Teil 1, Kapitel 4: Organisation des Einsatzes von IS

Betriebliche Einordnung (I)

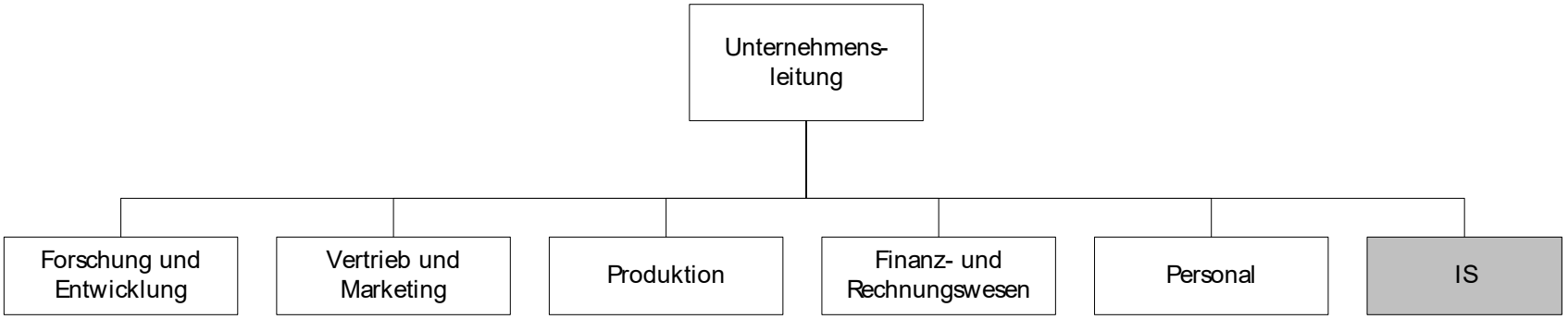


Abb. 4-1: IT-Abteilung als eine Hauptabteilung in der Linie

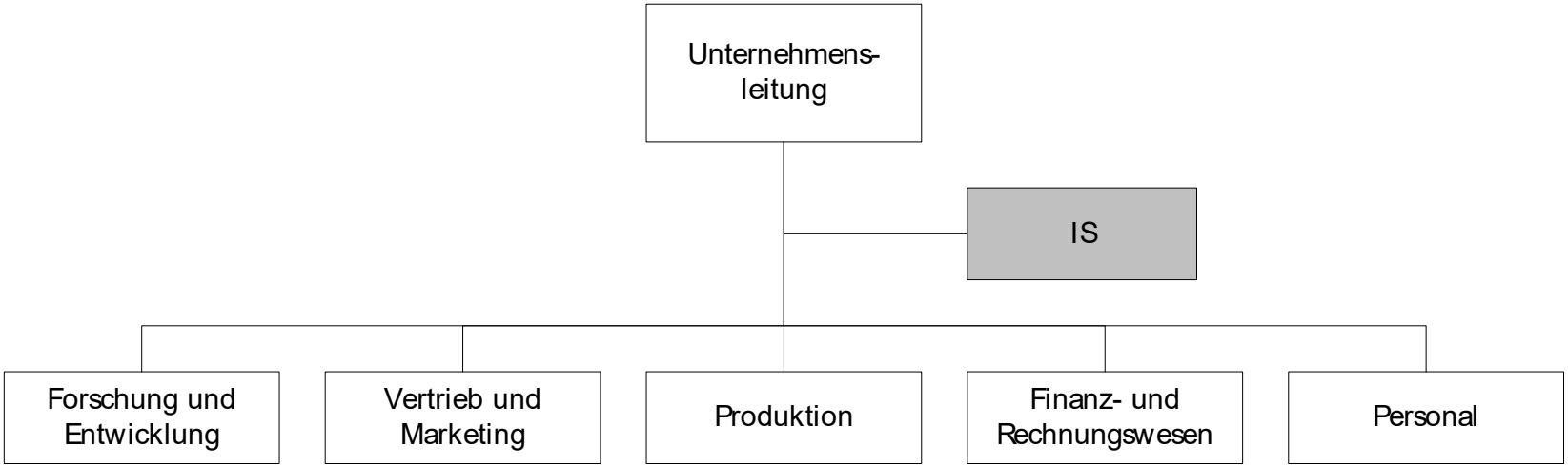


Abb. 4-2: IT-Abteilung als eine Stabsabteilung

Betriebliche Einordnung (II)

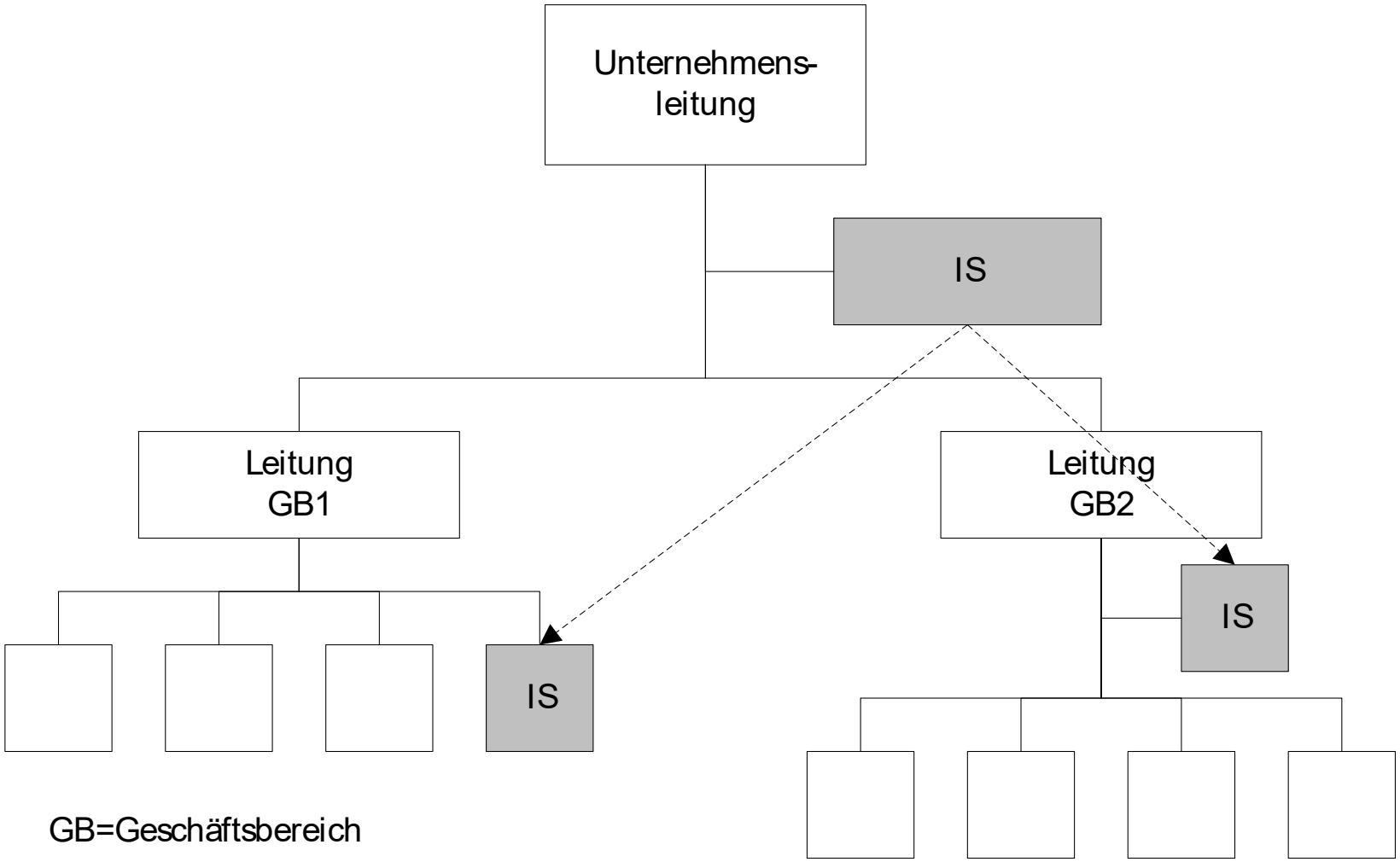
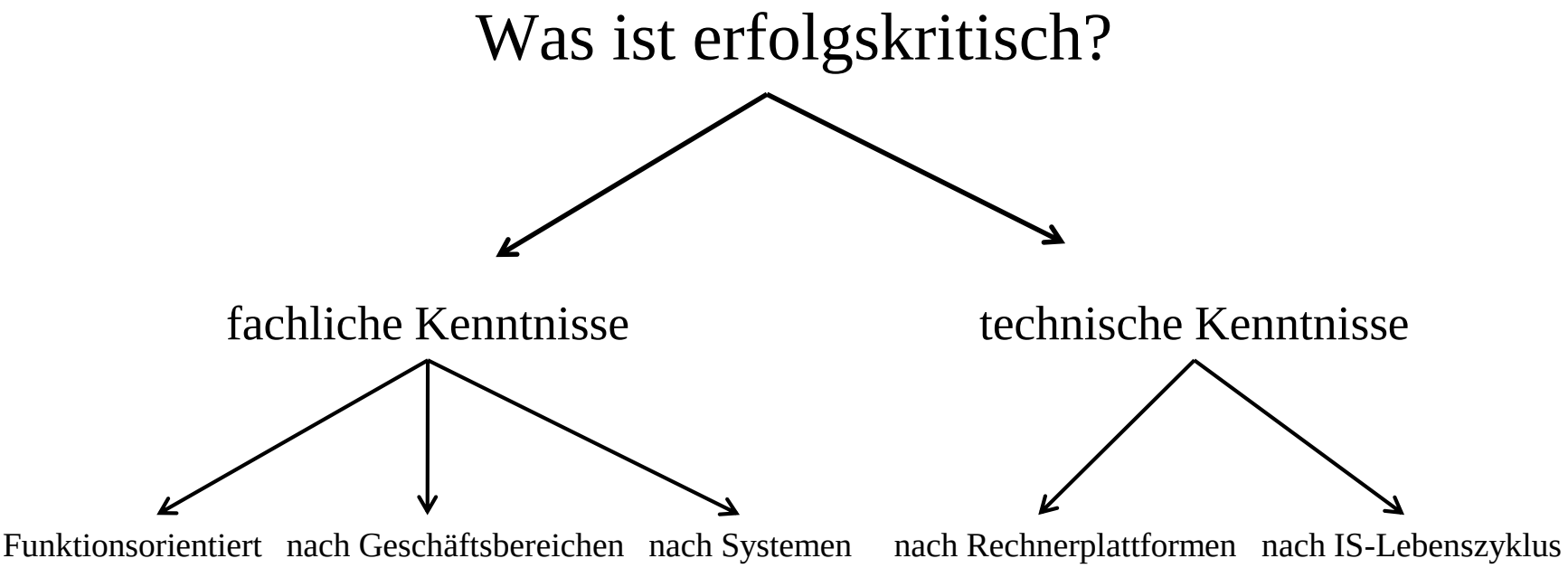


Abb. 4-3: Organisation der IT in einer divisionalisierten Unternehmung

Kriterien für die interne Organisation der IT-Abteilung



Interne Organisation der IT-Abteilung (I)

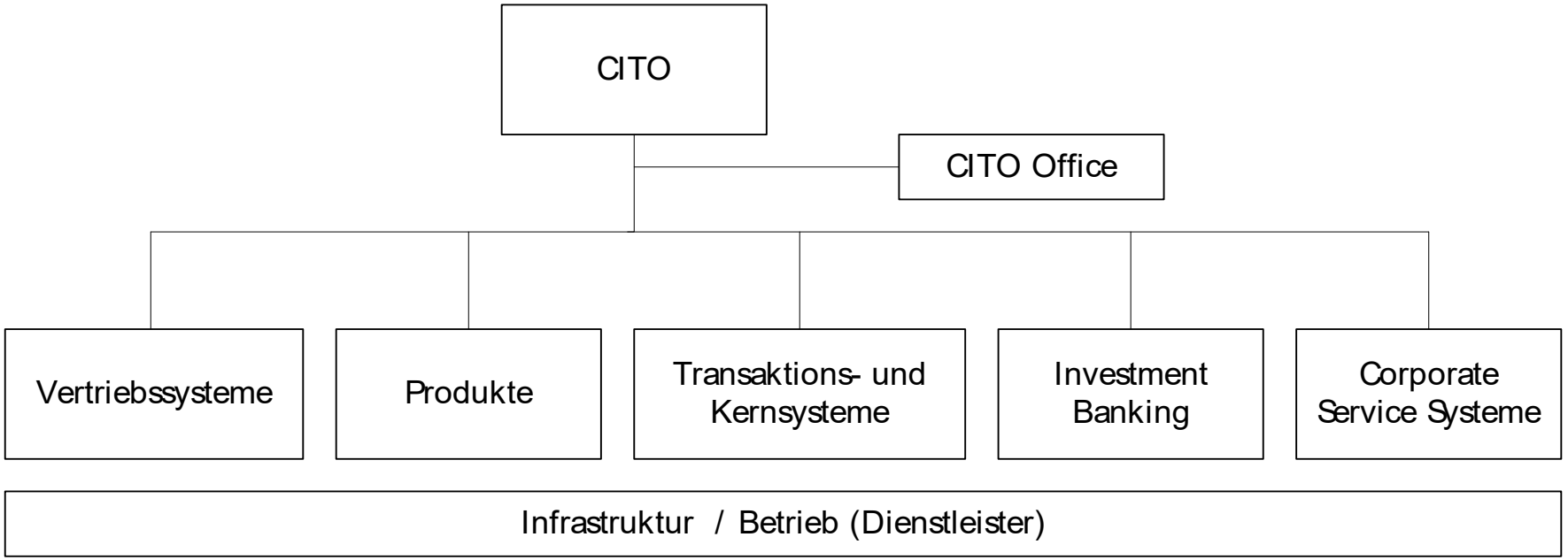


Abb. 4-4: Interne Organisation der IS-Funktion einer Bank

Interne Organisation der IT-Abteilung (II)

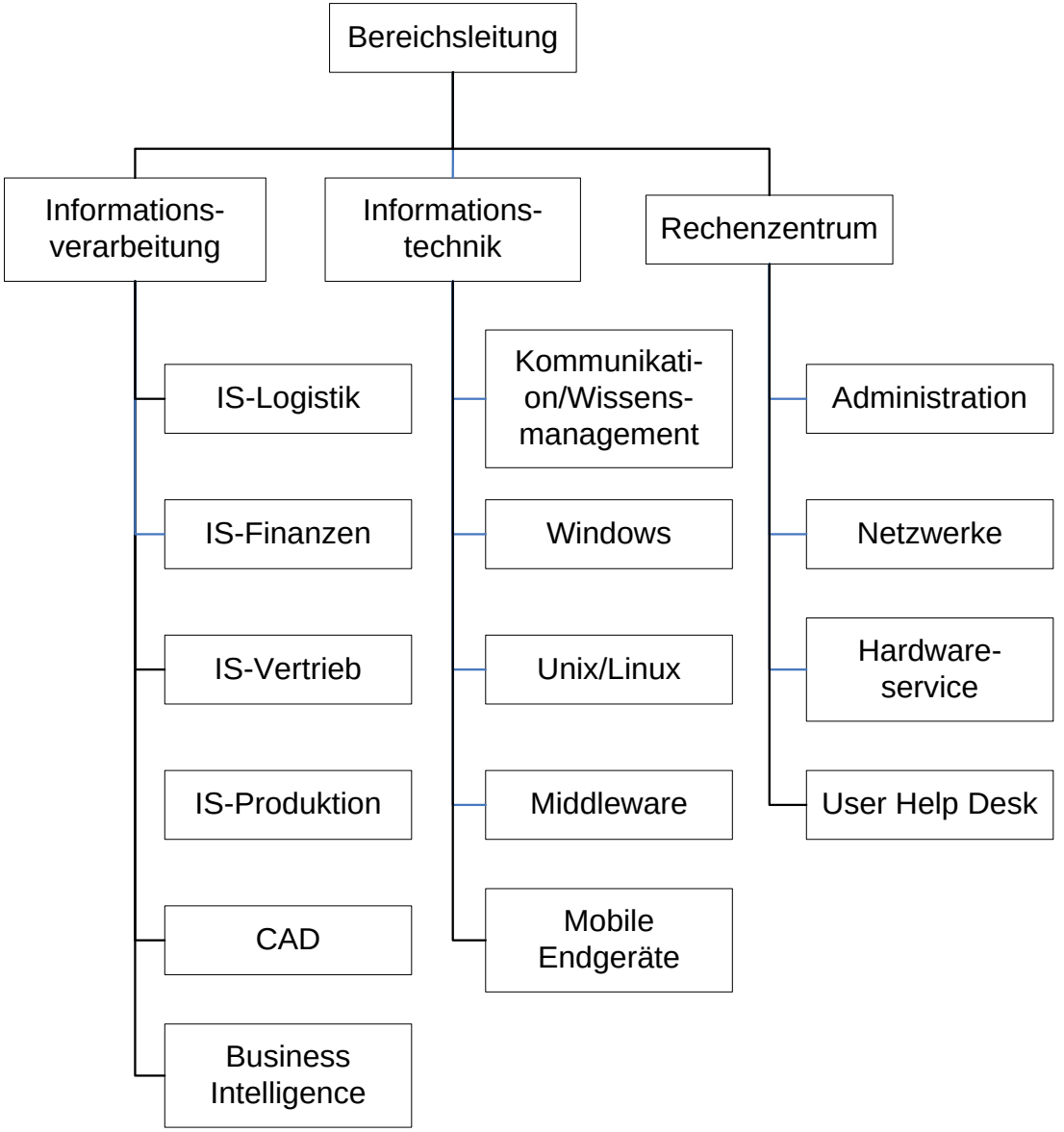


Abb. 4-5: Interne Organisation der IS-Funktion einer Industrieunternehmung

ITIL

(Information Technology Infrastructure Library)

Definition Service:
Ein Service ist eine Dienstleistung, deren Erbringung dem Serviceempfänger einen Nutzen stiftet. Dafür hält der Leistungserbringer die notwendigen Betriebsmittel und das Know-how vor und trägt die entsprechenden Kosten und Risiken (in Anlehnung an [Böttcher 2010, S.9])

Kernbereiche und Prozesse in ITIL V3

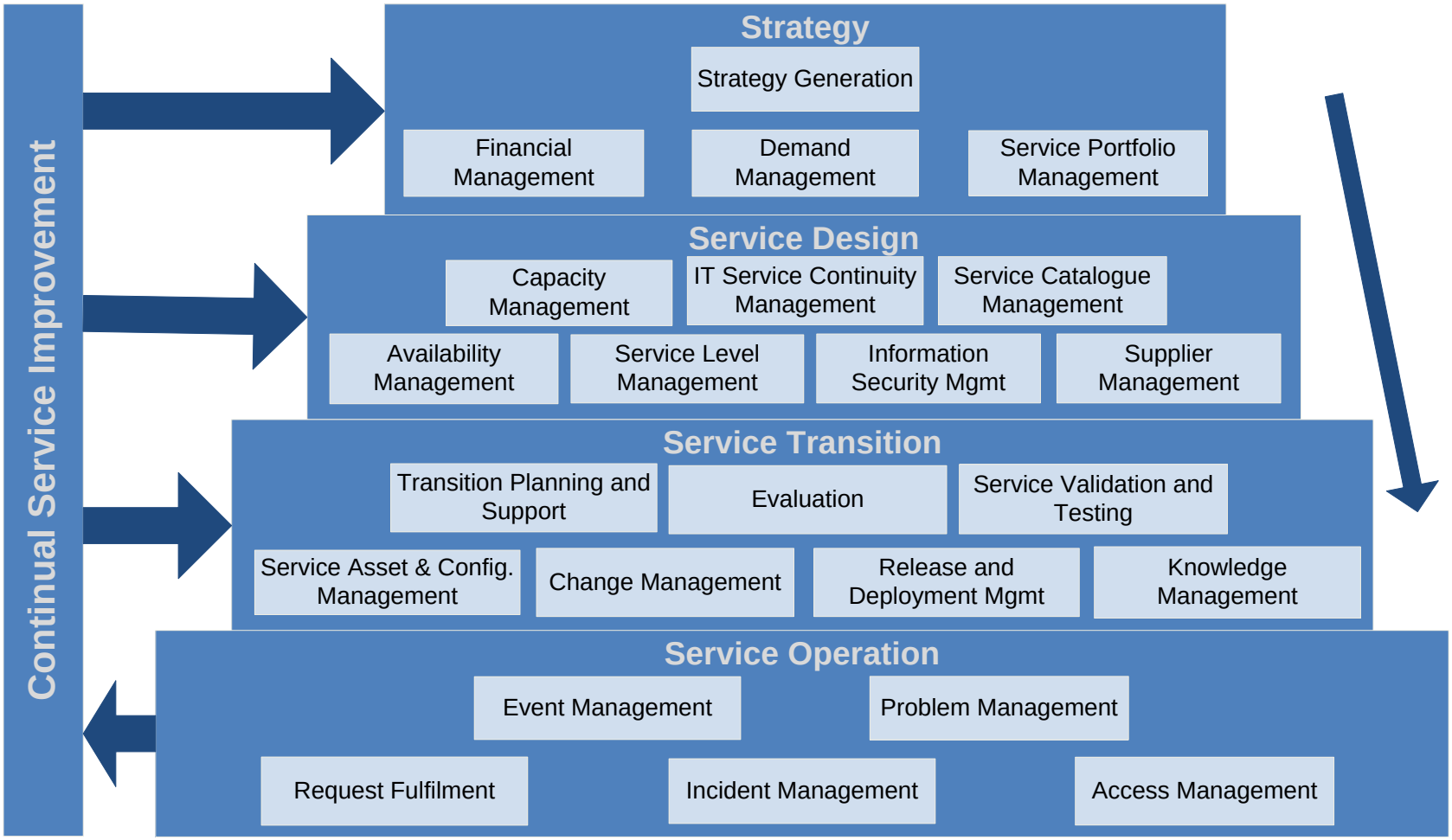


Abb. 4-6: Kernbereiche und Prozesse in ITIL V3

Kontinuierliche Verbesserung in sieben Stufen

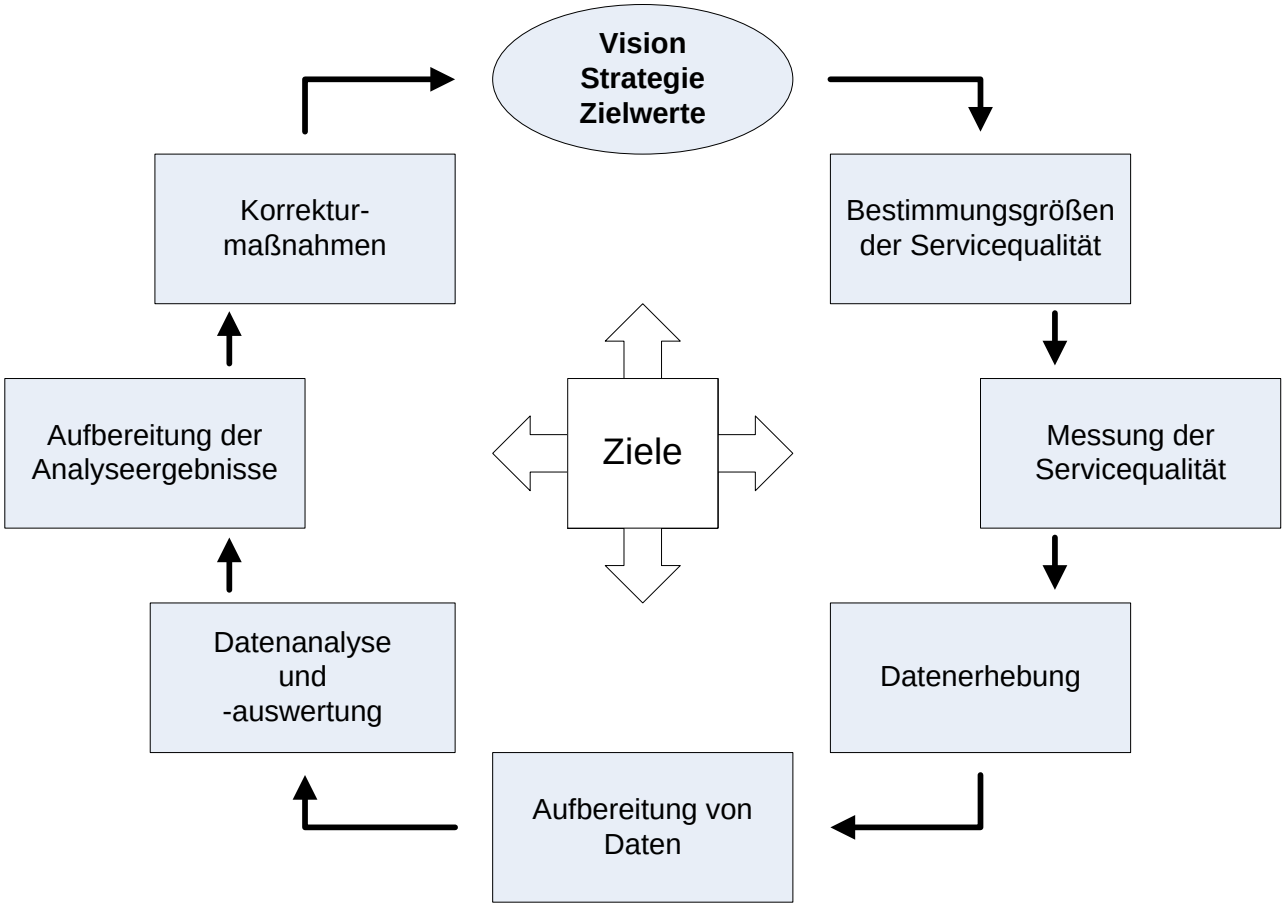


Abb. 4-7: Kontinuierliche Verbesserung in sieben Stufen (Böttcher 2010)

Beispiele für Service-Levels		
Störung	*Dienstleister*	*Wiederherstellung*
Netzwerkausfall einer Abteilung	Intern	4 Stunden
Keine Wertpapierkursversorgung	Intern	
Ausfall Server	Intern	
Ausfall SG-Gerät ohne Kundenfrequentierung	Extern	6 Stunden
Ausfall Arbeitsplatz ohne Ausweichmöglichkeit	Intern	
Zugriff auf Datenbank nicht möglich	Intern/Extern	12 Stunden
Anmeldung am Arbeitsplatz nicht möglich	Intern/Extern	
Ausfall Arbeitsplatz mit Ausweichmöglichkeit	Intern	24 Stunden
Gruppenkalender nicht nutzbar	Intern	
PDA synchronisiert nicht	Intern/Extern	40 Stunden
Druckerausfall mit Ausweichmöglichkeit	Intern/Extern	

Management der Sicherheit (I)

Relevante Gesetze und Bestimmungen

- Bundesdatenschutzgesetz (BDSG), Datenschutzgrundverordnung (DSGVO)
- Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)
- Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)
- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
- Sarbanes-Oxley-Gesetz (SOX)
- Basel II + III
- Solvency II

Management der Sicherheit (II)

Bausteine in den IT-Grundschutz-Katalogen (GSK) des Bundesamts für Sicherheit in der Informationstechnik (BSI):

- Infrastruktur (Gebäude, Räume usw.)
- IT-Systeme (Server und Clients sowie entsprechende Betriebssysteme, Telekommunikationsanlagen)
- Netze (Konzeption und Betrieb heterogener Netze inklusive Management- und Sicherheitsaspekten)
- Anwendungen (wie E-Mail, Standardsoftware und Datenbanken)

Übergreifende Konzepte:

- Datensicherheit, Virenschutz und Verschlüsselung
- Behandlung von Sicherheitsvorfällen und Outsourcing

Management der Sicherheit (III)

Bedrohungen:

- *Höhere Gewalt*
- *Organisatorische Mängel*
- *Menschliche Fehlhandlungen*
- *Technisches Versagen*
- *Vorsätzliche Handlungen*

Management der Sicherheit (IV)

Elementare Gefährdungen Anforderungen	G 0.18	G 0.19	G 0.31	G 0.44
CON.6.A1	X	X		
CON.6.A2		X		X
CON.6.A3		X	X	
CON.6.A4		X		
CON.6.A5		X		
CON.6.A6		X	X	
CON.6.A7		X	X	
CON.6.A8	X	X	X	
CON.6.A9		X		
CON.6.A10		X	X	
CON.6.A11		X		X

Tab. 4-1: Elementare Gefährdungen für den Baustein CON.6 (*Löschen und Vernichten)* [BSI 2018a]

Management der Sicherheit (V)

Gefährdungen	
G 0.18	Fehlplanung oder fehlende Anpassung
G 0.19	Offenlegung schützenswerter Informationen
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen
G 0.44	Unbefugtes Eindringen in Räumlichkeiten
Anforderungen	
CON.6.A1	Regelung der Vorgehensweise für die Löschung und Vernichtung von Informationen
CON.6.A2	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln und Informationen
CON.6.A3	Löschen der Datenträger vor und nach dem Austausch
CON.6.A4	Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern
CON.6.A5	Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern
CON.6.A6	Einweisung aller Mitarbeiter in die Methoden zur Löschung oder Vernichtung von Informationen
CON.6.A7	Beseitigung von Restinformationen
CON.6.A8	Richtlinie für die Löschung und Vernichtung von Informationen
CON.6.A9	Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern bei erhöhtem Schutzbedarf
CON.6.A10	Beschaffung geeigneter Geräte zur Löschung oder Vernichtung von Daten
CON.6.A11	Vernichtung von Datenträgern durch externe Dienstleister

Tab. 4-2: Gefährdungen und Anforderungen [BSI 2018a]

Management der Sicherheit (VI)

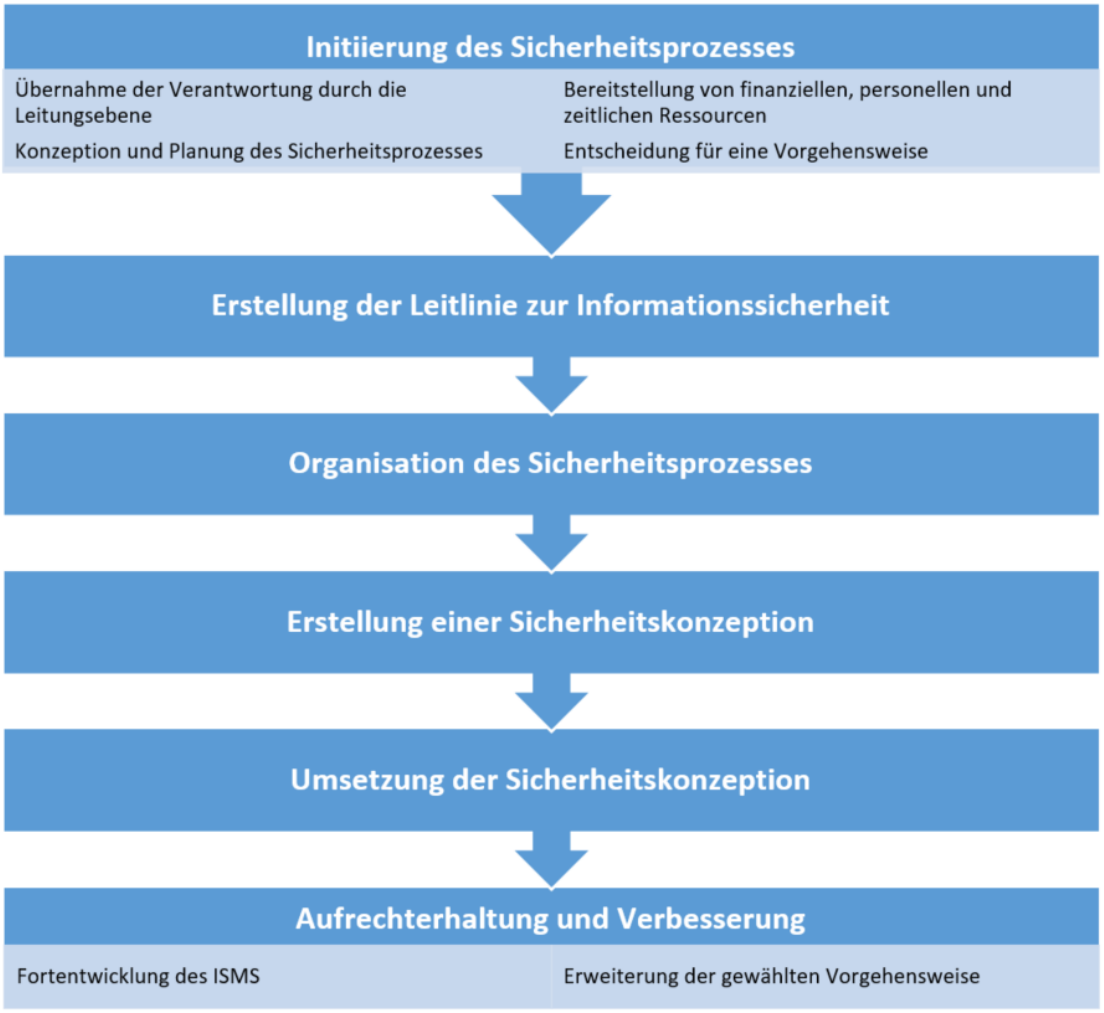


Abb. 4-8: Entwicklung des Managements der Informationssicherheit

Management der Sicherheit (VII)

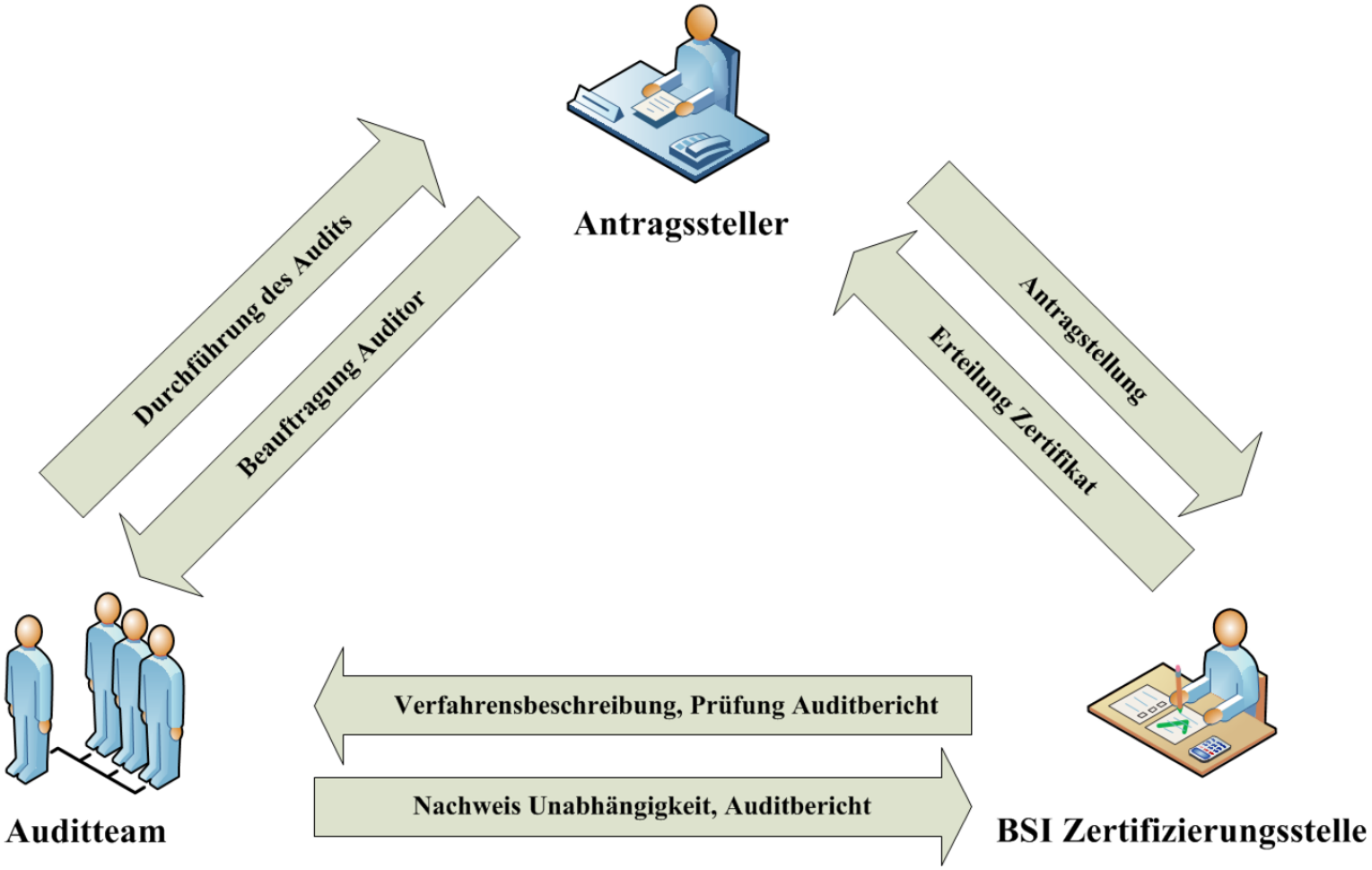


Abb. 4-9: Rollen im Zertifizierungsverfahren [BSI 2018b]

Datenschutz

DSGVO (englisch General Data Protection Regulation, GDPR)

- Gültig seit Mai 2018
- Gilt nicht für Privatpersonen
- Gilt auch für manuelle Datenverarbeitung
- Gilt für in der EU erhobene, personenbezogene Daten, auch wenn eine Identifizierung nicht stattfindet
- Verstöße mit bis zu 20 Mill. oder 4% des weltweiten Umsatzes strafbar
- Unternehmen müssen eine Datenschutzerklärung und einen (evtl. externen) Datenschutzbeauftragten haben. Beides muss leicht zugänglich sein.
- Datenschutzvorfälle müssen schnellstens gemeldet werden
- Recht auf Vergessenwerden

Blockchain

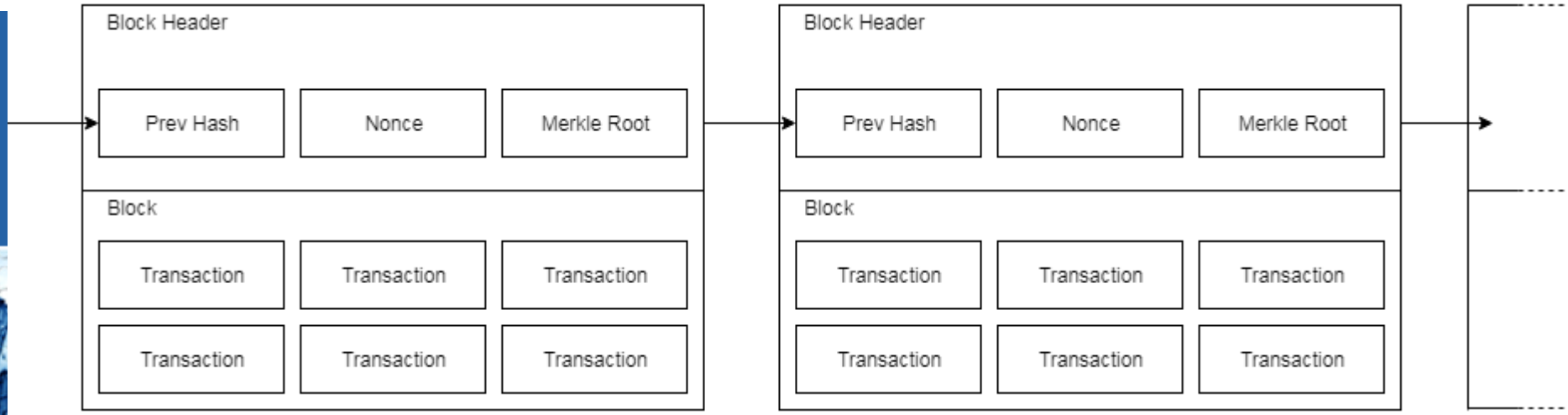


Abb. 4-10: Kettenbildung bei Bitcoins in Anlehnung an [Nakamoto 2008]

Outsourcing von IS-Funktionen

<table>
<tr><th>Spezifität
Frequenz</th><th>Niedrig</th><th>Mittel</th><th>Hoch</th></tr>
<tr><td>Selten</td><td rowspan="2">Markt</td><td colspan="2">Projekt</td></tr>
<tr><td>Häufig</td><td>Outsourcing</td><td>Hierarchie</td></tr>
</table>

Tab. 4-3: Bevorzugte Kontrollmechanismen (in Anlehnung an [Williamson 1986])

Begriffe im Kontext von Outsourcing

- *Cosourcing*
- *Insourcing*
- *Captive Sourcing*
- *Offshore-Outsourcing* oder kürzer *Offshoring*
- *Nearshoring*
- *Downsizing*
- *Rightsizing oder Rightsourcing*
- *Application Service Providing* (ASP)
- *Cloud Computing (XaaS)*

Cloud Computing

Definition:

Cloud Computing ist ein Modell, das einen bequemen Netzwerkzugang nach Bedarf zu einem gemeinsam genutzten Vorrat von konfigurierbaren Rechenressourcen (z.B. Netzwerke, Server, Speicherplatz, Anwendungen und Dienste) ermöglicht, die schnell und mit einem geringen Managementaufwand oder Anbieterinteraktion bereitgestellt und abgerufen werden können (übersetzt aus [Mell/Grance 2009])

Cloud Computing

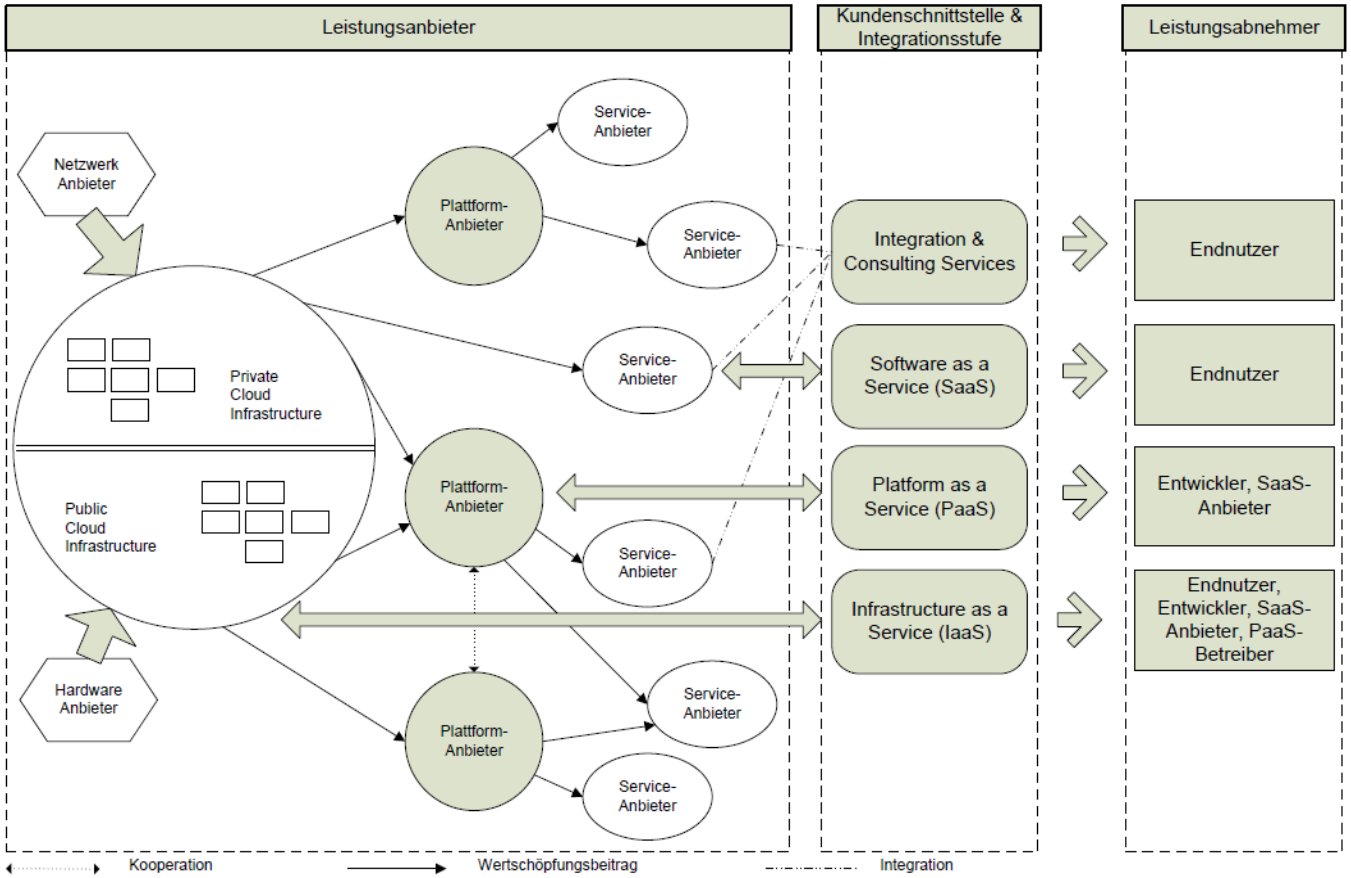


Abb. 4-11: Cloud Computing [Repschläger et al. 2010]

Cloud, Fog und Edge Computing

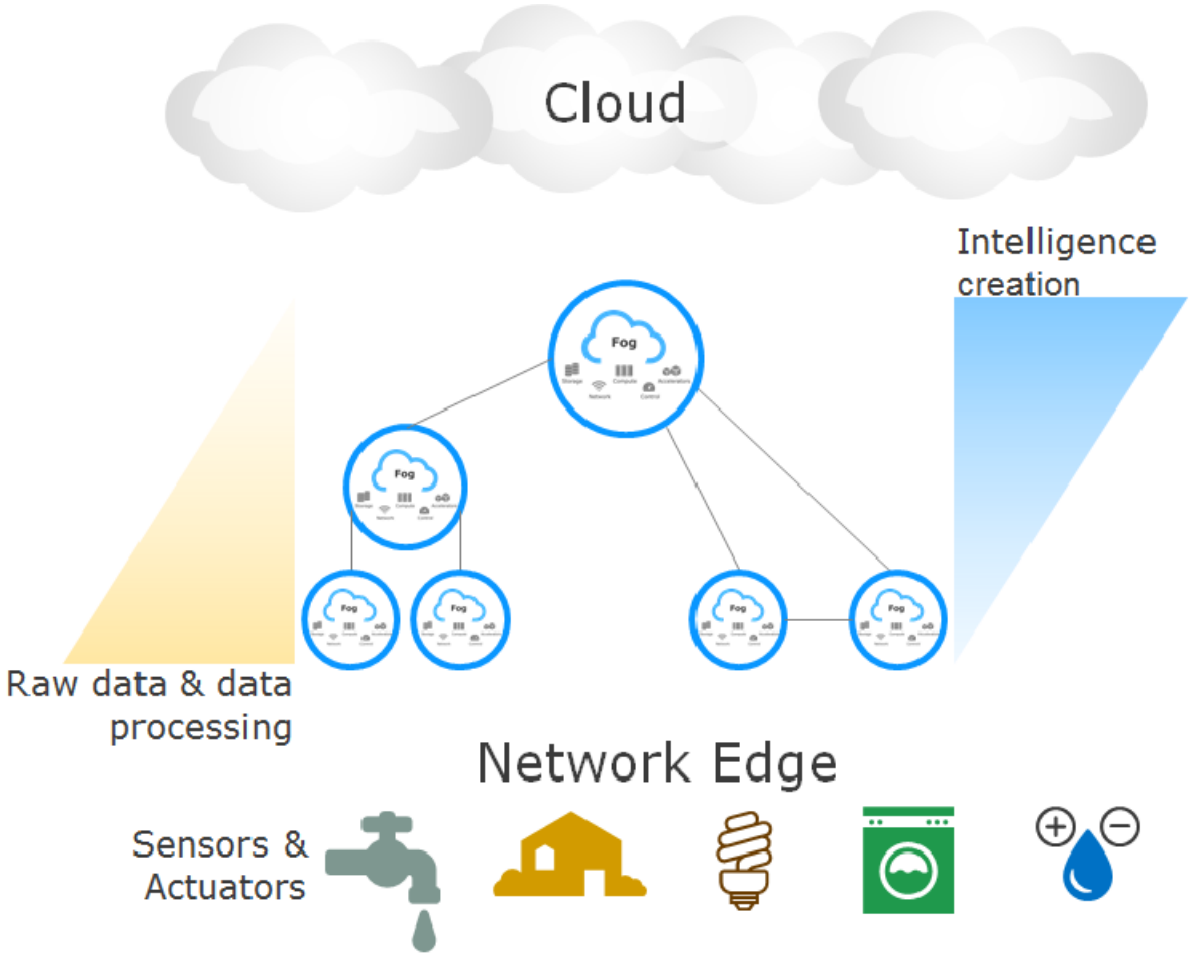


Abb. 4-12: Cloud, Fog und Edge Computing [OpenFog 2017]