IT-Sicherheit

- Sicherheit vernetzter Systeme -

Kapitel 2: Grundlagen

Folienversion: 18.10.2013

Kapitel 2: Inhalt

1. Grundlegende Ziele der IT-Sicherheit
2. Kategorisierung von Sicherheitsmaßnahmen
3. Standards der ISO/IEC 27000 - Reihe
4. Security vs. Safety

Ziele der Informationssicherheit

- Hauptproblem:

  Informationssicherheit (IS) kann nicht gemessen werden
  - Es gibt keine Maßeinheit für IS
  - Sicherheitskennzahlen (security metrics) sind bislang szenarienspezifisch und quantifizieren nur Teilaspekte

- Lösungsansatz: Indirekte Definition von IS durch (Teil-)Ziele

Vertraulichkeit	Confidentiality
Integrität	Integrity
Verfügbarkeit	Availability

Akronym CIA häufig in englischer IS-Literatur

1. Teilziel: Vertraulichkeit

- Definition:

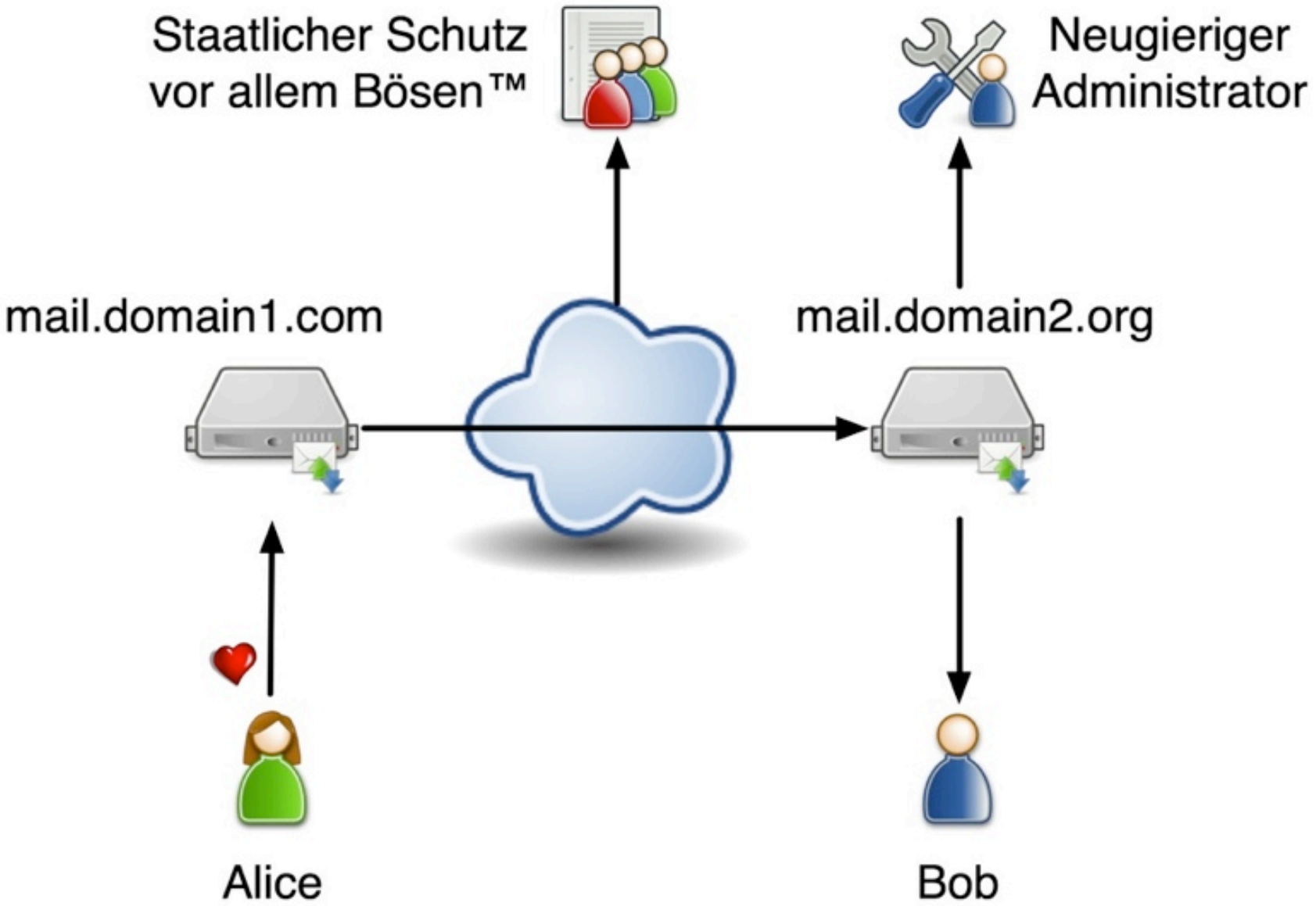
  Vertraulichkeit (engl. confidentiality) ist gewährleistet, wenn geschützte Daten nur von Berechtigten abgerufen werden können.

- In vernetzten Systemen zu betrachten bezüglich:
  - Transport von Daten (über Rechnernetze)
  - Speicherung von Daten (inkl. Backup)
  - Verarbeitung von Daten

- Typische Sicherheitsmaßnahme: Verschlüsselung

- Teilziel gilt als verletzt, wenn geschützte Daten von unautorisierten Subjekten eingesehen werden können.

Beispiel: Vertraulichkeit von E-Mails



2. Teilziel: Integrität

- Definition:

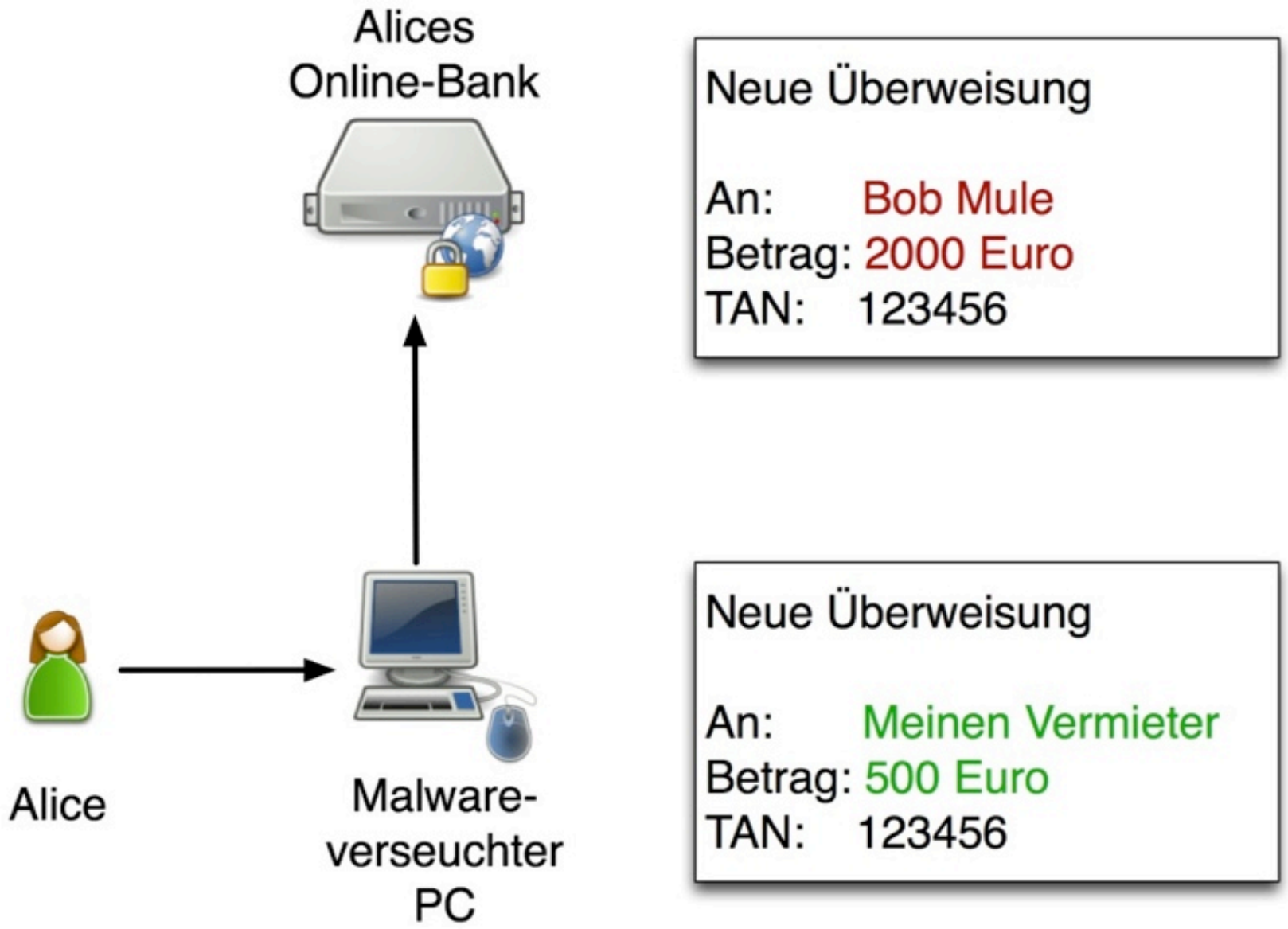
  Integrität (engl. integrity) ist gewährleistet, wenn geschützte Daten nicht unautorisiert und unbemerkt modifiziert werden können.

- Wiederum bei Transport, Speicherung und Verarbeitung sicherzustellen!

- Typische Sicherheitsmaßnahme: Kryptographische Prüfsummen

- Teilziel verletzt, wenn Daten von unautorisierten Subjekten unbemerkt verändert werden.

Beispiel: Integrität im Online-Banking



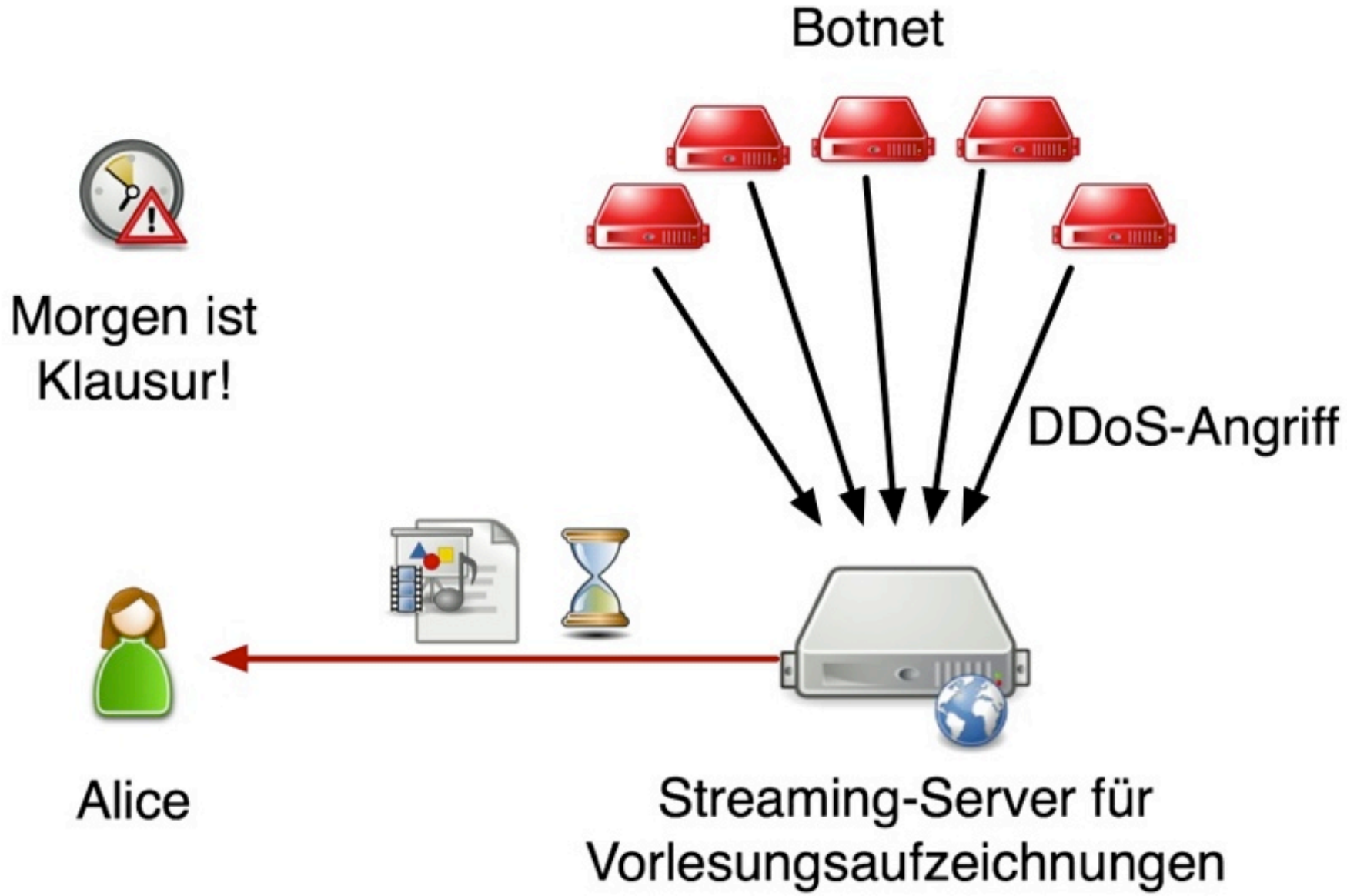
3. Teilziel: Verfügbarkeit

- Definition:

> Verfügbarkeit (engl. availability) ist gewährleistet, wenn autorisierte Subjekte störungsfrei ihre Berechtigungen wahrnehmen können.

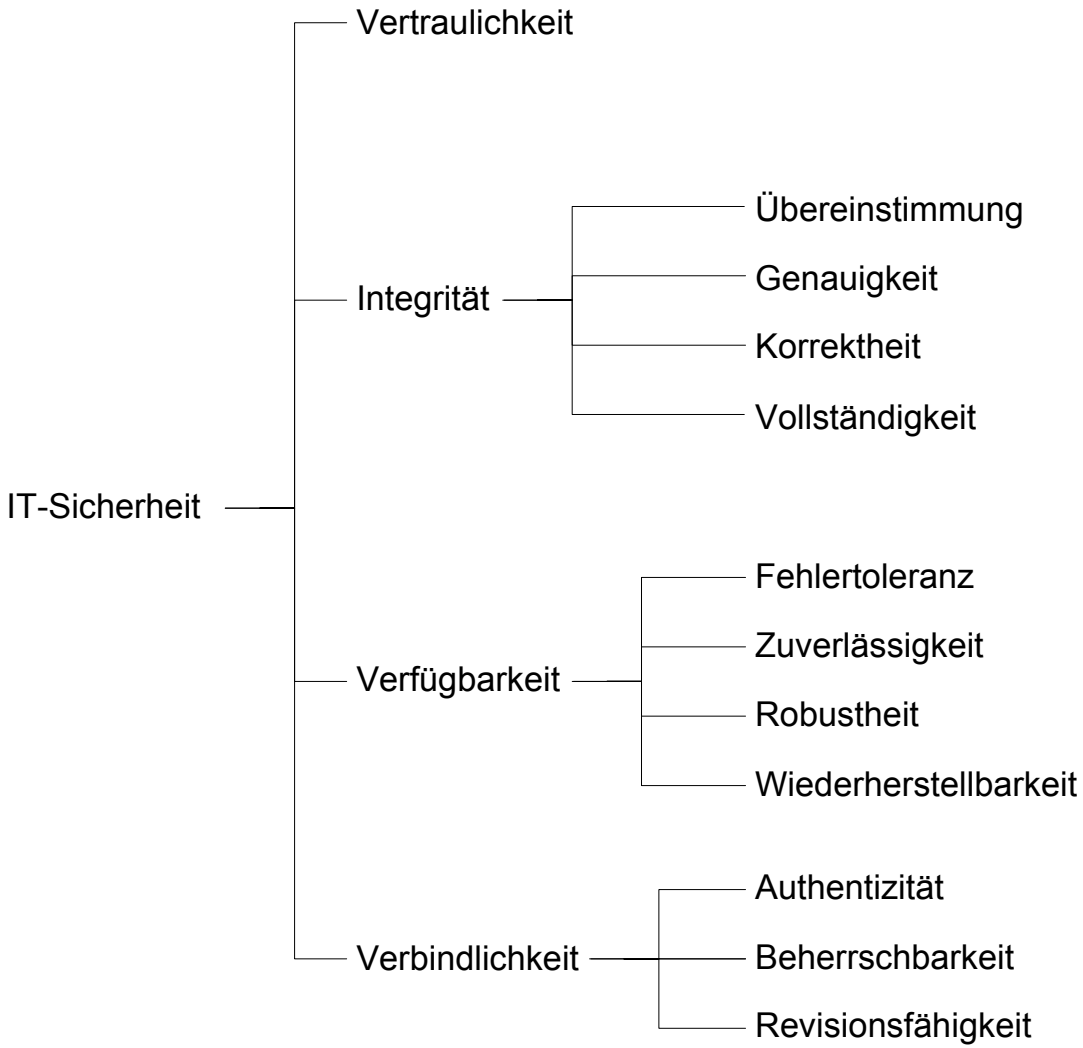
- Bezieht sich nicht nur auf Daten, sondern z.B. auch auf Dienste und ganze IT-Infrastrukturen.
- Typische Sicherheitsmaßnahme: Redundanz, Overprovisioning
- Teilziel verletzt, wenn ein Angreifer die Dienst- und Datennutzung durch legitime Anwender einschränkt.

Beispiel: Verfügbarkeit von Webservern



Ziele und abgeleitete Ziele in deutscher IS-Literatur

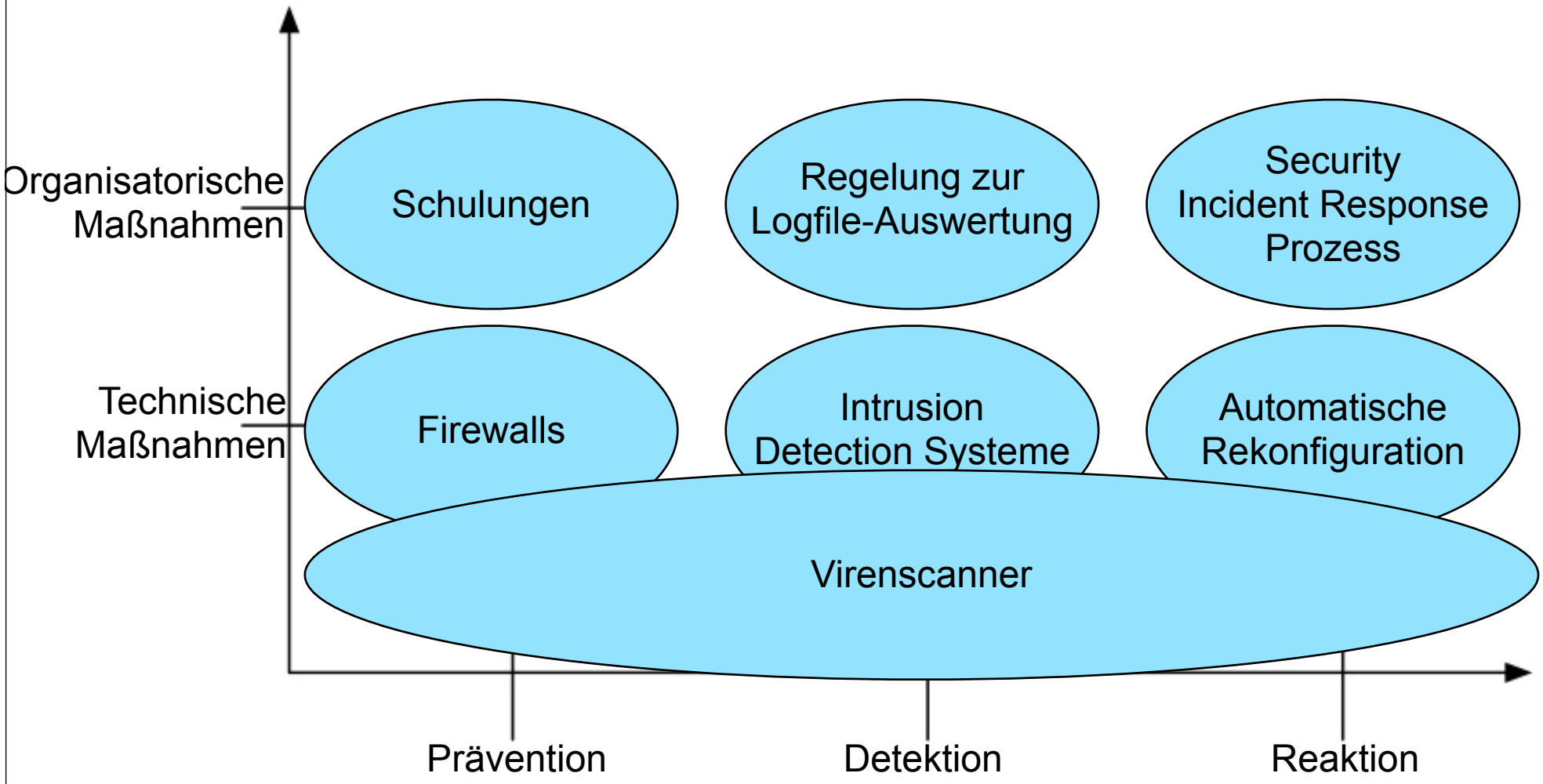
- Nach Prof. Hartmut Pohl, HS Bonn-Rhein-Sieg



Kapitel 2: Inhalt

1. Grundlegende Ziele der IT-Sicherheit
2. Kategorisierung von Sicherheitsmaßnahmen
3. Standards der ISO/IEC 27000 - Reihe
4. Security vs. Safety

Kategorisierung von Sicherheitsmaßnahmen



IS-Teilziele im Kontext des Angriffslebenszyklus

- Die Kombination aller in einem Szenario eingesetzten **präventiven** Maßnahmen dient der Erhaltung von *Vertraulichkeit*, *Integrität* und *Verfügbarkeit*.
- **Detektierende** Maßnahmen dienen dem Erkennen von unerwünschten Sicherheitsereignissen, bei denen die präventiven Maßnahmen unzureichend waren.
- **Reaktive** Maßnahmen dienen der Wiederherstellung des Soll-Zustands nach dem Erkennen von unerwünschten Sicherheitsereignissen.

Welche Maßnahmen werden benötigt?

- Grundidee:
  - Maßnahmenauswahl ist immer szenarienspezifisch
  - Risikogetriebenes Vorgehensmodell
- Kernfragestellungen:
  - Welche Sicherheitsmaßnahmen sollen wann und in welcher Reihenfolge ergriffen werden?
  - Lohnt sich der damit verbundene Aufwand (Investition/Betrieb)?
- Voraussetzungen:
  - Analyse des Schutzbedarfs
  - Überlegungen zu möglichen Angriffen und deren Auswirkungen
  - Ermittlung / Evaluation passender Lösungswege
  - Entscheidung möglichst auf Basis quantitativer (d.h. nicht nur qualitativer) Bewertung

Kapitel 2: Inhalt

1. Grundlegende Ziele der IT-Sicherheit
2. Kategorisierung von Sicherheitsmaßnahmen
3. Standards der ISO/IEC 27000 - Reihe
4. Security vs. Safety

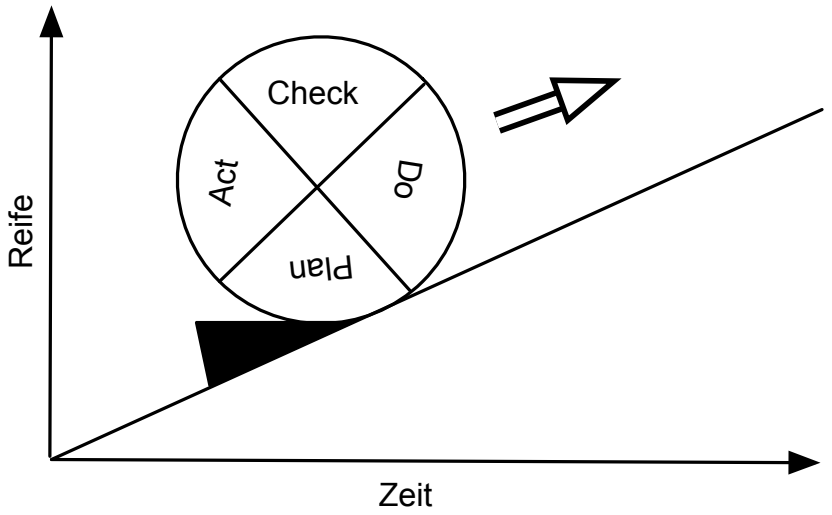
Motivation für ISO/IEC 27000

- Informationssicherheit Anfang der 1990er Jahre:
  - stark technikzentriert
  - Kosten-/Nutzenfrage kommt auf
  - Führungsebene wird stärker in IS-Fragestellungen eingebunden
- Wachsender Bedarf an Vorgaben und Leitfäden:
  - Kein „Übersehen“ wichtiger IS-Aspekte
  - Organisationsübergreifende Vergleichbarkeit
  - Nachweis von IS-Engagement gegenüber Kunden und Partnern
- Grundidee hinter ISO/IEC 27000:
  Anwendung der Grundprinzipien des Qualitätsmanagements auf das Management der Informationssicherheit

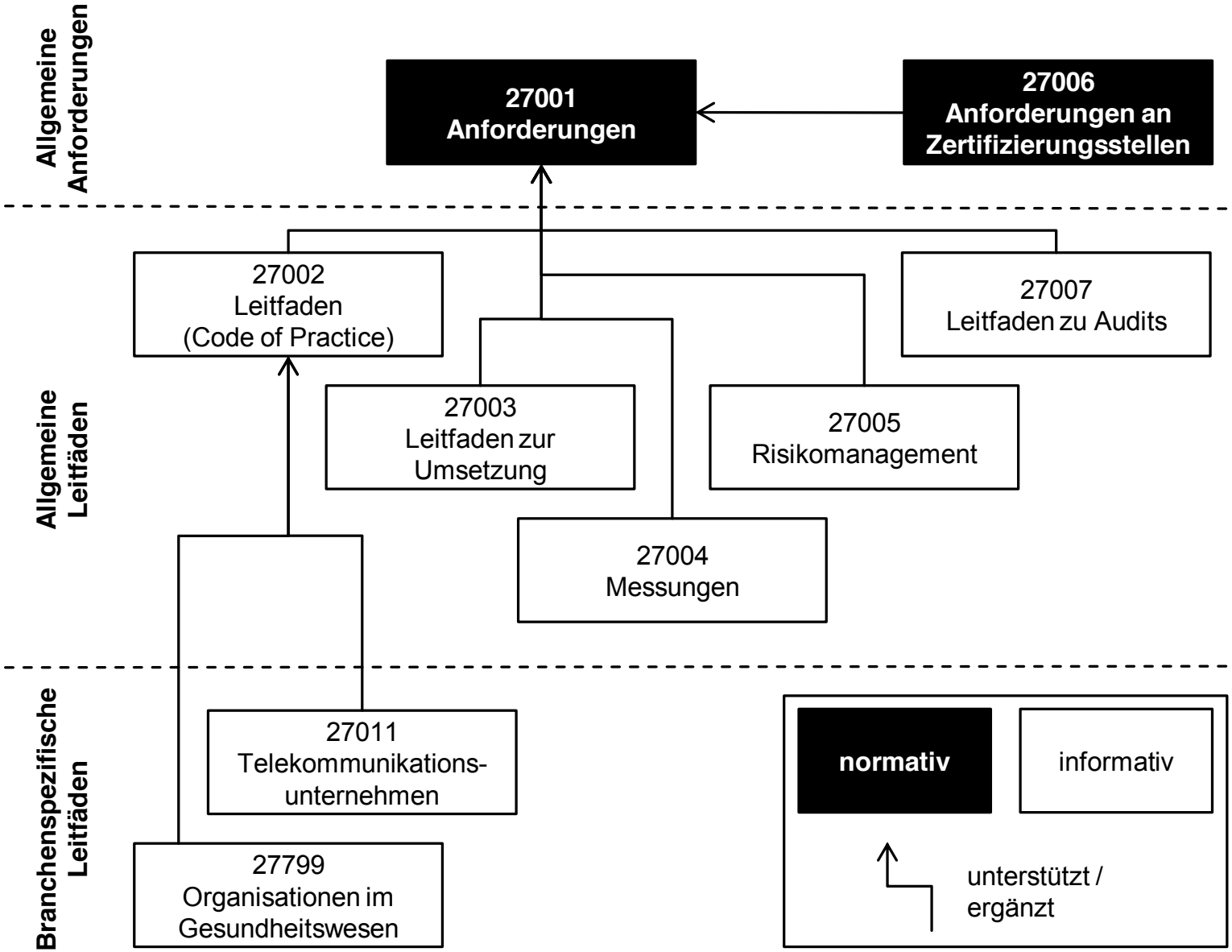
Internationale Normenreihe ISO/IEC 27000

- ISO/IEC 27000 wird mehrere Dutzend einzelne Standards umfassen
  - Mehr als die Hälfte davon ist noch in Arbeit und nicht veröffentlicht

- Norm ISO/IEC 27001 legt Mindestanforderungen an sog. Information Security Management Systems (ISMS) fest
  - Zertifizierungen möglich für:
    - Organisationen (seit 2005)
    - Personen (seit 2010)
  - Kernideen:
    - Kontinuierliche Verbesserung durch Anwendung des Deming-Zyklus
    - Risikogetriebenes Vorgehen
  - Seit 2008 auch DIN ISO/IEC 27001



ISO/IEC 27000 im Überblick



Wichtige Begriffe im Umfeld von ISMS

- (Informations-) Werte (engl. *assets*)
  - Alles, was für ein Unternehmen von Wert ist.
- Leitlinien
  - Anweisung, die formell durch das Management ausgesprochen wird.
- Prozesse
  - Ein Ablauf von zusammenhängenden oder wechselwirkenden Aktivitäten, die zu definierten Eingaben bestimmte Ergebnisse liefern.
- Verfahren
  - Vorgegebener Weg, eine Aktivität oder einen Prozess abzuwickeln.

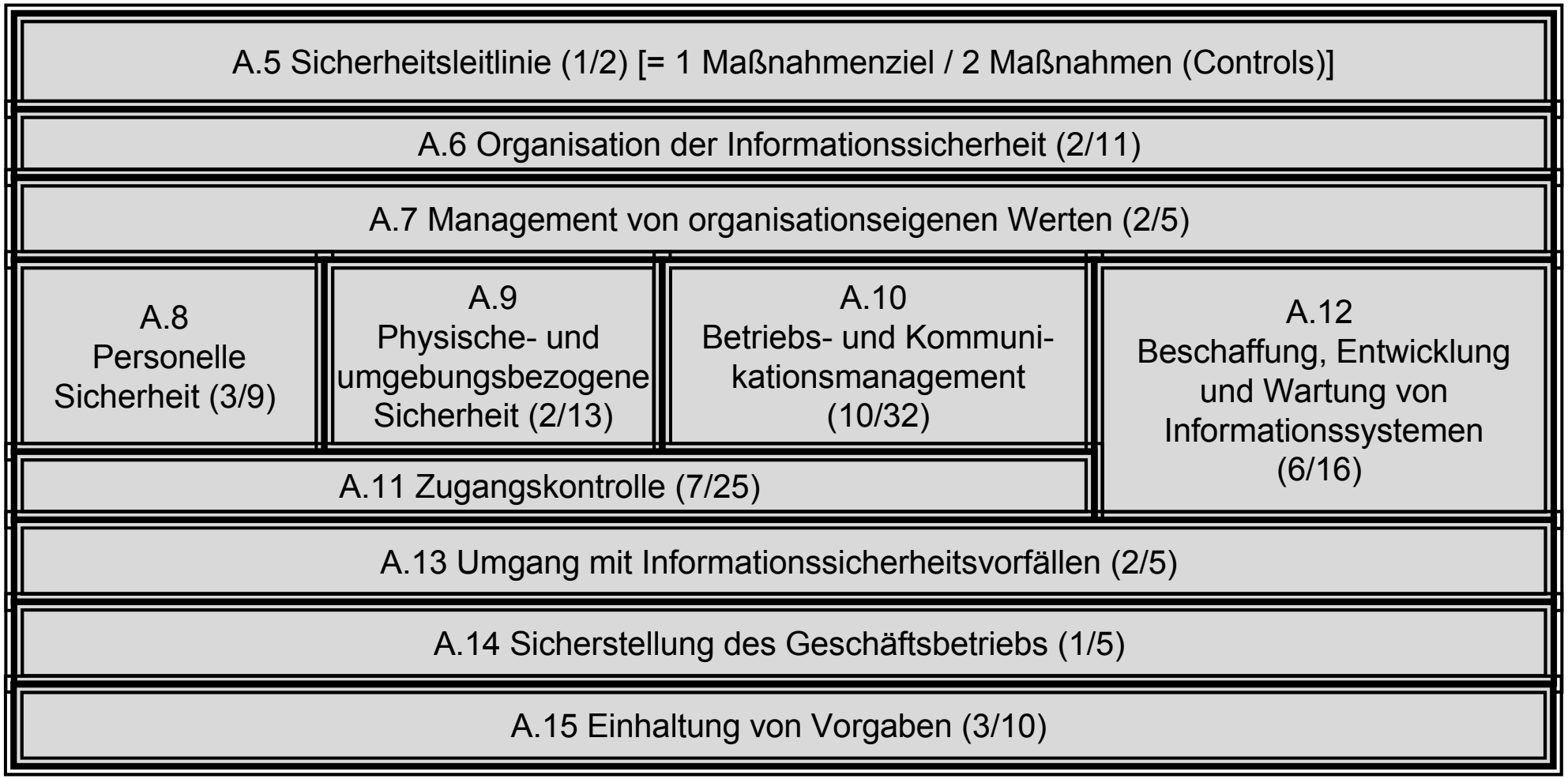
Informationssicherheits-Managementsystem (ISMS)

- Definition Managementsystem
  - System von Leitlinien, Verfahren, Anleitungen und zugehörigen Betriebsmitteln (inkl. Personal), die zur Erreichung der Ziele einer Organisation erforderlich sind.
- Definition ISMS:
  - Bestandteil des übergreifenden Managementsystems; es umfasst Einrichtung, Implementierung, Betrieb, Überwachung, Review, Wartung und Verbesserung der Informationssicherheit und stützt sich auf das Management von Geschäftsrisiken.
- Hinweis:
  - „System“ ist hier nicht im streng technischen Sinne, sondern als systematisches Rahmenwerk zu verstehen.

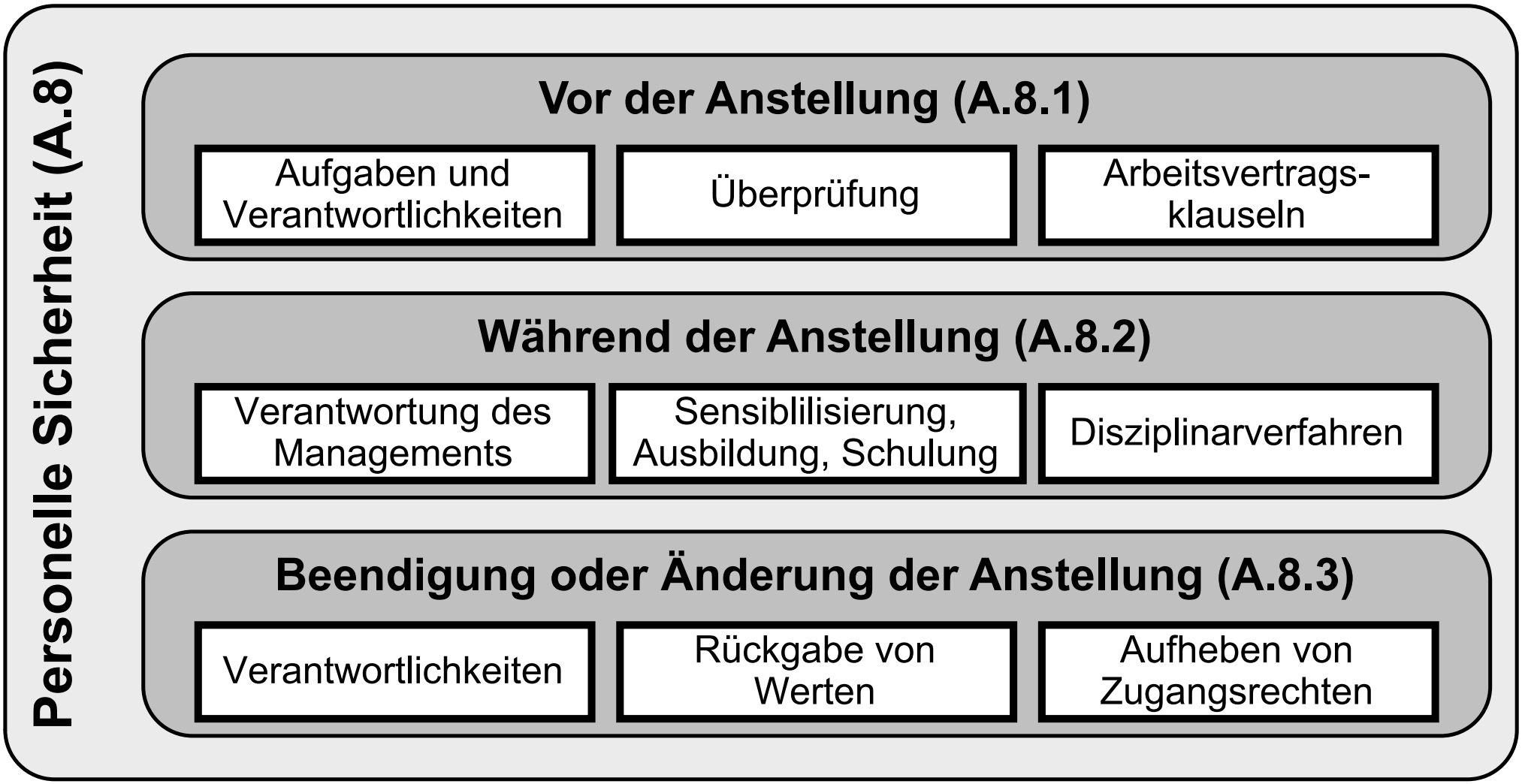
Kerninhalte von DIN ISO/IEC 27001:2008

- Begriffsdefinitionen
- PDCA-basierter Prozess zum Konzipieren, Implementieren, Überwachen und Verbessern eines ISMS
- Mindestanforderungen u.a. an Risikomanagement, Dokumentation und Aufgabenverteilung
- Normativer Anhang A enthält:
  - Definition von Maßnahmenzielen (control objectives)
  - Definition von Maßnahmen (controls)
- Umfang:
  - DIN ISO/IEC 27001:2008 - 45 Seiten
  - DIN ISO/IEC 27002:2008 - 144 Seiten

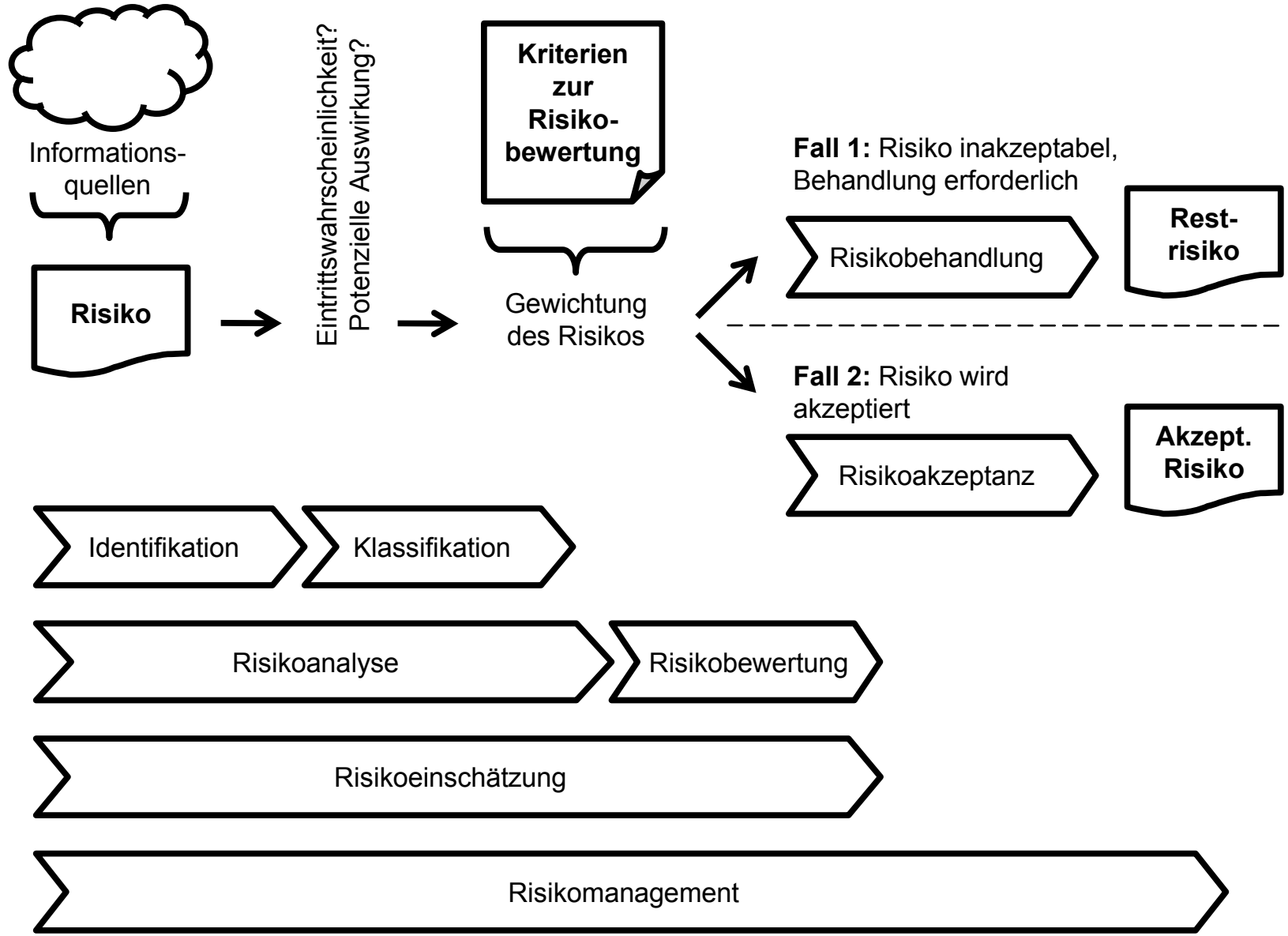
Maßnahmenziele und Maßnahmen: Überblick



Beispiel: Maßnahmen in ISO/IEC 27001 A.8



Grundlagen des Risikomanagements (ISO/IEC 27005)



Ausblick: ISO/IEC 27001:2013

ISO/IEC 27001:2005 – First Edition Annex A	ISO/IEC 27001:2013 – Second Edition Annex A
A.5 Security policy (1/2) A.5.1 Information security policy (2)	**A.5 Information security policies (1/2)** A5.1 Management direction for information security (2)
A.6 Organization of information security (2/11) A.6.1 Internal organization (8) A.6.2 External parties (3)	**A.6 Organization of information security (2/7)** A.6.1 Internal organization (5) → *Now: A.15* A.6.2 Mobile devices and teleworking (2)
A.7 Asset management (2/5) A.7.1 Responsibility for assets (3) A.7.2 Information classification (2)	→ *Now: A.8* → *Now: A.8.1* → *Now: A.8.2*
A.8 Human resources security (3/9) A.8.1 Prior to employment (3) A.8.2 During employment (3) A.8.3 Termination and change of employment (3)	**A.7 Human resource security (3/6)** A.7.1 Prior to employment (2) A.7.2 During employment (3) A.7.3 Termination and change of employment (1)
	A.8 Asset management (3/10) A.8.1 Responsibility for assets (4) A.8.2 Information classification (3) A.8.3 Media handling (3)
A.9 Physical and environmental security (2/13) A.9.1 Secure areas (6) A.9.2 Equipment security (7)	→ *Now: A.11* → *Now: A.11.1* → *Now: A.11.2*
A.10 Communication & operations mgmt. (10/32) A.10.1 Operational procedures and responsibilities (4) A.10.2 Third party service delivery management (3) A.10.3 System planning and acceptance (2) A.10.4 Protection against malicious & mobile code (2) A.10.5 Back-up (1) A.10.6 Network security management (2) A.10.7 Media handling (4) A.10.8 Exchange of information (5) A.10.9 Electronic commerce services (3) A.10.10 Monitoring (6)	→ *Now: A.8, A.12, A.13 & A.15* → *Now: A.12.1* → *Now: A.15.2* → *Now: covered (in parts) by A.17.2* → *Now: A.12.2* → *Now: A.12.3* → *Now: A.13.1* → *Now: A.8.3* → *Now: A.13.2* → *Now: covered (in parts) by A.14.1* → *Now: A.12.4*
A.11 Access control (7/25) A.11.1 Business requirement for access control (1) A.11.2 User access management (4) A.11.3 User responsibilities (3) A.11.4 Network access control (7) A.11.5 Operating system access control (6) A.11.6 Application and information access control (2) A.11.7 Mobile computing and teleworking (2)	**A.9 Access control (4/14)** A.9.1 Business requirements of access control (2) A.9.2 User access management (6) A.9.3 User responsibilities (1) A.9.4 System and application access control (5) → *Now: covered by A.9.4* → *Now: covered by A.9.4* → *Now: A.6.2*
A.12 Information systems acquisition, development and maintenance (6/16) A.12.1 Security requirements of inform. systems (1) A.12.2 Correct processing in applications (4) A.12.3 Cryptographic controls (2) A.12.4 Security of system files (3) A.12.5 Security in developm. & support processes (5) A.12.6 Technical vulnerability management (1)	→ *Now: A.14* → *Now: A.14.1* → *Now: --- (removed)* **A.10 Cryptography (1/2)** A.10.1 Cryptographic controls (2) → *Now: covered by A.12.5, A.14.3 and A.9.4* → *Now: A.14.2* → *Now: A.12.6*
	A.11 Physical and environmental security (2/15) A.11.1 Secure areas (6) A.11.2 Equipment (9)
	A.12 Operations security (7/14) A.12.1 Operational procedures and responsibilities (4) A.12.2 Protection from malware (1) A.12.3 Backup (1) A.12.4 Logging and monitoring (4) A.12.5 Control of operational software (1) A.12.6 Technical vulnerability management (2) A.12.7 Information systems audit considerations (1)
	A.13 Communications security (2/7) A.13.1 Network security management (3) A.13.2 Information transfer (4)
	A.14 System acquisition, development and maintenance (3/13) A.14.1 Security requirements of inform. systems (3) A.14.2 Security in developm. & support processes (9) A.14.3 Test data (1)
	A.15 Supplier relationships (2/5) A.15.1 Information security in supplier relationships (3) A.15.2 Supplier service delivery management (2)
A.13. Information security incident mgmt. (2/5) A.13.1 Reporting security events and weaknesses (2) A.13.2 Management of security incidents (3)	**A.16. Information security incident mgmt. (1/7)** A.16.1 Management of security incidents (7) → *Now: covered by A.16.1*
A.14 Business continuity management (1/5) A.14.1 Security aspects of bus. continuity mgmt.. (5)	**A.17 Information security aspects of business continuity management (2/4)** A.17.1 Information security continuity (3) A.17.2 Redundancies (1)
A.15 Compliance (3/10) A.15.1 Compliance with legal requirements (6) A.15.2 Compliance with security policies and standards, and technical compliance (2) A.15.3 Information systems audit considerations (2)	**A.18 Compliance (2/8)** A.18.1 Compl. w. legal & contractual requirements (5) A.18.2 Information security reviews (3) → *Now: A.12.7*
Total number of topic sections: 11 (5-15) Total number of control objectives: 39 **Total number of controls: 133**	Total number of topic sections: 14 (5-18) Total number of control objectives: 35 **Total number of controls: 114**

Quelle: Thomas Schaaf, ISO/IEC 27001:2013 –
Der neue Standard für Informationssicherheits-Management

Kapitel 2: Inhalt

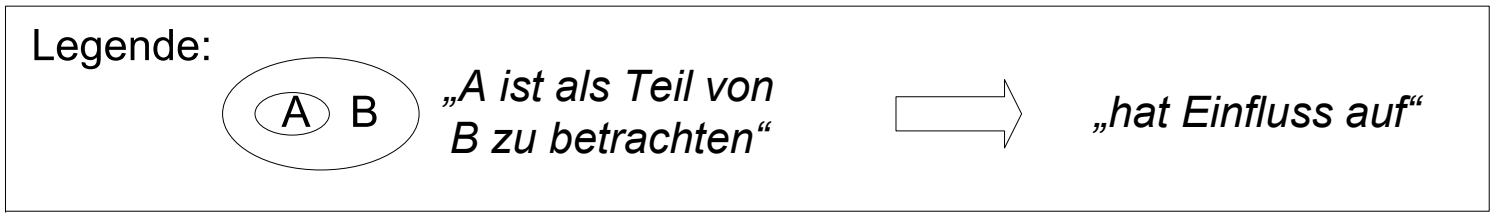
1. Grundlegende Ziele der IT-Sicherheit
2. Kategorisierung von Sicherheitsmaßnahmen
3. Standards der ISO/IEC 27000 - Reihe
4. Security vs. Safety

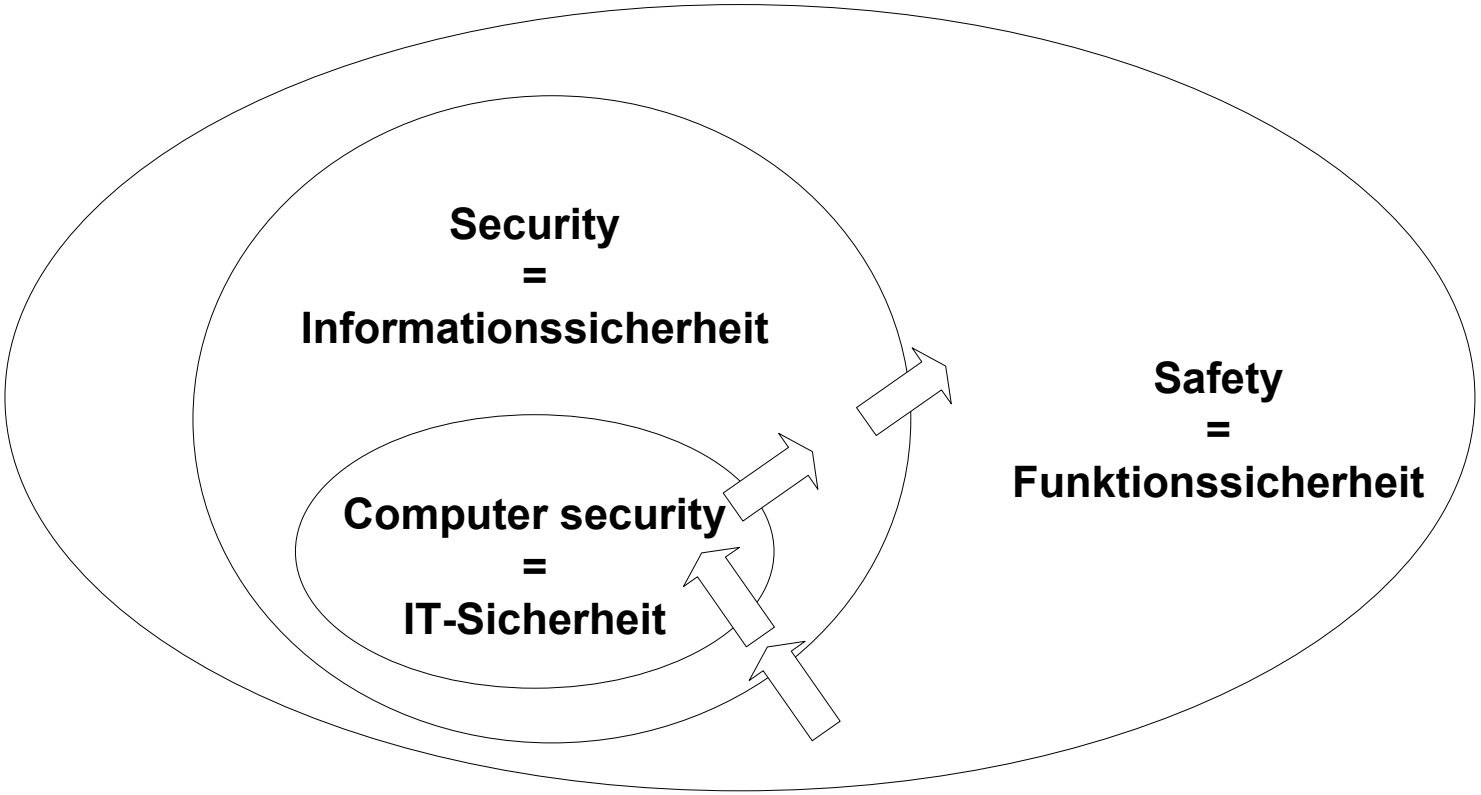
Unterscheidung von Security und Safety

- Beide Begriffe werden oft mit „Sicherheit“ übersetzt
- Typische Themen der Safety („Funktionssicherheit“)
  - Betriebssicherheit für sicherheitskritische Programme, z.B. Steuerung und Überwachung von Flugzeugen oder Kraftwerken
  - Ausfallsicherheit (Reliability)
  - Gesundheitliche Sicherheit / Ergonomie
- Typische Themen der Security („Sicherheit“ i.S.d. Vorlesung)
  - Security Engineering
  - Security Policies
  - Sicherheitsanforderungen:
    Identifikation, Authentisierung, Autorisierung, Zugriffskontrolle, ...
  - Sicherheitsmaßnahmen realisieren Sicherheitsanforderungen
  - „C I A” von Daten und Diensten

Einordnung Safety/Security (1/2)

(nach Hartmut Pohl)





Einordnung Safety/Security (2/2)

(nach Hartmut Pohl)