

Infrastruktur und Servicemanagement

INHALT

- ITIL Prozesse
 - Incident Management
 - Problem Management
 - Change Management

- Information Security management
 - Security : Eigenbetrieb vs. Outsourcing
 - Kalkulation der Risiken , Risikobewertung , Management

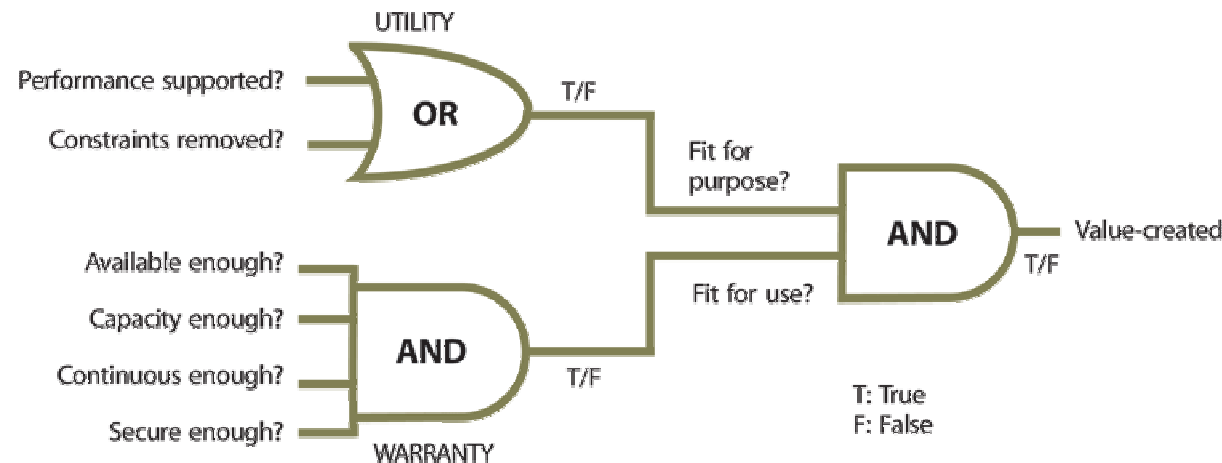
- Common Criteria

- **Verbesserung der Quality of Service – zuverlässigerer Business Support**
- **Verbesserte bzw. angepasste Systeme durch Definition von Service Levels**
- **Verbesserter Informationsstand hinsichtlich der gebotenen Services**
- **Klareres Verständnis der Leistungsfähigkeit und Möglichkeiten eines Betriebs**
- **Größere Flexibilität für die Geschäftsprozesse durch Verständnis der zugrunde liegenden Support Prozesse**
- **Steigende Kundenzufriedenheit, da die Support Teams wissen, was man von ihnen erwartet und dies auch geregelt durchführen**
- **Motivierteres Personal durch besseres Verständnis der zu erfüllenden Aufgaben**
- **Kürzere Durchlaufzeiten für Prozesse**

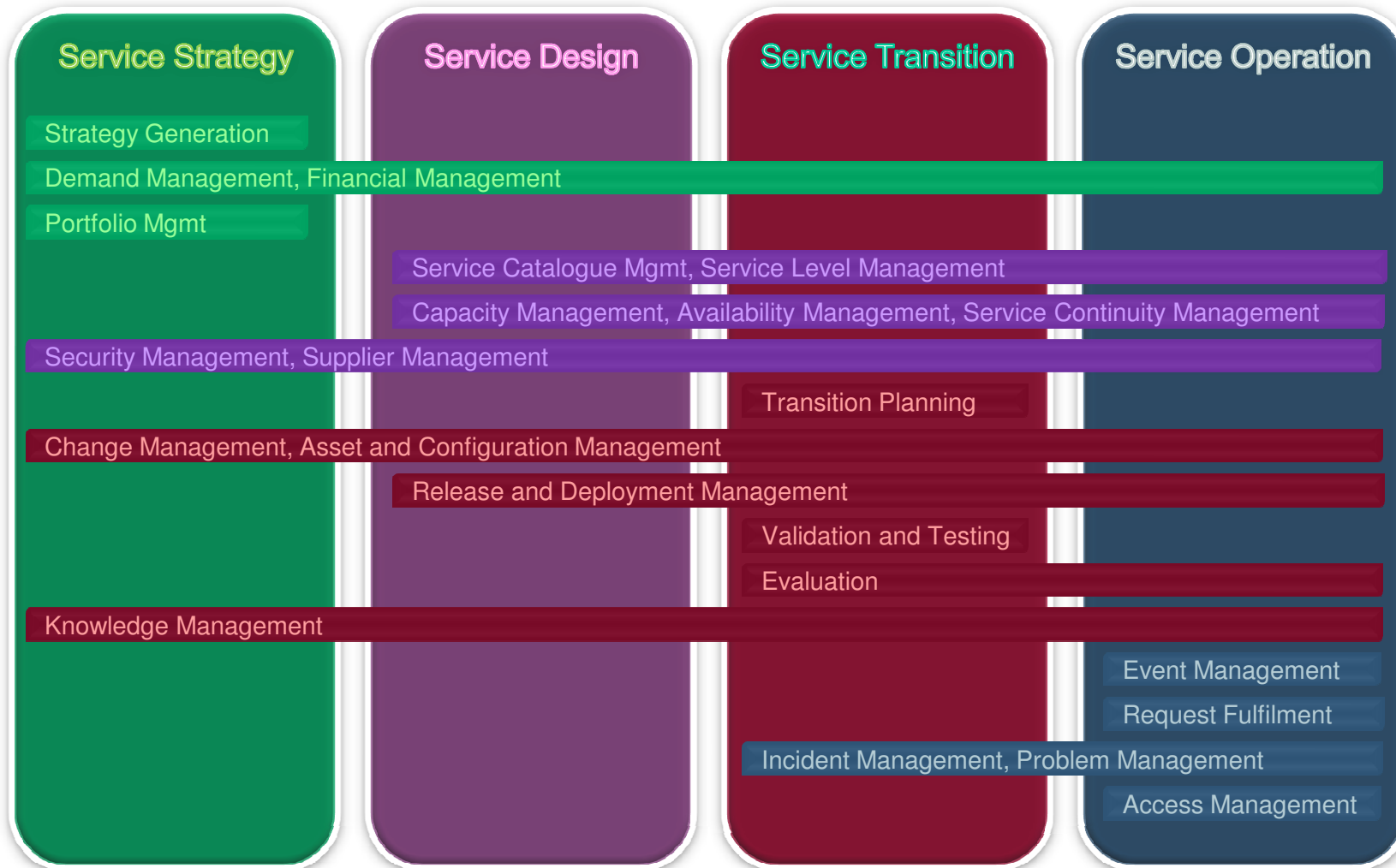
Gefahren bei der Implementation

- **Mangel an Awareness und Commitment**
- **Mangel an mittel- und langfristigem Budget**
- **Betroffene werden nicht zu Beteiligten gemacht**
- **Nicht-Beachtung der Human Speed of Change**
- **Trennung von Verantwortung und Entscheidungskompetenz**
- **Verlust der treibenden Person**
- **Motivationsmangel nach dem Kick-Off-Hype**
- **Unrealistische Ansprüche und Zeitpläne**
- **Probleme in der Änderung der Unternehmenskultur**
- **Unterschätzung der Arbeit und Disziplin**
- **Keine passende SW Unterstützung genehmigt**
- **Unpassende Projekt-Organisation (Change Projekt – kein technisches IT Projekt)**

- Aus Sicht des Kunden ist ein Service dann nutzenstiftend, wenn gleichermaßen sowohl die Funktionalität (Utility) als auch die Qualität (Warranty) den Erwartungen entspricht.
- **Utility** ist eine Funktionalität, die von einem Produkt oder Service angeboten wird, um einem bestimmten Bedürfnis gerecht zu werden. „Utility“ wird häufig auch bezeichnet als „das, was ein Produkt oder Service tut“. [Quelle: Glossar V3]
- **Warranty** ist eine Zusage oder Garantie, dass ein Produkt oder Service den vereinbarten Anforderungen entspricht. [Quelle: Glossar V3]



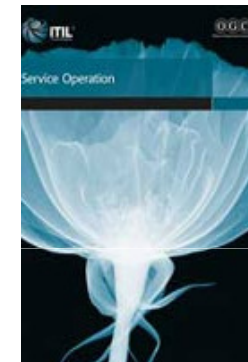
Die Prozesse im Lifecycle



- **Ziele**
 - **Reibungsloser Betrieb der Services**
 - **Koordination und Ausführung aller Aktivitäten um Services in der vereinbarten Qualität zu liefern**
 - **Datenerhebung und Auswertung zur Qualitätsverbesserung**
 - **Feedback in vorgelagerte Prozesse**
 - **Management aller operativen Ressourcen (inkl. Facilities)**
 - **Optimale Unterstützung der Anwender**
- **Inhalte**
 - **Schnellstmögliche Wiederherstellung von Services**
 - **Ursachenforschung bei Störungen**
 - **Abarbeiten von Fragen/Wünschen der Anwender**
 - **Management der Zugangsberechtigungen**

- **Guter Betrieb ist kein Zufall – er muss geplant werden**
- **Wesentliche Fragen**
 - **Können die Services in der zugesagten Qualität erbracht werden und wird das auch gemessen?**
 - **Sind Kunde und Anwender zufrieden?**
 - **Agiert der Service Desk als zentrale Anlaufstelle?**
 - **Ist das Personal ausreichend geschult?**
 - **Sind die Betriebskosten im geplanten Bereich?**
 - **Sind die erfassten Daten auch für Verbesserungen tauglich?**
 - **Gibt es eine Feedbackschleife ins Design und zur Transition?**
 - **Sind Effizienz und Effektivität bei der Leistungserbringung ausgewogen?**

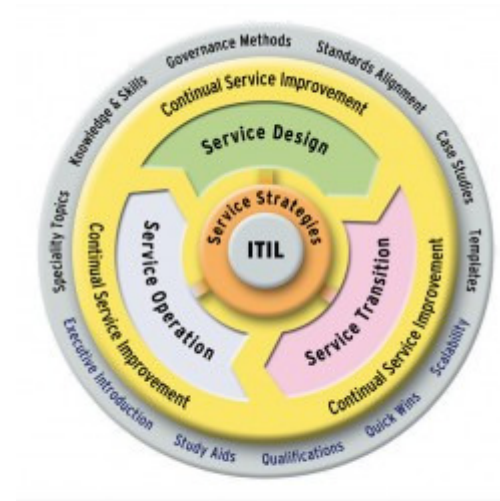
- Haupt-Prozesse
 - Event Management
 - Request Fulfillment
 - Incident Management
 - Problem Management
 - Access Management
 - Service Desk (Funktion)
 - Technical Management (Funktion)
 - Application Management (Funktion)
 - IT Operations Management (Funktion)



Service Operation

Service Operation

- Service Operation Prozesse
 - Event Management
 - **Incident Management**
 - Request Fulfilment
 - **Problem Management**
 - Access Management



Incident Management

Input

- Information on Incidents
 - From the Service Desk
 - From Monitoring Tools
- CMDB Information
- Details/Information on solving previous Incidents ("Known Errors")
- Incident Management Response

Incident Management

Output

- RfC to solve the incident
- Update the incident records (including solution and/or workaround)
- Solved/closed incident
- Inform customers
- Reporting to customers and/or management

Incident Management

Key Performance Indicators

- Number of incidents related to number of solved incidents
- Costs for every incident
- Required time for solving incidents
- Number or correct/incorrect escalated incidents
- Number or incidents that were solved with out "on location" support

Problem Management

Definition of a problem (by ITIL)

- The unknown cause of one or more incidents

Definition of a known error (by ITIL)

- A known error is an incident or a problem where a solution or workaround for the cause/reason is already known

Warum Problem Management?

- Schnelle und effektive Behebung von Problemen
- Methode zur Priorisierung der Ressourcen – die kritischsten Probleme werden zuerst gelöst
- Minimierung des wiederholten Auftretens von Problemen
- Verbesserte Produktivität der Support-Spezialisten
- Bereitstellung von Management Information

Problem Management

Aufgaben des Problem Management

Problem Management deckt drei Bereiche des Incident Lebenszyklus ab:

- Incident Control
- Problem Control
- Error Control

Problem Management

Incident Control

- Second Level Support (nach dem Help Desk) für Diagnose und Behebung schwieriger oder kritischer Incidents
- Koordination anderer Support-Spezialisten

Problem Control

- Identifizierung, Diagnose und Erfassung der zugrundeliegenden Ursachen
- vermeiden von wiederholten Problemen aufgrund einer bestimmten Ursache
- Analyse der Schwere des Problems sowie Erbringen des erforderlichen Supports
- Identifizieren potentieller Probleme

Problem Management

Error Control

- Initiieren von Requests for Change (Änderungsanforderungen), um dem Auftreten von Problemen vorzubeugen
- Beheben von Known Errors, unter Kontrolle des Change Management

Problem Management

Nutzen

- Höhere Produktivität der Anwender durch geringere Ausfallzeiten
- Höhere Produktivität der Support-Mitarbeiter
- Vermeiden von Ausfällen bzw. Minimierung der Folgen durch Nutzen der Informationen aus früheren Problemen
- Bessere Beziehungen zwischen Anwendern und IT-Services, dank einer besseren Service-Qualität
- Stärkere Kontrolle der IT-Services durch bessere Management Information

Problem Management

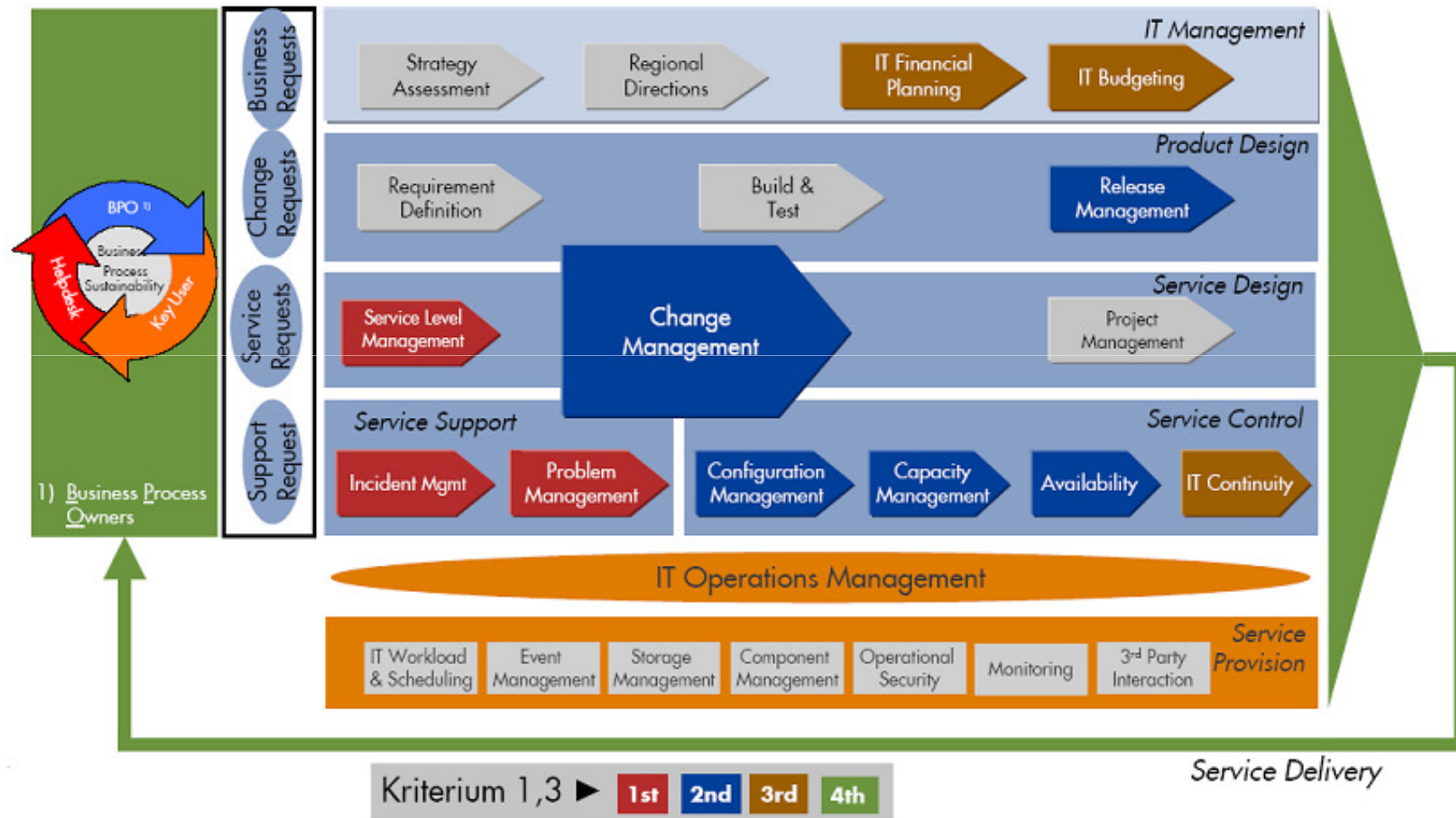
Kosten

- Die Anschaffungskosten sind relativ niedrig
- höhere Effizienz des IT-Support gleicht diese Kosten leicht aus

Potentielle Schwierigkeiten

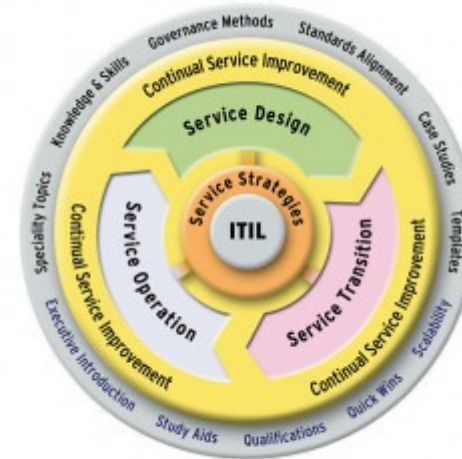
- Anwender verlangen direkten Zugang zu Problem Management oder anderen Support-Spezialisten
- Geringe Integration zwischen Incident Records und Problem oder Error Records
- Mitarbeiter sträuben sich gegen Veränderung

Priorisierte Prozesslandkarte



Service Transition

- Service Transition Prozesse
 - **Change Management**
 - Service Asset & Configuration Mgmt
 - Knowledge Management
 - Service Release Planning
 - Performance and Risk evaluation
 - Acquire Assets, Build and Test Release
 - Service Release Acceptance Test and Pilot
 - Entwicklung, Stilllegung and Transfer
- Common Operation Activities
- Technologische Überlegungen
- Implementierungsplanung



Change Management

ITIL's definition:

- Adding, modifying or removing of approved software, hardware and documentation

Warum Change Management?

- Changes sind natürlicher Bestandteil jeder sich entwickelnden Geschäftsumgebung
- Sicherstellung, daß Changes richtig analysiert und kontrolliert durchgeführt werden

Change Management

Gründe für Changes

- Lösung von Problemen, die sich aus Incident oder Problem Reports ergeben
- Reaktion auf Unzufriedenheit der Anwender
- Einführung eines neuen Configuration Item (CI)
- Upgrade von Komponenten
- Reaktion auf veränderte geschäftliche Anforderungen oder Ausrichtung
- Reaktion auf neue oder geänderte gesetzliche Regelungen
- Einführung neuer Produkte oder Services

Change Management

Aufbau des Change Management


Einführung eines Change Advisory Board (CAB)

- Mitglieder:
 - Change Manager (Vorsitz)
 - Kunden
 - Entwickler
 - IT Service Provider
 - Problemlöser
 - weitere durch die Changes Betroffenen

Change Management

Aufgaben des Change Management

- Bearbeiten von Requests for Change (RFCs)
- Planen des Change
- Realisieren des Change
- Dokumentieren des Change

 Unter **Service Sourcing** versteht man die Strategie und der Ansatz in Bezug auf die Entscheidung, ob ein Service intern bereitgestellt oder ob die Bereitstellung an einen externen Service Provider vergeben wird. Service Sourcing bedeutet zudem die Ausführung dieser Strategie.

- Mögliche Strategien hierzu sind
 - Insourcing: Erbringung der Leistung durch eigene Ressourcen
 - Outsourcing: Weitergabe wohldefinierter Aufgaben an Dritte
 - Co-Sourcing: Gemeinsames Erbringen von Aufgaben
 - Partnership or Multi-Sourcing: Ähnlich Co-Sourcing
 - Business Process Outsourcing: Sourcing ganzer Geschäftsteile
 - Application Service Provisioning: Software aus der Steckdose
 - Knowledge Process Outsourcing: Steigerung von BPO

Goals and Objectives

- **Umsetzung von Sicherheitsanforderungen des Kunden in Betriebsaspekte**
- **Sicherstellung eines gewissen Grundschutzes im Bereich der Vertraulichkeit, Verfügbarkeit und Integrität**
- **Gewährleistung von Informationssicherheit in allen Betriebsaspekten**
- **Herstellung eines angepassten Risikomanagementsystems / Umgang mit Risiken**

Basic Concepts

- Vertraulichkeit (Confidentiality)
 - Zugriff ist ausschließlich für autorisierte Senken gegeben
- Integrität (Integrity)
 - Vollständigkeit und Korrektheit der Daten ist zum Zeitpunkt der Verwendung gegeben und somit sind diese auch vor unerlaubter Manipulation geschützt
- Verfügbarkeit (Availability)
 - Informationen sind zum Zeitpunkt der Anforderung verfügbar und sind sicherheitstechnisch gegen Angriffe geschützt

Basic Concepts

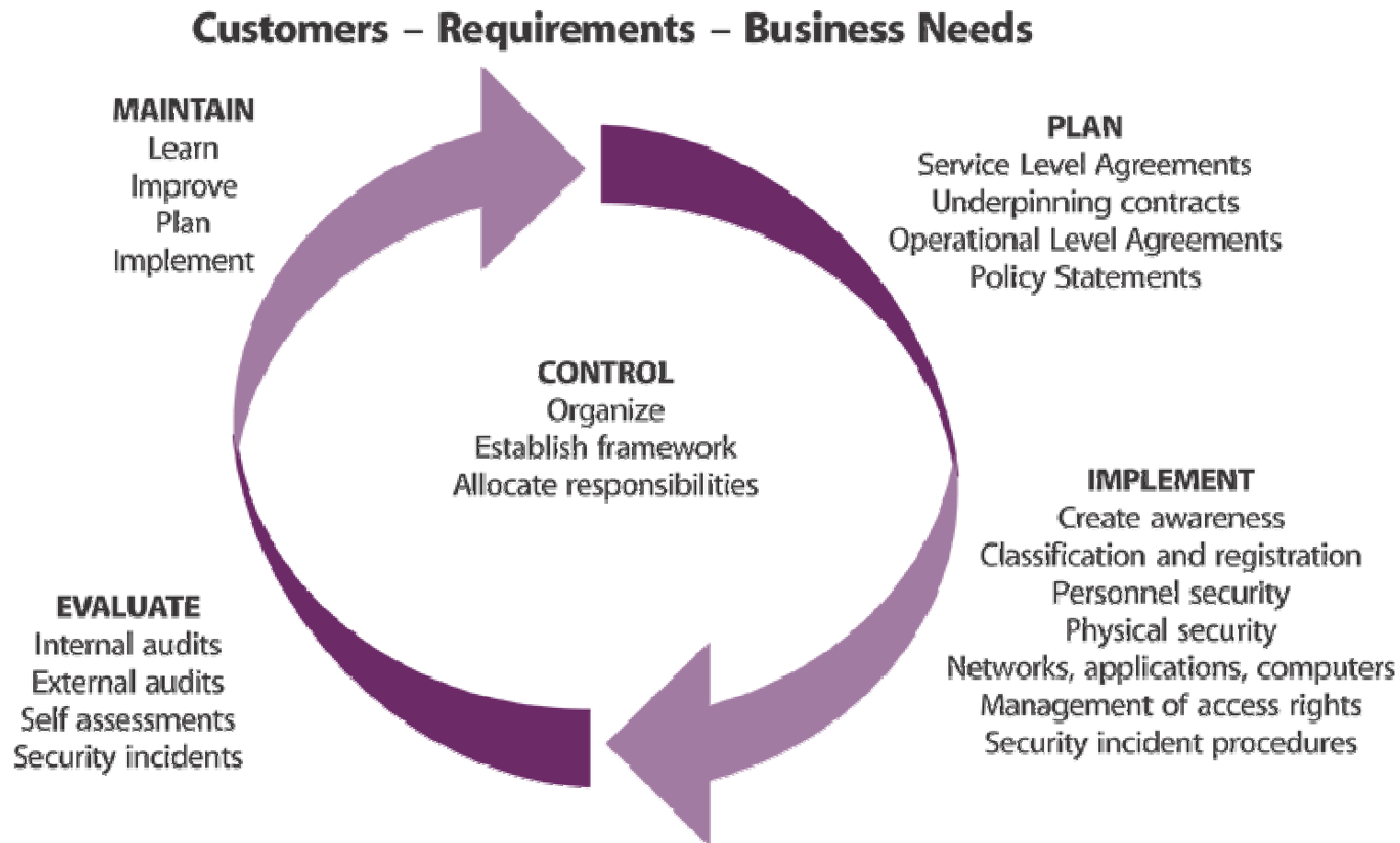
- Das InfoSec Framework besteht idR aus
 - Einer InfoSec Policy und spezifischen Anweisungen, sodass die Strategie, Regulative und Controls bedient werden können
 - Einem InfoSec Management System (ISMS) zum Management der Information Security
 - Einer Security Strategie, die sich an den Kundenzielen ausrichtet
 - Einem Satz aus Security Controls, die die InfoSec Policy unterstützen bzw. abbilden
 - Vorgaben zum Management der Risiken
 - Vorgaben zum Monitoring der Compliance
 - Pläne zur Kommunikation, zum Training, zu awarenessbildenden Maßnahmen, etc.

INHALT

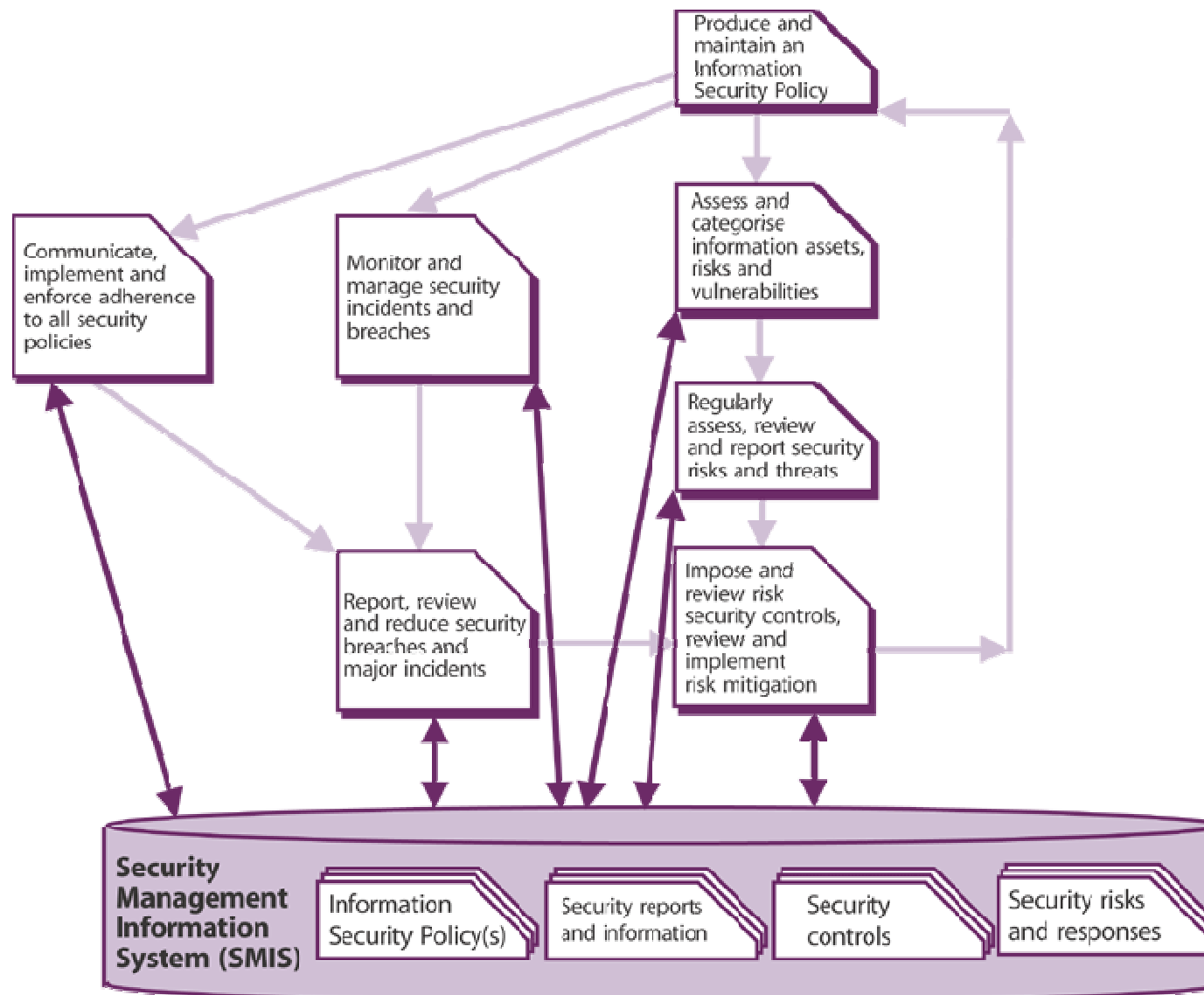
- ITIL Prozesse
 - Incident Management
 - Problem Management
 - Change Management

- Information Security management
 - Security : Eigenbetrieb vs. Outsourcing
 - Kalkulation der Risiken , Risikobewertung , Management

- Common Criteria



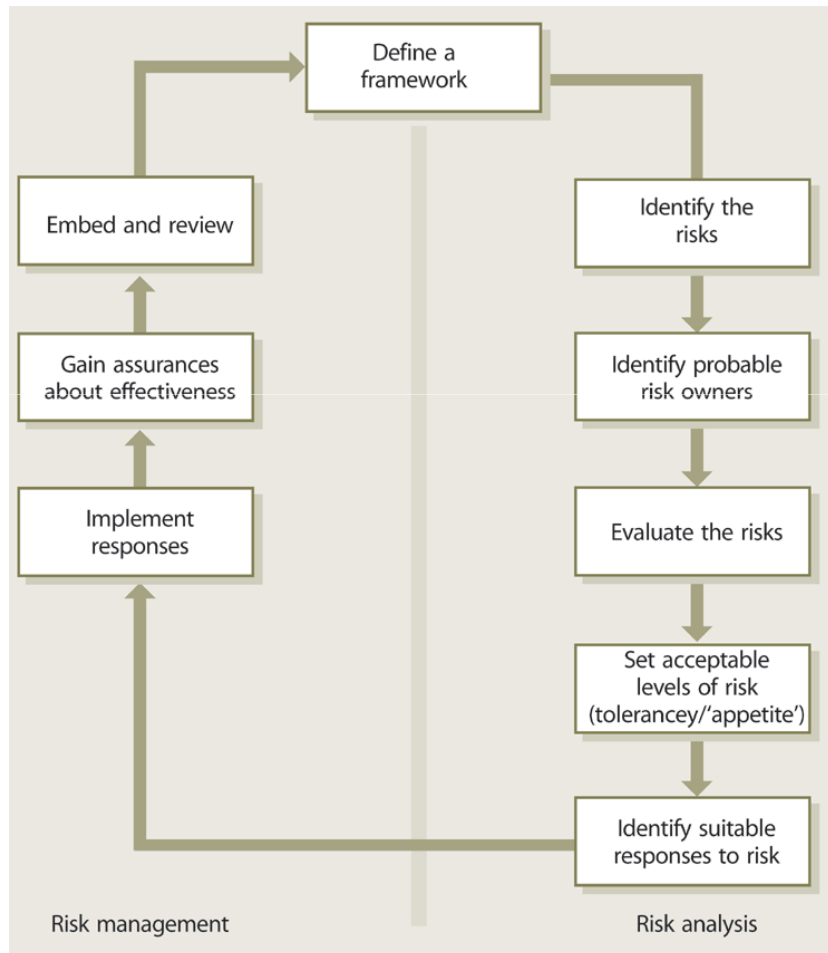
Information Security Management



Roles

- Security Manager
 - Entwicklung und Pflege des ISMS inkl. Policies, Anweisungen, etc.
 - Sicherstellung, dass die InfoSec Policy in Kraft gesetzt ist und befolgt wird
 - Identifizierung und Klassifizierung von IT Assets mit dem zugehörigen Schutzbedarf
 - Durchführung von Risiko Analyse und Risiko Management
 - Entwicklung von Security Controls
 - Monitoring von Security Verletzungen, Verfolgung von Security Incidents

- ✎ Ein Risiko ist ein mögliches Ereignis, dass zu Schaden oder Verlust führen oder auch das Erreichen von Zielen beeinträchtigen kann.
- Risiken werden durch die Wahrscheinlichkeit der Bedrohung, der Verwundbarkeit der betroffenen Assets und der Auswirkung beim Eintritt bewertet.



Management of Risk

- Risiko Analyse
- Risiko Management