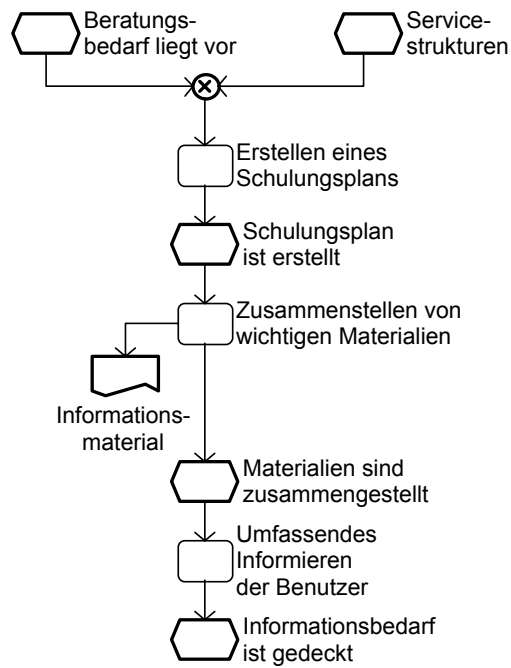


Abbildung 32: Beraten von nicht-fachlichen Projektleitern

#### 3.5.3.4 Bereitstellen von Netzwerkressourcen

Treten neue Anforderungen an das System auf, müssen diese zunächst vom Network Administrator analysiert werden. Danach wird von ihm geprüft, ob diese Anforderungen mit den derzeit zur Verfügung stehenden Ressourcen erfüllbar sind. Sind diese Anforderungen mit dem existierenden Ressourcenangebot nicht realisierbar, muss der Network Administrator ein Changemanagement durchführen, um die notwendigen Ressourcen bereitzustellen.

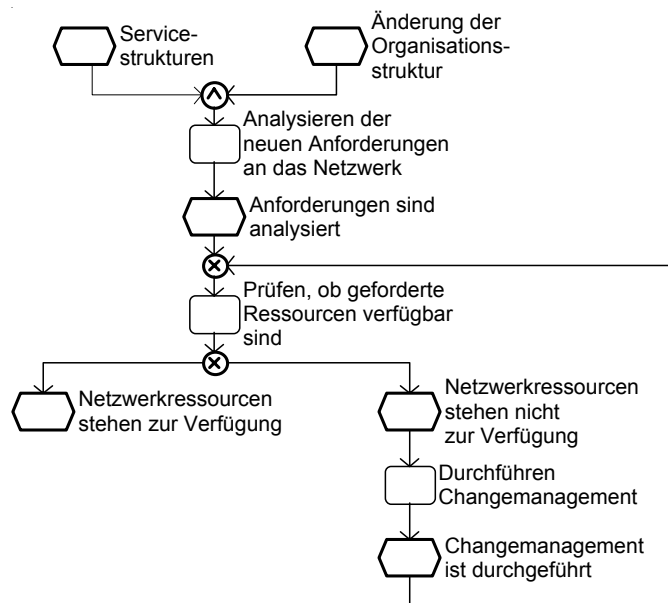


Abbildung 33: Bereitstellen von Netzwerkressourcen

##### 3.5.3.4.1 Tätigkeiten: Bereitstellen von Netzwerkressourcen

Um die notwendigen Netzwerkressourcen bereit zu stellen, muss der Network Administrator folgende Tätigkeiten durchführen:

- Analysieren der neuen Anforderungen an das Netzwerk
- Prüfen, ob geforderte Ressourcen verfügbar sind

Stehen die Netzwerkressourcen nicht zur Verfügung:

- Durchführen Changemanagement

##### 3.5.3.4.2 Kompetenzfelder: Bereitstellen von Netzwerkressourcen

Fähigkeiten/Fertigkeiten

- Anforderungen an das System analysieren können
- Ressourcenverfügbarkeit prüfen und beurteilen können
- Bedarfe abschätzen können
- Changemanagement durchführen können
- Dokumentieren können

Wissen

- Netzwerkdimensionen
- Netzwerkorganisation
- Kommunikationsarchitektur
- Betriebsarten



- Sitzungscharakterisierung
- Aktive Komponenten
- Passive Komponenten
- Topologien
- Strukturierte Verkabelung
- Standards
- Schnittstellen
- Übertragungssysteme, -techniken
- Übertragungsmedien
- Protokolle
- Referenzmodelle
- Prozess- und Organisationskenntnisse
- Spezielle Anforderung
- Dokumentationsstandards

### 3.6 Werkzeuge

---

Im Folgenden werden die Werkzeuge, die ein Network Administrator nutzt, dargestellt. Die Werkzeuge werden den Prozessen nicht direkt zugeordnet, um unübersichtliche Doppelnennungen zu vermeiden und weil es in den Teilprozessen Fault-, Performance- und Securitymanagement auf den zugrunde liegenden Störfaktor ankommt, welche Werkzeuge Verwendung finden.

Netzwerkmanagementsystem für Change-, Fault-, Security- und Performancemanagement (z.B. 46020, Netview, etc.)

Standardarbeitsplatz und Kommunikationsmedien (PC, Fax, Telefon Email, Office, Ping, Traceroute)

Fehlerraten- und Protokollmessgeräte (z.B. MOSES)

Protocolanalyzer (z.B. DA30)

Mechanisches Werkzeug

Handbücher, Dokumentationen

Intra- und Internet

Multimeter