

# Informationssicherheit im IT Service Management

*Bernhard Barz,*  
regio iT aachen

- Informationssicherheit
- Anforderungen der ÖV
- Informationssicherheit im IT Service Management
  - Prozess Informationssicherheit
  - Zusammenspiel mit anderen Prozessen
- Umsetzung Informationssicherheit

- Das Informations-Sicherheits-Management-System (ISMS) soll sicherstellen, dass adäquate und angemessene Sicherheitsmaßnahmen ausgewählt werden, die Informationswerte schützen und Vertrauen bei Interessenten erwecken

[ISO 27001: Informationssicherheits-Managementsysteme Anforderungen]

- „Das Ziel des Informations-Sicherheits-Managements (ISM) ist die Abstimmung zwischen IT-Sicherheit und „business security“ und die Sicherstellung, dass Informationssicherheit in allen „Services“ und „Service Management Aktivitäten“ effektiv gemanaged wird.

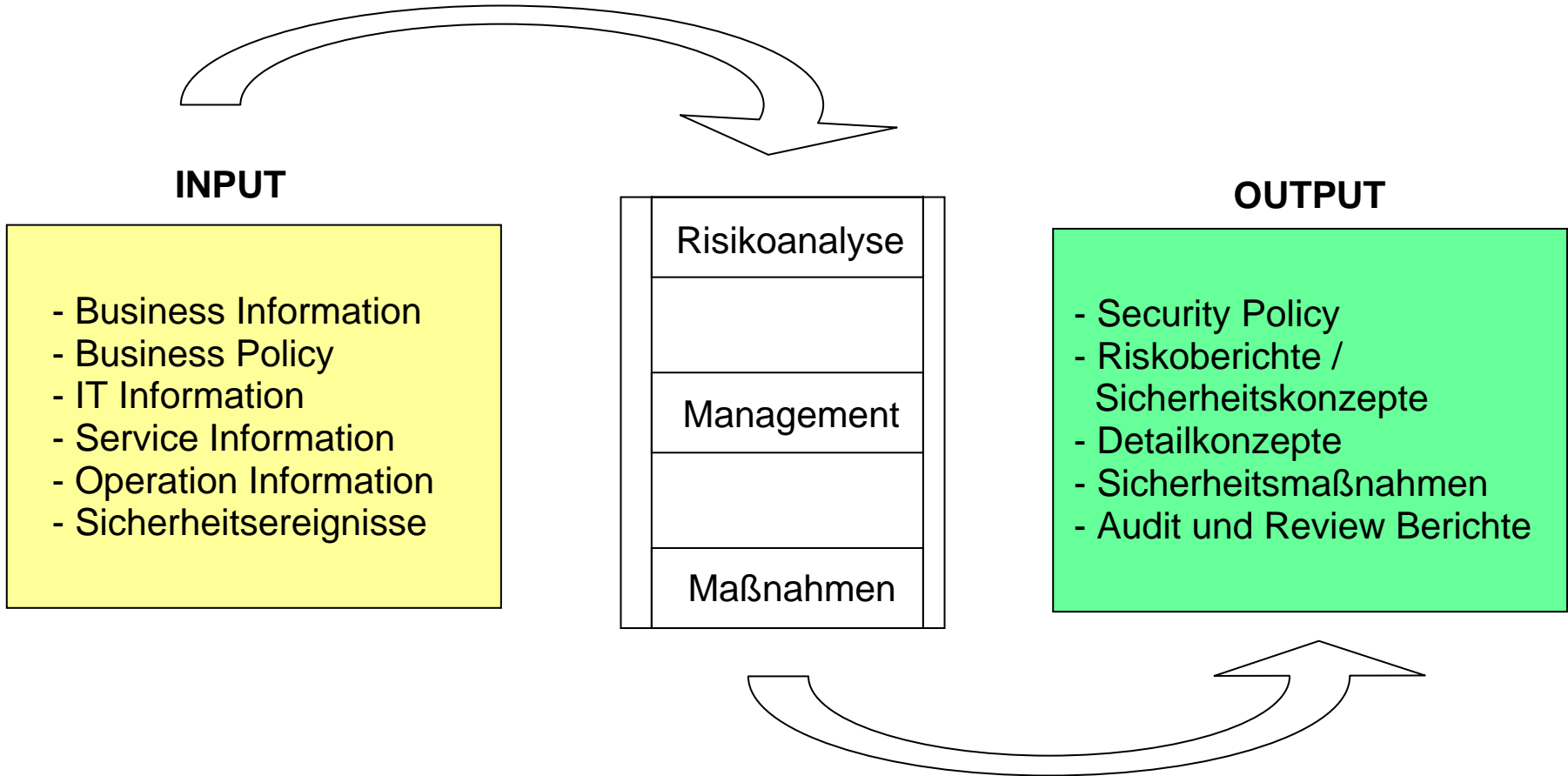
[ITIL v3: Service Design]

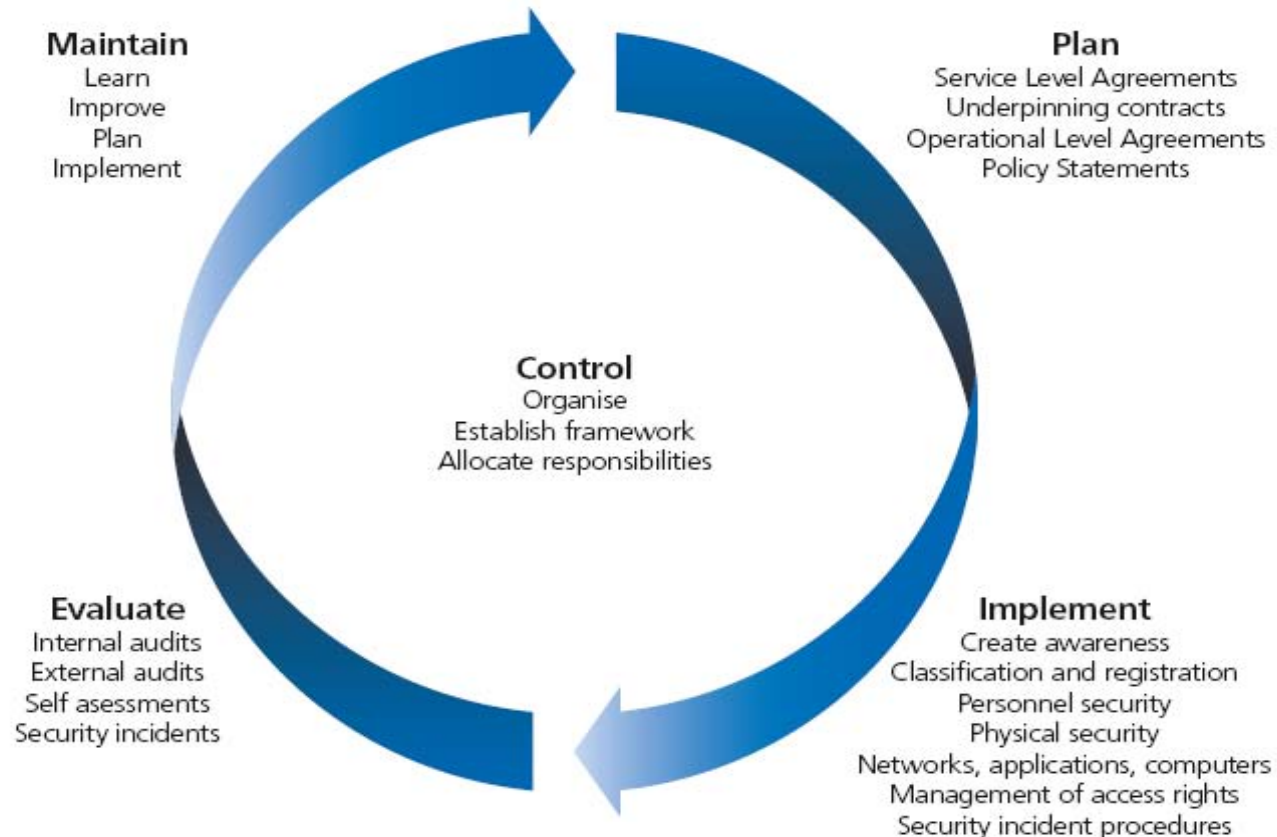
- Informations Sicherheits Leitlinie
- Sicherheitsmaßnahmen, die die Leitlinie unterstützen
- Risiko Management in Bezug auf den Zugriff (access) auf Services, Informationen und Systeme
- Management von Sicherheitsereignissen
- Management externer Dienstleister / Lieferanten

- Beherrschung der Abhängigkeit von Externen
- Nutzungskontrolle (access control)
- Sicherstellung der Informationssicherheit im Rahmen der „Corporate Governance“
  - Management von Sicherheitsrisiken
  - Verantwortlicher Umgang mit den Informations Ressourcen

- Gesetzliche Anforderungen
- Unterstützung der internen und externen Prozesse
- Zuverlässige IT-Services
  
- Beispiel: Doppische Buchführung
  - Wirtschaftsprüfer / GPA
  - IDW PS 330

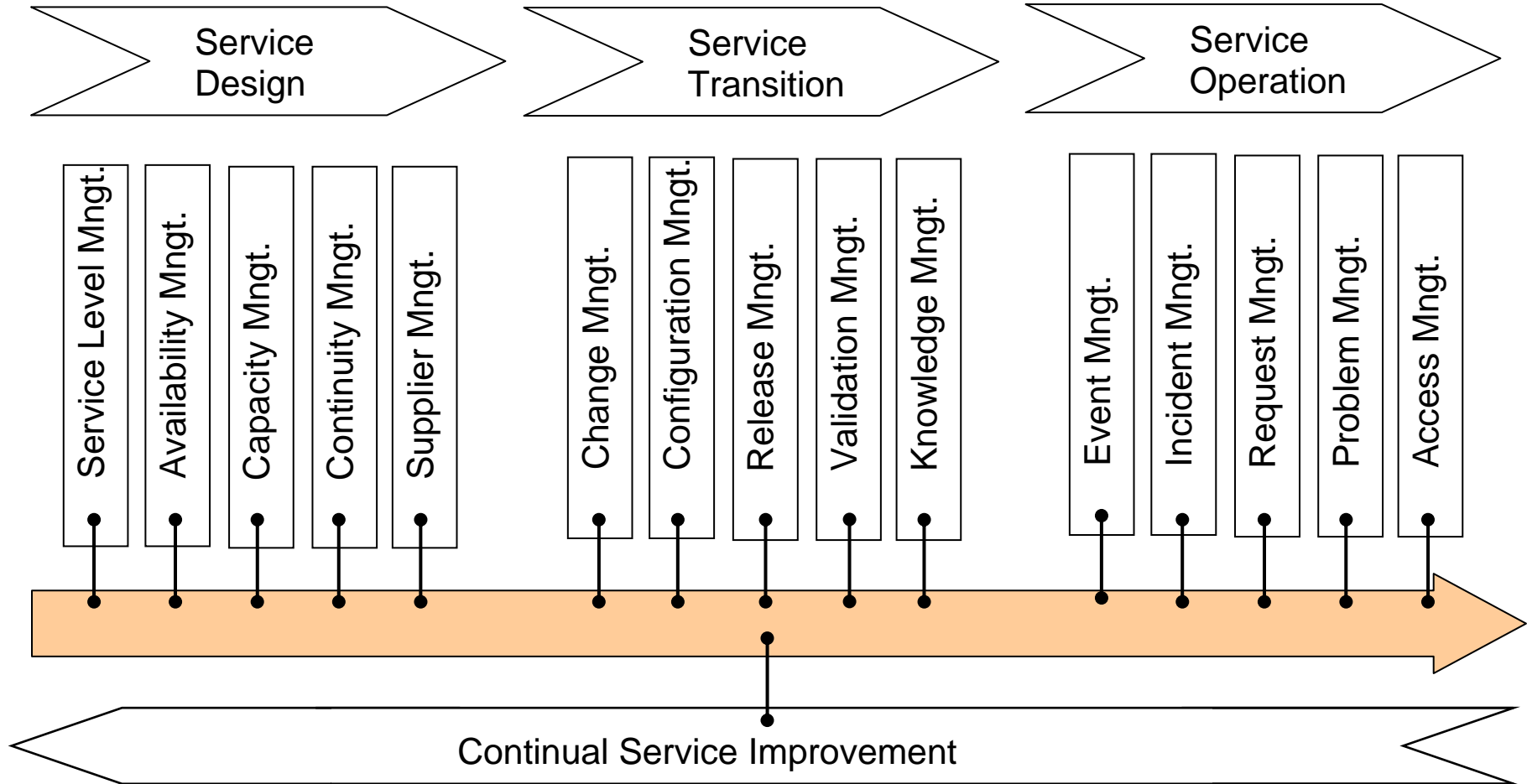
# Prozessdarstellung





Quelle: ITIL v3 SD p. 143

# Zusammenspiel mit anderen Prozessen



- Was ist notwendig bzw. wichtig?
  - Service Level Management
  - Availability bzw. Continuity Management
  - Change, Event, Incident und Request Management
  
- Rahmenbedingungen setzen
  - Sicherheitsorganisation
  - Erfassung der wichtigsten Services
  - Umfassende Sicherheitspolicy (ITIL +)

# Umsetzung der Informationssicherheit

---

- ISM – Prozess
  - starten
  - kontinuierlich verbessern

Fragen???

# Sicherheitspolicy und nachgelagerte Festlegungen

- Definition Risikomethoden und –kriterien
- Klassifikations- und Umgangsbestimmungen für Informationen
- Personelle Sicherheit
- Nutzungsbestimmungen für Assets (Hardware- / Software)
- Passwortrichtlinie
- E-Mail und Internet Policy (private / dienstliche Nutzung)
- Remote Access
- Externe Dienstleister
- Entsorgung von Datenträgern