Security Management in ITIL®

ein eigener Prozess mit Schnittstellen zu bestehenden Normen und Standards

Ullrike Buhl

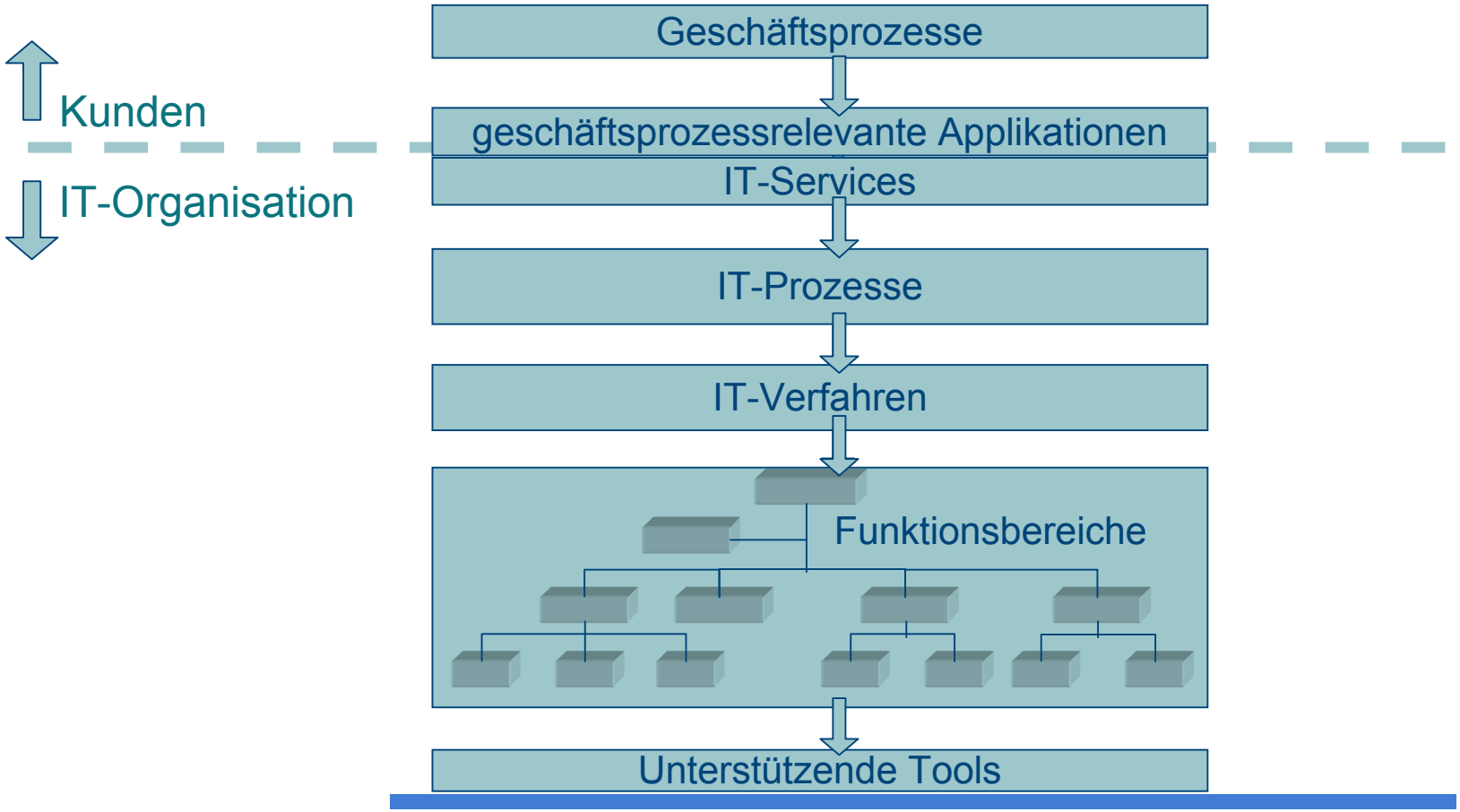
FCS Consulting & Training GmbH & Co. KG

- gegründet in 2003
- Erfahrung mit ITIL® seit 1999
- Beratung und Ausbildung zum Thema IT Service Management mit ITIL®
- Berater und Trainer sind zertifizierte ITIL® Service Manager mit langjähriger Erfahrung
- Vorbereitung von ISO 20000-Zertifizierungen (Abnahme z.B. durch TÜV Süd)
- Mitglied im itSMF e. V.

Die IT Infrastructure Library (ITIL®)

- De-facto-Standard für das IT Service Management (ITSM)
- Public Domain Framework für ITSM
- Von der OGC (Office of Government Commerce) herausgegeben
- Wird zusammen mit Vertretern aus der Praxis (Anwendern, Hersteller und Berater) weiterentwickelt
- Stellt „Best Practice"-Framework für das IT Service Management dar

Prozessmodell



Security Management nach ITIL®

Mission: Einführung und Erhaltung eines definierten Sicherheitsniveaus in der IT Organisation und geplantes Reagieren auf Security Incidents.

Vertraulichkeit (confidentiality)

Schutz der Informationen vor nicht autorisiertem Zugriff

Integrität (integrity)

Überwachung der Vollständigkeit und Korrektheit der Daten und der zugehörigen Systeme

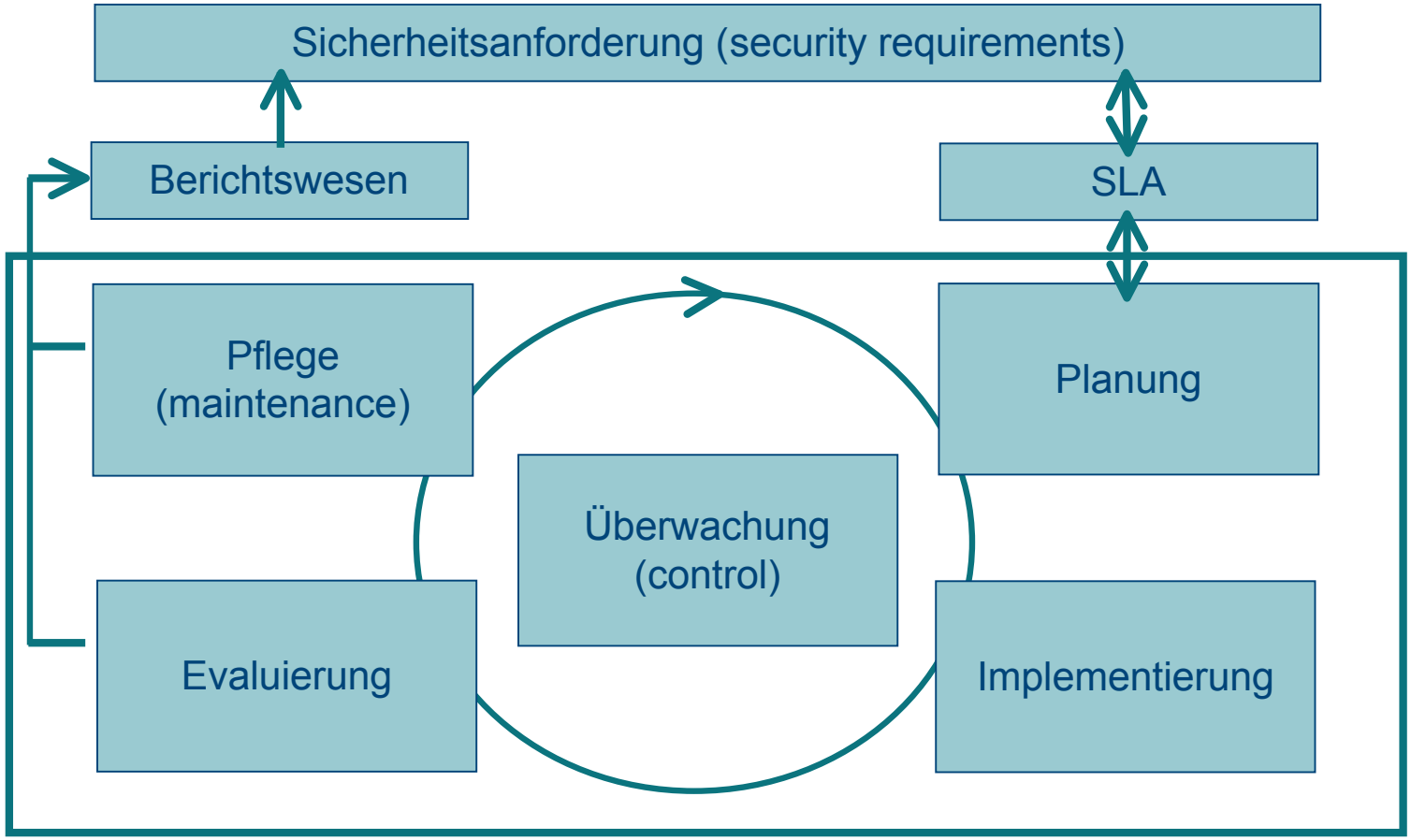
Verfügbarkeit (availability)

Stellt sicher, dass Daten verfügbar sind, wenn sie benötigt werden

Sicherheitsmaßnahmen

- Physikalische Sicherheitsmaßnahmen
- Technische Sicherheitsmaßnahmen
- Prozessorientierte Sicherheitsmaßnahmen
- Personelle Sicherheitsmaßnahmen

Security-Management-Prozess



Interaktion mit anderen Prozessen (Beispiele)

- **Change Management**
  IT Security gibt die Vorgabe für das Sicherheitsniveau, Change-Management sorgt auch während der Änderungsdurchführung für die Einhaltung
- **Incident Management**
  Jedes Security-Incident muss im Problem-Management untersucht werden
- **Release Management**
  Jedes neue Release wird nur abgenommen, wenn u.a. funktionierende Berechtigungsverfahren eingebaut sind

ITIL Security und BSI

- **BSI: Grundschutzhandbuch**
  Das „IT-Grundschutzhandbuch“ (jetzt: **IT-Grundschutz-Kataloge**) beinhalten Baustein-, Maßnahmen- und Gefährdungskataloge.

  Die Vorgehensweise nach IT-Grundschutz, Ausführungen zum IT-Sicherheitsmanagement und zur Risikoanalyse findet man unter **BSI-Standards**

ITIL Security und ISO

- **BS7799 ➔ ISO 17799 ➔ ISO 27001**
  Die BS7799:1995 wurde vom British Standard Institute 1995 aus dem „Code of practice“ im Bereich der Informationssicherheit übernommen.

  2000 adaptierte die ISO (International Standard Organisation) daraus den Teil 1 zur ISO 17799

  2002 gab es signifikante Änderungen an Teil 2 (u.a. PDCA-Konzept), woraus Version BS 7799-2:2002 entstand

  Die Weiterentwicklung des BS7799 ist die ISO/IEC 27001, die eine international gültige Zertifizierungsgrundlage darstellt.

Zusammenhang BSI und ISO

- **Grundschutzhandbuch und ISO**
  IT-Grundschutz beschreibt mit Hilfe der **BSI-Standards** und der **IT-Grundschutz-Kataloge** eine Vorgehensweise zum Aufbau und Betrieb eines **ISMS** (Managementsystem für Informationssicherheit).

  Dieses ISMS erfüllt die Anforderungen von ISO 27001 und ISO 17799:2005

ITIL® und Informationssicherheit

Quelle: Bundesamt für Sicherheit in der Informationstechnik

ITIL-Prozess / GSH-Baustein	Conf M	IM	SD	PM	ChM	RM	SLM	AvM	Cap M	ITSC M	FinM
IT-Sicherheitsmanagement	x					x	x	x			
Organisation	x	x		x	x	x	x	x	x		
Notfallvorsorgekonzept		x		x			x	x	x	x	
Datensicherungskonzept								x			
Computervirenschutzkonzept	x				x	x		x			
Behandlung von Sicherheitsvorfällen		x		x							
Hard- und Software-Management	x	x	x	x	x	x	x	x	x	x	
Outsourcing	x				x	x	x	x	x	x	
Verkabelung								x	x	x	
Serverraum								x		x	
Heterogene Netze								x		x	
Datenträgeraustausch						x		x			
Standardsoftware	x				x	x					
Archivierung								x	x		
Sicherheitsbedarfsfeststellung	x							x			

Synergien durch gleichzeitige Betrachtung (1)

- Sponsorship:
  Die Menschen sind der entscheidende Faktor
- Management of Change:
  Eine Kultur der Veränderung wird benötigt
- Reorganisation:
  Beide Themen sind *keine* IT-Projekte
- IT-Verfahren:
  ITIL® ist generisch, das Grundschutzhandbuch dagegen ist spezifisch

Synergien durch gleichzeitige Betrachtung (2)

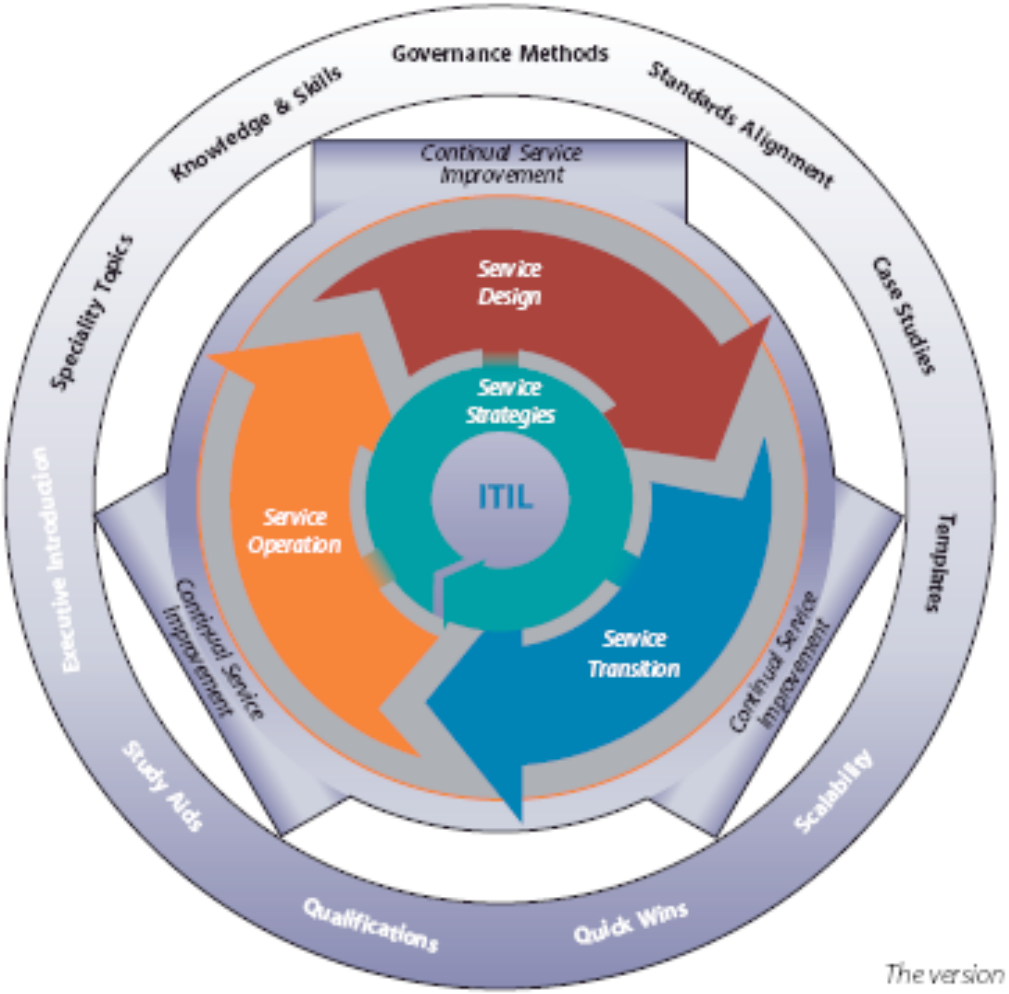
- Effizienz:
  Verzahnung des Service- und des Sicherheits-Mgmt.
- Effektivität:
  Bessere Qualität durch frühzeitige Berücksichtigung der Sicherheitsanforderungen
- Objektivität:
  Messbarkeit wird als Basis kontinuierlicher Verbesserung sichergestellt
- Transparenz:
  Kosten für Sicherheit können Services zugeordnet werden

Fazit

- IT Service Management und Grundschutz unterstützen sich gegenseitig
- Grundschutzhandbuch liefert konkrete Ansätze für IT-Verfahrensanweisungen
- ITIL® -Prozesse liefern Basisstrukturen für Sicherheit
- Für beide Themen sind vergleichbare Rahmenbedingungen nötig
- Es sind die gleichen Schwierigkeiten zu a[illegible]re[illegible]

großes Potential bei richtigem Vorgehen!

ITIL 3.0



The version 3 package