



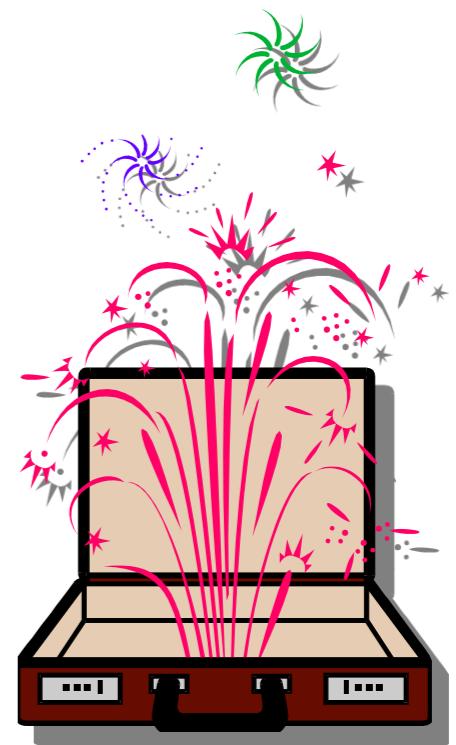
Sicherheitsnormen und Standards

DI Herfried Geyer

Wintersemester 2016/17

Agenda WS 16/17

- Informationssicherheit - Ziele, Motivation, Blickwinkel, Normierung, Überblick
- Informationssicherheits – Managementsystem gemäß ISO 27001:2013
- ISO 27002:2013 Controls & Control Objectives
- ISO 27003, 27004, 27005
- BSI Grundschutzhandbuch
- Cobit, NIST u.a.



Arbeitsgruppen / Teams

- > Sortieren sie sich zu Teams bis max. 4 Personen!
- > Überlegen sie sich eine Teambezeichnung (Branding, „kreativ“)
- > Die Teamstruktur soll bis Veranstaltungsende bestand haben
- > Binäre Voraussetzung zum Prüfungsantritt:
 - abgegeben + „sinnvoll“ = Antritt zu Prüfung
 - nicht abgegeben = **kein Antritt zur Prüfung**



Bewertung der Arbeiten

- > Jede Gruppe muss zumindest vier mal präsentieren!
- > Alle Gruppenarbeiten sind am e-Campus abzugeben (pro Team).
- > Jedes Team wählt seine „beste“ Arbeit aus, die mit zur Benotung beiträgt.
- > Benotung der ausgewählten Übung:
 - Gute Ausarbeitung in Form und Stil
 - Inhalt schlüssig und komplett
 - Erkennbar ist:
Das erlernte konnte angewendet, synthetisiert und ergänzt werden.
- > Wesentlich: Am Deckblatt jeder Abgabe alle Mitarbeitenden anführen!

Agenda Topic 1

- Informationssicherheit - Ziele, Motivation, Blickwinkel, Normierung, Überblick
 - Zielsetzungen, Anforderungen
 - Definitionen
 - Grundsätzliches zur Normierung
 - Überblick über die wesentlichsten Normen

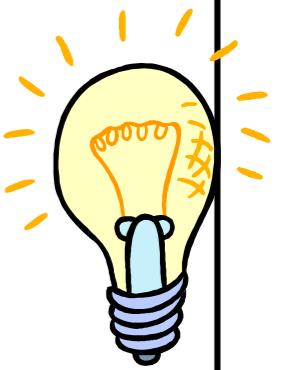
Für viele Organisationen stellt sich folgende Frage zu ihrer Informationssicherheit:

‘Wie können wir uns am besten schützen?’



Viel wichtiger wäre zuerst zu fragen:

1. *Warum* brauche ich überhaupt Sicherheit?
2. In *welchen Ausmaß* brauche ich Sicherheit ?
3. *Was* und gegen *wen* soll ich mich schützen?
4. Erst dann _____



Motivation - IS Forderungen - Ziele



Definitionen

Definition Vertraulichkeit:

Vertraulichkeit besteht darin, Daten nur dem Personenkreis zugänglich zu machen, der auch befugt ist, darauf zuzugreifen. Diese Befugnis ist wiederum durch Vereinbarungen geregelt, die sich unter anderem in der Berechtigungsvergabe auf IT - Systemen manifestieren.

Confidentiality:

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO/IEC 27000:2014]

Definitionen

Definition Verfügbarkeit:

Verfügbarkeit im Kontext der Informationssicherheit fordert, dass Daten und Applikationen vereinbarungsgemäß zur Verfügung stehen müssen.

Vereinbarungsgemäß bedeutet in diesem Zusammenhang, die Verfügbarkeit auf entsprechende Personen oder Dienste innerhalb abgestimmter Zeiträume, zumeist noch mit einer geringen Toleranz versehen, einzugrenzen.

Availability:

The property of being accessible and usable upon demand by an authorized entity [ISO/IEC 27000:2014]

Definitionen

Definition Integrität:

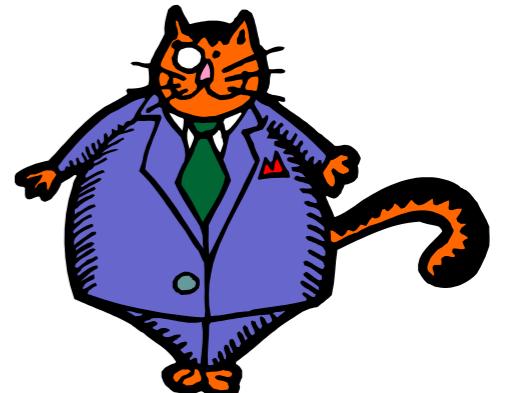
Diese Anforderung bedingt dafür Sorge zu tragen, dass Daten, Applikationen oder Systeme nicht unberechtigt verändert werden können beziehungsweise jegliche Veränderung bei Anwendung erkannt wird.

Integrity:

The property of protecting the accuracy and completeness (of assets)
[ISO/IEC 27000:2014]

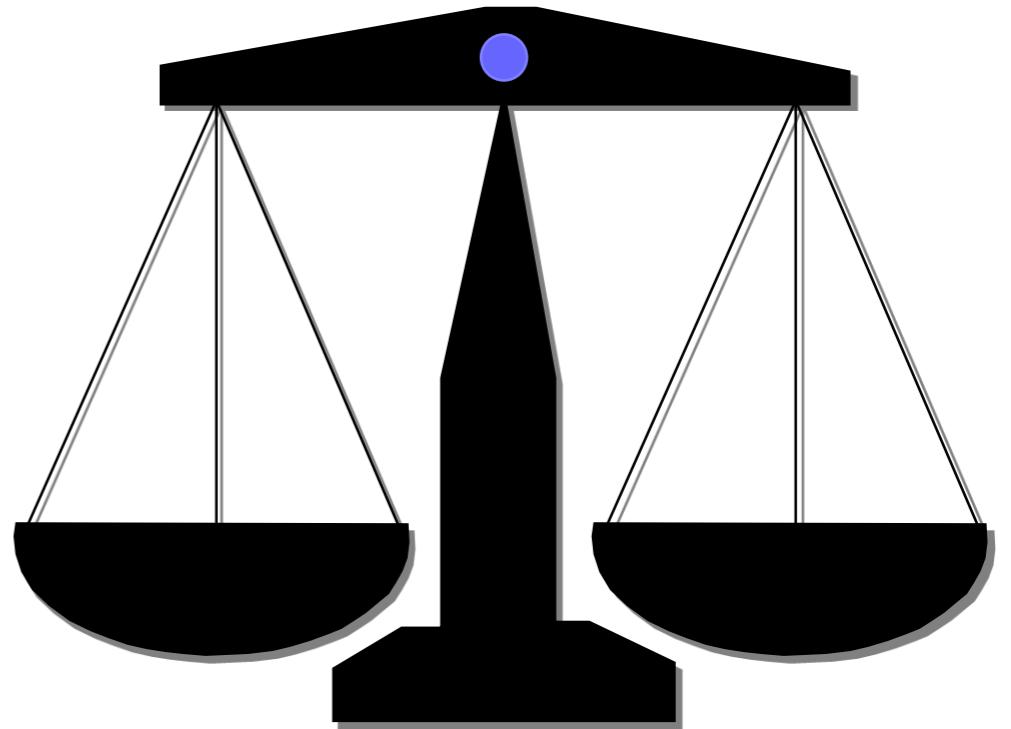
Motivation Top Management

- Erfüllen gesetzlicher Anforderungen
- Reduktion von Systemausfällen, dadurch konstantere Produktion bzw. Serviceerbringung
- Verhinderung von möglichem Imageverlust
- IS als Marketinginstrument
- IS als Voraussetzung für Beauftragung (Kundenanforderung)



Erfüllen gesetzlicher Anforderungen

- Datenschutzgesetz
- Urheberrecht
- E-Commerce Gesetz
- Verbandhaftungsgesetz
- Gesundheitstelematikgesetz
- Aktien-, GmbH Gesetz
- Informationssicherheitsgesetz

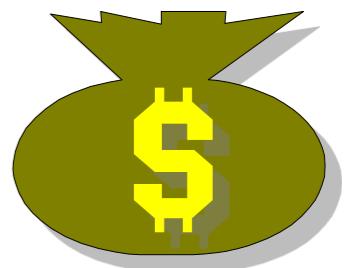


Erfüllen gesetzlicher Anforderungen

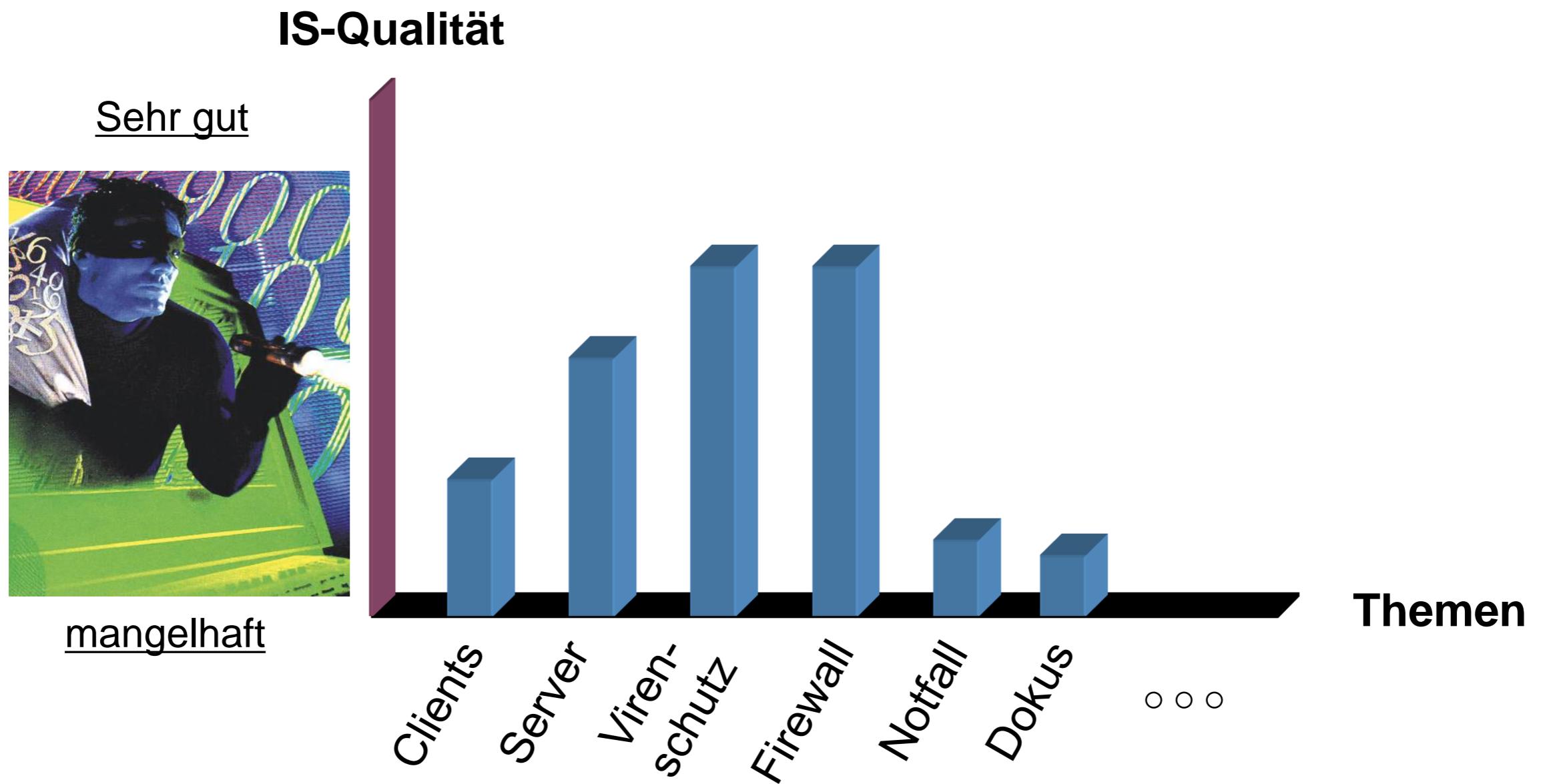
- § 118a StGB Widerrechtlicher Zugriff auf ein Computersystem
- § 119 StGB Verletzung des TK Geheimnisses
- § 119 a StGB Missbräuchliches Afangen von Daten
- § 120 (2a) StGB Missbrauch von Tonaufnahme- oder Abhörgeräten
- § 123 (1) StGB Auskundschaftung eines Gesch.- oder Betr. Geheimnisses
- § 126 abc Datenbeschädigung, Störung der Funktionsfähigkeit, Missbrauch von Computerprogrammen oder Zugriffsdaten
- § 148a Betrügerischer Datenverarbeitungsmissbrauch
- § 225a Datenfälschung

Konstante Produktion bzw. Serviceerbringung

- Einhalten von Verträgen (finanzialer Aspekt)
- Service Level Agreements / Operational Level Agreements
- Kundenzufriedenheit
- Hohe Qualität der Leistungserbringung
- Kostenreduktion bei Incidentmanagement
- Kostenreduktion bei Problemmanagement
- Geringe Ausschussproduktion



„Etablierte“ Informationssicherheit



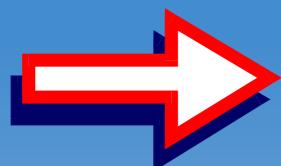
Einordnung IT-Sicherheit

Unternehmenssicherheit

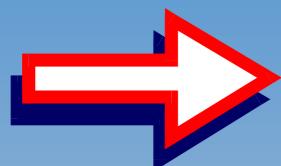
Informationssicherheit

IT-Sicherheit

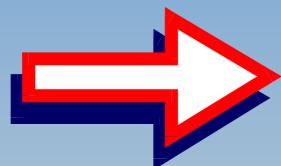
Sichtweisen hinsichtlich IS



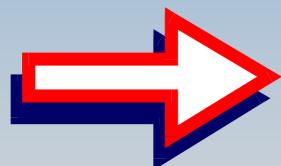
Geschäftsleitung / oberstes Management



IT-Management



Anwender



System-Administrator

Viele Wege führen zur IS!

Welcher ist der effizienteste?



Definition lt. EN ISO 9241-11:

- *Effektivität:* Die Genauigkeit und Vollständigkeit mit der [...] ein Ziel erreicht wird.
- *Effizienz:* Der im Verhältnis zur Genauigkeit und Vollständigkeit eingesetzte Aufwand, mit dem [...] ein Ziel erreicht wird.

Warum Normung?

Jeder Franken, der in die Internationale Normung investiert wird, bringt Vorteile im Wert von 25 Franken.

Die Teilnahme am Normungsprozess ist aus vielerlei Gründen ein strategisch wichtiger Entscheid. Denn es genügt nicht, die bestehenden Normen einfach nur zu nutzen. Marktfähig wird auf Dauer nur sein, wer aktiv bei der Erarbeitung von Normen mitwirkt, beispielsweise in einem Technischen Komitee (TK) der SNV. Aktive Mitarbeit bietet nämlich zwei entscheidende Vorteile: Informationsvorsprung und Mitsprache.

Unternehmen, die in den Normungsprozess involviert sind, können ihre Produkte und Dienstleistungen von Anfang an richtig entwickeln und erfolgreich auf den Markt bringen. Sie können durch Mitgestaltung der Rahmenbedingungen schneller Folgeprodukte entwickeln und so ihre Marktposition langfristig sichern und verbessern.

<http://www.snv.ch/>

Warum Normung?

Der volkswirtschaftliche Nutzen der Normung wird auf ungefähr 1 % des Bruttoinlandprodukts (BIP) geschätzt.

Zu diesem Ergebnis kam eine Studie des Deutschen Instituts für Normung (DIN), des Österreichischen Normungsinstitutes (ASI) und der Schweizerischen Normen-Vereinigung (SNV). Normung erzeugt also neben dem betriebswirtschaftlichen auch einen hohen volkswirtschaftlichen Nutzen. Für die Schweiz sind dies mehr als 4 Milliarden CHF pro Jahr - eine gewaltige Summe, die durch eine Reihe positiver Folgen der Normung zusammenkommt.

Warum Normung?

Positive Folgen der Normung:

- besserer Zugang für (öster.) Unternehmen zum Außenhandel
- kürzere Entwicklungszeiten für neue Produkte schnellere Zulassung von österr. Produkten im Ausland dank Produktkonformität
- Einsparungen durch Selbstdeklaration und Vermeidung von Drittprüfungen
- verbesserte Einkaufsprozesse dank Bezug auf Normen in der Produkte-Definition und -Qualität
- damit verbundene kürzere Lagerzeiten, Just-in-time-Produktion
- Produktsicherheit für Konsumenten
- Gesundheit und Sicherheit für die Gesellschaft
- Risikominderung in Betrieben und im öffentlichen Leben

Arten von Normen:

Die Normen werden im Wesentlichen von ihren Zielfunktionen bestimmt, die dann den Inhalt und die Verbindlichkeit der Normen bestimmen.

Man unterscheidet u.a.:

- Verständigungsnormen: definieren Begriffe, Symbole u.a.m.
- Produktnormen: beinhalten Gütefestlegungen und Leistungsmerkmale für Erzeugnisse
- Verfahrensnormen: beschreiben Berechnungs-, Herstellungs-, Betriebs- und Prüfverfahren

Definition der Normungsarbeit

Normung ist die planmäßige, durch die interessierten Kreise gemeinschaftlich durchgeführte Vereinheitlichung von materiellen und immateriellen Gegenständen zum Nutzen der Allgemeinheit.

Sie darf nicht zu einem wirtschaftlichen Sondervorteil einzelner führen.

Sie fördert die Rationalisierung und Qualitätssicherung in Wirtschaft, Technik, Wissenschaft und Verwaltung.

Sie dient der Sicherheit von Menschen und Sachen sowie der Qualitätsverbesserung in allen Lebensbereichen.

aus DIN 820-1, *Normungsarbeit - Grundsätze*

Was ist eine Norm?

Ein Dokument, das

- auf Konsens beruht
- von einem anerkannten Gremium angenommen wurde
- für die allgemeine und wiederholte Anwendung Regeln, Leitlinien oder Merkmale für Aktivitäten oder deren Ergebnisse aufstellt
- darauf abzielt, in einem gegebenen Kontext ein optimales Maß an Ordnung zu erreichen
- auf den konsolidierten Ergebnissen von Wissenschaft, Technologie und Erfahrung beruht

Konsens (Definition nach EN 45020)

„allgemeine Zustimmung, die durch Fehlen aufrechterhaltener Widersprüche gegen wesentliche Inhalte seitens irgendeines wichtigen Anteils der betroffenen Interessen und durch ein Verfahren gekennzeichnet ist, das versucht, die Gesichtspunkte aller betroffenen Parteien zu berücksichtigen und Gegenargumente auszuräumen.“

ANMERKUNG: Konsens bedeutet nicht notwendigerweise Einstimmigkeit.“

Normengesetz (BGBI. Nr. 240/1971)

§ 1. (1) Der Bundesminister für Bauten und Technik kann einem Verein, dessen Zweck die Schaffung und Veröffentlichung von Normen und dessen Tätigkeit nicht auf Gewinn berechnet ist, nach Maßgabe der folgenden Bestimmungen die Befugnis verleihen, die von ihm geschaffenen Normen als „Österreichische Normen“ („ÖNORMEN“) zu bezeichnen.



Rechtsverbindlichkeit

Normen

- bilden einen Maßstab für einwandfreies technisches Verhalten;
- stehen jedermann zur Anwendung frei, d. h. man kann sie anwenden, muss es aber nicht;
- sind im Rahmen der Rechtsordnung von Bedeutung;
- werden verbindlich durch Bezugnahme, z. B. in einem Vertrag zwischen privaten Parteien oder in Gesetzen und Verordnungen;
- dienen im Streitfall als Entscheidungshilfe (Beweis des ersten Anscheins).

Grundsätze der Normungsarbeit

- Freiwilligkeit
- Beteiligung aller interessierten Kreise
- Konsens
- Einheitlichkeit
- Widerspruchsfreiheit
- Sachbezogenheit
- Stand der Wissenschaft und Technik
- Wirtschaftlichkeit
- Allgemeiner Nutzen
- Internationalität

Wer arbeitet mit? Die „interessierten Kreise“

- Wirtschaft (=„Organisationen“)
- Öffentliche Hand (=„Gesellschaft“)
- Gewerkschaften (=„Gesellschaft“)
- Verbraucher (=„Gesellschaft“)
- Nichtregierungsorganisationen (=„Gesellschaft“)
- Andere (z.B. Wissenschaft, Berater) (=„Gesellschaft“)

Ausgewogene Vertretung soll gewährleistet sein!

Internationale Normung

Die weltweite Normung wird von der

- Internationalen Organisation für Normung (ISO), der
- Internationalen Elektrotechnischen Kommission (IEC) und der
- Internationalen Fernmeldeunion - Telekommunikationssektor (ITU-T),

alle mit Sitz in Genf, wahrgenommen.



Internationale Normung

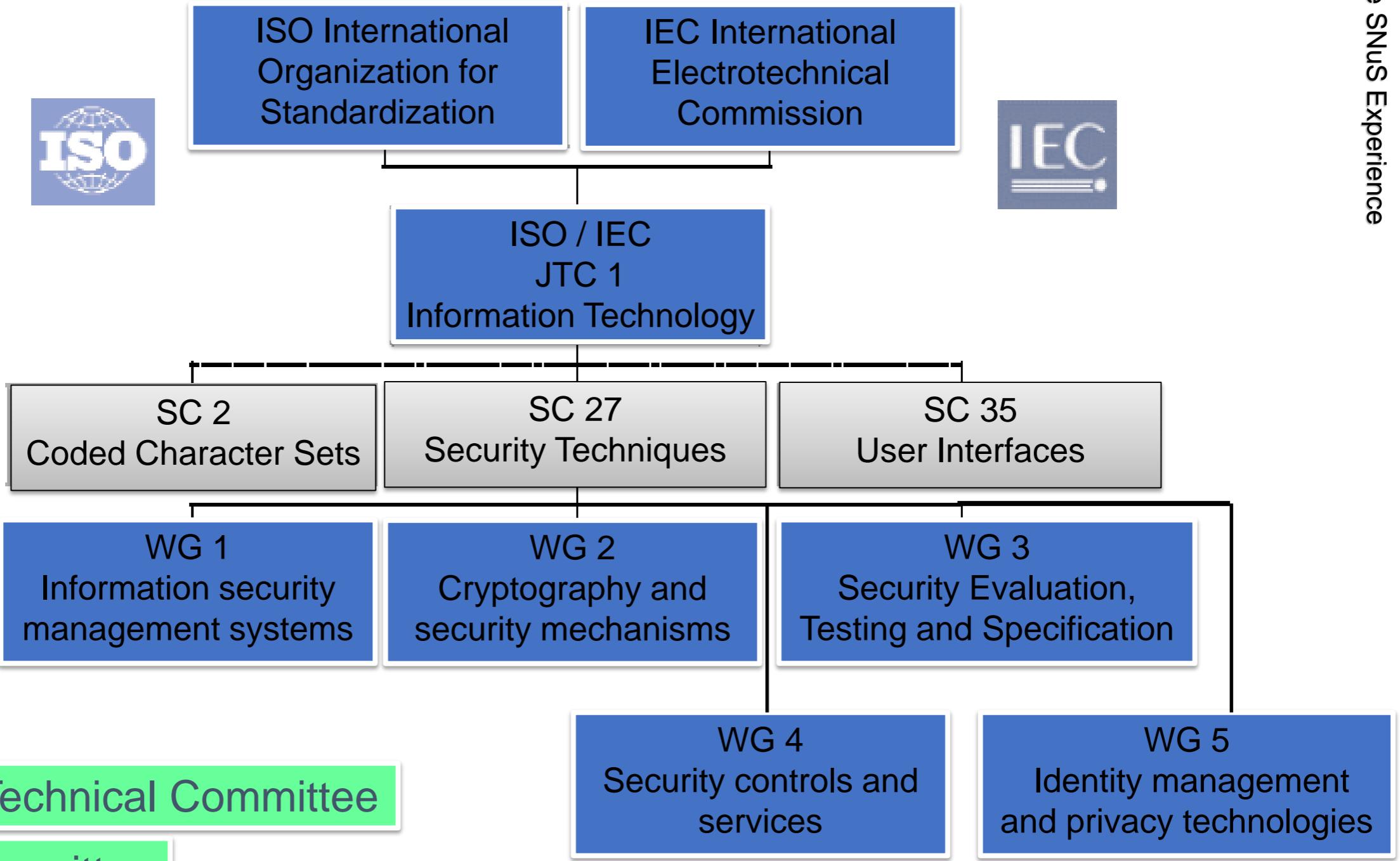
In der ISO arbeiten die nationalen Normungs-institute aus 120 Ländern zusammen.

- Österreich wird durch das Österreichische Normungsinstitut vertreten. (www.austrian-standards.at)
- Deutschland wird durch das Deutsche Institut für Normung DIN e. V. vertreten. (www.din.de)
- Schweiz wird durch die SNV Schweizerische Normen-Vereinigung vertreten. (www.snv.ch)

Ziele der Internationalen Normung

- Erarbeitung weltweit einheitlicher Normen (ISO- oder IEC-Normen)
- Erleichterung des internationalen Austauschs von Gütern und Dienstleistungen
- Verbesserte Zusammenarbeit auf wissenschaftlichem, technischem und ökonomischem Gebiet über die Grenzen hinweg zu aktivieren.

JTC1 / SC27 / WG1



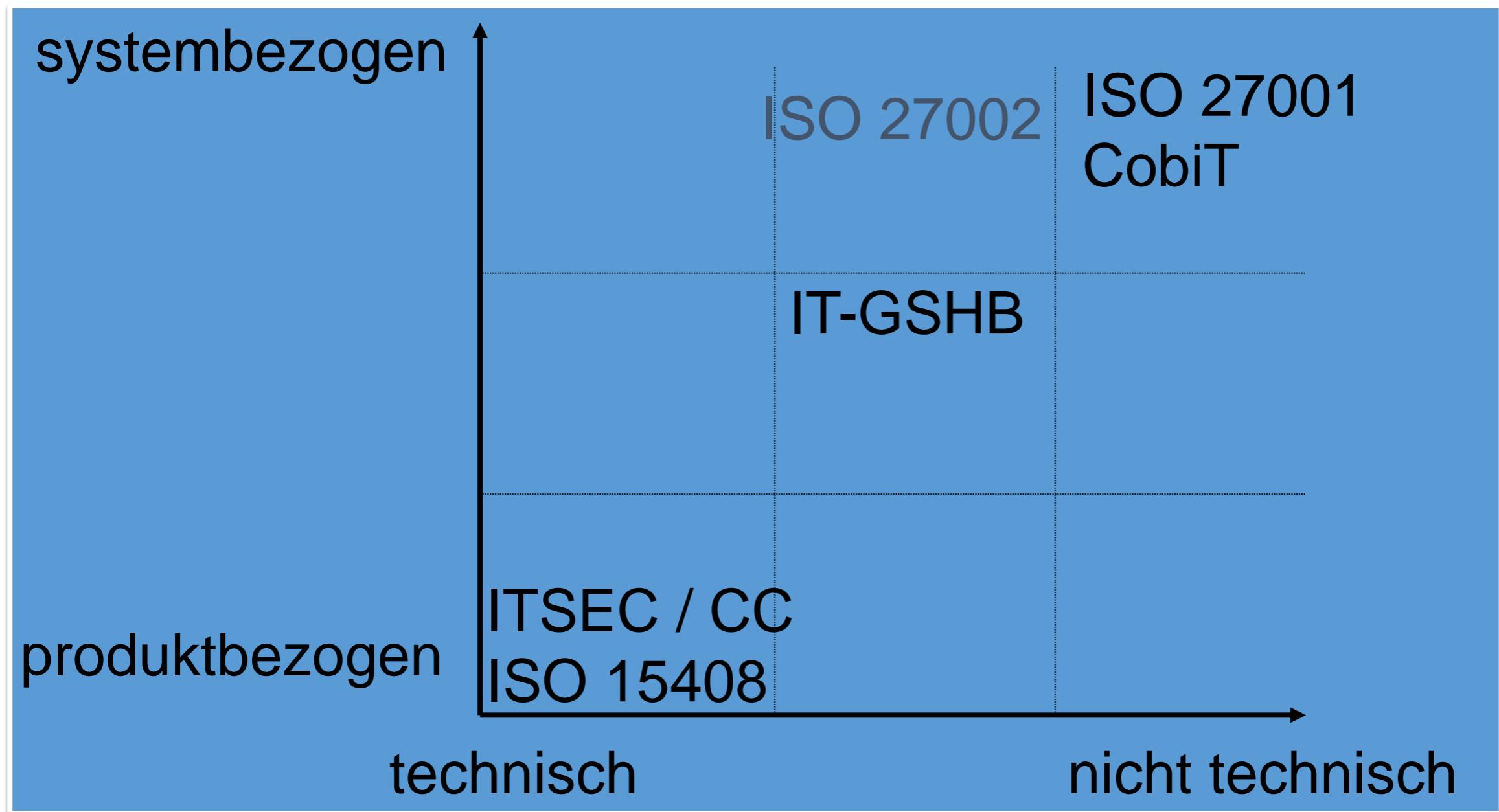
JTC1 Sub Committees

- > SC 02 – Coded Character Sets
- > SC 06 - Telecommunications and Information Exchange Between Systems
- > SC 07 - Software and System Engineering
- > SC 11 - Flexible Magnetic Media for Digital Data Interchange
- > SC 17 - Cards and Personal Identification
- > SC 22 - Programming Languages, their Environments and Systems Software Interfaces
- > SC 23 - Optical Disk Cartridges for Information Interchange
- > SC 24 - Computer Graphics and Image Processing
- SC 25 - Interconnection of Information Technology Equipment

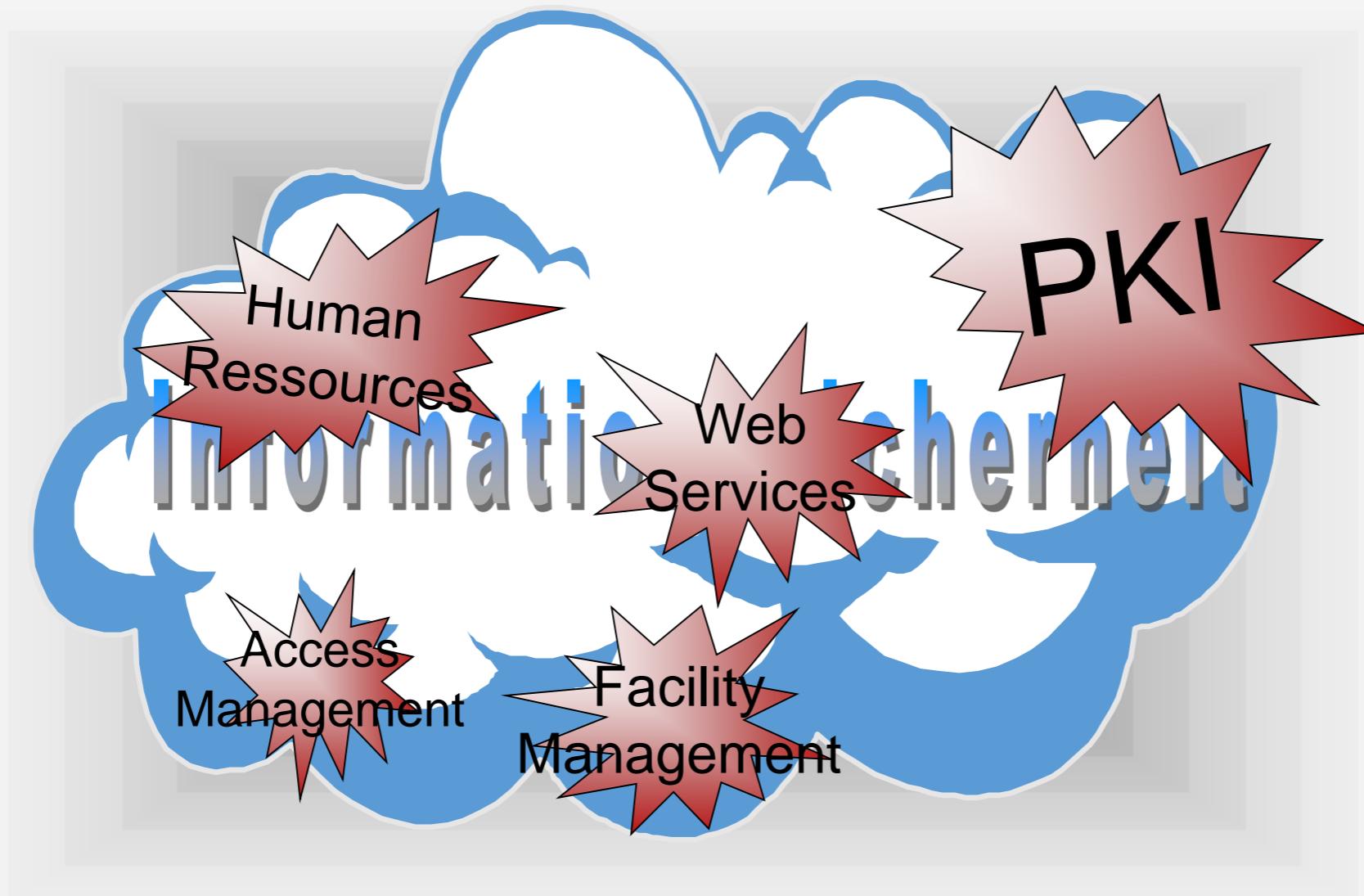
- > SC 27 - IT Security Techniques
- > SC 28 - Office Equipment
- > SC 29 - Coding of Audio, Picture, and Multimedia and Hypermedia
- > SC 31 - Automatic Identification and Data Capture Techniques
- > SC 32 - Data Management and Interchange
- > SC 34 - Document Description and Processing Languages
- > SC 35 - User Interfaces
- > SC 36 - Learning Technology
- > SC 37 - Biometrics

The SNuS Experience

Sicherheitsstandards Einordnung



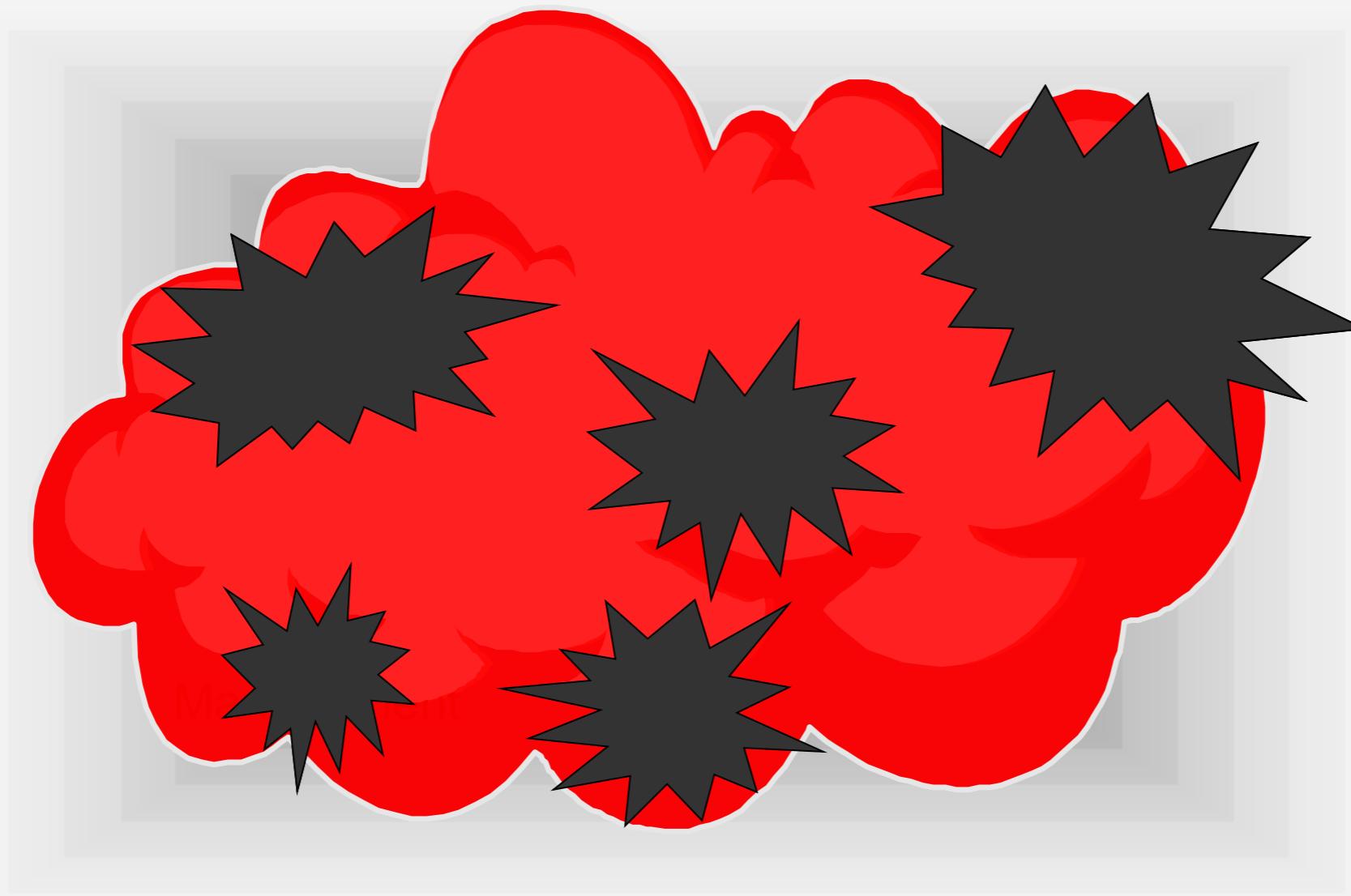
Kaleidoskop der IS-Abdeckung



Kaleidoskop der IS-Abdeckung

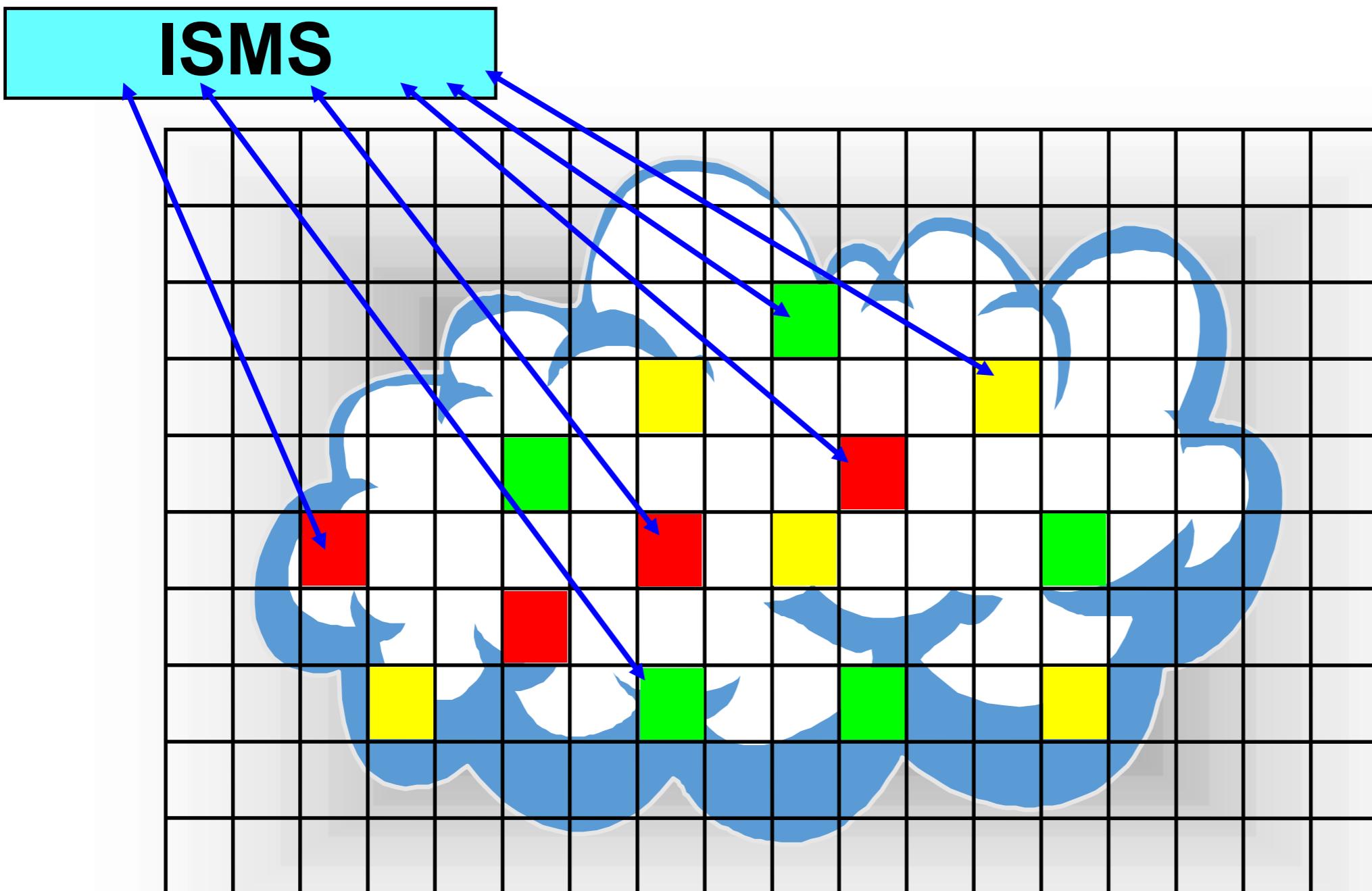


The SNuS Experience



Risiken, Potentiale, Wissen

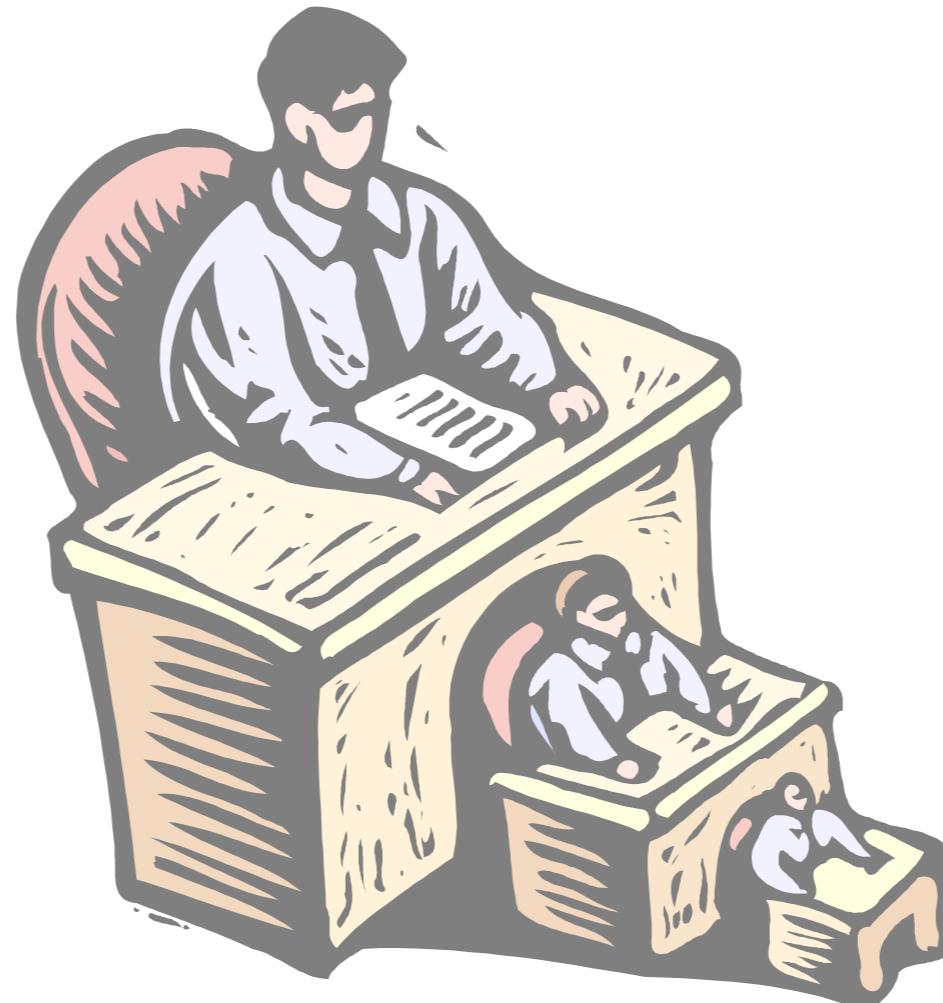
The SNuS Experience



IS - Managementsystem

Management: wesentliche Aspekte

- leiten
- planen
- kontrollieren
- überwachen
- steuern



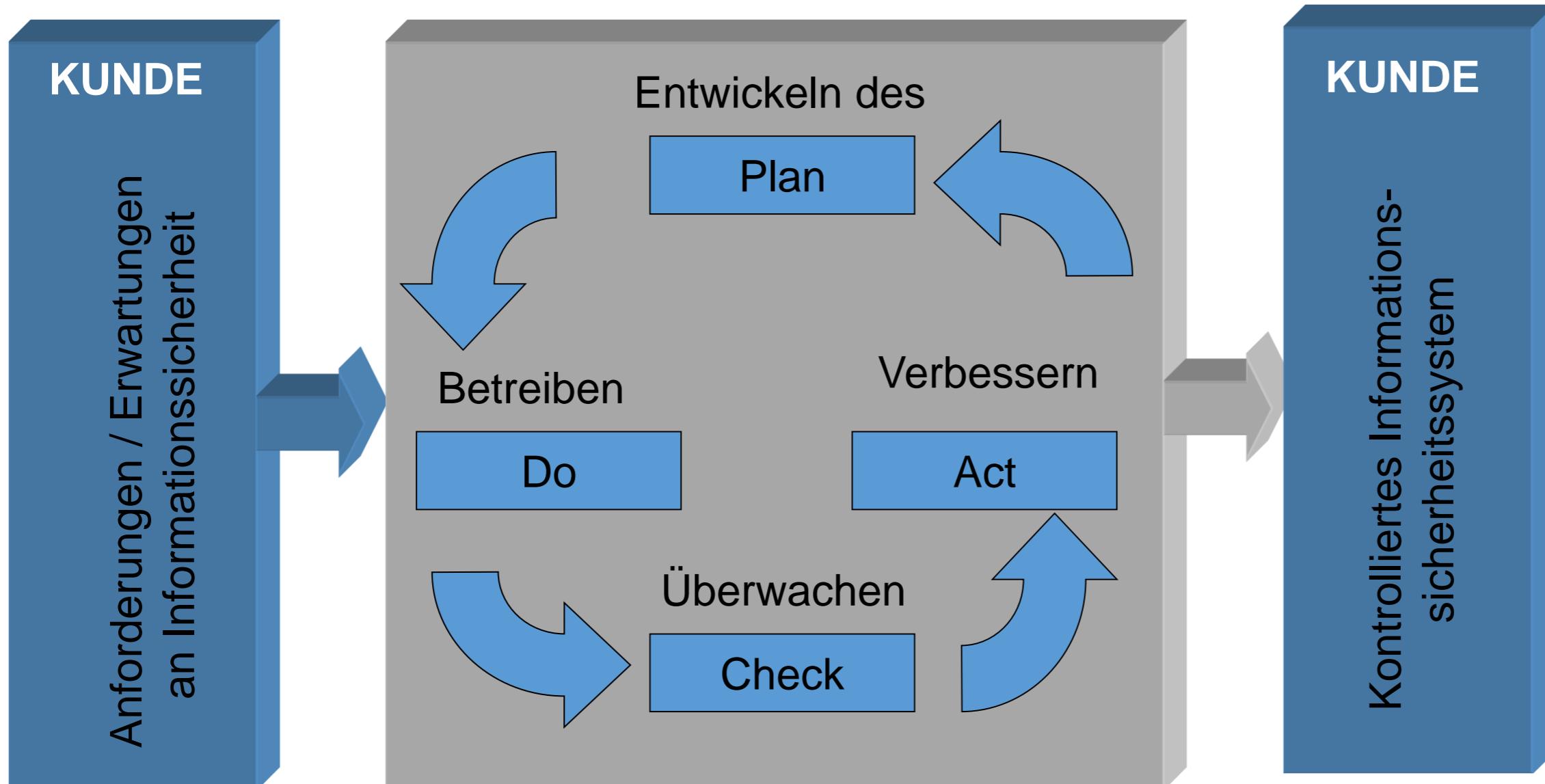
Durch Etablieren eines Managementsystems für Informationssicherheit werden die entsprechenden Risiken erkennbar und bewertbar, durch den Einsatz entsprechender Maßnahmen schließlich auch tragbar.

Historisch: ISMS It. BS7799:2-1999

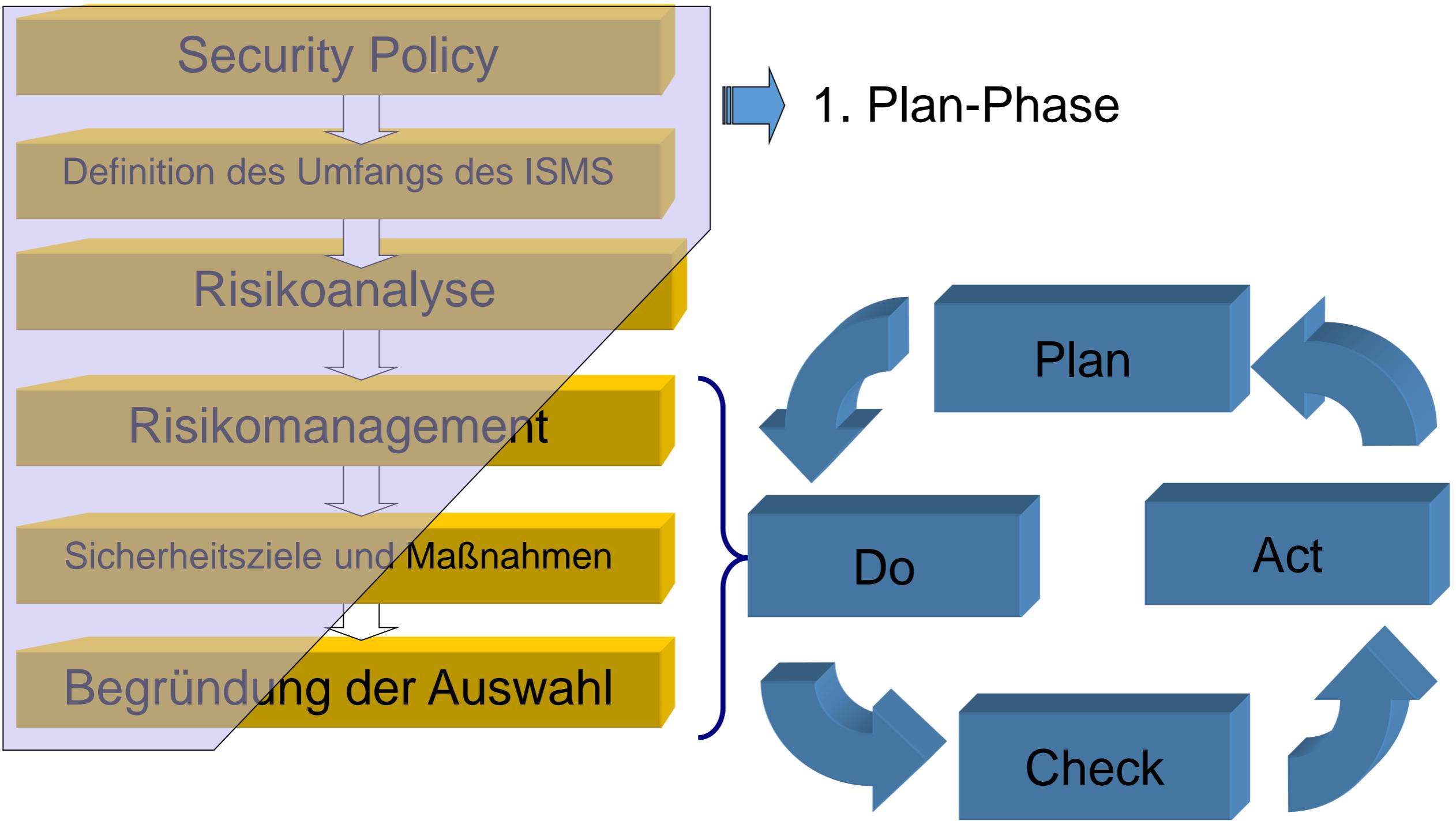


IS - Managementsystem

ISO 27001 - Das PDCA Modell



IS - Managementsystem



IS - Managementsystem

ISO 27001:2013

**Information technology - Security techniques -
Information security management systems –
Requirements**



IS - Managementsystem

ISO 27001:2013



Es erfolgt eine grundlegende Strukturänderung zur Vereinheitlichung mit anderen Managementstandards

Basis ist eine ISO Direktive, die an alle Entwicklungsgruppen ergangen ist und verpflichtend umzusetzen ist

ISO/IEC Directives, Part 1 Annex SL

Damit ist ein gemeinsames Rahmenwerk geschaffen, das vor allem Unternehmen unterstützt, die mehrere Normen(themen) in einem Managementsystem betreiben.

ISO 27001:2013

Die neue Struktur!

- Unternehmenszusammenhänge
(Context of the organization)
- Führungsverantwortung (Leadership)
- Planung (Planning)
- Voraussetzungen und Mittel (Support)
- Betrieb (Operation)
- Wirksamkeitsprüfung (Performance evaluation)
- Verbesserung (Improvement)



Unternehmenszusammenhänge (1)

(Context of the organization)

Wesentliche Anforderung:

Informationssicherheit muss in all seinen Ausprägungen und Belangen integraler Teil der Organisationsprozesse und –abläufe sein

Das bedeutet vor allem:

Dass Informationssicherheit als grundsätzlicher Anspruchsträger beim Design von

- Prozessen und Verfahren,
- Informationsverbünden und verarbeitenden Systemen sowie
- Maßnahmen einzubeziehen ist.

Unternehmenszusammenhänge (2)

(Context of the organization)

Kennenlernen und verstehen der Belange und Notwendigkeiten zur Informationssicherheit der Organisation (Umfeldanalysen, Unternehmensstrategie,...)

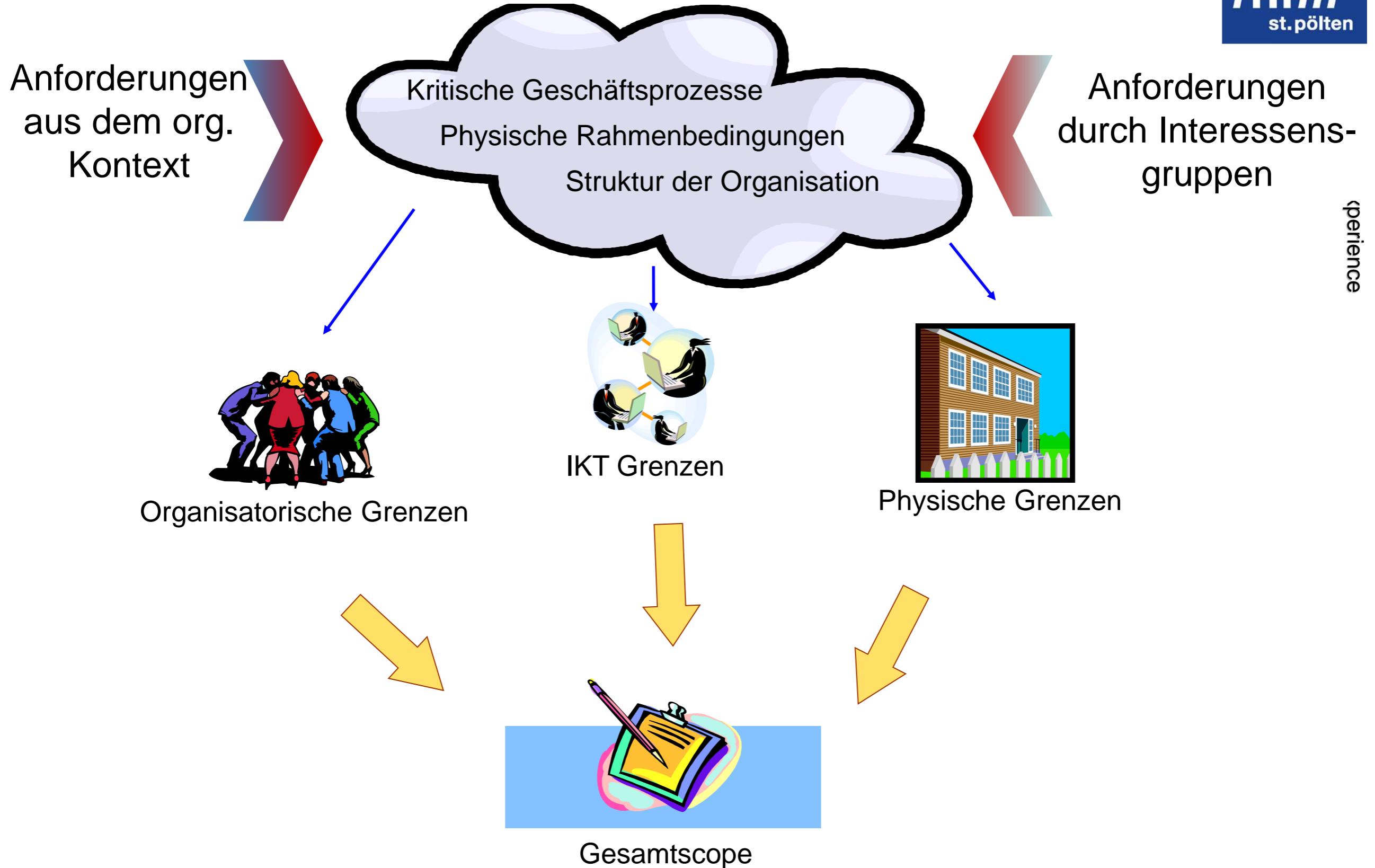
Verständnis entwickeln für die Anforderungen und Erwartungen externer Anspruchsgruppen

- Anspruchsgruppen bzgl. ISMS
- Anspruchsgruppen bzgl. IS

Festlegen des Scopes für das ISMS



Festlegen des Scopes für das ISMS



Die organisatorischen Grenzen

Eine Möglichkeit der Strukturierung ist, die Verantwortungsbereiche im Unternehmen, die mit den kritischen Geschäftsprozessen im Zusammenhang stehen, zu selektieren.

Dabei zu bedenken:

- Die Auswahl wird die Zusammensetzung des IS Management Forums beeinflussen
- Die Gesamtverantwortung sollte ungeteilt einer übergeordneten Stelle übertragen werden
- Alle relevanten Assets sind im Rahmen der Risikoanalyse zu bewerten und sollten damit innerhalb des Scopes sein
- Der ISMS PDCA Zyklus läuft nur innerhalb des Scopes.

Scope bzgl. Informations- und Kommunikationstechnologien

Alle IKT Systeme, die kritische Informationswerte verarbeiten, speichern und transportieren sind mit einzubeziehen

Dabei zu bedenken:

- Achtung: das ist keine technologisch bedingte Abgrenzung
- IKT Systeme sind i.d.R. organisationsübergreifend strukturiert
- Besonders zu beachten sind folgende Einflüsse, die auftreten können wenn Unternehmens- oder Staatsgrenzen überschritten werden:
 - Sozio-kulturelles Umfeld
 - Gesetzliche und vertragliche Verpflichtungen
 - Zuordnbarkeit von Schlüsselverantwortungen
 - Technische Einschränkungen (Kapazitäten, Verfügbarkeiten,...)

Die physischen Grenzen

Umfasst jene Niederlassungen, Außenstellen und Facilities, die Teil des ISMS sein sollen.

Dabei zusätzlich zu bedenken:

- phys. Voraussetzungen bei mobilen Zugang
- phys. Voraussetzungen bei Teleworking
- Anforderungen an Lieferanten (Service Delivery)
- Anforderungen bezüglich kableloser Kommunikation
(Überschreiten der phys. Grenzen)

Die Ergebnisse der organisatorischen, technischen und physischen Eingrenzung werden im Gesamtscopestatement zusammengefasst



ISO 27001:2013

Die neue Struktur!



The SNuS Experience

✓ Unternehmenszusammenhänge
(Context of the organization)

Führungsverantwortung (Leadership)

Planung (Planning)

Voraussetzungen und Mittel (Support)

Betrieb (Operation)

Wirksamkeitsprüfung (Performance evaluation)

Verbesserung (Improvement)

Verantwortung der Leitung (Leadership)

- Die Sicherheitsziele sind an die strategische Ausrichtung der Organisation angepasst
- Die Tätigkeiten und Verfahren des ISMS sind in die organisationseigenen Prozesse integriert
- Sicherstellen, dass ausreichend Ressourcen für den Betrieb des ISMS vorhanden sind
- Die Ziele und Aufgaben des ISMS nach innen und außen schlüssig vertreten
- Übergeordnet die Personen (Rollen) unterstützen, die das ISMS betreiben und weiterentwickeln
- Demonstrativ den (Führungs)anspruch der ISMS Management – Rollen aufzeigen

Verantwortung der Leitung (Leadership)

Management Commitment:

Die Entscheidungsträger verstehen den Sinn und Nutzen von IS und dem Betrieb eines ISMS. Unterstützung, Interesse und Engagement seitens des Managements ist somit gegeben

Management Commitment zeigt sich durch:

- Periodische Reviews durch die Leitung und eine enge Verknüpfung von IS und Geschäftstätigkeit
- Interesse und Kontrolle des Implementierungsfortschritts
- Sonderbudget für die ISMS Errichtung zur Verfügung stellen
- Schaffung eines IS-Forums, an dem die Schlüsselpositionen der Organisation teilnehmen, Management und Prozessverantwortliche wirken operativ an IS Vorhaben mit
- Review der Restrisiken, auch derer, die unter einer Akzeptanzschwelle liegen
- Bereitstellen von Personen mit entsprechenden Skills

Verantwortung der Leitung (Leadership)

Top Management setzt eine IS-Policy in Kraft die:

- Generelle Ziele und Prinzipien vorgibt, bzw. ein Framework zur Entwicklung derselben
- Stellung bezieht, dass gerechtfertigte Anforderungen an IS zu erfüllen sind
- Festlegt, dass das ISMS durch permanente Anpassungen und Verbesserungen seine Wirksamkeit bewahrt.

 - = Richtungsvorgabe seitens der Unternehmensführung

Verantwortung der Leitung (Leadership)

Top Management sorgt für die Zuordnung von Verantwortungen und Errichtung von Stellen zur

- Umsetzung und Abwicklung von IS und dem
- Betrieb des ISMS

Damit ist gewährleistet, dass

- das ISMS entsprechend der Vorgaben der Norm betrieben werden kann und
- Top Management über die Leistungsfähigkeit des ISMS informiert wird

ISO 27001:2013

Die neue Struktur!



The SNuS Experience

- ✓ Unternehmenszusammenhänge
(Context of the organization)
- ✓ Führungsverantwortung (Leadership)
 - Planung (Planning)
 - Voraussetzungen und Mittel (Support)
 - Betrieb (Operation)
 - Wirksamkeitsprüfung (Performance evaluation)
 - Verbesserung (Improvement)

Planung (Planning)

- Aktivitäten um Risiken und Chancen zu steuern
 - IS Risikoanalysen
 - IS Risikobehandlung
- IS Ziele und die Planung um diese zu erreichen



Risikoanalysen

- Einen Risikoanalyseprozess festlegen, der unter anderem sicherstellt, dass
 - alle wesentlichen Kriterien zur Risikoanalyse definiert sind (Akzeptanz, Bewertungsmethoden,...)
 - wiederholt durchgeführte Risikoanalysen konsistente, nutzbare und vergleichbare Resultate erzielen

also:



- IS Risiken identifizieren
- diese analysieren
- und evaluieren (den Kriterien entsprechend priorisieren)

Risikobehandlung

- Einen Riskobehandlungsprozess festlegen, der unter anderem sicherstellt, dass
 - angemessene Maßnahmen ausgewählt werden
 - diese mit dem „Statement of Applicability“ verknüpft werden
 - die Maßnahmenumsetzung durch einen dokumentierten Risikobehandlungsplan gesteuert wird
 - die Risikoowner dem Risikobehandlungsplan zustimmen und diesen unterstützen

Statement of Applicability

Festlegen der „Control objectives“ und „Controls“

- Referenzierung auf Anhang A, die 11 Kapitel der ISO 27002 als Arbeitsbasis!



Begründung der getroffenen Auswahl

- Begründung des Maßnahmeneinsatzes und der damit zu erreichenden Ziele



Begründen, welche Controls einzusetzen sind und ebenso welche nicht!

IS Ziele und Zielerreichung

- IS Ziele sind stichhaltig und wirtschaftlich angepasst zu definieren. Dabei folgendes beachten:
 - Den übergeordneten Zielsetzungen der IS-Policy genügen
 - Messbarkeit gewährleisten (wenn möglich)
 - Ergebnisse aus dem Risikomanagement einbeziehen
 - Die Ziele sind angepasst kommunizieren
 - auf Aktualität achten



IS Ziele und Zielerreichung

- Bei der Planung, wie diese Ziele zu erreichen sind ist folgendes zu dokumentieren:
 - Was wird gemacht?
 - Welche Ressourcen sind nötig
 - Wer ist verantwortlich
 - Wann wird die Umsetzung abgeschlossen sein
 - Wie werden die Ergebnisse geprüft

ISO 27001:2013

Die neue Struktur!



The SNuS Experience

- ✓ Unternehmenszusammenhänge
(Context of the organization)
- ✓ Führungsverantwortung (Leadership)
- ✓ Planung (Planning)
- Voraussetzungen und Mittel (Support)
- Betrieb (Operation)
- Wirksamkeitsprüfung (Performance evaluation)
- Verbesserung (Improvement)

Voraussetzungen und Mittel (Support)

→ Ressourcen

Die Organisation muss Ressourcen zur Planung, Errichtung, Wartung und Verbesserung des ISMS festlegen und zur Verfügung stellen

→ Kompetenz

→ Bewusstsein

→ Kommunikation



Voraussetzungen und Mittel (Support)

→ Kompetenz

- Rollenspezifische Kompetenzen festlegen
(etwa Ausbildungserfordernisse CISO)
- Bewertung, ob die eingesetzten Personen ausreichend kompetent sind (Ausbildung, Training, Erfahrung,...)
- wenn möglich (??) sollen die nötigen Schritte gesetzt werden, um über ausreichende Kompetenzen zu verfügen
- vorhalten entsprechender Dokumentation zum Nachweis der jeweiligen Kompetenzen

Voraussetzungen und Mittel (Support)

→ Bewusstsein

Alle in der Organisation tätigen Personen sollen sich über folgendes im Klaren sein:

- Die Inhalte der IS Policy
- Ihren Beitrag zur Effektivität des ISMS und der Informationssicherheit an sich
- die Implikationen bei nicht regelkonformen Verhalten

Voraussetzungen und Mittel (Support)

→ Kommunikation

Die Organisation muss festlegen, welche internen und externen Kommunikationspfade im Sinne des ISMS zu definieren sind. Zu beachten ist:

- Was wird kommuniziert?
- Wann erfolgt die Kommunikation
- Wer nimmt daran teil
- Wer soll die Kommunikation leiten
- Welche ISMS Prozesse sind betroffen



Anforderung an die Dokumentation 1

- ISMS Security Policy
- Umfang / Scope des ISMS
- Dokumente zum Risikomanagement (Methodik)
- Dokumentation der Risikobetrachtungen
- Plan zur Maßnahmenumsetzung
- Aufzeichnungen / Protokolle aus den Anforderungen der ISO 27001 und ISO 27002
- Begründung zu Auswahl der Maßnahmen und der damit verbundenen Ziele
- Dokumentation der Prozesse und Verfahren zum ISMS, (Auditpläne, -verfahren, Mgmt Review, KVP,...)



Anforderung an die Dokumentation 2

- Die Unterlagen müssen in ihrer aktuellsten Version jederzeit verfügbar sein (need to know)
- Periodische Überprüfung, gegebenenfalls Überarbeitung
- Alle in ISMS vorgesehenen Dokumente müssen in einer aktuellen Fassung vorliegen
- Ungültige Dokumente müssen aus dem Verkehr gezogen werden
- Änderungen am Dokument sowie dessen Revisionsstatus müssen erkennbar sein
- Dokumente aus externen Quellen müssen als solche erkennbar sein



Anforderung an die Dokumentation 3

Neben den allgemeinen Vorgaben zur Dokumentenlenkung sind folgende Anmerkungen interessant:

Das Ausmaß der Dokumentation des ISMS kann je nach Organisation unterschiedlich sein, abhängig von:

- Der Größe der Organisation, der Branche, ihrer Prozesse, Produkte und Services
- Der Komplexität ihrer Prozesse und deren Zusammenspiel
- Die Kompetenz der handelnden Personen

ISO 27001:2013

Die neue Struktur!



The SNuS Experience

- ✓ Unternehmenszusammenhänge
(Context of the organization)
- ✓ Führungsverantwortung (Leadership)
- ✓ Planung (Planning)
- ✓ Voraussetzungen und Mittel (Support)
- Betrieb (Operation)
- Wirksamkeitsprüfung (Performance evaluation)
- Verbesserung (Improvement)

ISMS Betrieb

Neu:

Die Organisation muss sicherstellen, dass „outgesourcete“ Prozesse gesteuert und kontrolliert werden

Alles weitere fast wie gehabt:

- Maßnahmen planen und umsetzen
- Auf Sicherheitsmängel durch Changes achten
- Risikoanalysen und Risikobehandlung weiterführen



ISMS Betrieb

- Planen, umsetzen und steuern aller Prozesse, die für den Betrieb eines ISMS und zur Erreichung von IS-Zielen erforderlich sind.



- Dokumentierte Nachweise über die bestimmungsgemäße Abwicklung der Prozesse und Verfahren



- Änderungen innerhalb der Organisation sind zu planen und Risiken / Konsequenzen zu ermitteln.



- Risikoassessment durchführen
- Risikobehandlung durchführen

ISO 27001:2013

Die neue Struktur!



The SNuS Experience

- ✓ Unternehmenszusammenhänge
(Context of the organization)
- ✓ Führungsverantwortung (Leadership)
- ✓ Planung (Planning)
- ✓ Voraussetzungen und Mittel (Support)
- ✓ Betrieb (Operation)
- Wirksamkeitsprüfung (Performance evaluation)
- Verbesserung (Improvement)

Überprüfung der Performance

Monitoring, Messung, Analyse und Evaluierung

Die Organisation muss folgendes festlegen:

- Was muss kontrolliert und bewertet werden
- Die eingesetzten Methoden zur Überwachung, Messung, Analyse und Evaluierung um korrekte Resultate zu erzielen
- Wann sind die Mess- und Prüfaktivitäten abzuwickeln
- Wer ist für Monitoring und Messung zuständig
- Wer ist für Analyse und Evaluierung zuständig

Überprüfung der Performance (2)

Internes Audit:

Die Organisation muss interne Audits in festgelegten Intervallen durchführen um:

- Die Konformität mit den eigenen Regelungen fest zu stellen
- Die Konformität mit den Vorgaben der Norm fest zu stellen

Grundsätzliche Prozessbeschreibung (Qualifikation, Scope, Frequenz, Methodik, Verantwortungen,...)

Auditunterlagen (Auditplan, Checklisten, Ergebnisse,...)

Überprüfung der Performance (3)

Management Review 1:

Das ISMS an sich, also all die Prozesse, Verfahren, getroffenen Entscheidungen, Ergebnisse, Probleme und Vorfälle, ist zu überprüfen.



- Im Rahmen eines geplanten, regelmäßig durchgeföhrten Reviews
- Nachzuweisen durch eine Dokumentation des Ergebnisses
- Ziel ist die Angemessenheit, Nachhaltigkeit und Effektivität sicherzustellen, etwa durch konkrete Vorschläge oder Anforderungen zur Verbesserung



Überprüfung der Performance (4)

Management Review 2:

Themen zum Management Review:

- Ergebnisse von Audits
- Ergebnisse aus ISMS Monitoring und Messung
- Status zu aktuell laufenden Verbesserungs- und Korrekturverfahren
- Follow Up's vergangener Managementreviews
- Trends hinsichtlich neuer Bedrohungen
- Status zum Risikomanagement
- interne und externe Veränderungen die das ISMS beeinflussen können

ISO 27001:2013

Die neue Struktur!



The SNuS Experience

- ✓ Unternehmenszusammenhänge
(Context of the organization)
- ✓ Führungsverantwortung (Leadership)
- ✓ Planung (Planning)
- ✓ Voraussetzungen und Mittel (Support)
- ✓ Betrieb (Operation)
- ✓ Wirksamkeitsprüfung (Performance evaluation)
- Verbesserung (Improvement)

Verbesserung (1)

Verbesserung:

bei „non Konformität“ muss reagiert werden:

- Aktivitäten starten, um die Situation zu bereinigen
- die (möglichen) Konsequenzen bearbeiten
- die Ursachen für die Abweichungen ermitteln und behandeln
- Die Effektivität der getroffenen Maßnahmen ermitteln
- Nachweise anlegen, um die Ursachen der Abweichungen und die Gegenmaßnahmen zu dokumentieren.



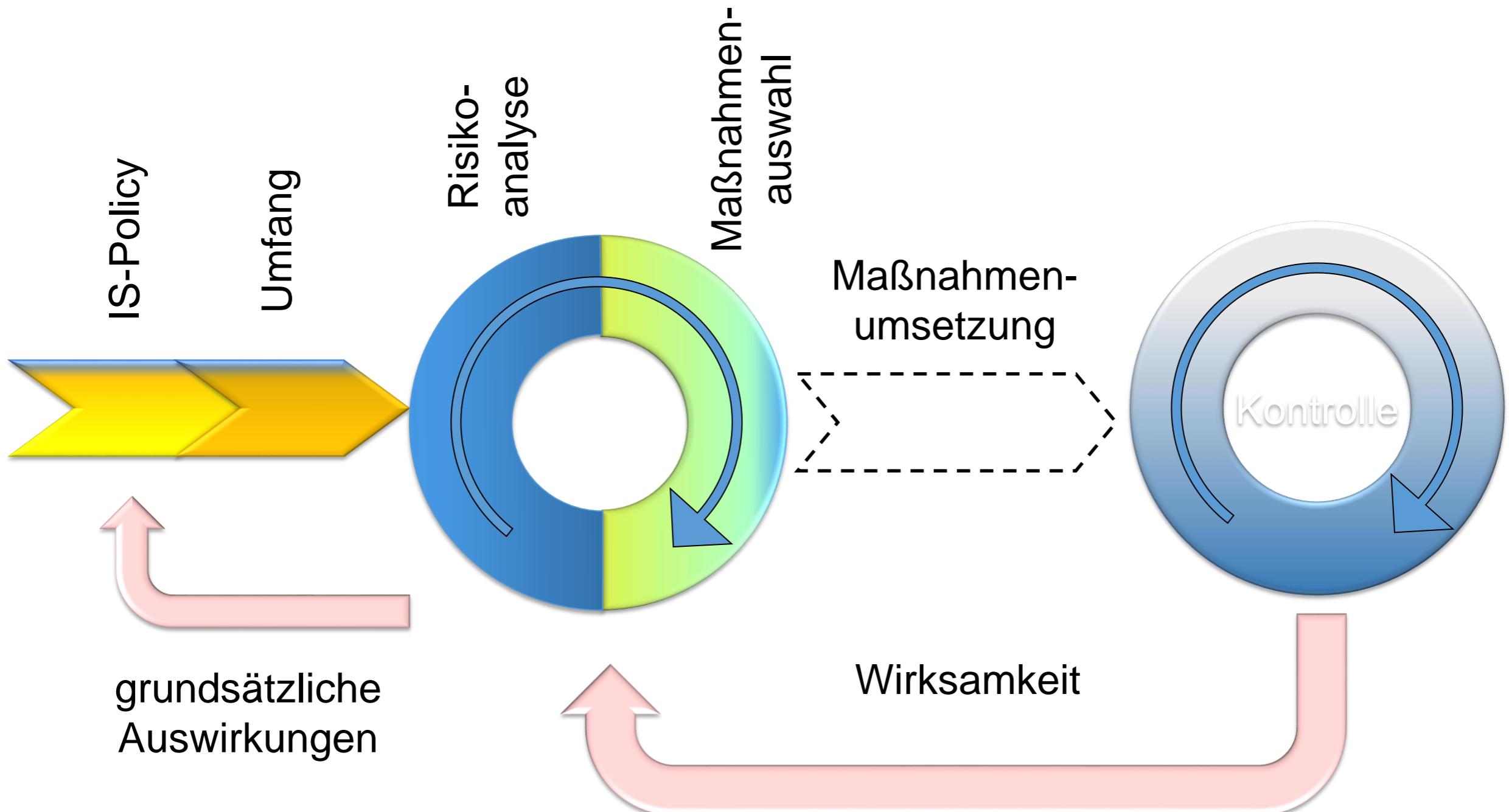
Das ISMS muss permanent verbessert werden,
um Angemessenheit und Wirksamkeit zu gewährleisten

ISO 27001:2013

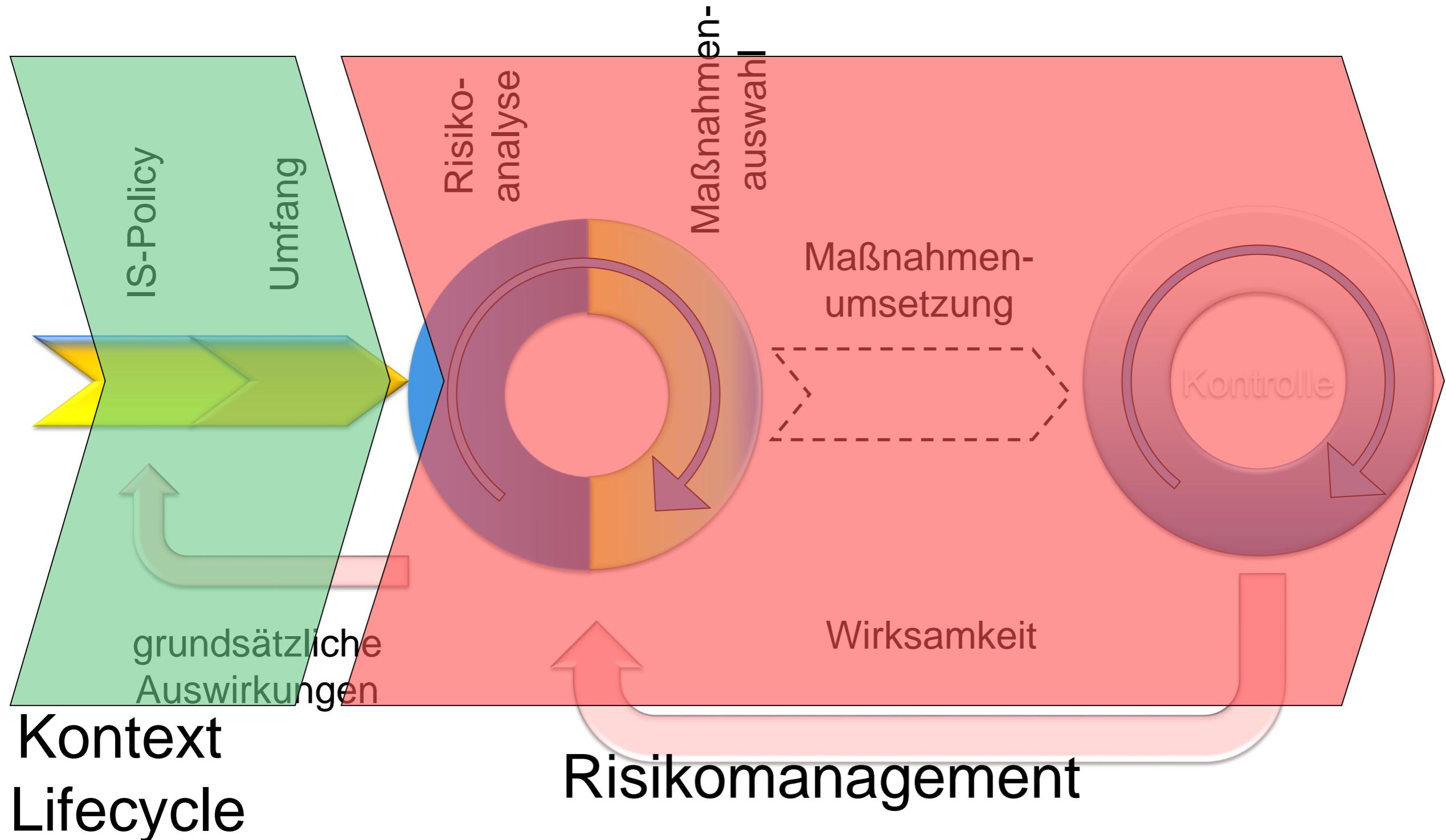
Die neue Struktur!

- ✓ Unternehmenszusammenhänge
(Context of the organization)
- ✓ Führungsverantwortung (Leadership)
- ✓ Planung (Planning)
- ✓ Voraussetzungen und Mittel (Support)
- ✓ Betrieb (Operation)
- ✓ Wirksamkeitsprüfung (Performance evaluation)
- ✓ Verbesserung (Improvement)

Zusammenfassung IS - Managementsystem



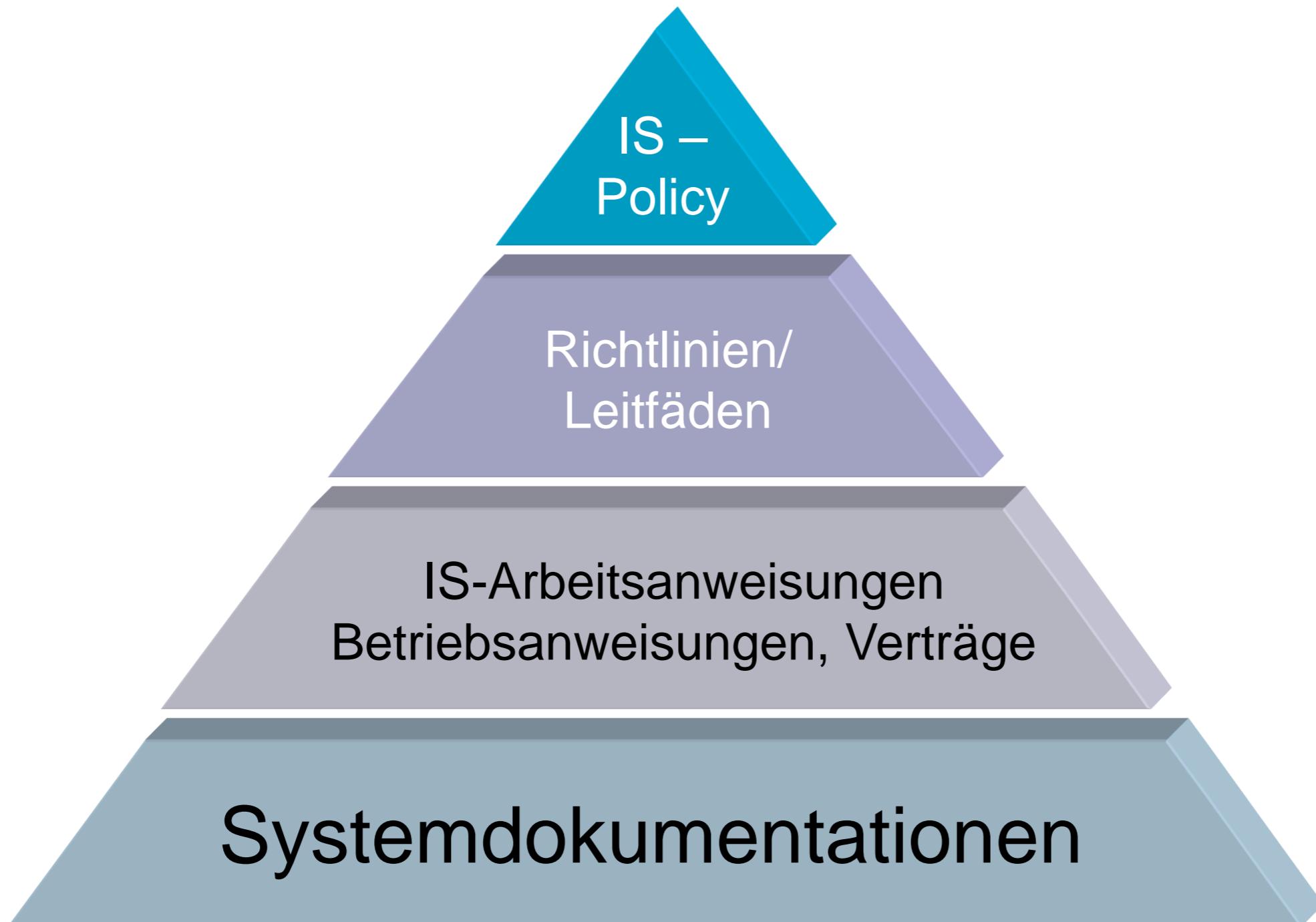
IS - Managementsystem



IS - Managementsystem



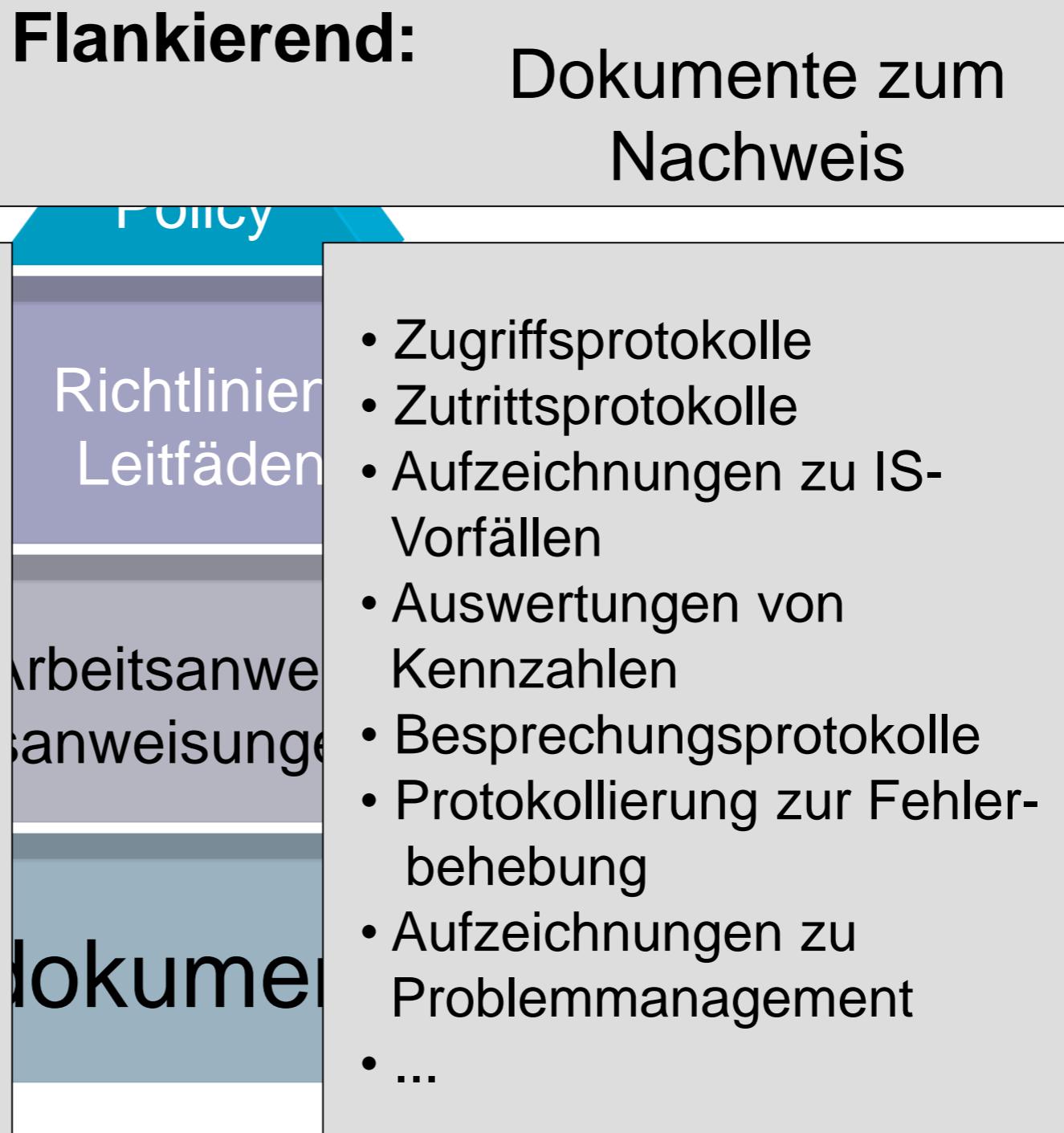
Dokumentenpyramide (1)



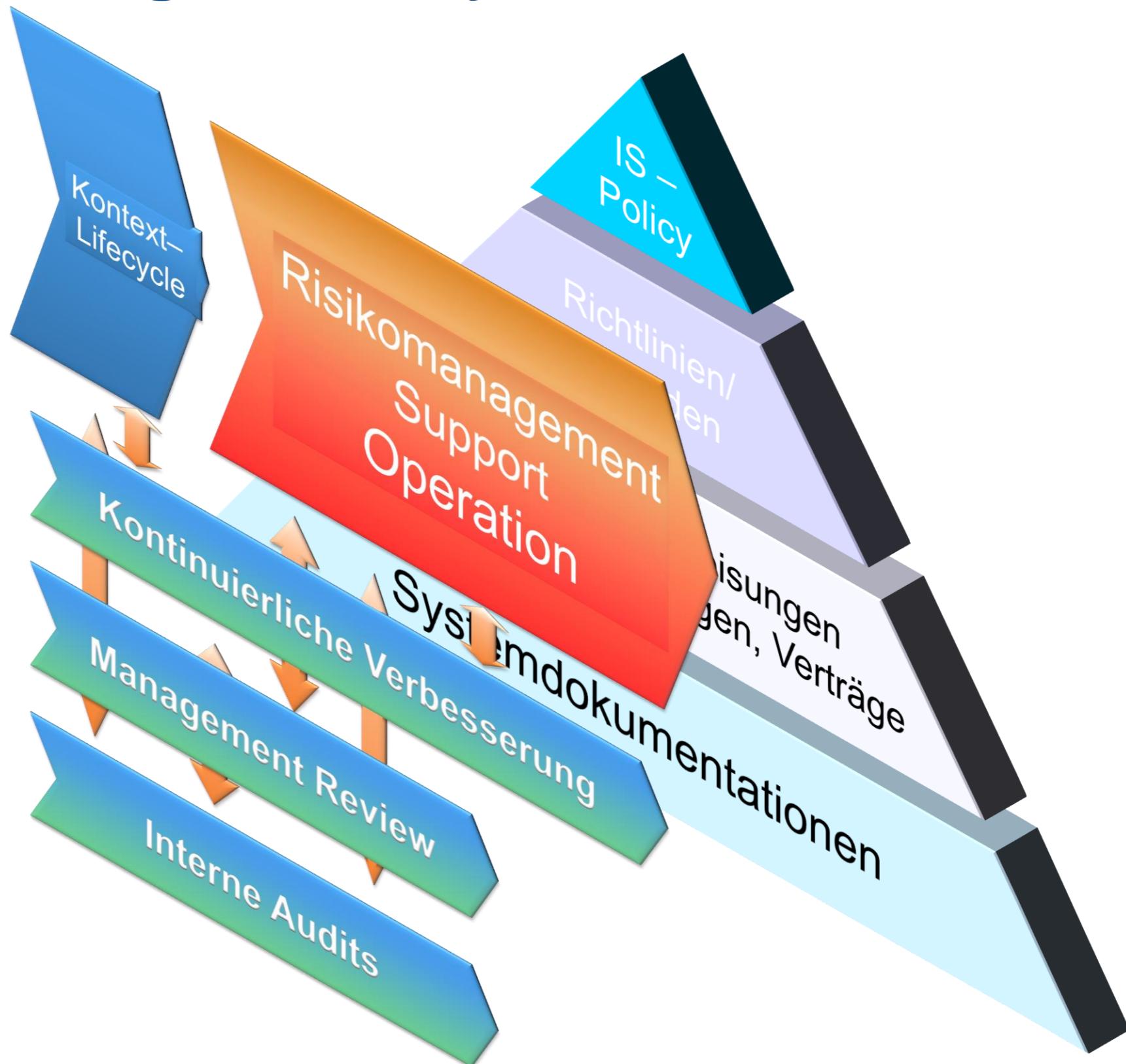
Dokumentenpyramide (2)

Operative Dokumente

- Risikomanagement- Dokumentationen
- Risikoanalyse Tabellen
- ISMS Prozessdokus
- Asset bezogene Dokus
- Massnahmentabellen
- Revisionsunterlagen
- Interne Vorschriften
- Weitergehende Literatur (Standards, Normen,...)
- ...



IS - Managementsystem



ISO 27002:2013

Code of practice

**Information technology - Security techniques - Code
of practice for information security controls**



Die 14 Kapitel der ISO 27002

- Security Policies
- Organisation of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical & environmental security
- Operations security
- Communications security
- System acquisition, development and maintainance
- Supplier relationships
- IS incident management
- IS aspects of business continuity management
- Compliance

Die 11 Kapitel der ISO 27002:2005

- Informationssicherheitspolitik (Security Policy)
- Organisieren der Informationssicherheit
- Management des Bestandes (Asset Management)
- Personenbezogene Sicherheit
- Physische und umgebungsbezogene Sicherheit
- Systemmanagement
- Systemzugriffsmanagement
- Systembeschaffung, -entwicklung und -wartung
- IS-Vorfallverwaltung (Incident Management)
- Business Continuity Management
- Einhaltung der Verpflichtungen

Die 3 Quellen für Sicherheitsanforderungen aus ISO 27002

- Risikoanalysen, ausgehend von der Unternehmensstrategie und den jeweiligen Zielsetzungen
- Rechtliche, regulative und vertragliche Anforderungen sowie das sozio-kulturelle Umfeld
- Vorgaben und Richtlinien sowie Anforderungen aus Service Management und Service Operation.



Security Policies

Vorgeschlagen werden 2 Ebenen (Niveauabstufungen)



1. „Information security policy“

1. Definition zu IS, Zielen und Prinzipien
2. Zuweisung von allgemeinen und spezifischen Verantwortungen zur IS
3. Prozesse um Abweichungen und Ausnahmen zu behandeln



2. Untergeordnete Policies (Richtlinienebene)

IS-Policy

- Definition von Information und Informationssicherheit und ggf. weiterführenden IS-relevanten Begriffen



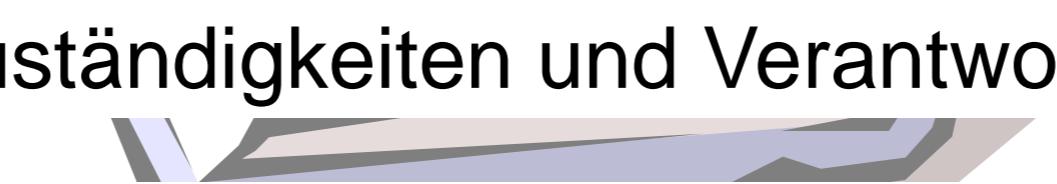
- Grundsätzliches zum Risikomanagement



- IS – Ziele der Organisation und deren Anwendungsbereich



- Strategien um diese Ziele zu erreichen



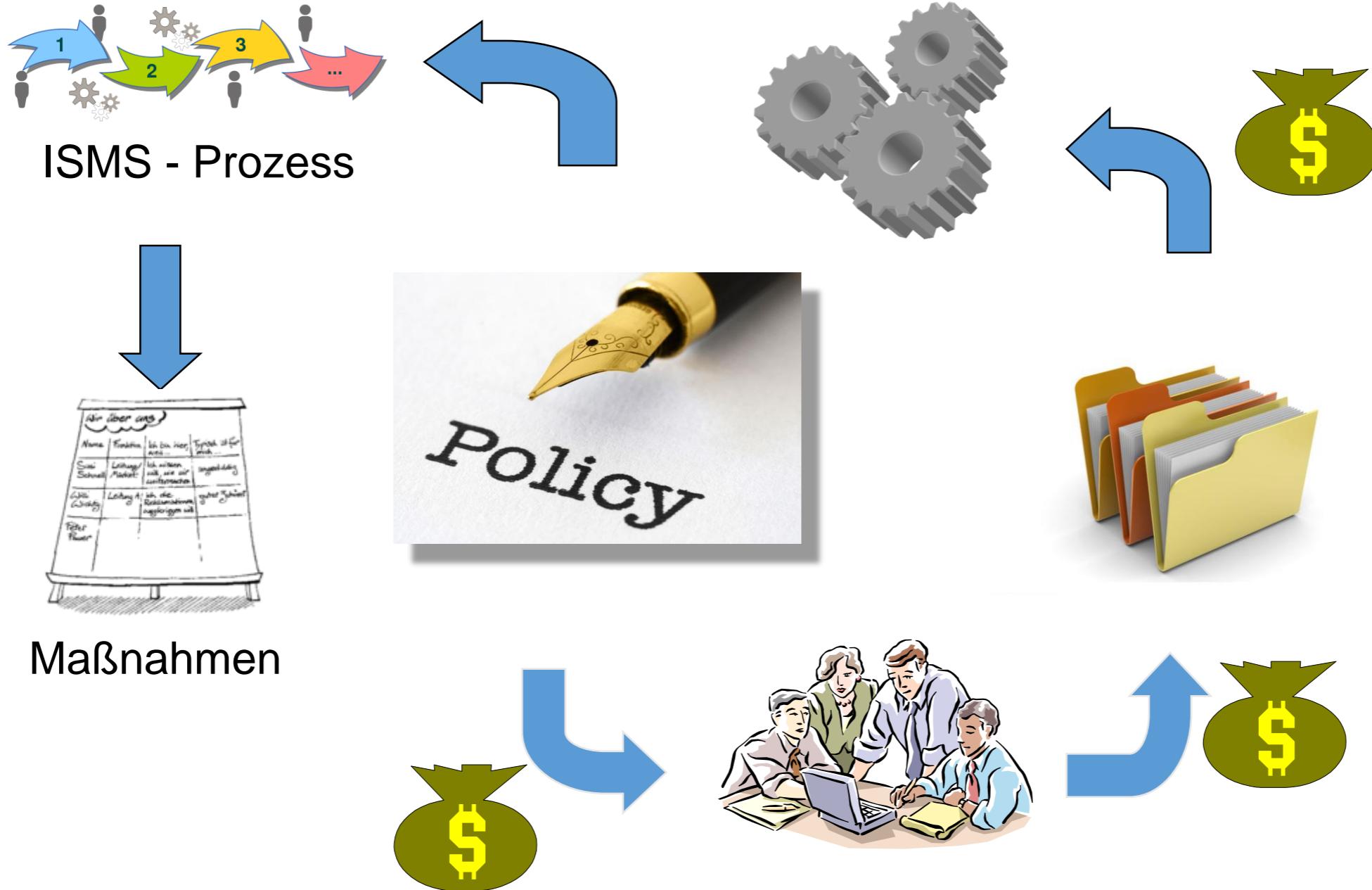
- Festlegung von Zuständigkeiten und Verantwortlichkeiten



- Statements zu organisationsspezifisch relevanten IS-Themen (etwa: rechtliche Aspekte, Notfallmanagement, Schulung,...)

- Verweise auf andere mitgeltende Dokumente

Warum eine IS Policy?



Security Policies

Untergeordnete Policies (Richtlinienebene)

- Access Management
- Klassifizierung von Informationen
- Physische und umgebungsbezogene Sicherheit
- Mitarbeiter bezogene Themen
- Backup & Recovery
- Malwareschutz
- Sicherheit in der Kommunikation
- Supplier Management

Security Policy Review



Die 14 Kapitel der ISO 27002

- ✓ Security Policies
- Organisation of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical & environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- IS incident management
- IS aspects of business continuity management
- Compliance

interne Organisation

Ziel: Aufbau einer Managementstruktur zur Steuerung der IS in der Organisation

- IS Rollen und Verantwortlichkeiten
- Pflichtentrennung
- Kontakt zu Behörden
- Kontakt zu Interessensgruppen
- IS im Projektmanagement



Rollen und Verantwortlichkeiten

Festlegen von Themen und Aufgaben für die Verantwortliche festzulegen sind (auszugsweise)

- IS-Prozesse und Verfahren
- Assets (auch lokale Verantwortungen)
- Risikomanagement und Risikoakzeptanz
- Koordination von IS Aspekten im Supplier Management

Wichtig: Festlegen, was die jeweilige Rolle an Aufgaben mit ein- und ausschließt, was Verantwortung im entsprechenden Zusammenhang bedeutet!

Weitere Anforderungen / Aufgaben

● Pflichtentrennung

Unvereinbarkeiten bei Tätigkeits- und Verantwortungsbereichen sind festzustellen und durch getrennte Handlungen und Verantwortungen zu bereinigen.

Entsprechend der Risikosituation ist festzulegen, wie die Pflichtentrennung realisiert werden kann.

● Kontakt mit externen Stellen (Behörden, Prüfer,...)

● Erfahrungsaustausch mit Know-How Trägern

Pflichtentrennung

Vorgabe: Unvereinbarkeiten sind festzustellen und durch geteilte Handlungen und Verantwortungen zu bereinigen

- Unterbindung von unbeabsichtigten oder mutwilligen Missbrauch
- In diesen Fällen darf keine Einzelperson Handlungen ohne explizite Autorisierung setzen
- In KMU ist besonders auch auf Unabhängigkeit der handelnden Personen zu achten

Weitere Anforderungen / Aufgaben

- Pflichtentrennung
- Kontakt mit externen Stellen (Behörden, Prüfer,...)

Es gilt festzulegen, in welchen Umfang wer (welche Rolle) welchen Kontakt pflegt und aufrecht erhält.

Überlegungen dazu ergeben sich aus:

- ✓ Incident Management, Notfall Management, Contingency Planning.
- ✓ Möglichen Anforderungen zeitnah über geänderte Gesetze und andere regulative Vorgaben informiert zu werden.
- ✓ Ggf. der Notwendigkeit mit Blaulichtorganisationen, Suppliern (Kommunikation, Strom, Wasser,...), und Kommunen in Kontakt zu bleiben

- Erfahrungsaustausch mit Know-How Trägern

Weitere Anforderungen / Aufgaben

- Pflichtentrennung
- Kontakt mit externen Stellen (Behörden, Prüfer,...)
- Erfahrungsaustausch mit Know-How Trägern

“Contact with special interest groups” um / zum:

- ✓ Austausch zu “best practice” Lösungen
- ✓ Am aktuellen Stand bleiben zu relevanten Informationen zu IS
- ✓ Versichern, dass man mit den “eigenen” Lösungen gut abgesichert ist
- ✓ Erhalt frühzeitiger Warnungen über Angriffe, Schwachstellen und Patches
- ✓ Austausch von Informationen über neue Technologien und Produkte
- ✓ Ansprechpartner bei der Bewältigung von Incidents oder Notfällen vorzuhalten

interne Organisation

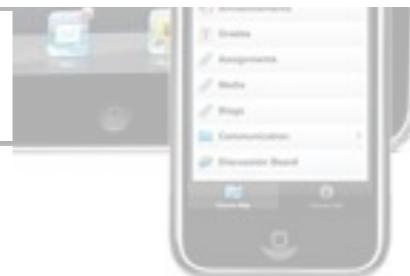
IS im Projektmanagement

Vorgabe: IS soll im Projektmanagement verankert sein, egal um welche Art Projekt es sich handelt. Damit soll erreicht werden dass:

- IS Ziele in die Projektziele integriert sind
- IS Risikoanalysen in frühen Projektstadium durchgeführt werden
- IS integrierter Teil aller Projektphasen ist

Mobile Geräte und Teleworking

- Erstellen einer Policy für mobile Geräte
 - Registrierung mobiler Geräte
 - Zugriffsschutz
 - Einsatz kryptographischer Verfahren
 - Anforderungen an physischen Schutz
 - Restriktionen zum Installieren von SW
 - Fernwirksames Löschen oder Aussperren
 - Datensicherung
 - Schutz vor Malware
 - Regeln zur Nutzung von Apps und Webservices
 - Regeln zum Umgang in der Öffentlichkeit



Mobile Geräte und Teleworking

- Erstellen einer Policy für Teleworking
 - Verfügbarkeit einer entsprechend sicheren Umgebung
 - Festlegung zur Arbeitszeit, Verfügbarkeit von Diensten
 - Bereitstellung von Kommunikationsgeräten / -methoden
 - Anforderungen physische Sicherheit
 - Regeln für den Zugriff durch Familienangehörige / Gäste
 - Regelungen bezüglich HW & SW Support und Wartung
 - Versicherungsschutz
 - Malwareschutz, Firewall und Backup
 - Verfahren zur Einstellung der Telearbeit

Die 14 Kapitel der ISO 27002

- ✓ Security Policies
- ✓ Organisation of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical & environmental security
- Operations security
- Communications security
- System acquisition, development and maintainance
- Supplier relationships
- IS incident management
- IS aspects of business continuity management
- Compliance

Human resource security

Zur Anstellung

- Screening
- IS Anforderungen im Arbeitsvertrag

Während der Beschäftigung

- Management-Verantwortung 
- IS Sensibilisierung, Ausbildung und Training
- Disziplinarverfahren 

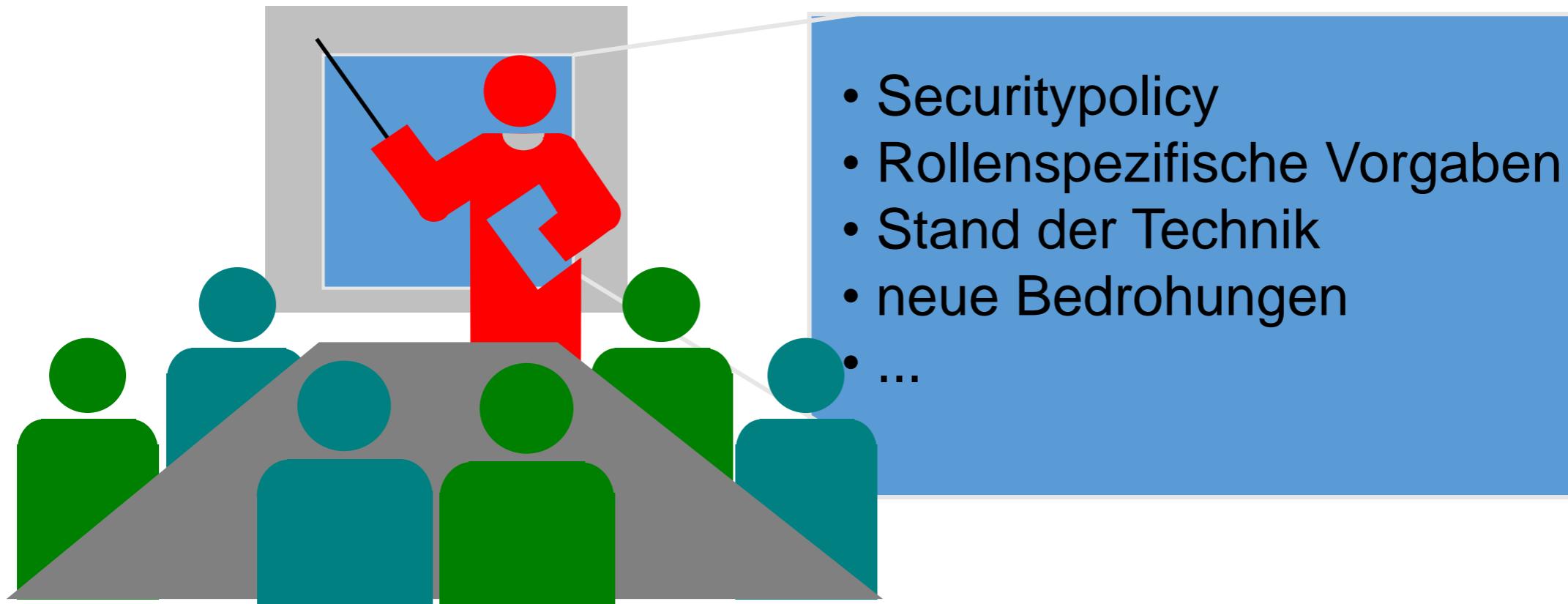
Beendigung oder Änderung der Beschäftigung

- Verantwortlichkeiten bei Veränderungen

Mitarbeiterauswahl - Screening

- Verfügbarkeit befriedigender Beurteilungen (persönlicher und geschäftlicher Natur)
- Eine Nachprüfung des Lebenslaufs des Bewerbers (Vollständigkeit und Korrektheit)
- Eine Bestätigung der vorgelegten Zeugnisse (Berufsausbildung, akademisch,...)
- Eine unabhängige Bestätigung der Personaldaten (Pass oder ähnliches)
- Detailliertere Überprüfungen der Kreditwürdigkeit bzw. des Strafregisters

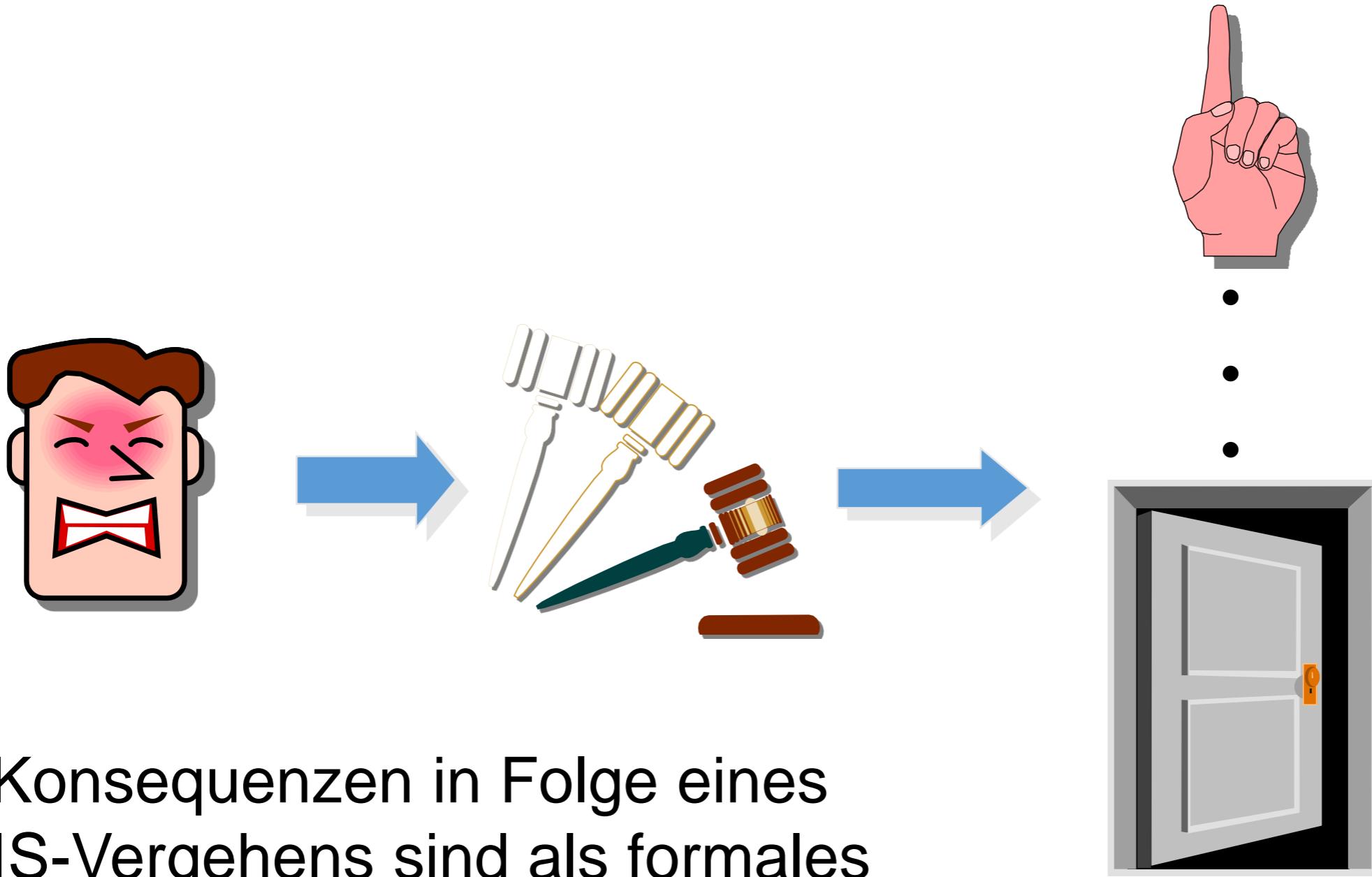
Schulung und Vertrauensbildung



Schulung beim Eintritt
und regelmäßig während der gesamten Dienstzeit

Führungskräfte müssen sich ihrer Vorbildwirkung bewusst sein

Disziplinarmaßnahmen



Konsequenzen in Folge eines IS-Vergehens sind als formales Verfahren zu beschreiben.

Beendigung oder Veränderungen im Arbeitsverhältnis



Verantwortliche Rollen und Verfahren
zur Beendigung des Dienstverhältnisses
sind zu definieren und zuzuweisen



Rückgabe des Firmeneigentums ist
sicherzustellen



Entzug oder Anpassung von Zutritts-
und Zugriffsberechtigungen ist
zeitgerecht durchzuführen

Die 14 Kapitel der ISO 27002

- ✓ Security Policies
- ✓ Organisation of information security
- ✓ Human resource security
- Asset management
- Access control
- Cryptography
- Physical & environmental security
- Operations security
- Communications security
- System acquisition, development and maintainance
- Supplier relationships
- IS incident management
- IS aspects of business continuity management
- Compliance

Asset Inventory (1)

Definition „asset“ aus ISO 27000:2009

asset

anything that has value to the organization



NOTE: There are many types of assets, including:

- a) **information;**
- b) software, such as a computer program;
- c) physical, such as computer;
- d) services;
- e) people, and their qualifications, skills, and experience;
- f) intangibles, such as reputation and image;

Asset Inventory (2)

- Die Organisation soll alle Assets identifizieren, die im Information-Lifecycle relevant sind.
- Ein Asset Inventory soll aktuell, vollständig und konsistent gehalten werden
- Für jedes Asset muss ein Verantwortlicher benannt sein
- Jedem Asset muss die entsprechende Klassifizierungsstufe zugewiesen sein.
- Regeln zum IS-konformen Einsatz der Assets sind festzulegen und einzuführen

Klassifizierung von Informationen

Sicher stellen, dass Informationen einen angemessen Schutz in Zusammenhang mit ihrer Wichtigkeit für die Organisation erhalten.

**Klassifizierung von
Informationen**

**Kennzeichnung von
Informationen**

Umgang mit Assets

Umgang mit Assets

- Umgang mit Medien entsprechend der gespeicherten Informationen



- Angemessene Zugriffsbeschränkungen



- Formale Aufzeichnungen über die Empfänger



- Schutz auch temporärer Kopien

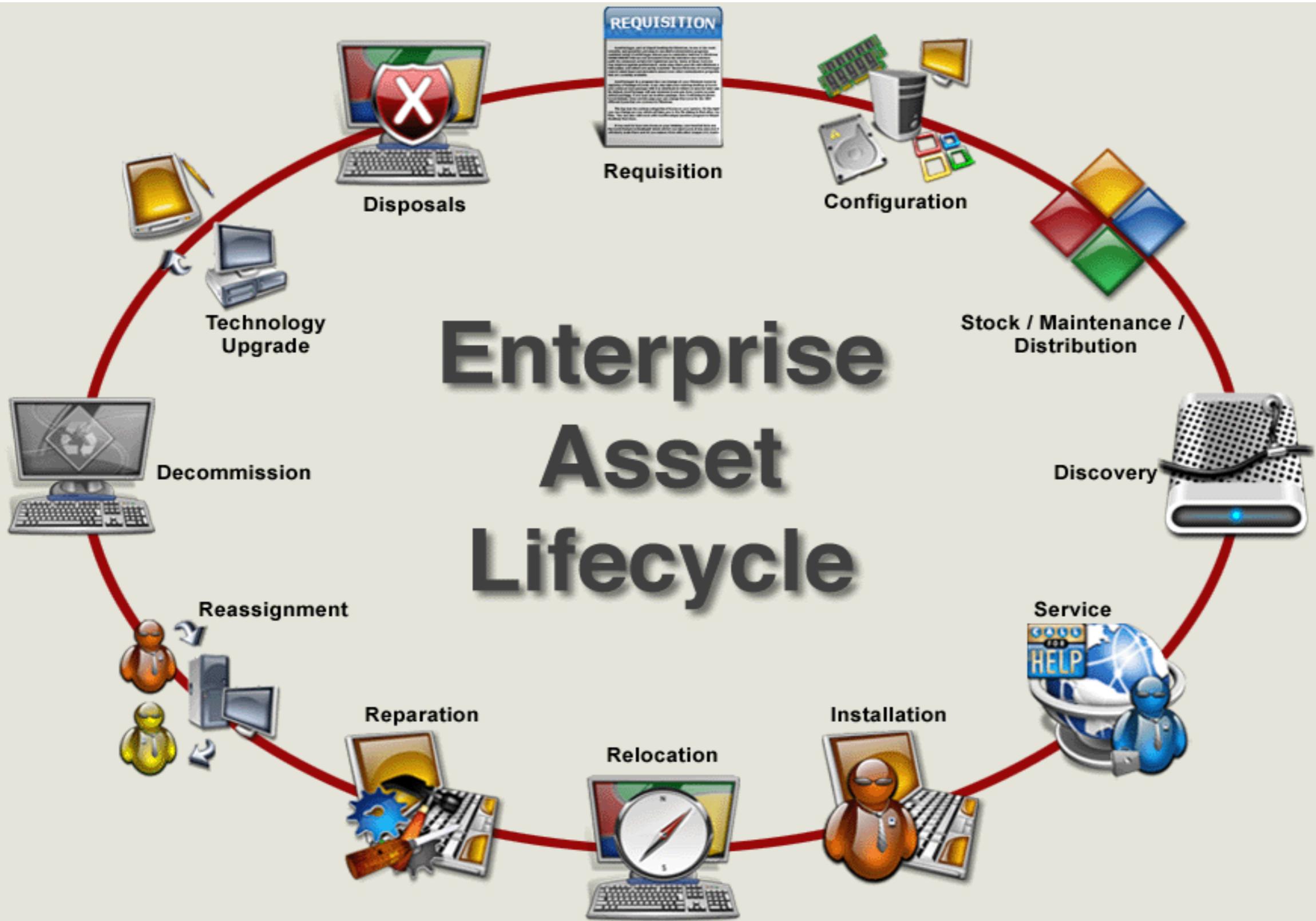


- Maximal mögliche Einschränkung der Verteilung



- Deutliche Kennzeichnung auch aller Kopien

Einbettung im Asset Lifecycle



Die 14 Kapitel der ISO 27002

- ✓ Security Policies
- ✓ Organisation of information security
- ✓ Human resource security
- ✓ Asset management
- Access control
- Cryptography
- Physical & environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- IS incident management
- IS aspects of business continuity management
- Compliance

Access Control - Übersicht

- Das Kapitel wurde etwas „enttechnisiert“ also eher mit Verwaltungsthemen versehen
- Das Kapitel „Netzwerkzugriffsmanagement“ wurde entfernt
- Dem „Anpassen“ von Berechtigungen wurde etwas mehr Platz gewidmet
- Die Verwaltung privilegierter Berechtigungen wird detaillierter behandelt
- Das Thema “Clear Desk Policy” ist zu physischer Sicherheit verschoben worden

Erstellen einer Zugriffspolicy

- Basis: Anforderungen aus Geschäftsanwendungen
- Festlegung grundlegender Prinzipien (need to know,...)
- Hohe Konsistenz zwischen Zugriffsberechtigungen und Schutzbedarf
- Einbeziehung bestehender Gesetze und Verträge
- Überlegungen zur Anwendung in stark vernetzten und verteilten Systemen
- Pflichtentrennung in der Berechtigungsverwaltung
- Aufzeichnung von Änderungen und Zugriffen zur Berechtigungsverwaltung
- Verwaltung privilegierter Berechtigungen

Verwaltung privilegierter Berechtigungen

Formeller Prozess zum Management von privilegierten Berechtigungen unter Beachtung folgender Aspekte:

- Welche Systeme oder Prozesse sind betroffen
(Betriebssystem, DB-, Netzwerk-, Ticketmanagement, Applikationen,...)
- Basis: “need to use” und “event by event”
- Aufzeichnungen für Vergabe oder Änderung
- Verfallsdatum vorsehen
- Priv. Berechtigungen sollten nicht an “normale” Useraccounts vergeben werden
- Regelmäßige Überprüfungen der bestehenden Berechtigungen durchführen



Zugriffsmanagement bei Applikationen

Im Rahmen der Zugriffspolicy wären folgende Punkte zu beachten, wenn Individualsoftware eingesetzt wird:

- Funktionen zur Rechteverwaltung vorsehen, die ausreichend granular sind
- Verwalten von Berechtigungen anderer Applikationen
- Nicht nur funktionelle Einschränkungen vorsehen, sondern auch Datenzugriffe einschränkbar machen
- Einschränken von Datenüberleitungen in andere Applikationen oder Outputs
- Schutz gegen Angriffe vorsehen (Anti Hacking)
- Protokollierung durch die Applikation ermöglichen

Überprüfung von Berechtigungen

user Accounts:

- periodisch
- nach Funktionsänderungen
- nach internen Umorganisationen
- nach Verlassen der Organisation



privilegierte Accounts:

- sollten häufiger (unabhängig) geprüft werden als user accounts
- Änderungen sind zu protokollieren um Überprüfbarkeit zu gewährleisten

Systemprogramme und -befehle

können Systemeinstellungen ändern, daher

- sind Verfahren zur Identifikation und Autorisierung vorzusehen
- sind Systemprogramme von Applikationen “rechtlich” zu trennen
- sind Systemprogramme nur einer limitierten Anzahl vertrauenswürdiger User zugänglich
- ist der Einsatz von Systemprogrammen, -befehlen zu protokollieren

Achtung: Verfahren zur Berechtigungsverwaltung von Systemprogrammen sind zu dokumentieren

Zugriff auf “Sourcecode”

Zugriff auf Sourcecode, Libraries und assoziierten Informationen (Spezifikationen, Design, Testpläne,...) sollte beschränkt werden um unberechtigte Änderungen zu verhindern und vor Know How Abfluss zu schützen.

- Wo möglich Sourcecode nicht auf operativen Systemen belassen (Zugriffsberechtigungen etwa durch Administratoren)
- Sourcecode ist genauso wie andere Informationswerte entsprechend der gegebenen Klassifizierungsstufen zu handhaben

Die 14 Kapitel der ISO 27002

- ✓ Security Policies
- ✓ Organisation of information security
- ✓ Human resource security
- ✓ Asset management
- ✓ Access control
- Cryptography
- Physical & environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- IS incident management
- IS aspects of business continuity management
- Compliance

Cryptography

Ziel:

Durch angemessene Anwendung kryptographischer Technologien und Verfahren die Vertraulichkeit und Integrität der Informationen zu schützen

Im Rahmen einer Policy sollte u.a. folgendes geklärt werden:

- Begründung zum Einsatz, abgeleitet aus den IS Zielen
- Zuordnung der möglichen Technologien zum Schutzniveau
- Einsatz bei mobilen Geräten, im Themenumfeld “BYOD”, für Home- und Teleworking
- Einsatz im Sinne von data loss- und data leakage prevention

Kontraindikationen! (Malewareprotection, Datenverlust,...)

Cryptography

Schlüsselmanagement

Einsatz einheitlicher Verfahren (Mindestanforderungen) zur:

- Schlüsselgenerierung im Umfeld unterschiedlicher Technologien und Produkte
- Zuordnung und Verteilung von Schlüsselmaterial, Zertifikaten und der Aktivierung der Schlüssel
- Speicherung und Hinterlegung von Schlüsselmaterial
- regelmäßigen Erneuerung (Austausch) des Schlüssel-materials
- Behandlung kompromittierter Schlüssel (und der betroffenen Applikationen / Daten)
- Aufzeichnung und Protokollierung aller Aktivitäten im Crypto - Themenumfeld

Die 14 Kapitel der ISO 27002

- ✓ Security Policies
- ✓ Organisation of information security
- ✓ Human resource security
- ✓ Asset management
- ✓ Access control
- ✓ Cryptography
- Physical & environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- IS incident management
- IS aspects of business continuity management
- Compliance

Zutrittschutz

- Besucher sind vorab anzukündigen, ggf. auf bestimmte Bereiche zu beschränken
- Zutrittsprotokollierung (Datum, Zeit, Name,...) ist vorzusehen (für Besucher und Mitarbeiter)
- Personenüberwachung den Sicherheitszonen anpassen
- Identifikationskarten sind offen zu tragen, unbekannte Personen ohne ID sind dem Sicherheitsdienst zu melden
- Zutritt ist (zuverlässig) aufzuzeichnen und die Aufzeichnungen sind regelmäßig zu überprüfen
- Zutrittsberechtigungen zu Sicherheitsbereichen sollten regelmäßig überprüft werden

Schutz vor externen Bedrohungen

- Gefahrenstoffe in angemessener Distanz zu Sicherheitsbereichen aufbewahren
- Ersatzequipment und Backupmedien sollten in sicherer Distanz aufbewahrt werden
- Sicherheitseinrichtungen zur Detektion und zum Bekämpfen von Schadensereignissen sollten installiert sein (und getestet werden)
- Angelieferte Materialien und Geräte sollten hinsichtlich Explosionsstoffe, Gifte oder andere natürliche oder künstliche Gefahren untersucht werden
- Ggf. einen Quarantänebereich einrichten

Liefer- und Ladebereiche

- Liefer- und Ladebereiche dürfen auch nur von autorisierten Personen betreten werden
- Liefer- und Ladebereiche sollten so gestaltet sein, dass anlieferndes Fremdpersonal die Organisationsliegenschaften nicht betreten kann
- Äußere und innere Türen sollten insgesamt als Schleuse fungieren
- Angeliefertes Material ist im Sinne von Assetmanagement zu registrieren (Überprüfung der Bestellung)
- Angeliefertes Material sollte überprüft werden, ob am Weg manipuliert wurde (Versiegelung, Verpackung, einschlägige Beschädigungen,...)

Wartung von Geräten

- Einhaltung vom Hersteller vorgegebener Serviceintervalle
- Reparaturen und Service nur von berechtigten Personal
- Aufzeichnungen anlegen von vermuteten und tatsächlichen Fehlern sowie von Wartung und Reparatur
- Wenn nötig sollten vertrauliche Informationen von den zu wartenden Geräten entfernt werden
- Nach Fehlerbehebung oder Wartung sollte sichergestellt werden, dass keine unbeabsichtigte Manipulation stattgefunden hat

Geräte / Assets außer Haus

- Öffentliche Bereiche: ständige Beaufsichtigung, unauffälliger Transport

- Schutzvorschriften von Herstellern beachten

<..\..\Beispielunterlagen\FTS-04230-Specification-for-DataCenter.pdf>

<http://docs.ts.fujitsu.com/dl.aspx?id=e4813edf-4a27-461a-8184-983092c12dbe>

- Beschränkung der Möglichkeiten und Genehmigungen außer Haus zu arbeiten

- Wenn Geräte mehreren Mitarbeitern zur Verfügung stehen, sollte die jeweilige Zuordnung protokolliert werden

Clear Desk Policy

- Informationen höherer Klassifizierungstufen sind, wenn sie nicht benötigt werden, versperrt aufzubewahren
- Darauf achten, dass sich auf Whiteboards und Flipcharts keine klassifizierten Informationen finden
- Arbeitsplatzgeräte sind gegen unberechtigten Zugriff zu sperren und gegen Diebstahl zu schützen
- Unberechtigte Benutzung von Kopierern ist zu verhindern
- Medien mit klassifizierten Inhalten sollten umgehend von Druckern und Kopierern entfernt werden

Die 14 Kapitel der ISO 27002

- ✓ Security Policies
- ✓ Organisation of information security
- ✓ Human resource security
- ✓ Asset management
- ✓ Access control
- ✓ Cryptography
- ✓ Physical & environmental security
- Operations security
- Communications security
- System acquisition, development and maintainance
- Supplier relationships
- IS incident management
- IS aspects of business continuity management
- Compliance

Sicherheit beim Betrieb

- Betriebsverfahren
- Schutz vor Schadsoftware
- Backup
- Aufzeichnung und Überwachung
- Steuerung operativer Software
- Management technischer Schwachstellen
- Überlegungen zur Überwachung technischer Systeme

Dokumentation der betrieblichen Verfahren

Detaillierte Beschreibung der Einzelheiten bei

- Installation und Konfiguration der Systeme
- Backup und Restore 
- Job-scheduling inclusive der Abhängigkeiten
- Instruktionen zur Fehler- und Ausnahmenbehandlung, incl. Vorgaben zum Einsatz von Systemdienstprogrammen
- Verfahren zum Change Management 
- Support und Eskalationskontakte
- Systemrestart und Wiederherstellverfahren für den Fall von unkonsolidierten Ausfällen
- Management von Audit- und Loginformationen

Change Management

Detaillierte Beschreibung der Einzelheiten bzgl.:

- Identifizierung und Aufzeichnung signifikanter Changes
- Planen und testen von Changes
- Impact Assessment und Sicherheitsrisiken
- Formelle Genehmigungsverfahren für Changes
- Überprüfung, dass alle Sicherheitsvorschriften eingehalten werden
- Kommunikation der Detailinformationen zum Change an alle relevanten Personen
- Fall-Back Verfahren und Rückabwicklung bei unvorhergesehenen Ereignissen

Kapazitätsmanagement

Der Einsatz der Ressourcen ist zu überwachen, anzupassen und zukünftige Anforderungen zu planen

Zu beachten: Die Kritikalität der jeweiligen Systeme, sowie deren Betriebskosten sind einzubeziehen



Beispiele:



- Entfernen unnötiger Datenbestände
- Entfernen nicht benötiger Systeme und Services
- Optimierung von Systemprozessen und Scheduling
- Reduzierung von Systemkapazitäten für weniger kritische Services

Trennung Entwicklung Test und Betrieb

- Regeln aufstellen zur Überleitung von SW von Entwicklung zum Betrieb
- Entwicklungswerkzeuge sollten nicht von operativen Systemen aus zugreifbar sein
- Für Test, Entwicklung und Betrieb sollten unterschiedliche Accounts verwendet werden
- Klassifizierte Daten sollten nicht in Testumgebungen verwendet werden, außer es sind die gleichen Sicherheitsmaßnahmen gesetzt
- Tests sollten nicht in operativen Umgebungen durchgeführt werden

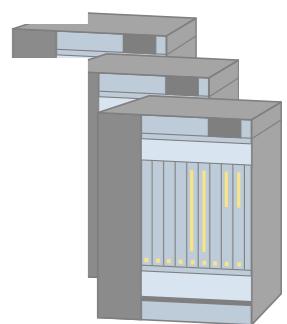
Schutz vor schädigender Software (Malware)

- Richtlinie:

Ausschließlich genehmigte und lizenzierte SW einsetzen



- Installation und ständige Aktualisierung von Antivirensoftware



- Regelmäßige Überprüfung von kritischen Systemen auf nicht genehmigte Dateien oder Software



- Klare Regelungen für das Vorgehen bei Virenangriffen



- Etablieren von Frühwarnprozessen (CERT)



- Wiederherstellungspläne für den Virennotfall



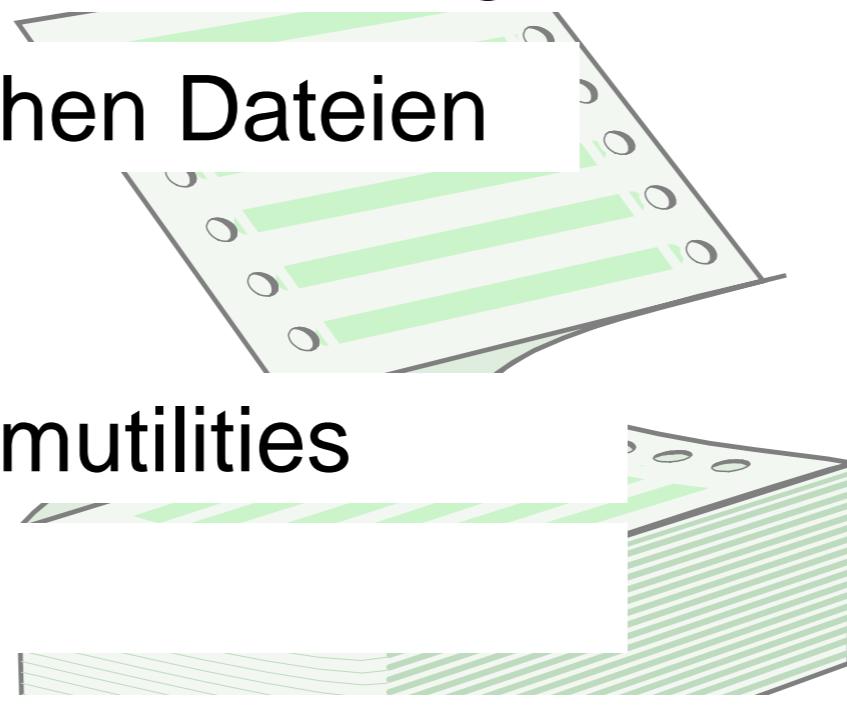
- Isolierte Umgebungen schaffen für Systeme mit sehr hohem Schadensimpact

Datensicherung

- Aufbewahrung der Datenträger in sicherer Entfernung
- Aufbewahrung der Datenträger in sicherer Umgebung
- Bei hohen Sicherheitsansprüchen: Verschlüsselung
- Regelmäßiger Test der Wiederherstellverfahren
- Austausch der Sicherungsdatenträger entsprechend der Herstellerangaben
- Lückenlose Protokollierung der Sicherungsvorgänge
- Regelung für Arbeitsplatzrechner
- Das Ausmaß von Datensicherung ist den Geschäftsanforderungen anzupassen

Protokollierung Was?

- Systemstart und -stop
- Systemfehler und Korrekturtätigkeiten
- Handling mit kritischen Dateien
- Internetnutzung
- Nutzung von Systemutilities
- Systemalarme
- Aktivierung / Deaktivierung von Sicherheitssystemen
- ✓ Datum, Uhrzeit, Name der handelnden Person (Kennung), betroffenes Equipment



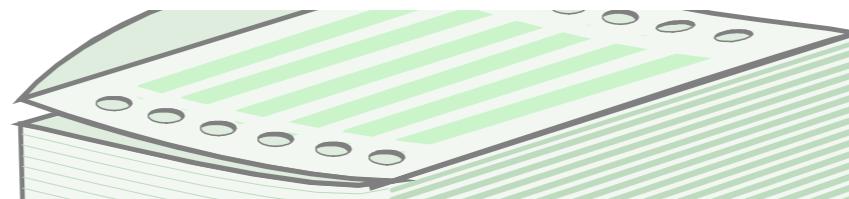
Protokollierung der Systembenutzung

Verfahren und Kontrolle

- Protokolierungsniveau entsprechend der Risikoanalysen



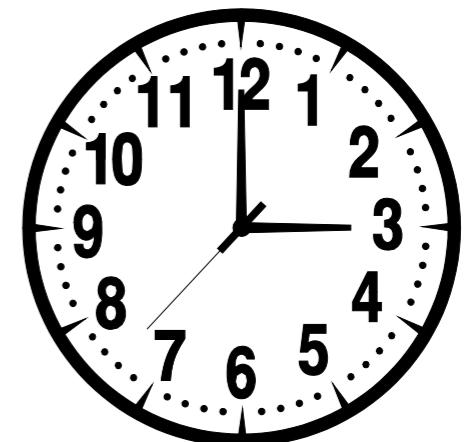
- Häufigkeit der Überprüfung entsprechend der Risikoanalysen



- Überprüfung durch unabhängige Stellen, e.v. Stichproben



Vertraulich!!



Installation operativer Software

- Updates von Applikationen oder Libraries nur durch geschultes Personal
- Auf operativen Systemen sollte sich nur geprüfter ausführbarer Code befinden
- Änderungen und Neuinstallationen nur in Betrieb setzen nach entsprechend geplanten Tests
- Rollbackstrategie vorsehen
- Aufzeichnen aller Änderungen an den Systemen
- Aufbewahren alter Versionen, wenn damit alte archivierte Datenbestände verarbeitet wurden

Schwachstellenmanagement

- Definieren von Rollen und Verantwortlichkeiten zum „technical vulnerability management“
- Informationsquellen zum Schwachstellenmanagement sind entsprechend der eingesetzten Technologie auszuwählen (auch Überprüfung der Qualität)
- Vorgaben zur standartisierten Behandlung von potentiellen Schwachstellen
- Schwachstellenmanagement sollte mit Incident Management verknüpft sein, um mögliche Incidents bereits vorab zu antizipieren
- Schwachstellenmanagement ist regelmäßig zu evaluieren

Überlegungen zu IT System Checks

Ziel: Auswirkungen auf den operativen Betrieb durch technische Prüfungen zu minimieren



- Prüfanforderungen bezüglich Vergabe von Berechtigungen sind zu bewerten und genehmigen



- Der Umfang der technischen Checks ist zu vereinbaren (Permission to attack)



- Checks sollten wenn möglich auf „read only“ Berechtigung reduziert werden



- Vertiefende Prüfungen sind vorab zu genehmigen, Checks, die Einfluss auf Systemverfügbarkeiten haben sind außerhalb der Geschäftszeit durchzuführen

Die 14 Kapitel der ISO 27002

- ✓ Security Policies
- ✓ Organisation of information security
- ✓ Human resource security
- ✓ Asset management
- ✓ Access control
- ✓ Cryptography
- ✓ Physical & environmental security
- ✓ Operations security
- Communications security
- System acquisition, development and maintainance
- Supplier relationships
- IS incident management
- IS aspects of business continuity management
- Compliance

Management der Netzwerksicherheit

- Verantwortungen und Verfahren dokumentieren
- Trennung Netzwerkbetrieb von Rechnerbetrieb
- Maßnahmen zur Sicherstellung von Vertraulichkeit und Integrität übertragener Daten vorsehen
- Koordination der Verfahren (etwa mit Systems Operations, ext. Partnern, ITIL,...)
- Auf lückenlose Protokollierung und angemessene Überprüfung der Logs ist zu achten
- Authentifizierung der Geräte im Netzwerk
- Restriktionen bezüglich Geräteintegration

Datenaustausch

Vertraulichkeitserklärungen

- Beschreibung der betroffenen Informationen
- Dauer der Gültigkeit
- Vorgehen bei Ablauf des Agreements
- Verantwortungen und Maßnahmen der Unterzeichner
- Darstellung erlaubter Verwendung der Informationen
- Verfahren zur Aufzeichnung und Meldung von Verstößen
- Aktionen im Falle von Fehlhandlungen

Die 14 Kapitel der ISO 27002

- ✓ Security Policies
- ✓ Organisation of information security
- ✓ Human resource security
- ✓ Asset management
- ✓ Access control
- ✓ Cryptography
- ✓ Physical & environmental security
- ✓ Operations security
- ✓ Communications security
- System acquisition, development and maintainance
- Supplier relationships
- IS incident management
- IS aspects of business continuity management
- Compliance

Analyse der Sicherheitsanforderungen

(für netzwerkbasierte Services)

- Anf. an die Verlässlichkeit der Authentifizierung
- Autorisierung zur Bereitstellung der Daten
- Anf. bzgl. Vertraulichkeit, Integrität, Nachweis der Versendung und vom Erhalt sowie ‚non reputation‘
- Vertraulichkeit und Integrität bzgl. Bestelldaten, Bezahlverfahren, Kundendaten und Zahlungsnachweis
- Verhindern von Verlust oder Duplikation der Transaktionsinformationen
- Haftung bei Betrug

Policy zur sicheren SW-Entwicklung

- Sichere Entwicklungsumgebung
- Sicherheit durch die angewandte Entwicklungsmethode
- „Secure Coding Guidelines“ zur jeweiligen Programmiersprache
- Sicherheitsanforderungen in der Designphase
- Sicherheits-Checkpoints zu den Projektmeilensteinen
- Sichere Sourcecodeverwaltung
- Anforderungen an die Entwickler (Know-How,...)
- Anspruch an die Entwickler Schwachstellen zu erkennen und zu vermeiden

Verfahren zur SW-Entwicklung

- Sicherheit in allen Architekturebenen einbringen (Business Daten, Applikation, Technologie,...)
 - Die eingesetzte Technologie auf bekannte Schwachstellen, das Design auf Angriffsmuster prüfen
 - Die Evaluierungsverfahren und Methoden permanent aktualisieren
-
- SW-Designvorgaben für kritische Funktionen (Login, Account-Management, Kommunikation,...)
 - Die eigenen Ansprüche auf Dritte übertragen (Prüfung der Sicherheitsprinzipien für SW-Entwicklung beim Partner)

SW-Entwicklung durch Dritte

- Vertragliche Regelungen (Eigentümer des Sourcecodes, Urheberrechte, Dokumentationsumfang...)
- Vereinbarungen bzgl. sicheres Design, Entwicklungs- und Testmethoden
- Die Bedrohungsmodele mit dem AN abstimmen
- Einfordern von Nachweisen, dass die vereinbarten Standards eingehalten werden
- Einfordern von Nachweisen, dass Tests mögliche schädigende Inhalte erkennen konnten
- Vertragliche Regelung bzgl. Lieferantenaudits
- Festlegung, wer verantwortlich ist, einschlägige Gesetze einzuhalten / umzusetzen

Test der Systemsicherheit

- Abgeleitet von Bedrohungsmustern Testfälle vorgeben
- Konkrete Testvorgaben mit Inputs und erwarteten Outputs gestalten
- Testaktivitäten ab der Designphase integrieren

Test der Systemakzeptanz



- IS-Forderungen zentral in Test und Abnahme einbinden
- Prüfen, ob bestehende Sicherheitsmaßnahmen (Virenschutz, IPS,...) weiter anwendbar sind

Testdaten

- Einsatz von Produktivdaten vermeiden
- Berechtigungsmanagement im Testfeld soll dem der operativen Umgebung entsprechen



- Für jede Überleitung von Produktivdaten auf Testsysteme sind separate Genehmigungen erforderlich



- Produktivdaten sind unmittelbar nach den Tests nachhaltig zu löschen



- Überleitung und Einsatz von Testdaten ist zu protokollieren

Die 14 Kapitel der ISO 27002

- ✓ Security Policies
- ✓ Organisation of information security
- ✓ Human resource security
- ✓ Asset management
- ✓ Access control
- ✓ Cryptography
- ✓ Physical & environmental security
- ✓ Operations security
- ✓ Communications security
- ✓ System acquisition, development and maintainance
- Supplier relationships
- IS incident management
- IS aspects of business continuity management
- Compliance

Supplier Relationships

IS-Policy für Geschäftsbeziehungen mit AN (1)

- Arten von Zulieferern (IT-Service, Logistik, Finanzleistungen, IT-Infrastruktur,...)
- Prozess zum Management von mehreren unterschiedlichen Zulieferbeziehungen
- Festlegungen und Überwachung von Datentransfers von und zu Zulieferern
- Sicherheitsvorgaben für den Datentransfer (ggf. Verweis auf andere Policies – etwa Klassifizierung)
- Prozesse und Verfahren zur Überprüfung der Einhaltung der Vereinbarungen
- Prüfungen bzgl der Integrität und Richtigkeit der Lieferungen



neu: Supplier Relationships

IS-Policy für Geschäftsbeziehungen mit AN (2)

- Verpflichtungen beim Lieferanten um die Informationen entsprechend zu schützen
- Verfahren um unvorhergesehene Ereignisse gemeinsam zu bearbeiten
- Vorgaben bzgl. Stabilität und ggf. Wiederherstellbarkeit von Leistungen durch Dritte
- Awareness Trainings für MitarbeiterInnen, die mit Lieferanten in Kontakt treten
- Sicherheitsvereinbarungen mit Lieferanten
- Sicherheit in der Transitionsphase

Supplier Relationships

Sicherheit in Lieferantenverträgen (1)

- Beschreibung der betreffenden Informationen und Zugriffs- Austauschverfahren
- Vereinbarung zur Klassifizierung der Informationen
- Gesetzliche Vorgaben (Datenschutz, Urheberrecht,...) sowie Angaben wie diese einzuhalten sind
- Vereinbarte Sicherheitsmaßnahmen (Zugriff, Prüfung, Überwachung,...)
- Regeln zur Anwendung der Informationen und ggf. Ausschlüsse
- Explizite Liste von Personen, die Zugriff auf die Informationen erhalten

Supplier Relationships

Sicherheit in Lieferantenverträgen (2)

- Konkrete Incidentmanagement Vorgehensweisen
- Konkrete Schulungsanforderungen
- Vorgaben für Subbeauftragungen
- Sicherheitsansprechpartner beim Lieferanten
- Verfahren zur gemeinsamen Defekt- und Konfliktbewältigung
- Nachweise die durch den Lieferanten zu erbringen sind
- Verpflichtungen des Lieferanten, die Einhaltung von Sicherheitsbestimmungen zu prüfen

Supplier Relationships

Überwachung und Prüfung der Leistungen

- Überwachen der vereinbarten Servicelevels
- Kontrollieren der Service Reports (Steering Meetings)
- Auditplanung unter Einbeziehung der Service Reports und möglicher offener Punkte
- Überprüfung von Aufzeichnungen bzgl. Incidents beim Lieferanten und deren Bearbeitungsverläufe
- Vorgehen im Problemmanagement, unterstützen bei der Problemlösung
- Überprüfen der Sicherheitsanforderungen der Lieferanten an ihre Lieferanten

Die 14 Kapitel der ISO 27002

- ✓ Security Policies
- ✓ Organisation of information security
- ✓ Human resource security
- ✓ Asset management
- ✓ Access control
- ✓ Cryptography
- ✓ Physical & environmental security
- ✓ Operations security
- ✓ Communications security
- ✓ System acquisition, development and maintainance
- ✓ Supplier relationships
- IS incident management
- IS aspects of business continuity management
- Compliance

Management von Sicherheitsvorfällen und Verbesserungen

Verfahren zu:

- technischen und organisatorischen Monitoring
- analysieren von IS-Ereignissen
- aufzeichnen von Aktivitäten zum Incidentmanagement
- Umgang mit Ergebnissen forensischer Untersuchungen
- Ausbildung von MitarbeiterInnen im Incidentmanagement
- Reporting von Incidents und Schwachstellen
- Überprüfung und Bewertung von IS-Ereignissen
(auch hinsichtlich Escalation Richtung Notfallmanagement)

Berichtswesen bzgl. IS-Incidents

- Vorhalten von Berichtsformularen, wegen Vollständigkeit und Nachvollziehbarkeit
- Beschreibt das korrekte, vereinbarte Verhalten zur Incidentbehandlung (keine Alleingänge, Aufzeichnungen zu Details, weitergehende Meldewege,...)
- Verweise auf Disziplinarmaßnahmen für Fälle von mutwilligen schädigenden Handlungen
- Angepasste Feedbackverfahren, um den Meldern die weitere Abwicklung und Lösung zu vermitteln



Beispiele für berichtenswerte Ereignisse

- ineffektive Sicherheitsmaßnahmen
- Untererfüllung von Integritäts-, Vertraulichkeits- oder Verfügbarkeitsvorgaben
- menschliche Fehlleistungen
- Verfehlungen bezüglich interner Securitypolicies
- Unterlaufen von Maßnahmen zur phys. Sicherheit
- ungesteuerte Systemänderungen
- Defekte in SW oder HW
- Zugriffsverletzungen



Prüfung der Relevanz

Der Ansprechpartner zum Incidentmanagement bewertet den jeweiligen Incident auf Basis vorgegebener Maßstäbe

- Incident oder IS-Incident
- Frequenz des Auftretens
- Schadenserwartung (Art)
- Schadenserwartung (Höhe)
- Abschätzung der Bereinigungszeit
- Notfallrelevanz



Reaktion auf Incidents

folgende Aktivitäten sollten überlegt werden:

- Beweissammlung unmittelbar starten
- Forensische Analysen zur weiteren Bewertung
- Eskalation
- Aufzeichnung der Folgeaktivitäten
- Weitere Stellen / Rollen über das Auftreten des Incidents informieren (need to know)
- Abwenden von Sicherheitsschwachstellen, die im Rahmen der Erhebung aufgetaucht sind
- formeller Abschluss nach Incidentbehandlung

Die 14 Kapitel der ISO 27002

- ✓ Security Policies
- ✓ Organisation of information security
- ✓ Human resource security
- ✓ Asset management
- ✓ Access control
- ✓ Cryptography
- ✓ Physical & environmental security
- ✓ Operations security
- ✓ Communications security
- ✓ System acquisition, development and maintainance
- ✓ Supplier relationships
- ✓ IS incident management
- IS aspects of business continuity management
- Compliance

IS aspects of BCM

Planung von IS Continuity

- Grundsätzliche Frage: Wie wird IS nach einem Notfall, Krise, Katastrophe wieder hergestellt?
- Festlegung ob IS Continuity im BCM oder DRM stattfindet
- Ggf. eine Business Impact Analyse für IS vornehmen



IS aspects of BCM

Implementierung von IS Continuity

Anforderung: IS muss auch bei Notfällen, Krisen, Katastrophen (ggf. eingeschränkt) funktionieren

- Installieren einer Managementstruktur zu Planung, von Bearbeitung und Behebung von Notfällen
- Sicherstellen, dass dann auch kompetentes Personal verfügbar ist (vorab nominieren)
- Dokumentierte Pläne zur Schadensfallsabwicklung, Wiederherstellung & Kommunikation, um Informationssicherheit ehestmöglich auf ein vorgegebenes Niveau zu bringen

IS aspects of BCM

Überprüfen und Einschätzen von IS Continuity

Anforderung: Prüfung der Wirksamkeit unter möglichst realistischen Bedingungen

- Die Funktionalität testen
- Das Wissen und die Skills der handelnden Personen sicherstellen
- Sicherstellen, dass IS Continuity Maßnahmen auch nach Änderungen an Systemen oder Verfahren im Notfall wirksam sind

Anm.: Einplanen von Redundanzen auch auf Verfahrensebene (etwa zwei Verschlüsselungstechnologien)

Auswahl Standards zu BCM/DR

unternehmensweit

BS 25999
(Business Continuity Management)

ISO 22301:2012
BCM Systems Requirements

ISO 22313:2013
BCM Systems Guidance

ISO/PAS 22399:2007
Guideline for incident preparedness and operational continuity management

BSI Standard 100-4
(Notfallmanagement)

NIST SP 800-34
Contingency Planning Guide for IT Systems

ITIL, ISO 20000
Service Continuity Management

BCI GPG 2008

IT/IS-spezifisch

ISO 27002
BCM

ISO 27031:2011
Guidelines for ICT readiness for BCM

ISO 24762:2008
Guidelines for ICT DR Services

BS British Standard

BSI Bundesamt für Sicherheit in der Informationstechnik

BCI Business Continuity Institute

GPG Good Practice Guide

Die 14 Kapitel der ISO 27002

- ✓ Security Policies
- ✓ Organisation of information security
- ✓ Human resource security
- ✓ Asset management
- ✓ Access control
- ✓ Cryptography
- ✓ Physical & environmental security
- ✓ Operations security
- ✓ Communications security
- ✓ System acquisition, development and maintainance
- ✓ Supplier relationships
- ✓ IS incident management
- ✓ IS aspects of business continuity management
- Compliance

Einhaltung der Verpflichtungen

- Identifikation anzuwendender Gesetze
- Erfüllung von Verträgen
- Überprüfung zur Einhaltung der Security Policy und technischer Normen
- Systemaudit / Schutz der Audittools
- Sammeln und bewerten von Beweisen

Die 14 Kapitel der ISO 27002

- ✓ Security Policies
- ✓ Organisation of information security
- ✓ Human resource security
- ✓ Asset management
- ✓ Access control
- ✓ Cryptography
- ✓ Physical & environmental security
- ✓ Operations security
- ✓ Communications security
- ✓ System acquisition, development and maintainance
- ✓ Supplier relationships
- ✓ IS incident management
- ✓ IS aspects of business continuity management
- ✓ Compliance

ISO 27004

**Information technology
-- Security techniques --
Information security management -- Measurement**



Agenda:

- Ziele, Kontext
- Errichtungsmodell – Modellierung der Methoden
- Einige Detailüberlegungen
- Bewertung des Messmodells

Zielsetzungen der Messthematik

Feststellen der Effektivität der implementierten Maßnahmen

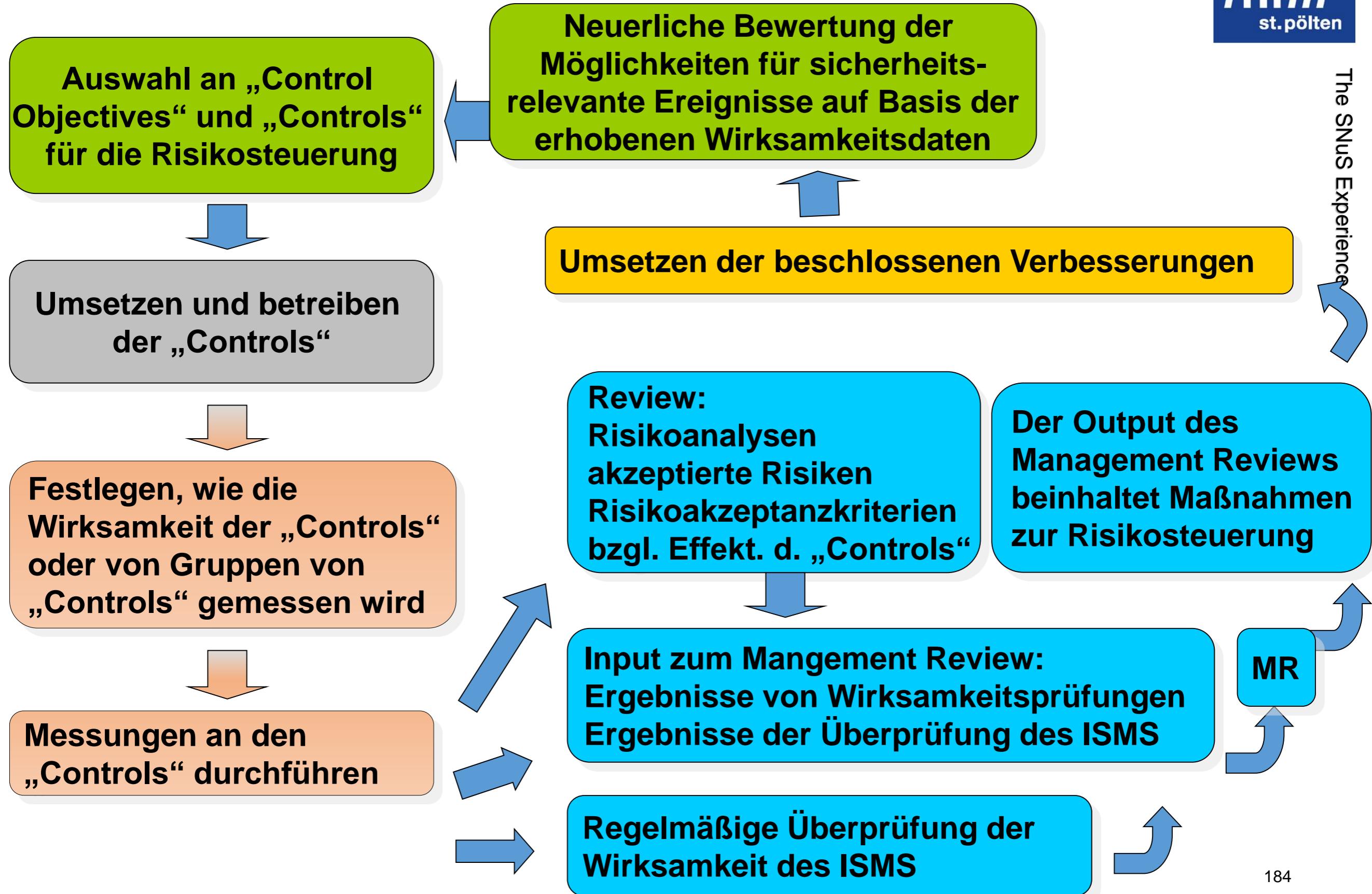
Feststellen der Wirksamkeit des gesamten ISM Systems

Bereitstellen von Statusinfos zu ISMS Aspekten als Input zu:
Management Reviews
Kontinuierlichen Verbesserungs - Prozess (KVP)
Security Audits

Den „Wert“ des ISMS und der IS für die Organisation / das Unternehmen zu vermitteln

Input zu Risikoassessment- und Risikobehandlungsverfahren liefern

Messungen im 27001 Kontext



Messungen im 27001 Kontext

PLAN

Auswahl an „Control Objectives“ und „Controls“ für die Risikosteuerung

Neuerliche Bewertung der Möglichkeiten für sicherheits-relevante Ereignisse auf Basis der erhobenen Wirksamkeitsdaten

ACT

Umsetzen und betreiben der „Controls“

Festlegen, wie die Wirksamkeit der „Controls“ oder von Gruppen von „Controls“ gemessen wird

Messungen an den „Controls“ durchführen

DO

Umsetzen der beschlossenen Verbesserungen

Review:
Risikoanalysen
akzeptierte Risiken
Risikoakzeptanzkriterien
bzgl. Effekt. d. „Controls“

Der Output des Management Reviews beinhaltet Maßnahmen zur Risikosteuerung

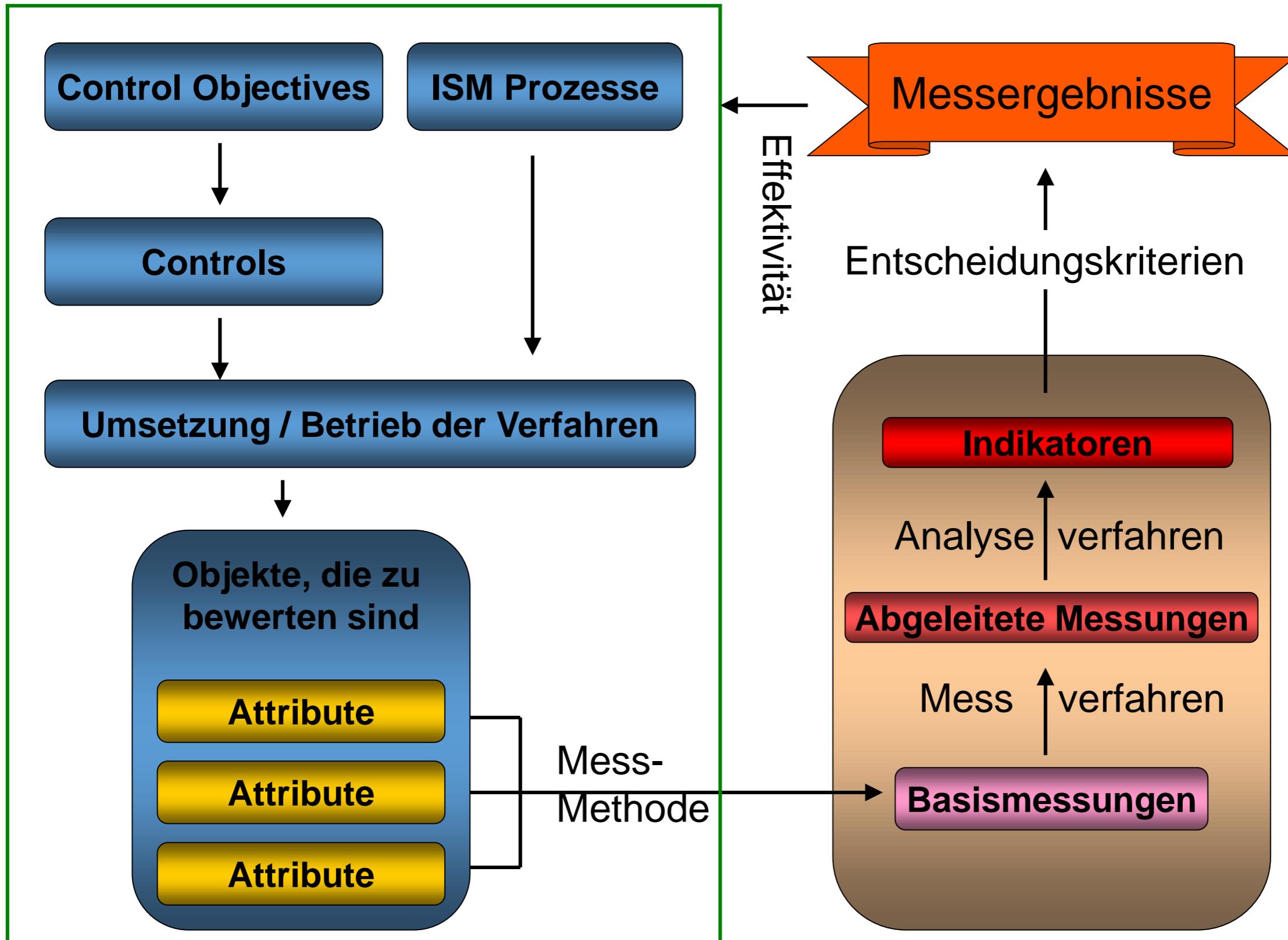
Input zum Management Review:
Ergebnisse von Wirksamkeitsprüfungen
Ergebnisse der Überprüfung des ISMS

MR

Regelmäßige Überprüfung der Wirksamkeit des ISMS

CHECK

Modell für IS-Messungen



Kriterien für ein ISM Metriksystem

- Strategiebezogen: Abgestimmt auf die IS-Strategie der Organisation / des Unternehmens
- Quantitativ: Numerische empirische Daten eher als Meinungen
- Vernünftig / Wirtschaftlich: Die Datenmengen und Auswertungsverfahren im Verhältnis zum Nutzen
- Verifizierbar: Externe Prüfer sollen zu selben Ergebnissen gelangen
- Langfristig gültig: Die Messergebnisse sollten über mehrere Messperioden hinweg vergleichbar sein
- Sinnvoll: Die Messergebnisse müssen im Kontext IS anwendbar sein

Einmal mehr: Das Errichtungsmodell!

-  Gesamtscope definieren
-  Festlegen wo Informationsbedarf besteht, somit wo Messungen und Bewertungen durchzuführen sind
-  Daraus abgeleitet Identifikation der Objekte und deren Attribute
-  Gestalten der Durchführungsdetails
-  Erstumsetzung und Anwendbarkeitsprüfung
-  Umsetzen der Verfahren zur Datenerhebung und -analyse
-  Erstellen der Rahmendokumentation

Überlegungen zum Scope



Den Initialscope möglichst eingeschränkt gestalten



Objekte erstmal beschränken auf:

- einfache Maßnahmen
- kritische Informationswerte
- essentielle Verfahren

die auch für die Stakeholder interessant sind



Eine reduzierte Menge an aussagekräftigen Messergebnissen vorsehen, um deren Anwendbarkeit in der Organisation erkennen zu können (ggf. Kulturproblem)

Wer sind „Stakeholder“



Entscheidungsträger (Management) oder andere Rollen, die etwa für ihre Aufgaben im Rahmen des ISMS Informationen benötigen



Personen, die die Wirksamkeit von Maßnahmen prüfen müssen



Informationseigentümer, die auf Grund der Sicherheitsrelevanz hohen Informationsbedarf haben



Personen die Daten erheben (Attribute auswerten)



Personen, die die Analysen durchführen und die Ergebnisse kommunizieren



Personen, die das Metrikensystem selbst überprüfen

Achtung: Vertraulichkeitsstatus der Ergebnisse nicht außer Acht lassen

Einbettung in das ISMS

-  Definition von Rollen und Verantwortlichkeiten hinsichtlich Gestaltung, Abwicklung und Optimierung des Metrikensystems
-  Datenerfassung und Datengenerierung entsprechend den Verfahren des ISMS steuern (ggf. Verfahren anpassen)
-  Änderungen bei der Datenerfassung den Betroffenen mitteilen
-  Die Kompetenz der Datenerfasser sicherstellen (Skills bezüglich Datenarten, Tools, Verfahren und andere Anforderungen)
-  Regelungen und Zielsetzungen zum Metrikensystem erstellen
-  Datenanalyse und Reporting möglichst in bestehende Prozesse integrieren um Beständigkeit und Nachvollziehbarkeit zu sichern
-  Überwachen und überprüfen der Ergebnisse (Systemüberprüfung)

Das Metrikensystem muss ein Teil des ISMS werden

Festlegen des Informationsbedarfs

Ausgangspunkt der Überlegungen sind generelle Zielsetzungen (IS-Policy) sowie auch konkrete Detailziele (Control Objectives)



Eine Auswahl an Beispielen findet sich im Anhang A der ISO 27004



Durchaus brauchbar als Arbeitsbasis sind die „Control Objectives“ der ISO 27002, sofern sie mit den Unternehmenszielen korrelieren



Zusätzlich bieten in der Regel noch:

- Complianceanforderungen und
- Ergebnisse des Risikomanagements

dankbare Zielsetzungen

Auswahl der Objekte und Attribute

Werden abgeleitet vom Informationsbedarf und den damit in Verbindung zu bringenden Unterlagen, Verfahren, Prozessen,...

Beispiele:

- Produkte und Services
- Assets (siehe Assetmanagement ISO 27002)
- Nachweise, Aufzeichnungen, Protokolle, Logfiles,...
- Dokumente, Anforderungen, Managemententscheidungen,...
- Örtliche Gegebenheiten (Außenstellen, Zutrittsanlagen,...)
- Zulieferungen Dritter

Bereits bei der Auswahl der Objekte auf realistische Attributierung und leistbaren Aufwand bei der Datenerhebung achten!

Vorgehensweise zur Modellierung

Festlegen einer Messsystematik (Verfahren, Prozesse, Verantwortungen) unter Beachtung folgender Punkte:

- Branche / Geschäftscharakteristika
- Organisationsstruktur
- Örtlichkeiten
- Eingesetzte Technologien
- Vertragliche / gesetzliche Verpflichtungen

Auswahl jener „Control Objectives“ und „Controls“ aus dem ISMS, die in den Messverfahren Eingang finden

Definieren der IS-Indikatoren für die ausgewählten Maßnahmen

Einbinden der Auswahl in das Statement of Applicability

Faktoren zur Intensität der Messung

Messungen können in unterschiedlichsten Detaillierungsgraden durchgeführt werden, abhängig etwa

-  Von der Anzahl und Kritikalität der Risiken denen man ausgesetzt ist
-  Von der Verfügbarkeit von Ressourcen
-  Branchenerfordernissen
-  Von der Anzahl von Incidents, die es zu reduzieren gilt
-  Von der Managementstruktur des Unternehmens (werden Messergebnisse tatsächlich als Basis für Verbesserungen herangezogen)
-  Unternehmens-, Organisationsgröße
-  Von der Komplexität und Struktur der zu bemessenden Thematik

Selbst bei Messungen und Messverfahren mit geringer Detailtiefe sind die Verfahren und Ergebnissauswertungen immer wieder zu optimieren

Erhebung der Daten

Welche Daten wie zur Verfügung gestellt werden ist zu dokumentieren, diesbezüglich weiters:

- Die Datenquellen der definierten Daten
- Verantwortliche Rollen für Datenzulieferung
- Datum / Uhrzeit der Zulieferung (Häufigkeit)
- Art und Weise der Übermittlung

Zu beachten ist, dass unter Umständen auch aktuelle Daten seitens Managementebene anzufordern sind. Auch hier sind obige Festlegungen zutreffend.

Beispiele für Datenquellen

Interne & externe Audits:

Etwa um den Reifegrad des Metrik und Messsystems selbst zu bestimmen

Risikoanalysen:

Etwa um die Risikolevel von Services zu bestimmen

Ergebnisse von speziell entwickelten checklistenbasierten Untersuchungen

Auswertungen von Aufzeichnungen, Logfiles, Protokollierungen

Durch automatisierte Auswertungen von Abläufen in IT-Systemen (IDS, Virenstatistiken, Helpdeskfragen, systemspez. Fehler,...)

Typen von IS-Messungen

Performance Messungen

Die Effektivität einzelner Maßnahmen oder Maßnahmenbündel

Gegenüberstellung der IST-Performance und der Anforderungen aus Risikobetrachtung, gesetzlichen und vertraglichen Grundlagen IS-Regeln der Organisation, u.a.

Messung des Entwicklungsgrades

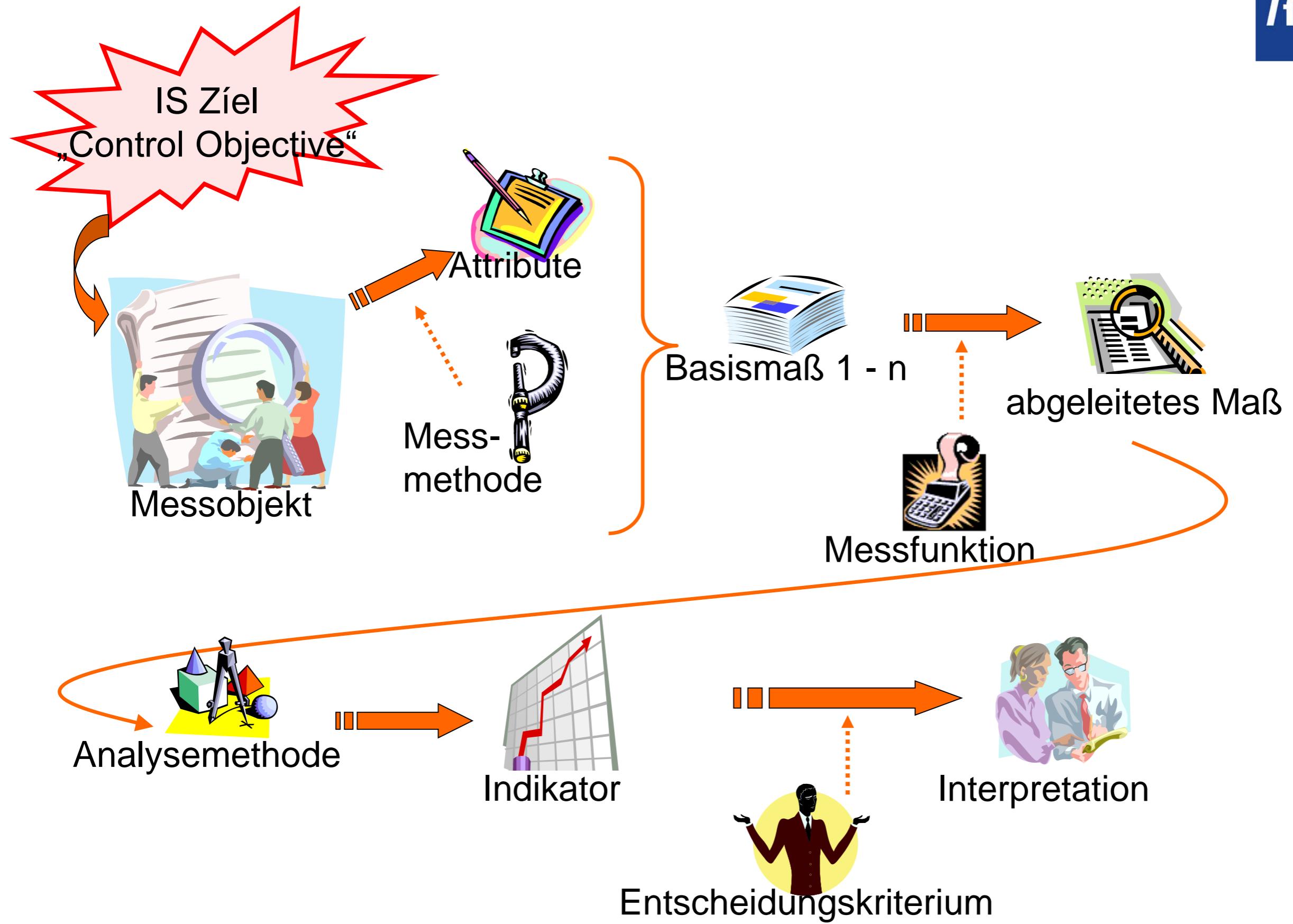
Fortschritte bezüglich Security - Performance

Fähigkeit des IS-Systems auf Veränderungen schnell zu reagieren
(Reifegrad von Systemen)

Kritische Erfolgsfaktoren

-  Zuteilung ausreichender Ressourcen (bedingt Ressourcenplanung)
-  Ein existierendes ISMS mit eingeführten Prozessen und Verfahren
-  Quantifizierbare Größen die einen Zusammenhang mit den ISMS Zielen bilden
-  Einfach zu erhebende Basisdaten, die als Grundlage zu den Messverfahren herangezogen werden können
-  Sicherstellen, dass die Basisdaten in der geforderten Qualität in konsistenter Periodik erhoben und analysiert werden
-  Die Evaluation des Metrikensystems selbst und die Möglichkeit Verbesserungen umzusetzen
-  Planung auch von längerfristigen Messreihen, anlegen eines Pools historischer Daten
-  Sicherstellen, dass die Messergebnisse auch angewandt werden (Stakeholder erkennen einen Nutzen)

Der Ablauf beispielhaft



Gestalten der Durchführungsdetails (measurement construct development)

Überlegungen zu Messmethoden:

-  Jedem „Basismaß“ (ergibt sich aus dem Attribut) muss eine Messmethode zugeordnet werden (dokumentiert)
-  Durch Anwendung der Messmethode wird aus dem Attribut ein Wert gewonnen, der dem „Basismaß“ zugeordnet wird.
-  Die Messmethode quantifiziert somit ein Attribut, das bedingt auch eine definierte Einheit – Vergleiche können später natürlich nur zwischen Messergebnissen gleicher Einheit gezogen werden.
-  Für jede Messmethode sollte auch ein Verifizierungsverfahren eingesetzt werden (Vertrauen in die Ergebnisse gewährleisten)
-  Das Maß der Korrektheit, Abweichung und Varianz sollten der Methode zugeordnet werden können
-  Die Messmethode soll über längere Zeit anwendbar bleiben

Gestalten der Durchführungsdetails (measurement construct development)

Beispiele für Messmethoden:

- Befragungen
- Beobachtungen
- Checklistenbasierte Untersuchungen
- Überprüfung / Erhebung von Know How / Skills
- Systemüberprüfungen
- Testverfahren (Design, Operation)

Subjektive Messmethode:

Quantifizierung durch Einschätzungen von Menschen

Objektive Messmethode:

Quantifizierung auf Basis eindeutiger Regeln (Zählen, errechnen,...)

Sampling: Feststellen einer statistisch ausreichenden Menge von Messdaten

Gestalten der Durchführungsdetails (measurement construct development)

Auswahl von Messfunktionen:

Messfunktionen bilden aus mehreren Basismaßen ein
abgeleitetes Maß (derived Measure)



Messfunktion kann aus unterschiedlichen beliebig komplexen Verknüpfungen und Funktionen bestehen etwa:

- Statistische Methoden (Mittelwert, Varianz, Verteilungen,...)
- Gewichtungen
- Kombinieren von quantitativen und qualitativen Maßzahlen
- log und exp Funktionen um klarere Darstellungen zu erhalten
- Herstellen von Verhältnissen
- ...

Gestalten der Durchführungsdetails (measurement construct development)

Analytisches Modell:

Das „analytische Modell“ bildet aus abgeleiteten Maßzahlen und ggf. auch Basismaßzahlen sogenannte Indikatoren

-  Das analytische Modell kombiniert Messergebnisse so, dass Stakeholder sinn- und wertvolle Erkenntnisse ableiten können
-  Das analytische Modell muss geeignet sein Ergebnisse zu liefern, auf die definierte Entscheidungskriterien anwendbar sind
-  Die Darstellung der Indikatoren ist ebenfalls festzulegen, und in der Regel abhängig von den Vorstellungen der Stakeholder (graphisch, textuell, kombiniert)

Hinweis: ISO TR 10017 „statistical techniques for ISO 9001“

Gestalten der Durchführungsdetails (measurement construct development)

Entscheidungskriterien:

-  Entscheidungskriterien müssen sich aus den IS-Zielen (Control Objectives) ableiten und diesen zugeordnet dokumentiert werden.
-  Die Einheit oder Art des Indikators muss sich den Entscheidungskriterien anpassen (€, %, p, Trend,...)
-  Der Interpretationsspielraum sollte möglichst gering sein!
-  Die Entscheidungskriterien können sich im Sinne der permanenten Verbesserung im Laufe der Zeit ändern.

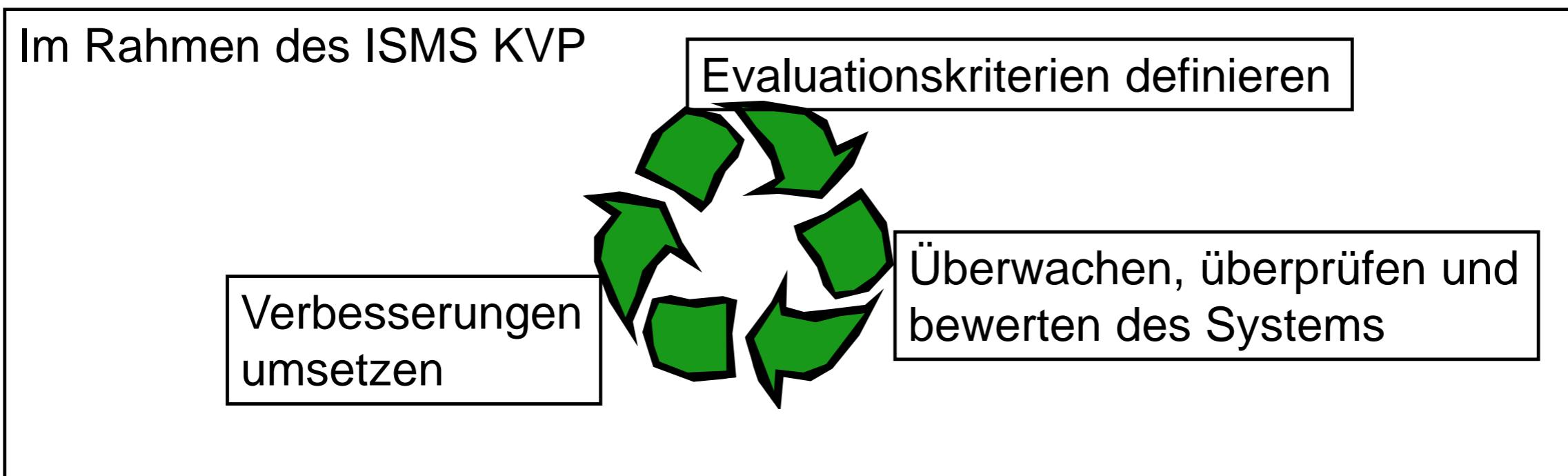
Beispiel: Das Ergebnis muss zwischen 0,99 und 1,01 liegen,
andernfalls wurden die Ziele nicht erreicht

Überlegungen zur Evaluierung des Metrikensystems

Überprüfen hinsichtlich:

- effiziente Verfahren
- Abwicklung wie geplant
- Eignung, Änderungen an Maßnahmen herbeizuführen
- Eignung, Änderungen am ISMS oder am Umfeld zu bewirken
- Grundsätzliche Erfüllung der ursprünglichen und aktuellen Anforderungen

Ein Plan zur Wirksamkeitsprüfung muss vorliegen:



Überlegungen zur Evaluierung der Messergebnisse

Folgende Kriterien könnten nützlich sein:



Messergebnisse:

- sind einfach zu verstehen
- werden zeitnah vermittelt
- objektiv, vergleichbar und reproduzierbar



Die Verfahren zur Generierung der Messergebnisse:

- sind definiert
- einfach abzuwickeln
- werden eingehalten



Die Messergebnisse sind gut geeignet als Entscheidungsgrundlage zu fungieren



Die Messergebnisse zielen nicht an den Anforderungen vorbei

Verbesserung der Messverfahren

Zusammenfassend: Regelmäßig festzustellen ist ob das Messsystem:



Geeignet ist, kontinuierlich die geforderten Messwerte zur Entscheidungsfindung zu liefern



Sicher stellt, dass die Datenquellen, die Messverfahren und alle damit verbundenen Aspekte geeignet sind, korrekte Werte liefern



Wirtschaftlich ist, also der Nutzen die Kosten des Systems deutlich übersteigt

ISO 27005

**Information technology - Security techniques
– Information security risk management –**



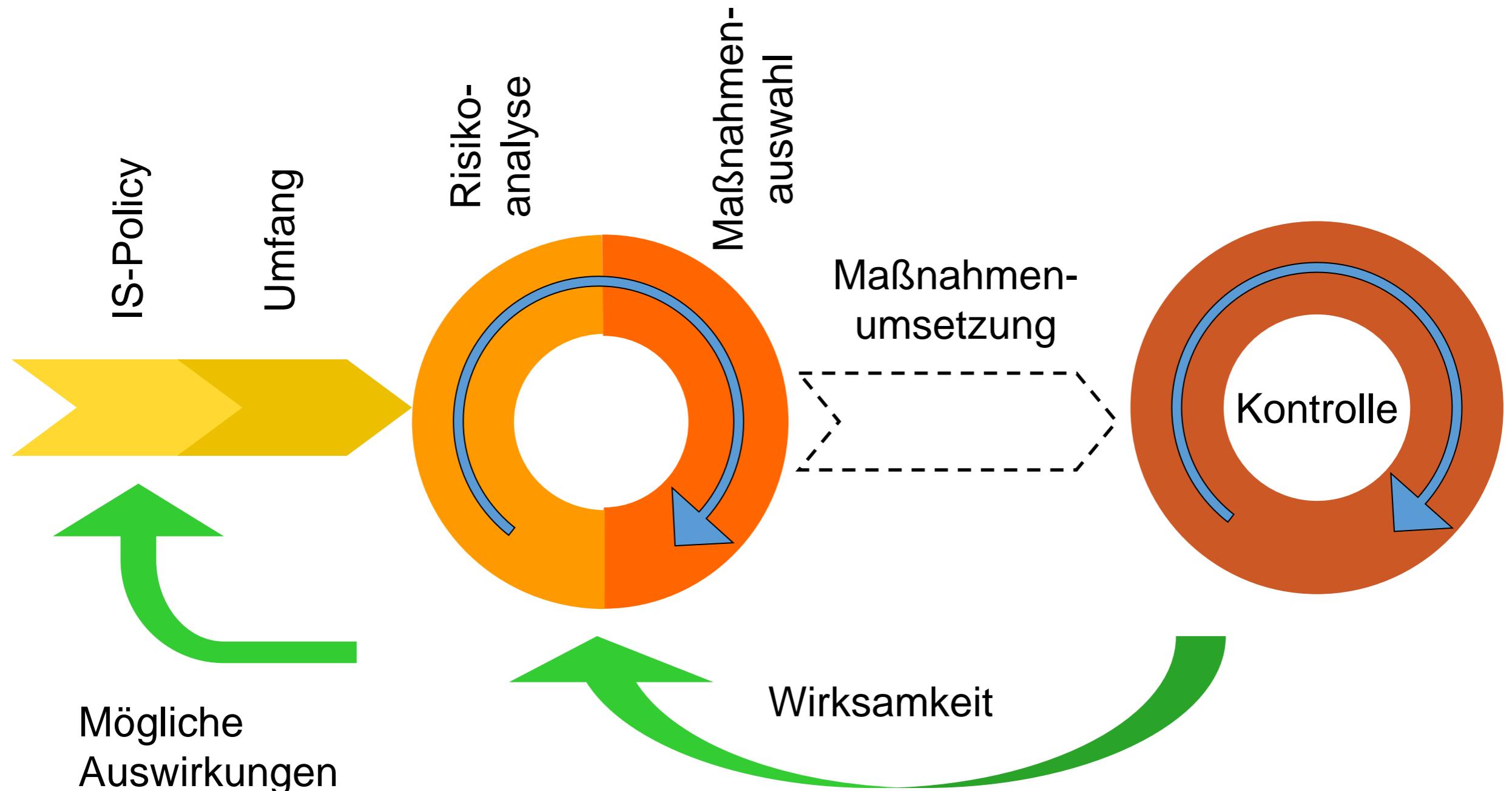
Agenda Risikothematik

Definitionen / Eingrenzung

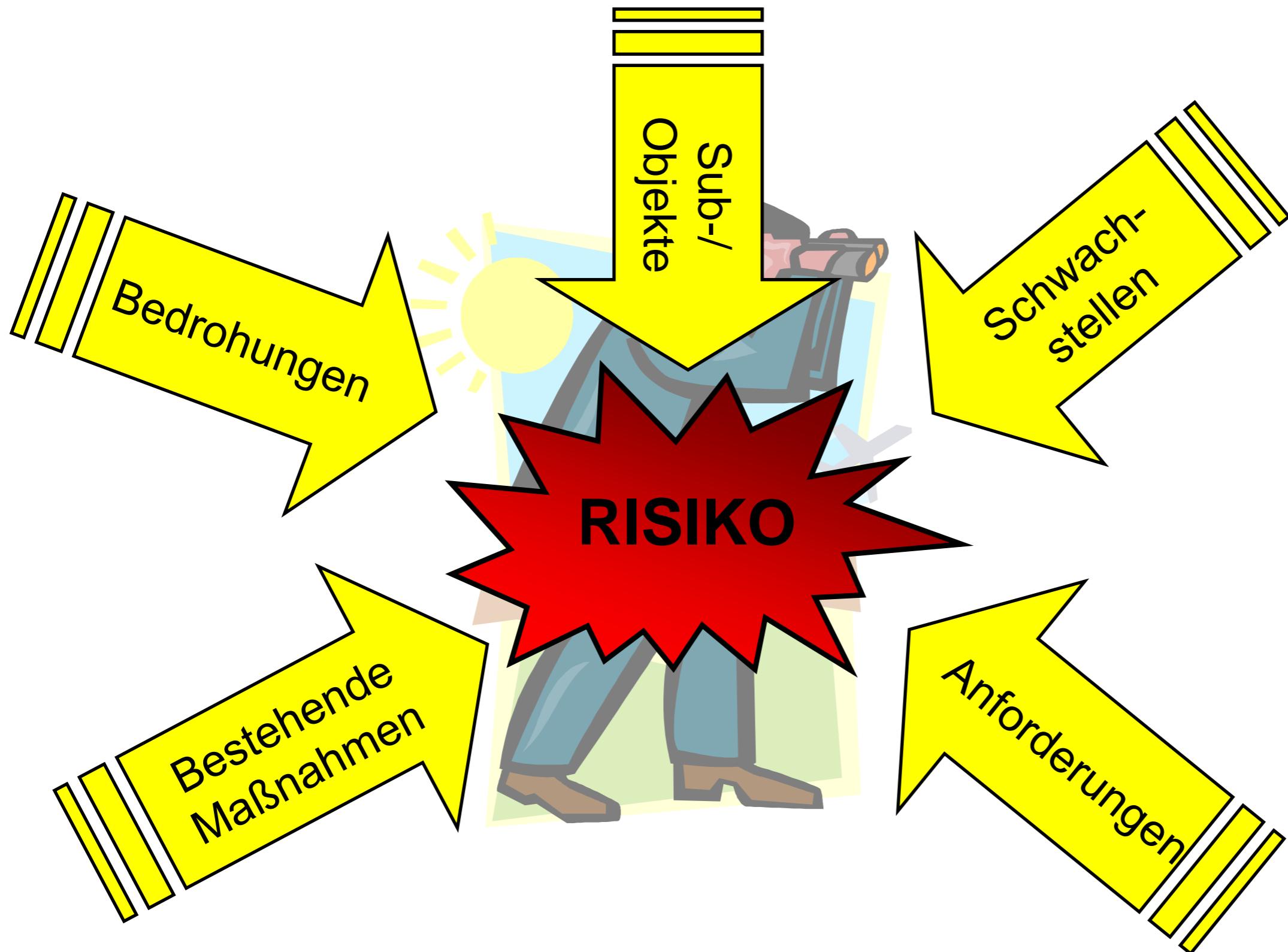
Risikomanagement „klassisch“

Grundschatzansatz

ISMS - Risikomanagement



Risiko - Umfeld



ISO 27005 Grundsätzlich

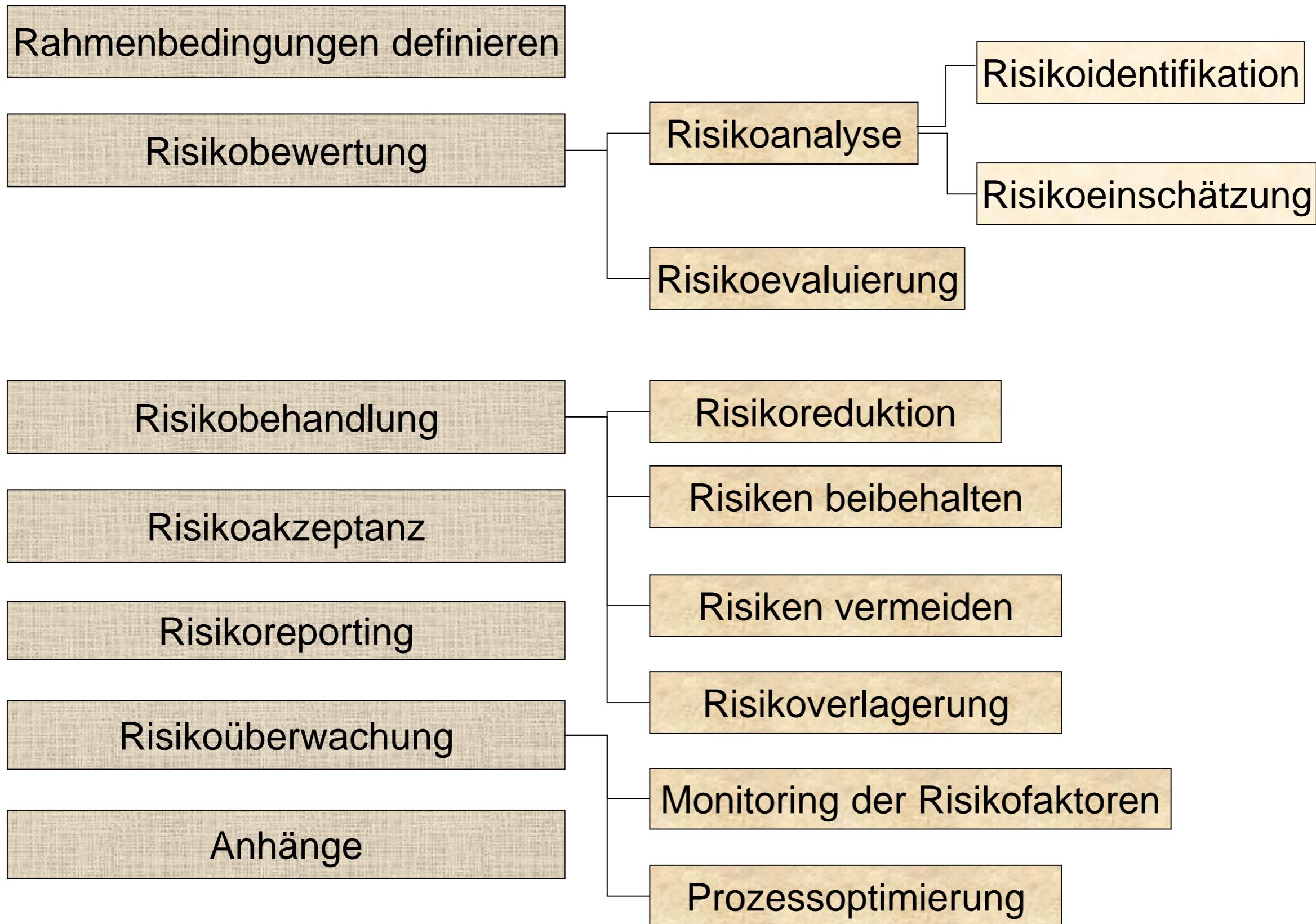
Veröffentlichung im Juni 2011

Ersetzt die ISO 13335-3:1998 und 13335-4:2000

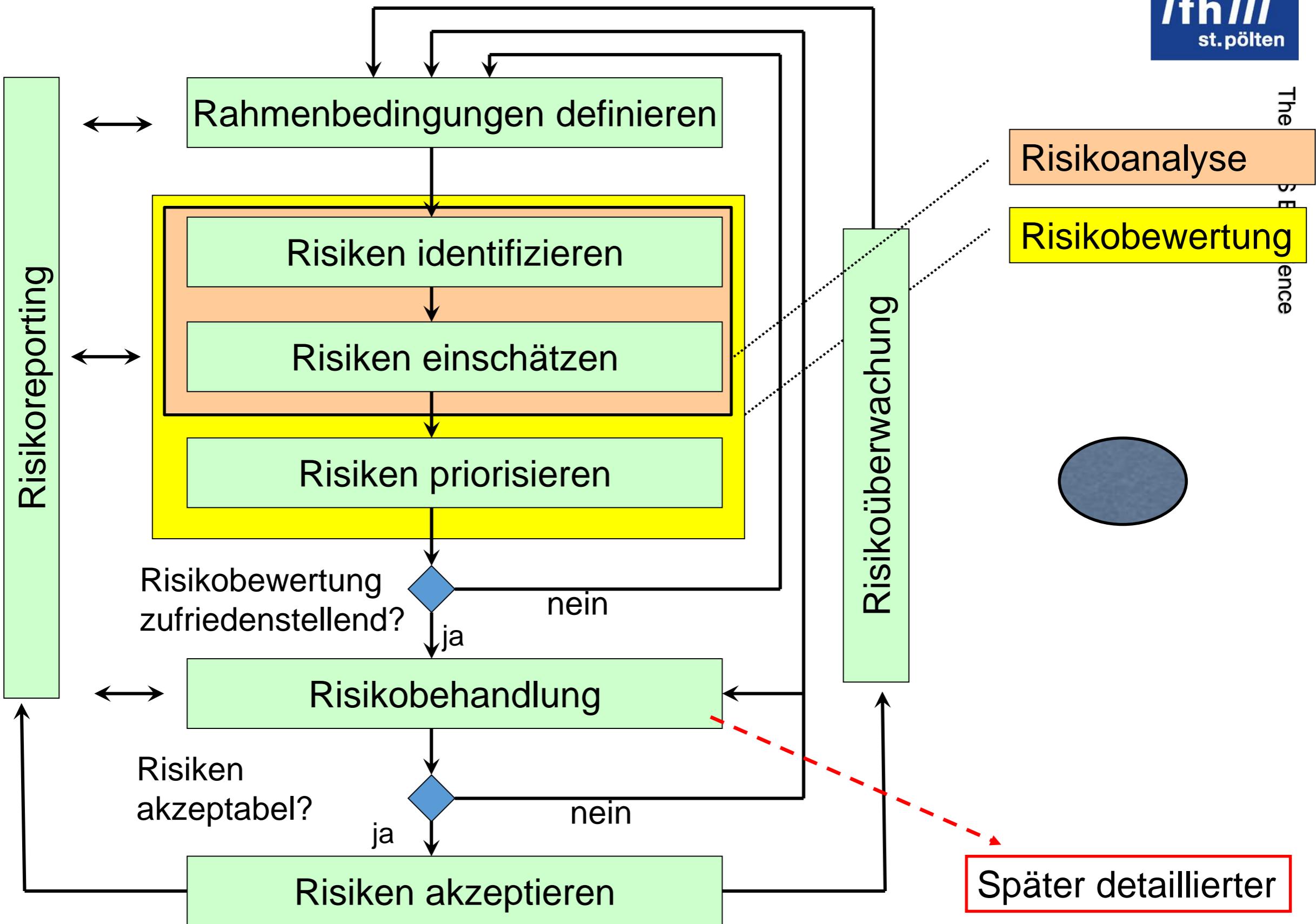
Beschreibt IS-Risikomanagementprozesse und daraus abgeleitete Aktivitäten

In den Anhängen A – E werden Beispiele und Listen angeführt, die als Implementierungshilfe zu sehen sind

ISO 27005 Struktur



ISO 27005 Struktur



Rahmenbedingungen definieren (1)

Vorab die Frage: Welche Ziele verfolgen wir mit der Implementierung von RM?



Betreiben eines ISMS



Complianceanforderungen, Nachweise etwa für due diligence



Als Basis für Business Continuity Pläne



Als Basis für Incident Handling



Detailliertere Erhebung von Sicherheitsanforderungen eines Produkts, Services, Verfahrens,...

● ● ●

Rahmenbedingungen definieren (2)

Grundsätzliche Kriterien festlegen, etwa folgende:

-  Grundlagen und Rahmenbedingungen zur Risikoevaluierung
 - z.B.: Welche Einflussgrößen werden herangezogen
 - Welche Anforderungsziele existieren (c,a,i)...
-  Rahmenbedingungen zur Feststellung der Auswirkungen
 - Was wird als Schadensszenario anerkannt, bzw.
 - muss bedacht werden.
 - Wie können Szenarien hinsichtlich ihrer Auswirkungen verglichen werden.
-  Kriterien zur Risikoakzeptanz
-  Umfang und Grenzen definieren
-  Organisation und Verantwortlichkeiten für IS-RM

Rahmenbedingungen definieren (3) >

Kriterien zur Risikoakzeptanz

Grundsatz: Jedes Unternehmen / jede Organisation muss seine Akzeptanzkriterien individuell definieren

-  Unterschiedliche Risikoarten werden unterschiedliche Schwellwerte bedingen
-  Ex. Management kann auch Entscheidungen abseits dieser Werte treffen
-  Manche Risiken sollten generell nicht akzeptiert werden (§)
-  Temporäre Risikoakzeptanz sollte ebenfalls bewertet werden

Schwellwertbeispiel: Verhältnis von erwarteten Profit zu Schadenshöhe

Rahmenbedingungen definieren (4) >

Umfang und Grenzen

Was muss in die Überlegungen mit einbezogen werden, was definitiv nicht, dazu folgende Kriterien:

-  Strategische Geschäftsziele, Strategien, Policies
-  Geschäftsprozesse
-  Organisationsstruktur
-  Das soziale und kulturelle Umfeld
-  Rechtliche und vertragliche Anforderungen
-  Informationssicherheitsrelevante Werte
-  Der organisationsweite Risikomanagementansatz
-  Schnittstellen innerhalb der Organisation oder zu Partnern

Rahmenbedingungen definieren (5) >

Organisation und Verantwortlichkeiten für IS-RM

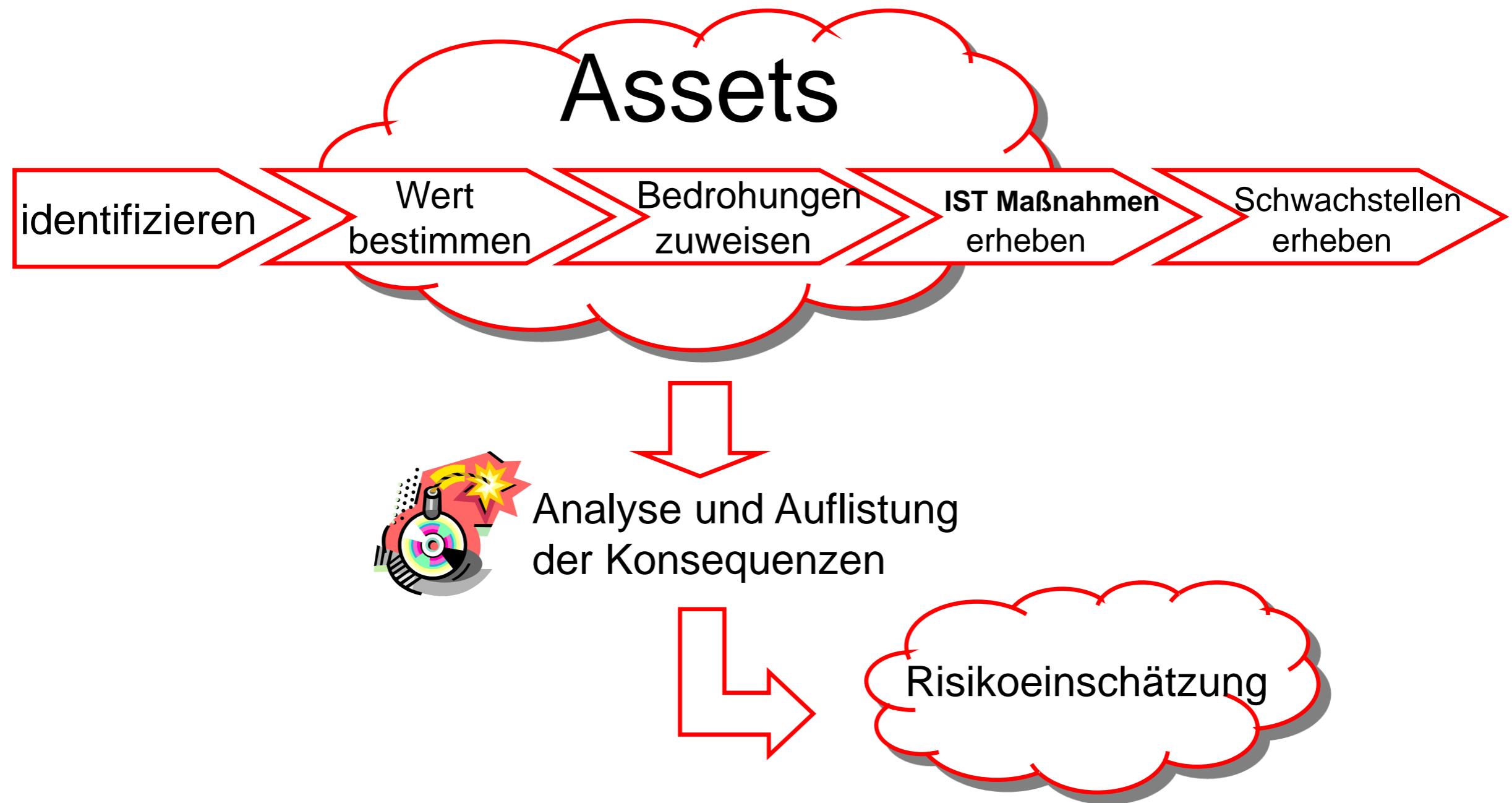
Personen, Rollen Verantwortlichkeiten, Kommunikationsbasis:

-  Identifizieren der Stakeholder
-  Festlegen der Rollen und Verantwortlichkeiten auch bei den Partnern
-  Herstellen der Schnittstellen zu anderen Risikomanagement-funktionen im Unternehmen
-  Festlegen von Eskalationspfaden
-  Sicherstellen, dass das RM Modell dem Unternehmen / der Organisation angepasst ist

Risikobewertung >

Risikoanalyse > Risikoidentifikation > Erhebung der Assets

Ein Asset im Sinne der ISO 27005 ist alles, was einen Wert für die Organisation besitzt und daher schützenswert ist



Risikobewertung >

Risikoanalyse > Risikoidentifikation > Erhebung der Assets

Folgende Untergliederung ist in der ISO 27005 angeführt:



Primäre Assets

- Geschäftsprozesse und -aktivitäten
- Informationen



Unterstützende Assets

- IT-Hardware
- Software
- Netzwerk
- Personal
- Gebäude / Infrastruktur
- Organisationsstruktur

⋮

Detailliertere Auflistungen in Annex B

Risikobewertung >

Risikoanalyse > Risikoidentifikation > Werteanalyse

Grundsätzliches zur Werteanalyse:



Sachwerte

- Zeitwert
- Wiederbeschaffungswert
- Wert für einen potentiellen Angreifer
- Schaden für die Organisation aus einem Verlust oder Modifikation



Immaterielle Werte

- Wert für einen potentiellen Angreifer
- Schaden für die Organisation aus einem Verlust oder Modifikation

Ermitteln und Darstellen von Abhängigkeiten der identifizierten Objekte zueinander

Zu beachten: In der Regel entsprechen Wertekombinationen nicht der Summe der Einzelwerte

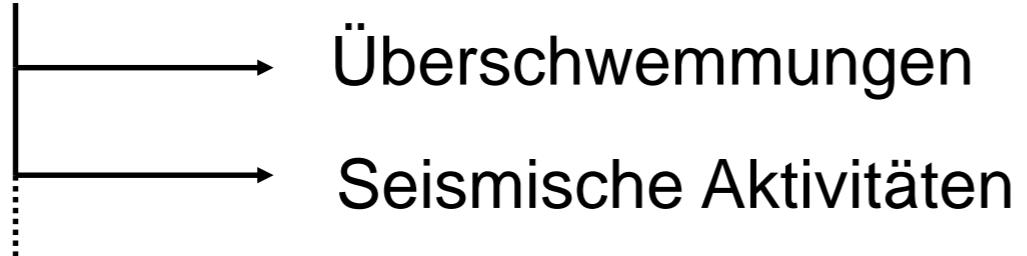
Risikobewertung >

Risikoanalyse > Risikoidentifikation > Bedrohungsanalyse

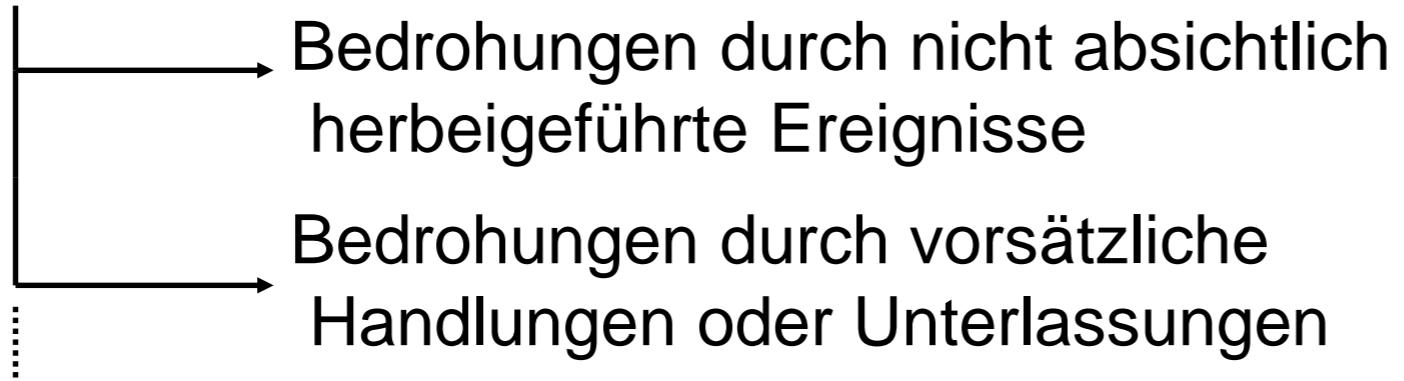
Grundsätzliches zur Bedrohungsanalyse:



Naturgegebene Bedrohungen



Bedrohungen durch Menschen



ISO 27005 Anhang C, einschlägige Literatur

Risikobewertung >

Risikoanalyse > Risikoidentifikation > Erhebung bestehender Maßnahmen



Um eine Baseline zur Risikobewertung zu bilden werden bestehende Sicherheitsmaßnahmen erhoben und den Objekten zugeordnet.

Weiters muss überprüft werden ob die vorgeblich eingesetzten Maßnahmen tatsächlich wirksam sind.

Sicherheitsmaßnahmen, deren Wirksamkeit nicht gewährleistet ist, suggerieren Sicherheit, die möglicherweise nicht gegeben ist.

Risikobewertung >

Risikoanalyse > Risikoidentifikation > Schwachstellenanalyse

Grundsätzliches zur Schwachstellenanalyse:

Schwachstellen finden sich prinzipiell an allen identifizierten Objekten

Schwachstellenlisten liegen in der einschlägigen Literatur vor, (Grundschutzhandbuch, ISO 27005 Anhang D)

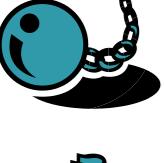
Schwachstellenlisten verleiten dazu, diese als vollständig einzuschätzen → Individuelle Schwachstellen ermitteln!

Eine Schwachstelle an sich verursacht noch keinen Schaden, ist aber die Voraussetzung, die es einer Bedrohung ermöglicht wirksam zu werden.

Risikobewertung >

Risikoanalyse > Risikoidentifikation > Analyse der Konsequenzen

Potentielle Arten von Konsequenzen wären:

-  Zeitliche / personelle Ressourcen um Erhebungen und Wiederherstellung durchzuführen
-  Stehzeiten (Serviceerbringung, Produktion,...)
-  Verlust möglicher Aufträge
-  Gefahr für Leib und Leben
-  Finanzielle Aufwendungen für spezielle Verfahren zur Wiederherstellung
-  Verlust von Image, Reputation und Gunst

Risikobewertung >

Risikoanalyse > Risikoeinschätzung > Einschätzungsmethoden

Heterogene Detailtiefe der Analysen

Risikoanalysen können in unterschiedlichsten Detaillierungsgraden durchgeführt werden, abhängig etwa

-  Von der Kritikalität der Assets
-  Vom Ausmaß der bekannten Schwachstellen
-  Von der Häufigkeit des Auftretens von bestimmten Incidents

Art der Analyse:

Qualitativ, Quantitativ, oder eine Kombination daraus je nach Situation und Zielsetzung

Risikobewertung >

Risikoanalyse > Risikoeinschätzung > Einschätzungsmethoden

Qualitative Methoden werden eingesetzt:

-  Als initiale Analyse, um festzustellen zu welchen Themen detailliertere Analysen nötig sind
-  Wenn die Qualität der Ergebnisse zur Entscheidungsfindung ausreicht
-  Wenn die grundlegenden Daten und Informationen für eine quantitative Analyse nicht ausreichen

Wesentlicher Nachteil ist die Abhängigkeit von subjektiven Beeinflussungen
Daher sollte auch hier weitestgehend auf Fakten Bezug genommen werden

Risikobewertung >

Risikoanalyse > Risikoeinschätzung > Einschätzungsmethoden

Quantitative Methoden:



Die Qualität ist sehr stark abhängig von der Korrektheit und Vollständigkeit der zugrunde liegenden Daten sowie der Aussagekraft der angewendeten Modelle



Wenn ausreichend Daten von Sicherheitsvorfällen vorhanden sind beziehe sich die hauptsächlich auf „alte“ Risiken, Für „neue“ Risikoarten sind in der Regel nicht ausreichend seriöse Informationen vorhanden

Wesentlicher Nachteil ist, dass bei fehlender Faktenbasis dennoch eine Illusion von Genauigkeit und Richtigkeit entstehen kann

Die Art und Weise wie Konsequenzen und Wahrscheinlichkeiten dargestellt und verknüpft werden ist abhängig von Risikoart und Zielsetzungen

Überlegungen zu Eintrittswahrscheinlichkeiten

Eine quantitative Bewertung täuscht eine nicht existente Genauigkeit vor!

Behelfsweise werden Klassen eingeführt, wobei die Definition der Intervallgrenzen erforderlich ist

4	sehr häufig
3	häufig
2	mittel
1	selten
0	sehr selten

4	einmal pro Minute
3	einmal pro Stunde
2	einmal pro Tag
1	einmal pro Jahr
0	einmal alle 10 Jahre

Risikobewertung >

Risikoevaluierung

Ziel: Die nun erhobenen Risiken sollen hinsichtlich der Basiskriterien (Kontext etablieren) und den Akzeptanzkriterien bewertet werden

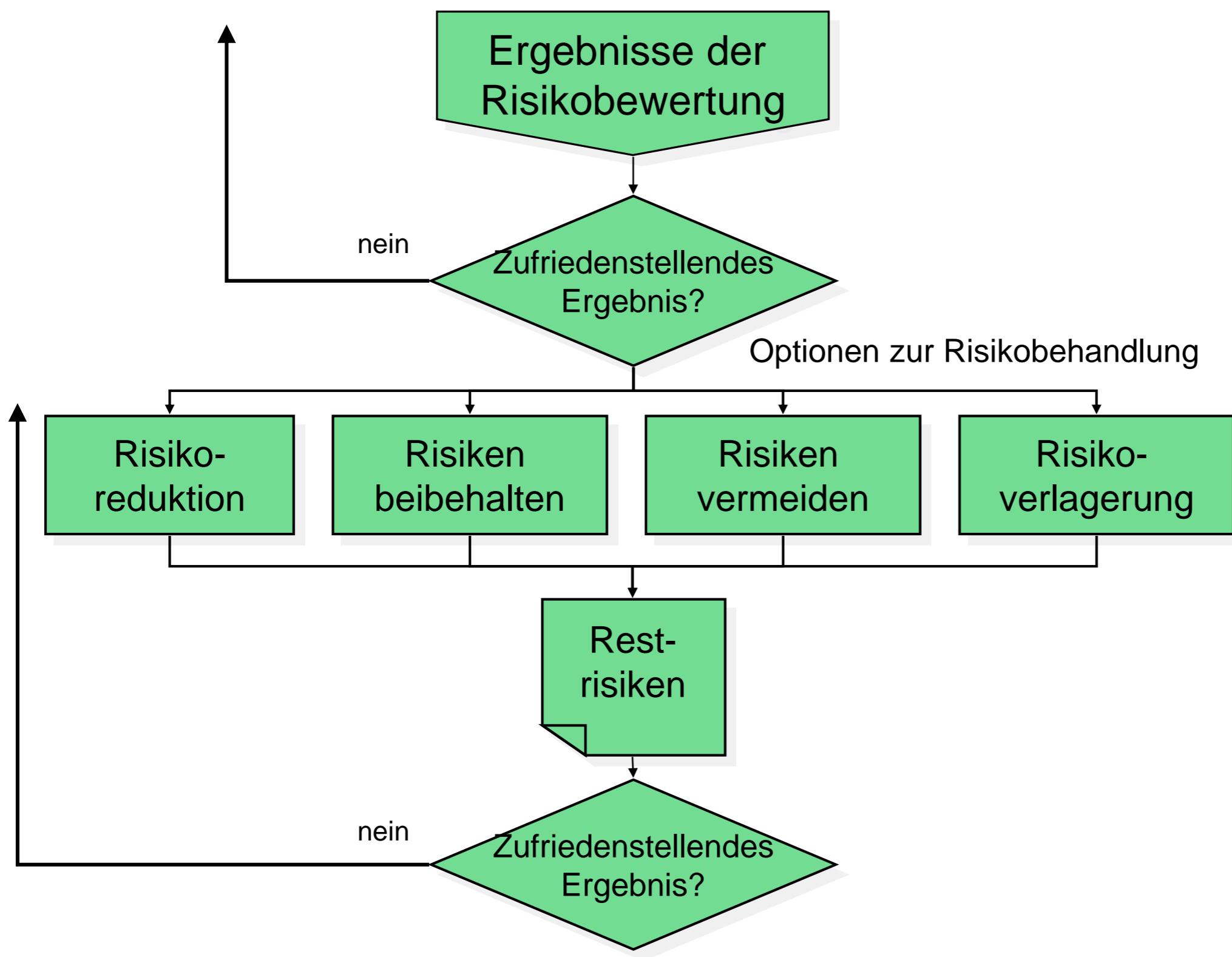
Die Risikoevaluierung bildet somit eine Entscheidungsbasis etwa

 ob für einzelne Risiken überhaupt weitere Aktivitäten zu setzen sind

 für die Priorisierung der Risiken

Weitere Überlegungen sind anzustellen, wie etwa Risikokombinationen oder spezielle Ansprüche aus einzelnen Geschäftsprozessen

Das Ergebnis hier zum Abschluss der Risikobewertung sollte eine Liste mit priorisierten Risiken sein



Risikoakzeptanz

Thema Risikoakzeptanz ist deutlich komplexer als die simple Entscheidung ob ein Risiko über oder unter einem Schwellwert liegt

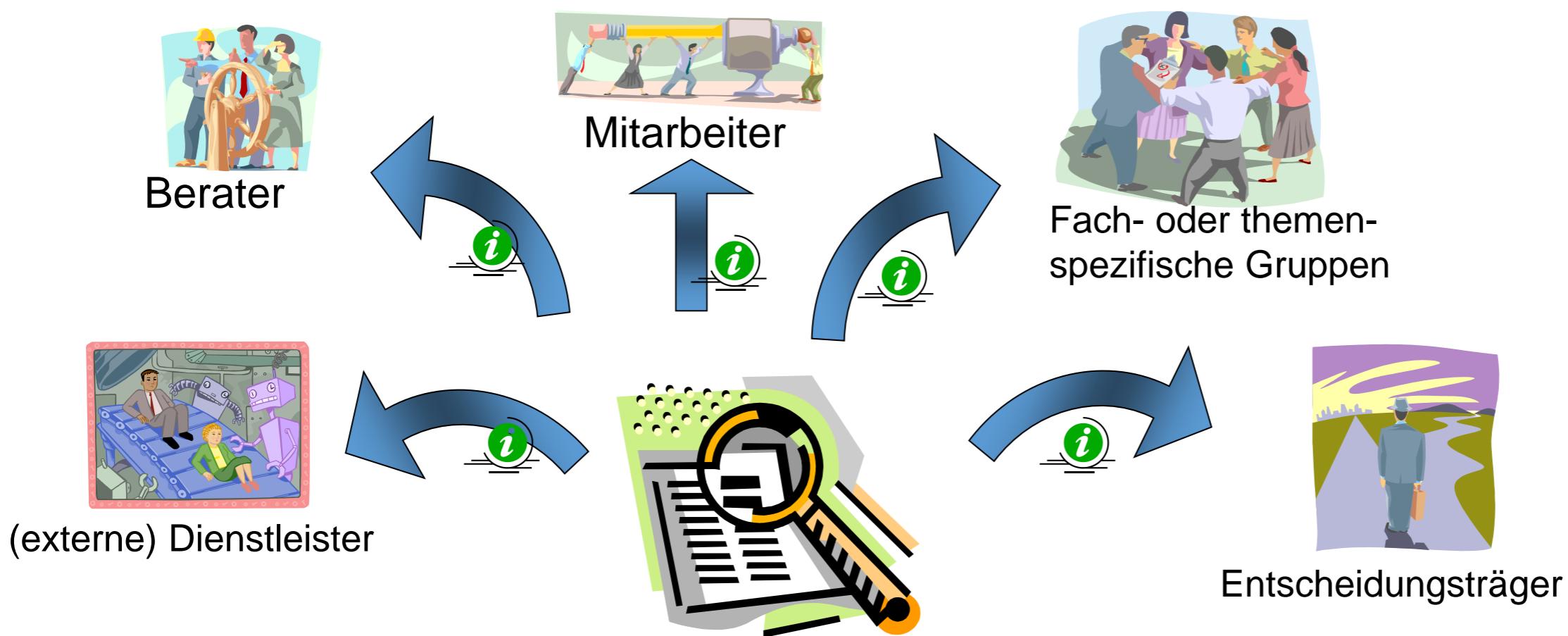
- ☞ Je detaillierter die Akzeptanzkriterien formalisiert sind, desto reproduzierbarer und nachvollziehbarer werden die einzelnen Entscheidungen
- ☞ Werden individuell Entscheidungen getroffen, die nicht den Kriterien entsprechen, wäre eine Überprüfung / Überarbeitung nötig

Akzeptanzkriterien können sich in

- Werten (Währung, Verhältnis, Aufzählungen,...) oder
- Beschreibungen (solange wir mit Kunden A im Kontakt sind, ... manifestieren)

Risikoreporting

Wesentlich ist, zu wissen welche Risiken an welche Rollen und Gremien kommuniziert werden



Ergebnisse von Risikobewertungen sind in der Regel zumindest vertraulich!

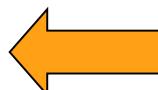
Risikoreporting (2)

Welche Zielsetzungen sind relevant:



Den Risikobehandlungsplan umsetzen

Ausschließen von Unverständnis zwischen Stakeholdern und Entscheidungsträgern



Entscheidungen einfordern / unterstützen

Die Wege und Umstände bei der Incidentbekämpfung reduzieren

Den Entscheidungsträgern ihre Verantwortung vor Augen führen

Sicherheitsbewusstsein zu verbessern



Neue sicherheitsrelevante Informationen erhalten

Feedback zu Risikoanalyse und -management

Risikoüberwachung >

Monitoring der Riskofaktoren



Ziel: Immer aktuelle Einflussgrößen im permanent verändernden Umfeld der Risikothematik

Folgende Faktoren sollten ins Monitoring einbezogen werden:

- Neue Assets, Wertänderungen bei bestehenden Assets
- Bedrohungssituation
- Neue oder veränderte Schwachstellen
- Zuordnungssituation Schwachstelle - Bedrohung
- Änderungen bei den Auswirkungen

Risikoüberwachung >

Prozessoptimierung



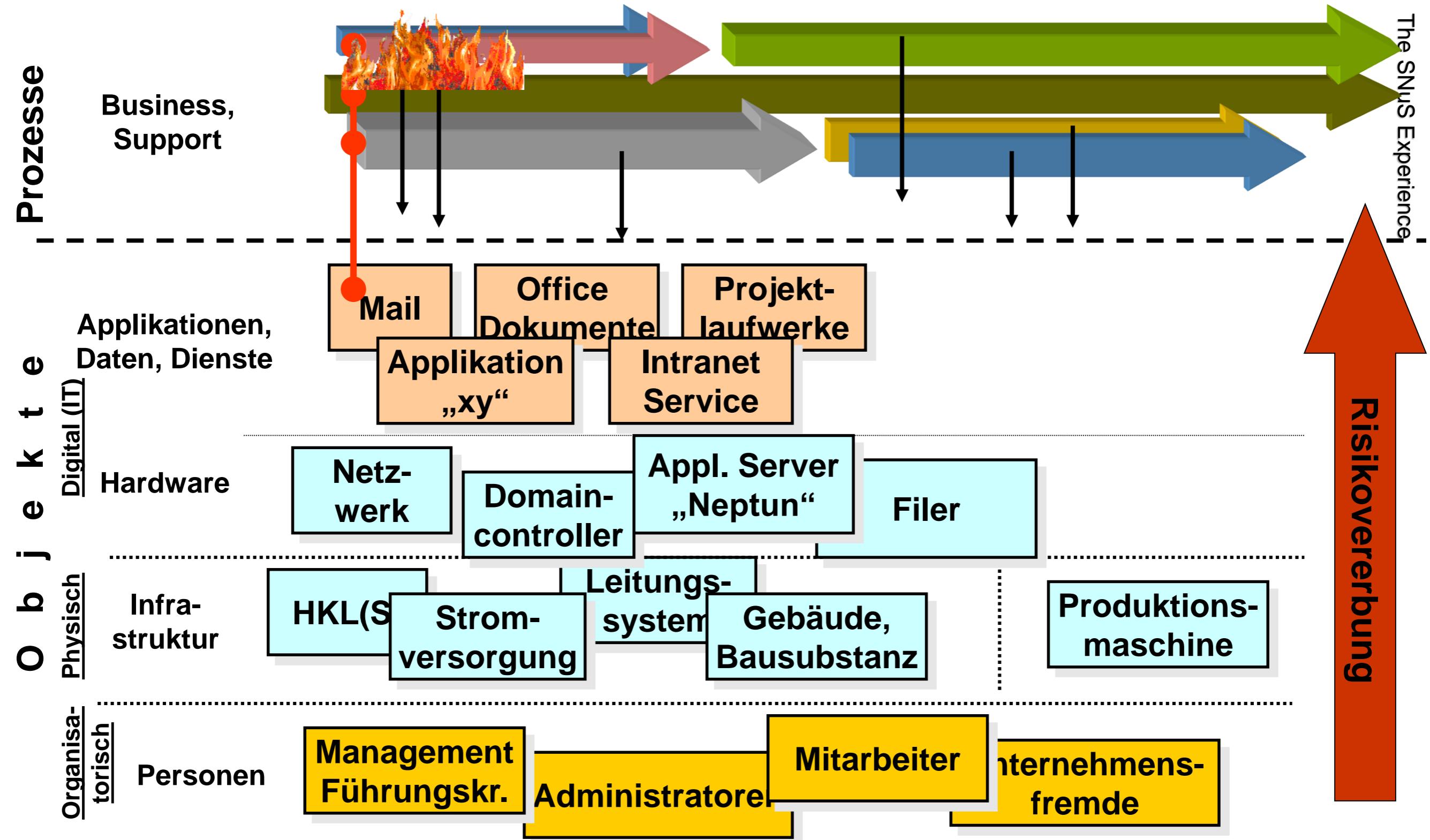
Ziel: Die Ergebnisse des Risikomanagements müssen möglichst exakt und angemessen bleiben.

Daher sind die Prozesse und Verfahren permanent zu überprüfen und gegebenenfalls zu optimieren.

- Rechtlicher Kontext
- Wettbewerb, Mitbewerb
- Modell zur Risikobewertung
- Kategorien und Bewertungsmodelle für Assets
- Kriterien zur Schadensermittlung
- Grundlagen zur Bestimmung der Risikoakzeptanz
- Verfügbarkeit der finanziellen Ressourcen
- Verfügbarkeit von Skills und Know How



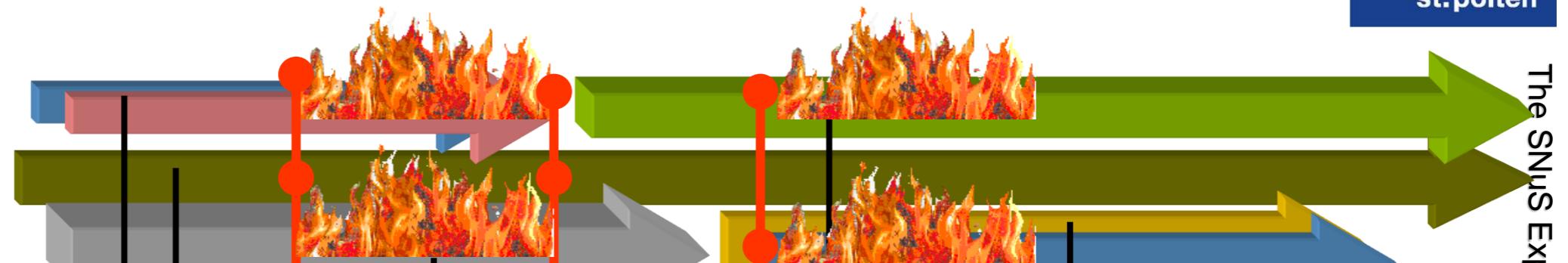
Prozesse - Objekte



Prozesse - Objekte

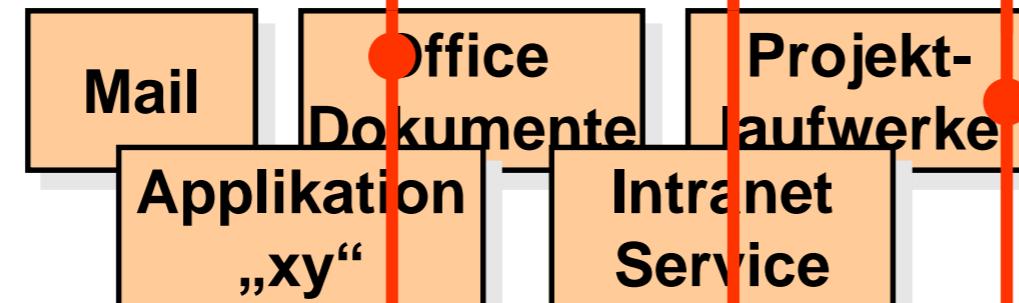
Prozesse

Business,
Support



Objekte

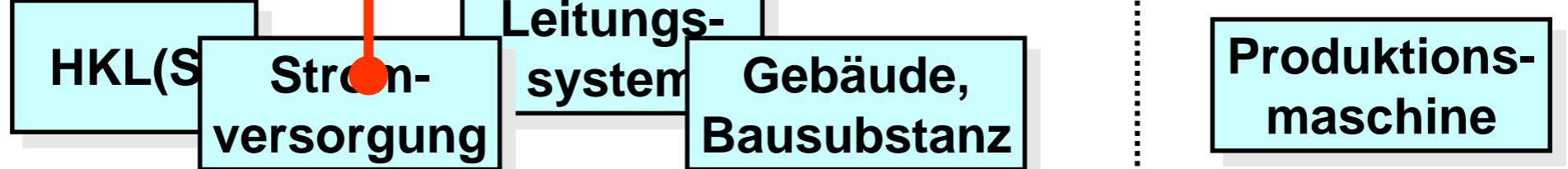
Applikationen,
Daten, Dienste



Hardware



Physisch



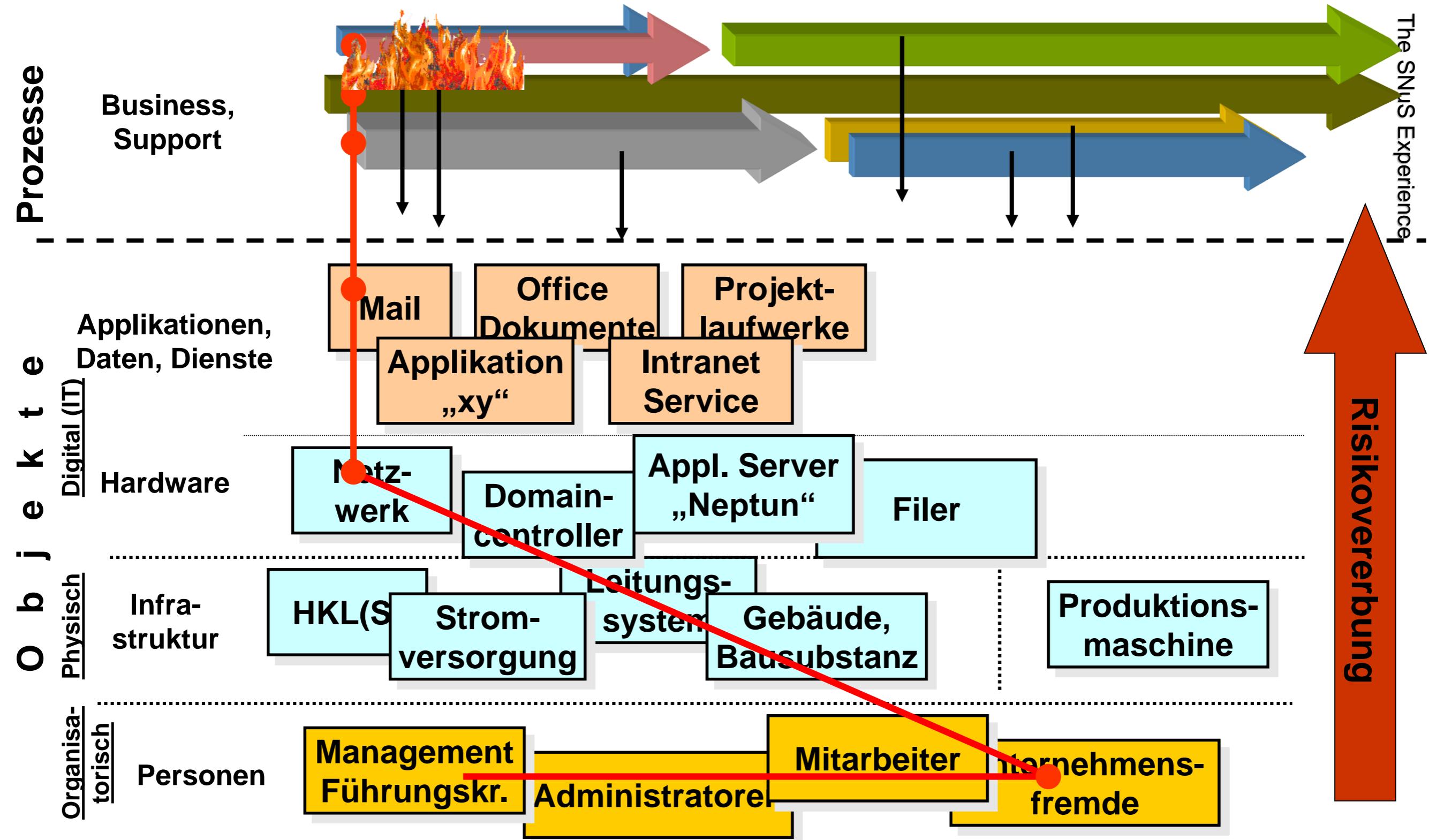
Organisatorisch
Personen



The SNUS Experience

Risikovererbung

Prozesse - Objekte



Prozesse - Objekte

Prozesse

Operativ,
Support

IS - Anforderungen ermitteln

Objekte

Digital (IT)
Applikationen,
Daten, Dienste

IS - Anforderungen zuordnen

Physisch
Hardware

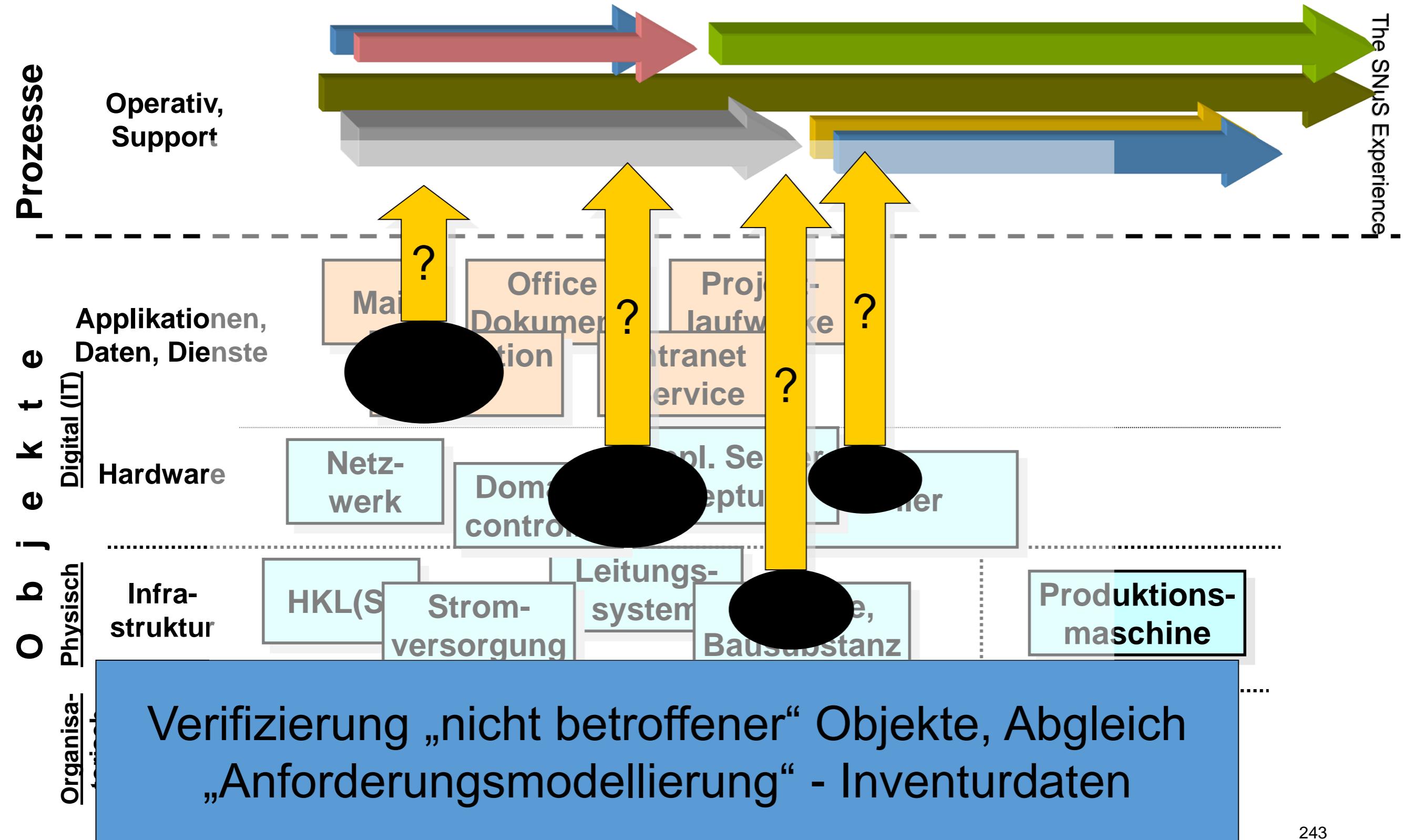
IS - Anforderungen zuordnen

Organisatorisch
Personen

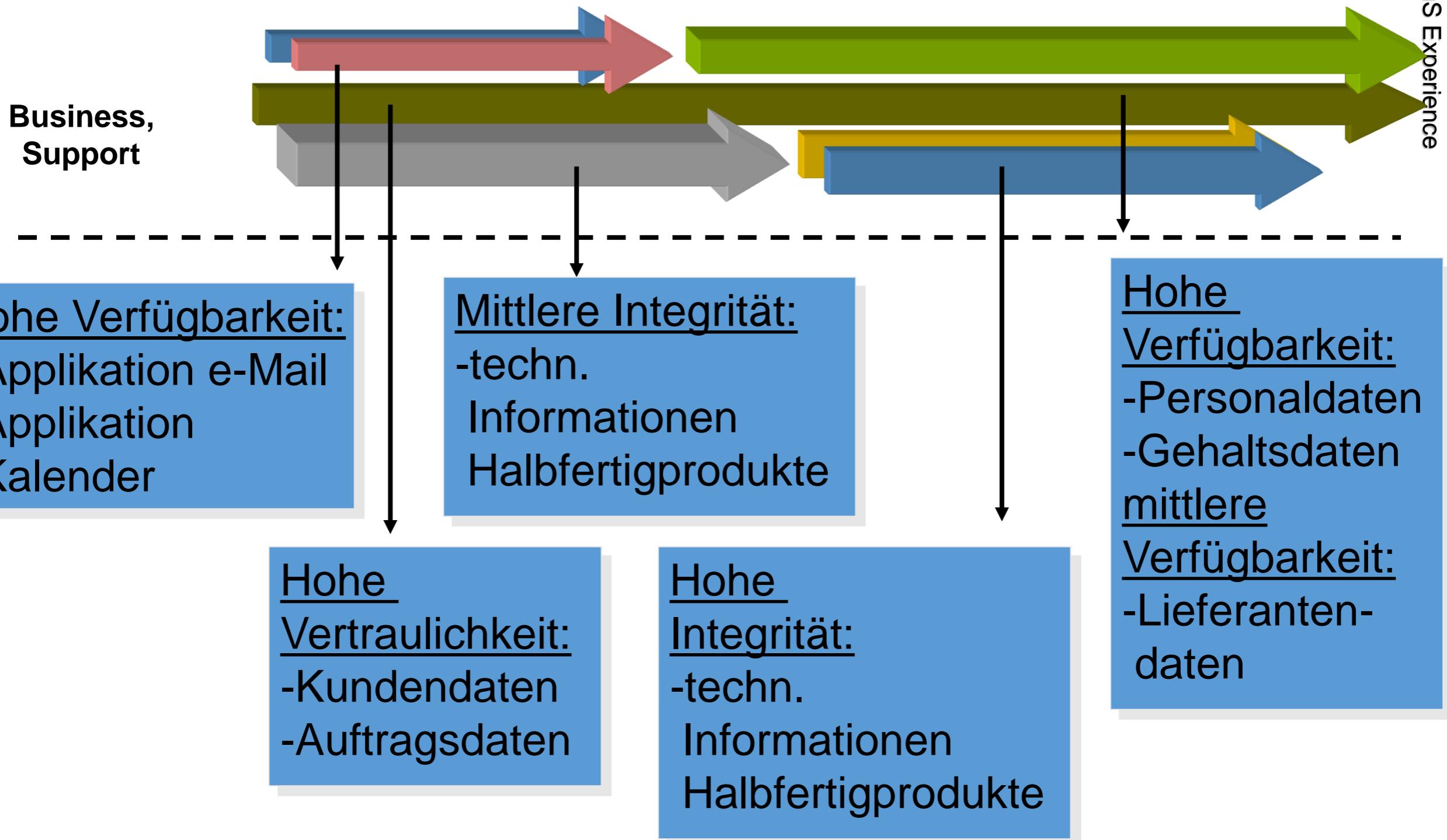
IS - Anforderungen zuordnen

IS - Anforderungen zuordnen

Prozesse - Objekte



Anforderungen ermitteln



Risikobewertung

Betrachtetes Objekt:

Risikobewertung

Betrachtetes Objekt:

Applikationsserver „Neptun“

<u>Bedrohungen</u>	<u>Status</u>	<u>Häufigkeit</u>	<u>Impact</u>	<u>Risiko</u>
<i>Feuer</i>				
<i>Sabotage</i>				
<i>Diebstahl</i>				
<i>Stromausfall</i>				
<i>Manipulation</i>				

Risikobewertung

Klasse	Status ~ akt. Reifegrad	Häufigkeit ~ Eintrittshäufigkeit	Impact ~ Schadenshöhe
1	Keine Maßnahmen	Unwahrscheinlich	Kein Schaden
2	Undokumentiert, individuell	Gering	Geringer Schaden
3	Dokumentiert, aktiv	Mittel	Signifikanter Schaden
4	Wirksamkeitsprüfung	Hoch	Schwerer Schaden
5	Optimiert, gesteuert	Sehr hoch	Unternehmensbedrohend

Risikobewertung

Betrachtetes Objekt:

Applikationsserver „Neptun“

<u>Bedrohungen</u>	<u>Status</u>	<u>Häufigkeit</u>	<u>Impact</u>	<u>Risiko</u>
<i>Feuer</i>	2	3	5	7,5
<i>Sabotage</i>	4	2	4	2
<i>Diebstahl</i>	4	3	3	2
<i>Stromausfall</i>	4	4	3	3
<i>Manipulation</i>	2	3	4	6

Risikobewertung

Betrachtetes Objekt:

Applikationsserver „Neptun“

The SNUS Experience

<u>Bedrohungen</u>	<u>Risiko</u>	<u>Maßnahmen</u>	<u>Kosten</u>
<i>Feuer</i>	7,5	Brandschutz	12.000 €
<i>Manipulation</i>	6	Isolierte Sicherheitszone	5.000 €
<i>Stromausfall</i>	3		
<i>Sabotage</i>	2		
<i>Diebstahl</i>	2		

Festlegung: Risiken unter dem Wert 6 werden nicht betrachtet

Risikobewertung

Betrachtetes Objekt:

Applikationsserver „Neptun“

<u>Bedrohungen</u>	<u>Risiko</u>	<u>Maßnahmen</u>	<u>Kosten</u>	<u>RnM</u>
<i>Feuer</i>	7,5	Brandschutz	12.000 €	3
<i>Manipulation</i>	6	Isolierte Sicherheitszone	5.000 €	3
<i>Stromausfall</i>	3			
<i>Sabotage</i>	2			
<i>Diebstahl</i>	2			

Festlegung: Risiken unter dem Wert 6 werden nicht betrachtet

Risikobewertung

Betrachtetes Objekt:

Applikationsserver „Neptun“

<u>Bedrohungen</u>	<u>Risiko</u>	<u>Maßnahmen</u>	<u>Kosten</u>
<i>Manipulation</i>	6	4-Augen Prinzip	500 €
		Isolierte Sicherheitszone	5.000 €
		Protokollierung	500 €
		Mitarbeiterauswahl	- €
		...	

Risikobewertung

Katalog: Maßnahme - Bedrohung

<u>Maßnahme</u>	<u>Bedrohung</u>	<u>Komponenten</u>	
Isolierte Sicherheitszone	Manipulation	Server „Neptun“ Server „Osiris“,...	
	Brandschaden	...	
	Unbefugter Zutritt		
	...		

In weiteren Schritten wird...

... eine Kosten - Nutzen Analyse durchgeführt
(maximale Wirkung bei minimalen Kosten)

... eine Reihung der Maßnahmen entsprechend
ihrer Priorität erstellt

... ein Maßnahmenpaket zur Restrisikoabdeckung
abgestimmt

... ein Risikoreport erstellt

RM

IT-Grundschutz - Idee

- Typische Abläufe und IT-Komponenten überall ähnlich
- Wichtig:
 - Wiederverwendbarkeit
 - Anpassbarkeit
 - Erweiterbarkeit
- Typische Gefährdungen, Schwachstellen und Risiken
- Typische Geschäftsprozesse und Anwendungen
- Typische IT-Komponenten
- Gerüst für das IT-Sicherheitsmanagement wird gebildet



IT-Grundschutzhandbuch



BSI-Standards + Loseblattsammlung

IT-Grundschutz aktuell

IT-Grundschutzkataloge

IT-Grundschutz-Kataloge

Kapitel 1: Einleitung

Kapitel 2: Schichtenmodell und Modellierung

Kapitel 3: Glossar

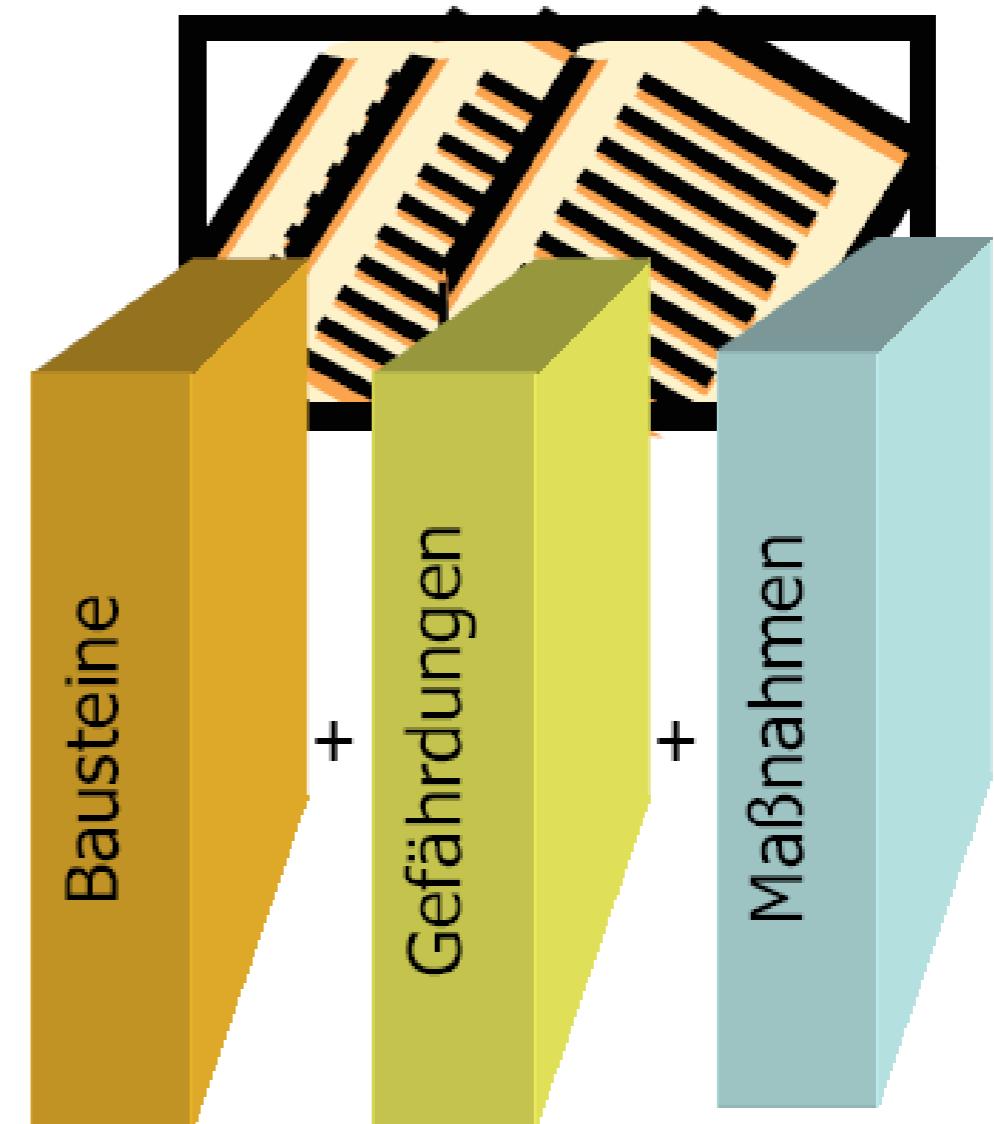
Kapitel 4: Rollen

- **Bausteinkataloge**

- Kapitel B1 "Übergreifende Aspekte"
- Kapitel B2 "Infrastruktur"
- Kapitel B3 "IT-Systeme"
- Kapitel B4 "Netze"
- Kapitel B5 "IT-Anwendungen"

- **Gefährdungskataloge**

- **Maßnahmenkataloge**



Loseblattsammlung

IT-Sicherheitsmanagement

BSI-Standard 100-1:

Managementsysteme für
Informationssicherheit

BSI-Standard 100-2:

Vorgehensweise nach
IT-Grundschatz

BSI-Standard 100-3:

Risikoanalyse auf der Basis von
IT-Grundschatz

BSI-Standard 100-4:

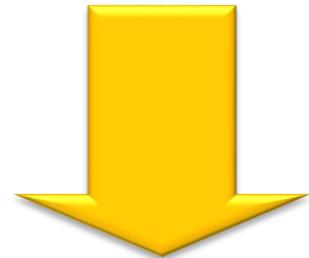
Notfallmanagement



Der Grundsatzansatz

Ziel:

Den Aufwand zur Erstellung eines IT-Risikokonzepts stark begrenzen



Die Auswahl der Maßnahmen erfolgt auf Basis vorgegebener Kataloge

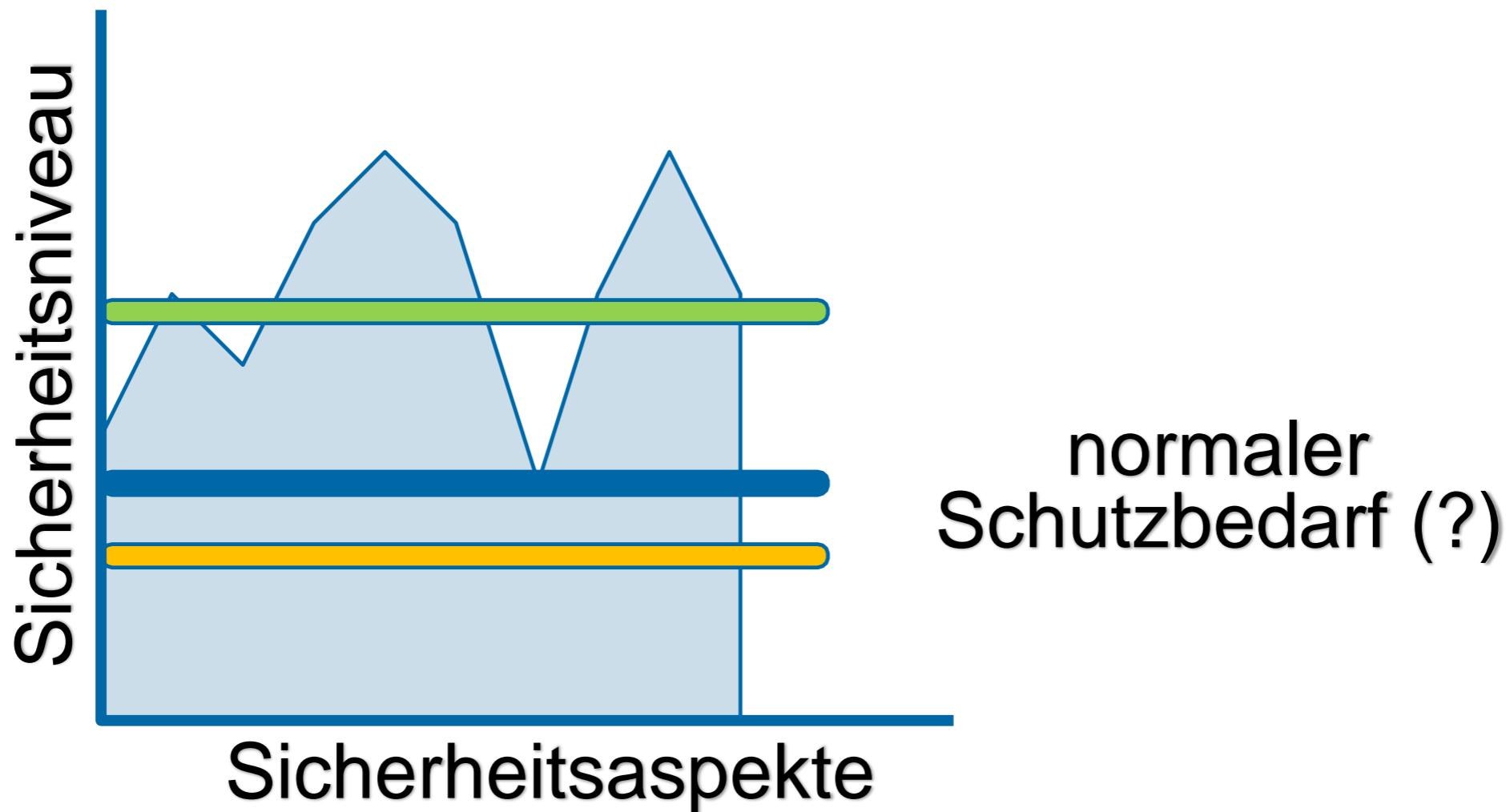
Für Asset und Bedrohungen existieren entsprechende Listen

Grundschutz Vor- / Nachteile

Vorteile:

- Aufwand der Risikoanalyse wird reduziert
- Es wird “schnell” ein relativ hohes Niveau für die “häufigsten” Bedrohungen erzielt
- Grundschutzmaßnahmen sind relativ “kostengünstig” zu realisieren

Erreichbares Sicherheitsniveau



Grundschutz Vor- / Nachteile

Nachteile:

- Der Grundschutzlevel deckt in der Regel die tatsächlichen Bedürfnisse nur ungenau ab
- Detailfragen für einzelne sensible Themen werden nicht berücksichtigt
- Der Katalog suggeriert eine Vollständigkeit, die nicht gegeben ist

Grundschutz - Wie funktioniert's ?

IT - Strukturanalyse

- ⇒ Erfassung der IT, der IT-Anwendungen
- ⇒ Gruppenbildung

Schutzbedarfsfeststellung

IT - Grundschutzanalyse

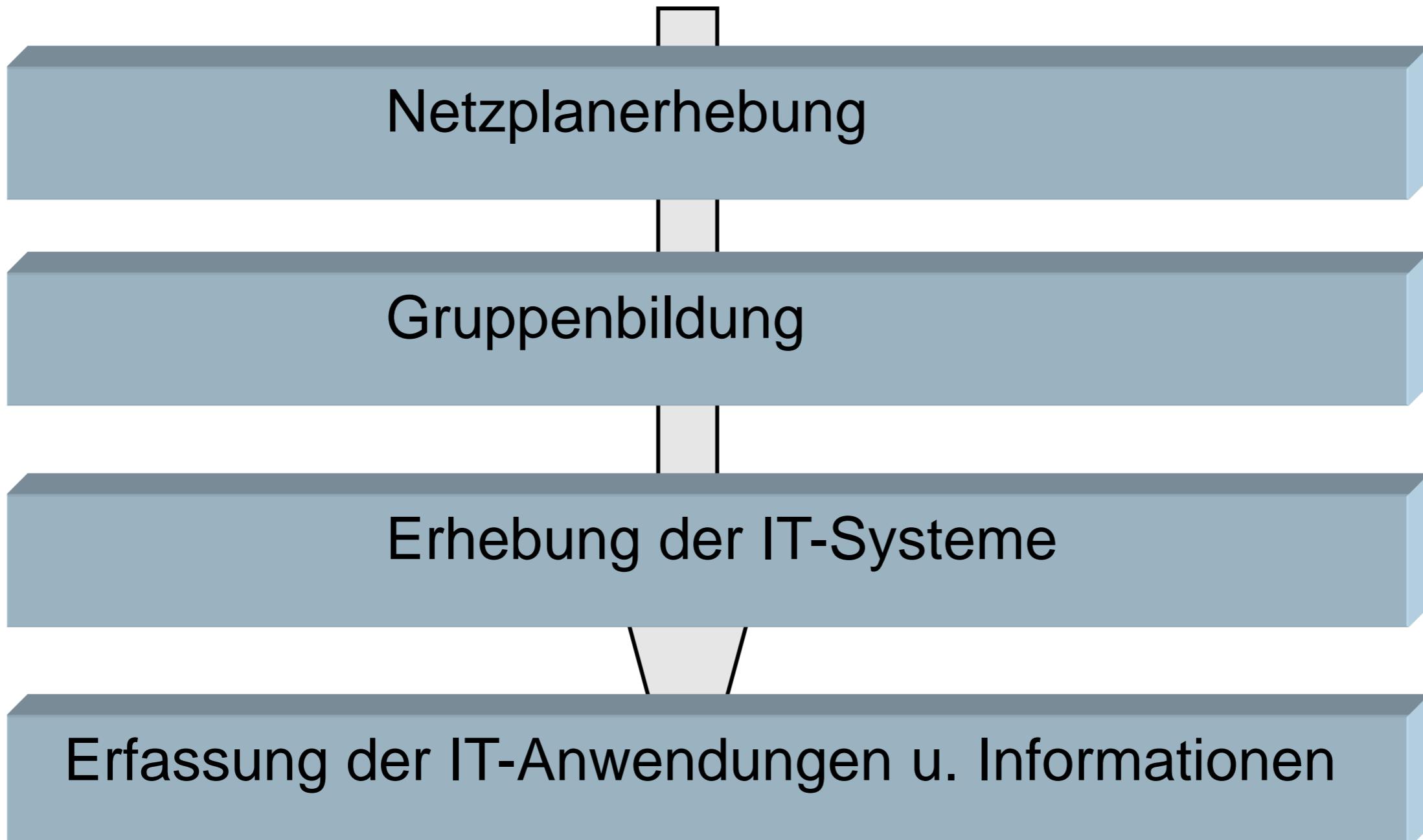
- ⇒ Modellierung nach dem Grundschutzansatz
- ⇒ Basis Sicherheitscheck mit Soll - Ist Vergleich



Ergänzende
Sicherheits-
analyse

Realisierungsplan

IT-Strukturanalyse



Schutzbedarfsfeststellung

Definition der Kategorien (Listen im GSHB)

Betrachtung von Schadenszenarien
(Fragenkatalog im GSHB)

Dokumentation der Ergebnisse

Schutzbedarfsfeststellung der Systeme
zu beachten:
Maximum Prinzip, Abhängigkeiten,
Kumulationseffekt, Verteilungseffekt

Schutzbedarfsfeststellung

Schutzwirkung von Standard-Sicherheitsmaßnahmen nach IT-Grundsatz sind:

für die Schutzbedarfskategorie "normal,"

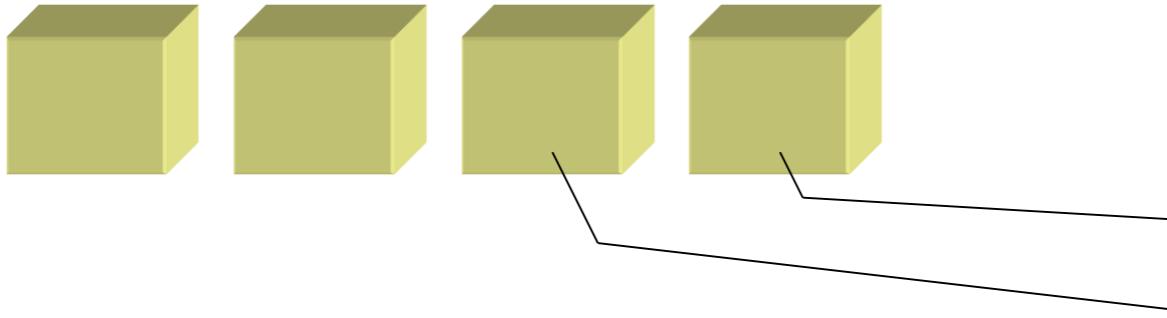
- im Allgemeinen ausreichend und angemessen

für die Schutzbedarfskategorie "hoch" und "sehr hoch"

- Basisschutz und Ausgangsbasis
- zusätzliche Sicherheitsmaßnahmen sollten durch ergänzende Sicherheitsanalyse ermittelt werden (BSI-Standard 100-3)

IT -Grundschutzanalyse

Schicht 1: Übergreifende Aspekte



Bausteine zur Schicht 1

Sicherheitsorganisation
Personal

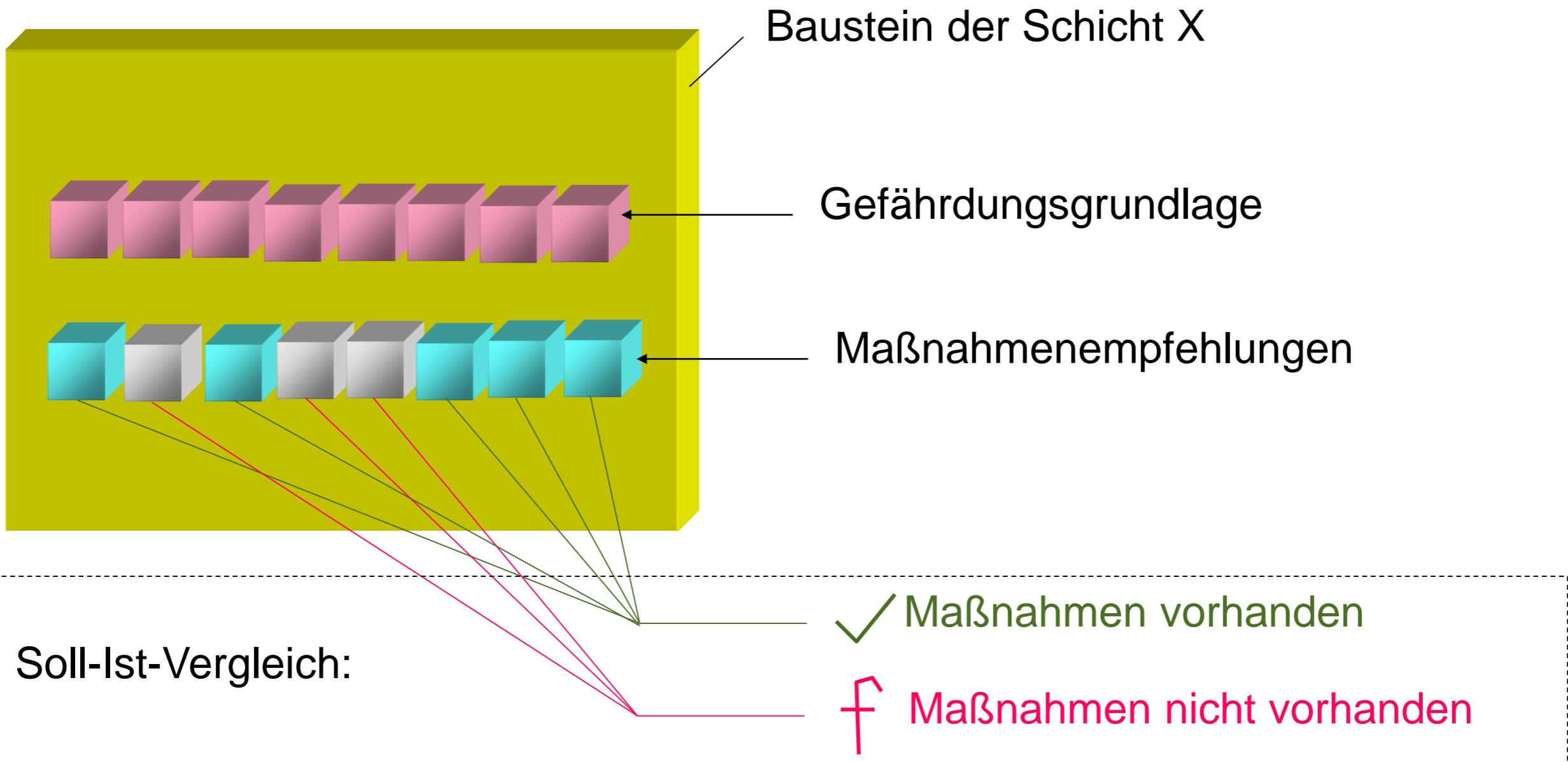
Schicht 2: Infrastruktur

Schicht 3: IT - Systeme

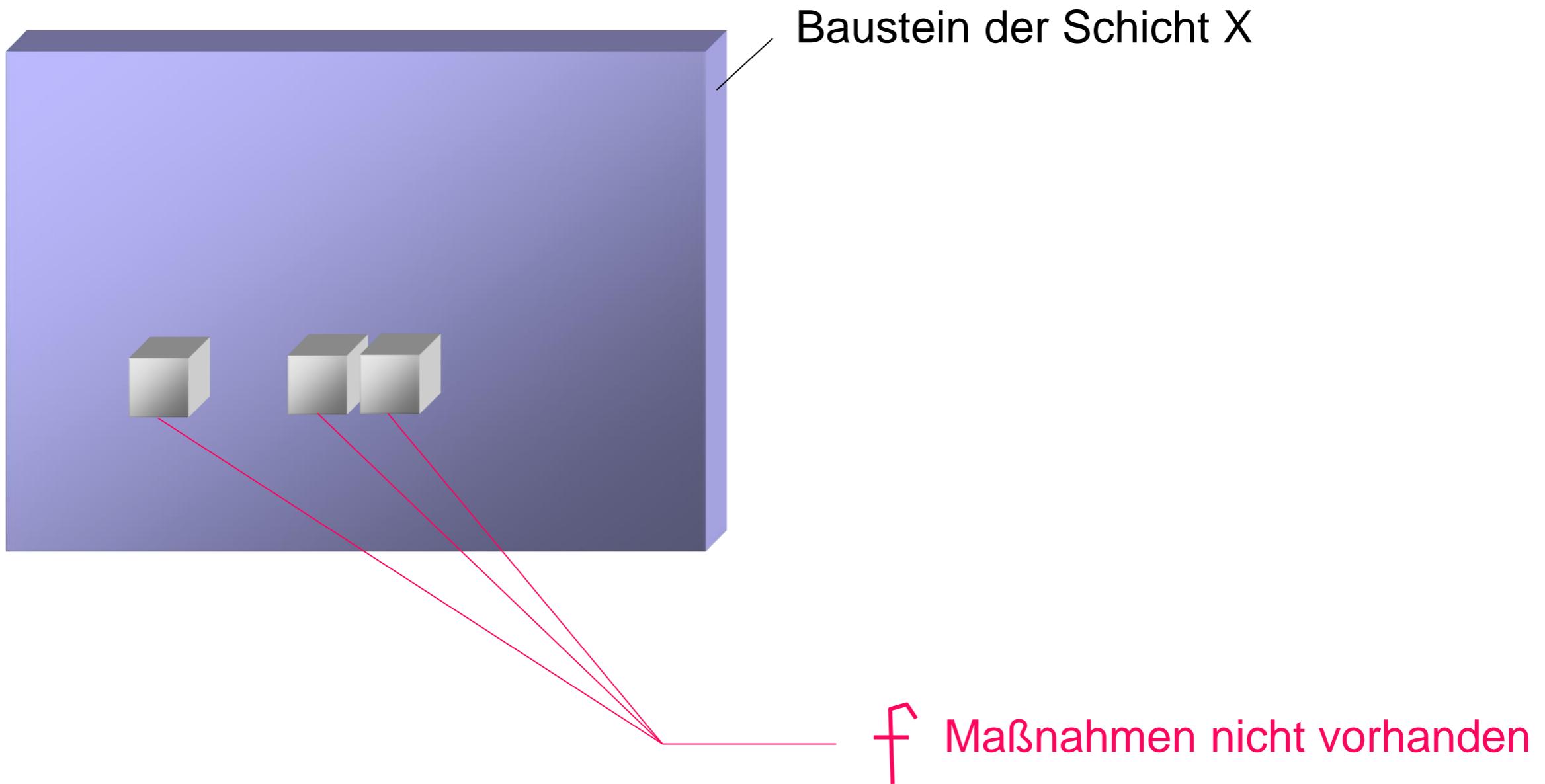
Schicht 4: Netze

Schicht 5: IT - Anwendungen

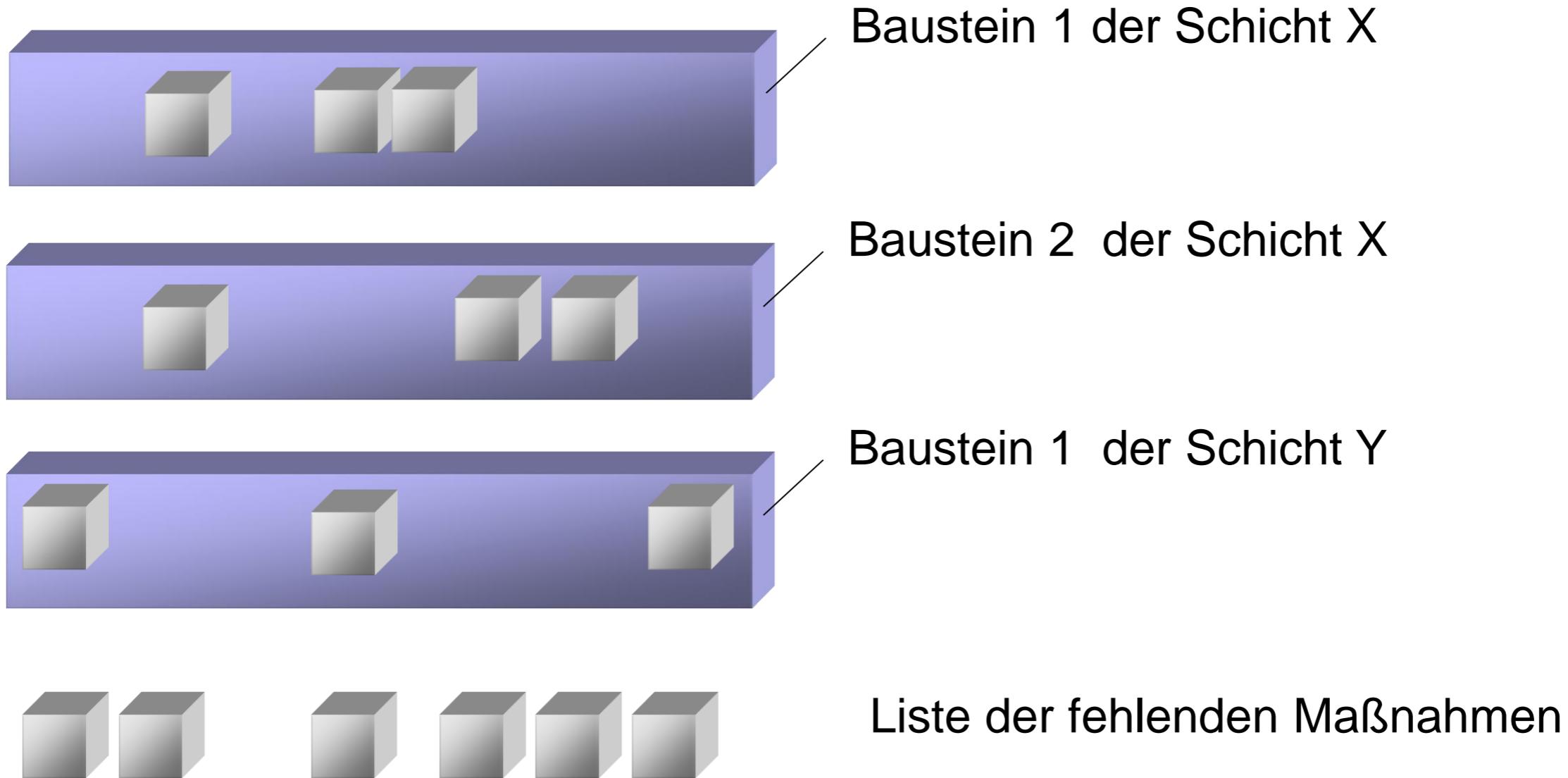
IT-Grundschatzanalyse



IT-Grundschatzanalyse



Grundschatzanalyse



Die Maßnahmen sind im Katalog unabhängig
von den Schichten und Bausteinen sortiert

Grundschatzanalyse

Daraus ergibt sich ein Umsetzungsplan im wesentlichen wie bei der klassischen Risikoanalyse, allerdings mit bereits sehr konkreten Umsetzungsbeschreibungen



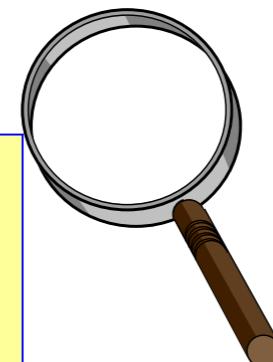
Common Criteria / ISO 15408



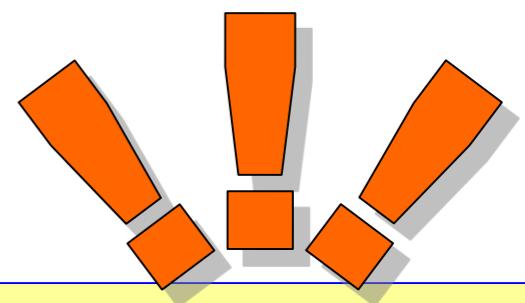
Zielsetzung Sicherheitskriterien?



„Ist dieses IT-Produkt sicher?“
„Ist mein IT-System sicher?“



ToDo: objektive Bewertung der
Qualität von Sicherheitskriterien



Ziel: Wissen über die Sicherheitsaspekte eines Systems
/ Produkts und dadurch Vertrauen in die Qualität

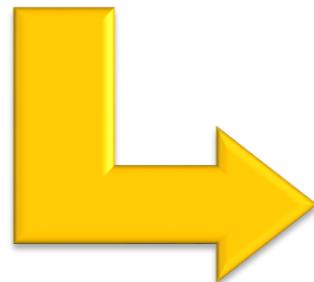
Möglichkeiten der Evaluierung

Vertrauen in die Angaben / Aussagen des Herstellers

Tests / Evaluierungen selbst durchführen

Prüfung durch eine neutrale Instanz

- objektive Bewertung
- allgemeine (internationale) Anerkennung
- gegen vorgegebene Anforderungen („Kriterien“)

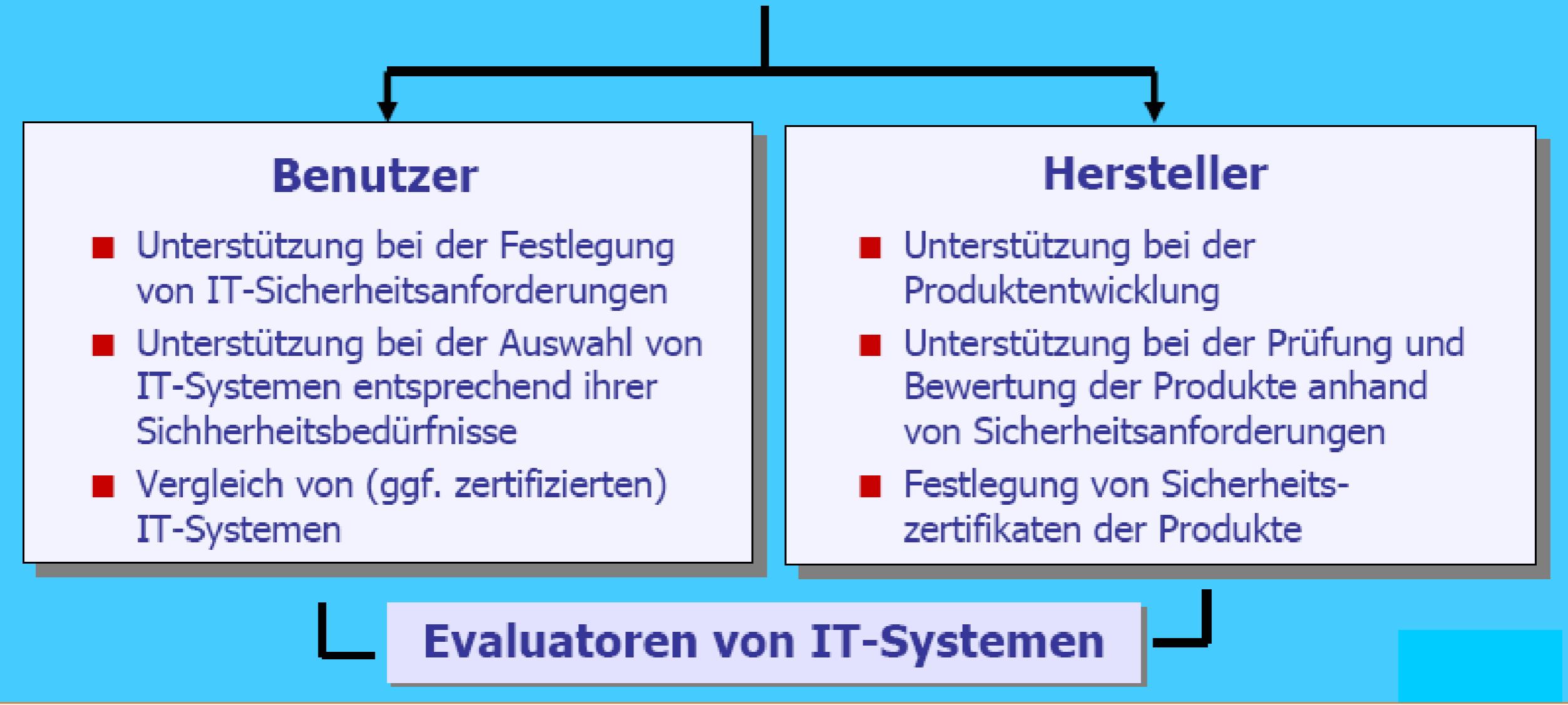


Zertifizierung

Basisforderung:

Hersteller und Benutzer von IT-Systemen benötigen weltweit akzeptierte einheitliche Evaluationskriterien zur Überprüfung und Bewertung der IT-Sicherheit von Produkten, Komponenten bzw. Systemen der IT !

Leitfaden als Prüf- und Bewertungsschema der IT-Sicherheit von IT-Systemen



1. Kriterienwerk TCSEC (Orange Book)

Trusted Computer System Evaluation Criteria

- ⇒ Anfang 1980 am US National Computer Security Center entwickelt
- ⇒ Klassifizierung der Sicherheit von IT-Systemen nach 4 Hierarchiestufen:
D, C, B, A (höchste Stufe)
- ⇒ Nachteile u.a.:
 - einseitige Ausrichtung auf zentrale Betriebssysteme, so dass verteilte Systeme nicht erfasst werden
 - Vernachlässigung von benutzerspezifischen Sicherheitsinteressen
 - Erfüllung einer Sicherheitsfunktionalität kann nicht nach der Wirksamkeit der Schutzmechanismen gegenüber Bedrohungen bewertet werden (Maß an Vertrauenswürdigkeit fehlt)

2. Kriterienwerk ITSEC

Information Technology Security Evaluation Criteria

- ⇒ Funktionsklassen mit Sicherheitsanforderungen für spezifische Anwendungsklassen
- ⇒ Klassifizierung der Sicherheit nach 7 Evaluationsstufen von E0 (unzureichend) bis E6 (ausgezeichnet)
- ⇒ Es können Hardwarekomponenten und Software für unterschiedliche Anwendungsbereiche bewertet werden
- ⇒ Nachteile u.a.:
 - Nach wie vor Konzentration auf zentrale Systeme
 - Zertifikate sind nicht weltweit anerkannt (u.a. nicht in USA)

3. Kriterienwerk Common Criteria

Common Criteria for Information Technology Security Evaluation

- ⇒ Standard ISO/IEC 15408 (kurz: CC) besteht aus den 3 Teilen
- ⇒ Entwickelt in Zusammenarbeit mit Kanada, Frankreich, Deutschland (BSI) , Holland, GB und USA
- ⇒ Seit 1996 vom gemeinsamen Technischen Komitee JTC 1 der ISO und IEC als internationaler Standard erarbeitet.
- ⇒ CC Version 3.1 ist seit 2006 veröffentlicht und wird in Deutschland vom BSI zur Evaluierung verwendet, noch nicht mandatory (dzt. Release 4 aktuell)
- ⇒ Stellt eine einheitliche Basis dar, mit der Sicherheitsanforderungen an den Untersuchungsgegenstand spezifiziert werden können
- ⇒ Definiert ein Prüfverfahren, mit dem Sicherheitseigenschaften von Produkten und Systemen der IT auf strukturierte Weise untersucht werden können; je höher die Vertrauenswürdigkeitsstufe desto tiefergehender ist die Prüfmethode

Begriffe

- Target of Evaluation (TOE) / Evaluationsgegenstand (EVG):
 - Objekt, an das Sicherheitsanforderungen gestellt werden, z.B.: Betriebssystem
- TOE Security Policy (TSP) / Sicherheitsvorgaben:
 - Reihe von Regeln, die steuern wie Gegenstände des TOE verwaltet u. geschützt werden
- TOE Security Functions (TSF):
 - HW, SW, Firmware des TOE worauf die konkrete Durchsetzung der TSP basiert

Common Criteria / ISO 15408

„Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“

➤ Teil 1: Einführung und allgemeines Model (introduction and general model)

Hierin werden die Grundlagen der IT-Sicherheitsevaluation und der allgemeine Geltungsbereich der CC erläutert. In den Anhängen werden Schutzprofile (Protection Profile) und Sicherheitsvorgaben (Security Target) für den zu prüfenden Evaluationsgegenstand (EVG) beschrieben.

Umfang: CC 3.1 93 Seiten,
 ISO 15408-1 52 Seiten

Common Criteria / ISO 15408

➤ Teil 2: Funktionale Sicherheitsanforderungen (functional requirements)

Dieser Teil enthält einen umfangreichen Katalog von Funktionalitätsanforderungen. Er stellt ein empfohlenes Angebot für die Beschreibung der Funktionalität eines Produktes bzw. Systems dar, von dem jedoch in begründeten Fällen abgewichen werden kann. Im Anhang finden sich Hintergrundinformationen. Zusätzlich werden Zusammenhänge zwischen Bedrohungen, Sicherheitszielen und funktionalen Anforderungen aufgezeigt.

Umfang:	CC 3.1	321 Seiten
	ISO 15408-2	248 Seiten

Common Criteria / ISO 15408

- Teil 3: Anforderungen an die Vertrauenswürdigkeit
(assurance requirements)

Hier sind die Anforderungen an die Vertrauenswürdigkeit aufgelistet.

Wichtig ist, dass ein Evaluationsergebnis immer auf einer Vertrauenswürdigkeitsstufe (EAL) basieren sollte, eventuell ergänzt durch weitere Anforderungen. Die CC geben sieben hierarchische EAL-Stufen vor (siehe unten).

Umfang:	CC 3.1	233 Seiten
	ISO 15408-3	162 Seiten

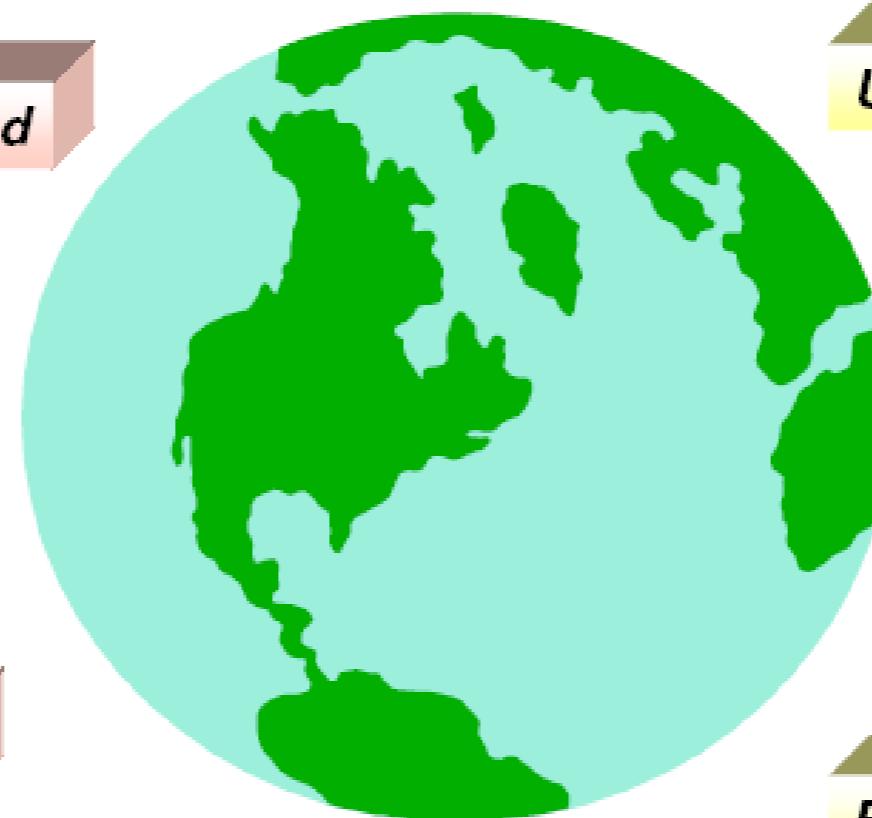
Common Criteria - Anerkennung

- Die Anerkennung der Zertifikate ist im so genannten Common Criteria Recognition Arrangement (CCRA) geregelt. Neben den 8 ausstellenden Ländern akzeptieren 12 weitere Länder offiziell die ausgestellten Zertifikate bis zu einer festgelegten Vertraulichkeitsstufe.
- Darüber hinaus akzeptieren eine große Menge weiterer Länder inoffiziell ebenfalls diese Zertifikate.
- Die Anzahl der ausstellenden und akzeptierenden Länder verändert sich jährlich.

CC Anerkennung

Anerkennende und zertifizierende Nationen

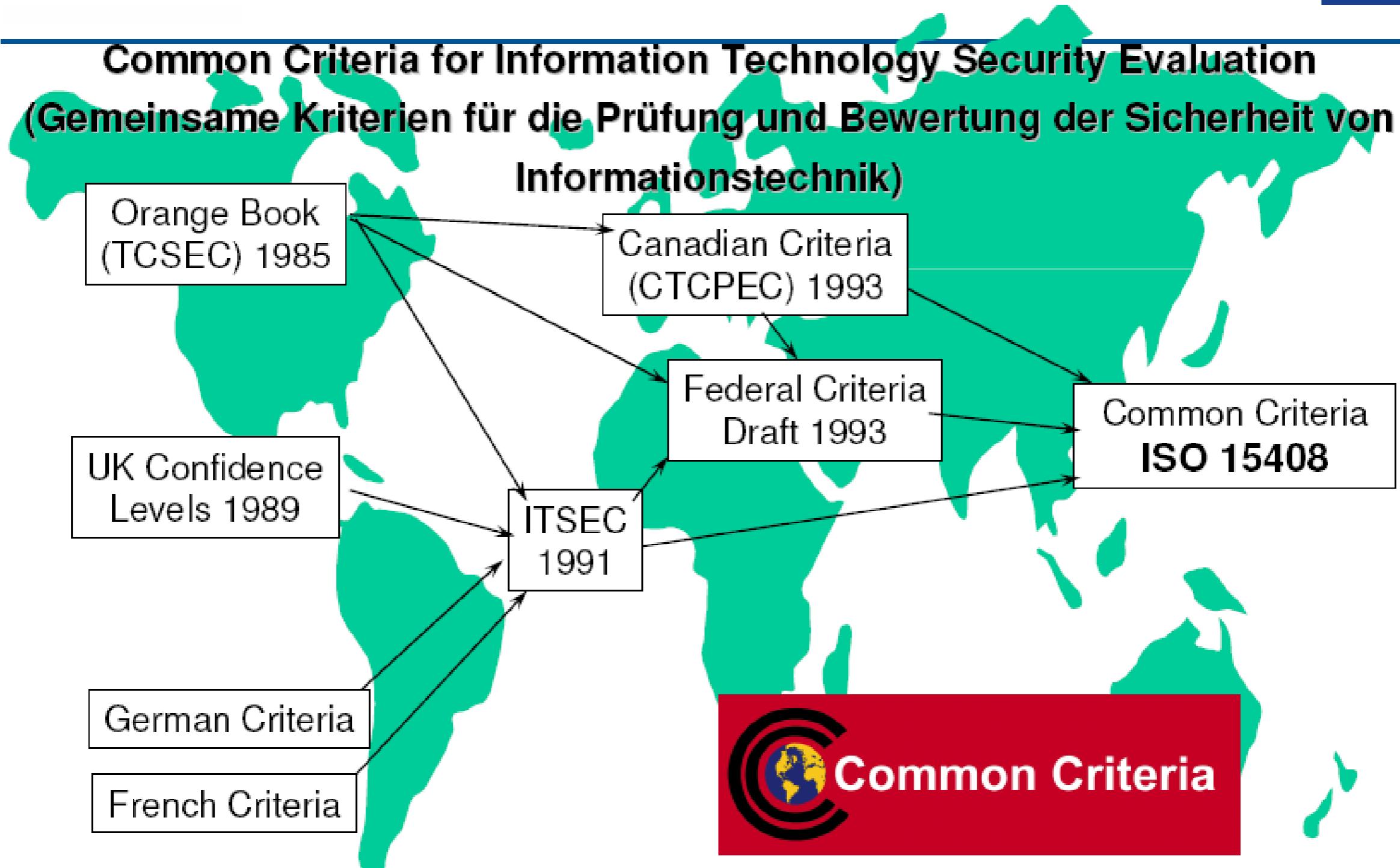
Australien und Neuseeland
USA Kanada
Deutschland
Großbritannien
Frankreich Spanien
Niederlande Japan
Südkorea Norwegen



Anerkennende Nationen

Ungarn Griechenland
Singapur Türkei
Israel Italien
Indien Schweden
Finnland Österreich
Tschechien

CC Entwicklung / Geschichte



CC / ISO 15408 Security Framework

Sicherheitsumfeld (security environment)

Gesetzl., vertragl. Anforderungen, interne Policies, definieren den Kontext in dem ein EVG eingesetzt wird.

Sicherheitsziele (security objectives)

Sollen den Anforderungen des Sec. Environment Rechnung tragen

EVG Sicherheitsanforderungen (TOE security requirements)

Die EVG individuelle Konkretisierung der Sicherheitsziele

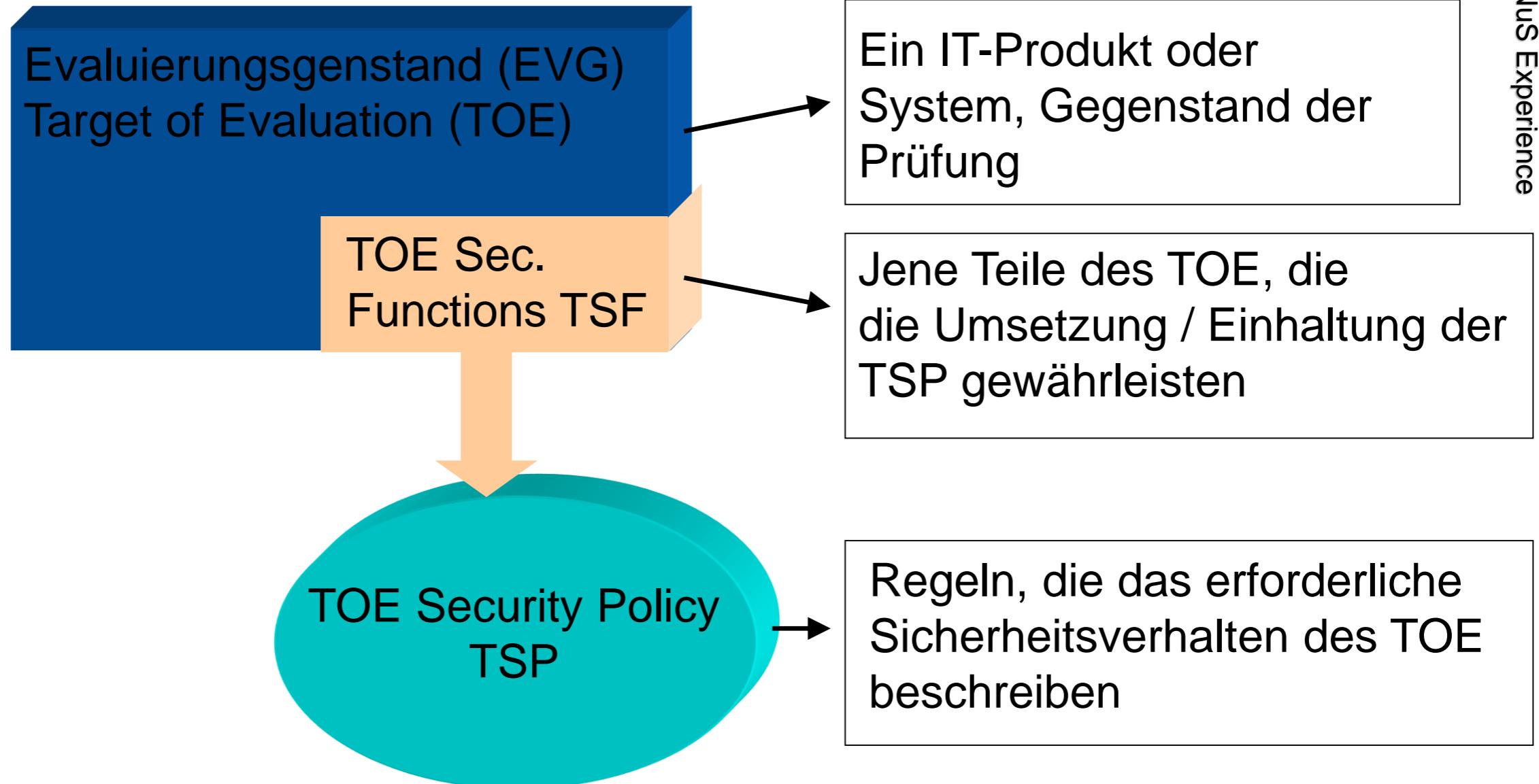
EVG Sicherheitsspezifikationen (TOE sec. specifications)

Definieren konkrete Realisierungsvorgaben für ein EVG

EVG Erstellung (TOE implementation)

Realisierung entsprechend der Vorgaben

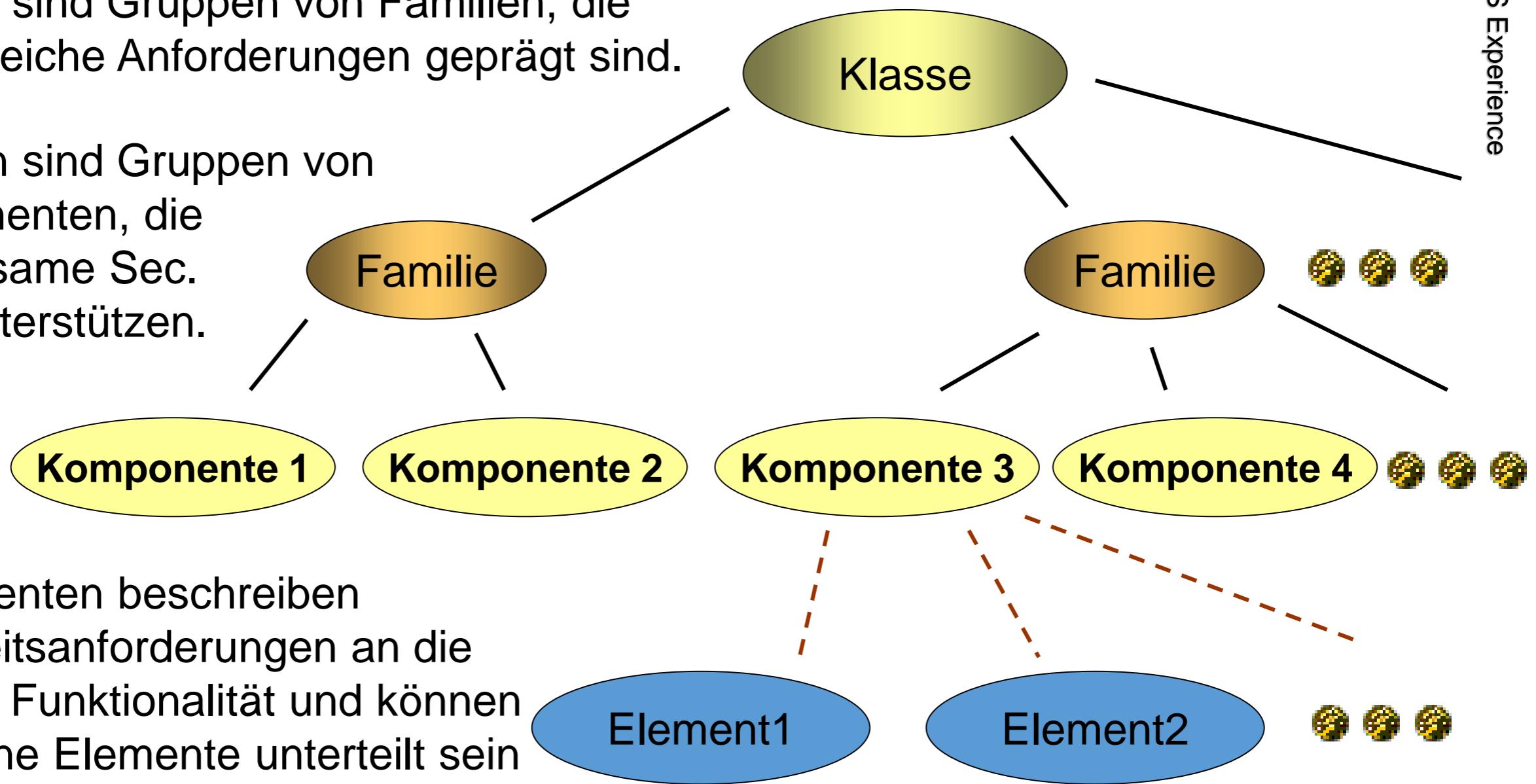
CC / ISO 15408 TOE-TSF-TSP



Ordnungsschema der Sicherheitsanforderungen

Klassen sind Gruppen von Familien, die durch gleiche Anforderungen geprägt sind.

Familien sind Gruppen von Komponenten, die gemeinsame Sec. Ziele unterstützen.



Komponenten beschreiben Sicherheitsanforderungen an die konkrete Funktionalität und können in einzelne Elemente unterteilt sein

Elemente sind unteilbare Sicherheitsanforderungen (erfüllt / nicht erfüllt)

Die Syntax (Component Naming Convention)

Klassenbezeichnung: 3 Char. Z.B.: FMT

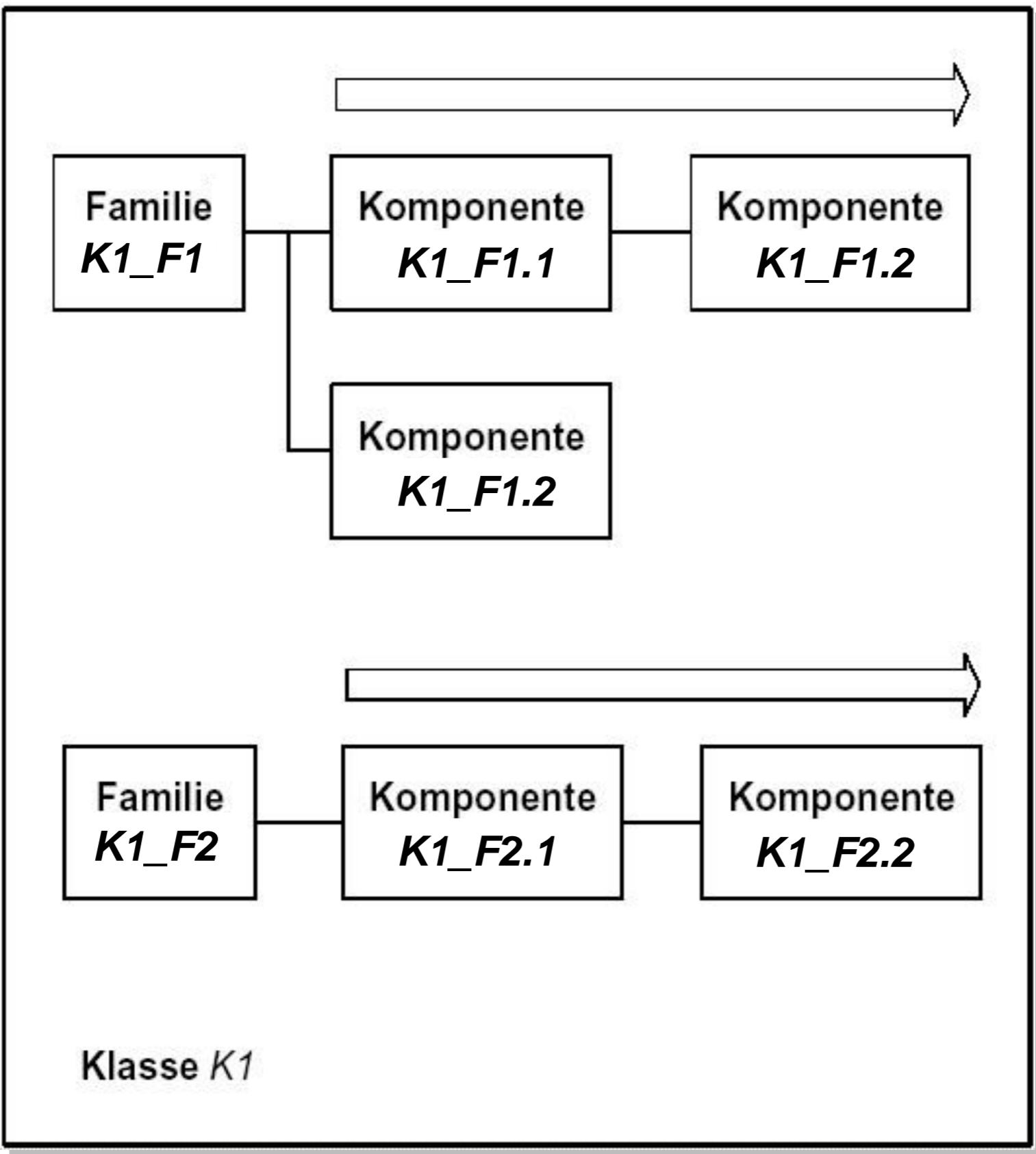
Familienbezeichnung: _3 Char. Z.B.: FMT_SMR

Komponentenbezeichnung: .Zahl Z.B.: FMT_SMR.2

Elementbezeichnung: .Zahl Z.B.: FMT_SMR.2.3

Es gibt 11 Funktionalitätsklassen und 8 Vertrauenswürdigkeitsklassen
(assurance classes)

Schemadarstellung Klasse – Familien - Komponenten



Klassenbezeichnungen Teil 2

(in Klammern die Anzahl der Familien)

<i>Funktionale Klasse</i>	Sicherheitsanforderung
FAU (6)	Sicherheitsprotokollierung
FCO (2)	Kommunikation
FCS (2)	Kryptographische Unterstützung
FDP (13)	Schutz der Benutzerdaten
FIA (6)	Identifikation und Authentisierung
FMT (6)	Sicherheitsmanagement
FPR (4)	Privatsphäre
FPT (16)	Schutz der TSF (TOE Security Function)
FRU (3)	Betriebsmittelnutzung
FTA (6)	TOE-Zugriff
FTP (2)	Vertrauenswürdiger Pfad/Kanal

Beispiel aus ISO 15408-2

Security management roles (FMT_SMR)

Family Behaviour

This family is intended to control the assignment of different roles to users. The capabilities of these roles with respect to security management are described in the other families in this class.

Component levelling



FMT_SMR.1 Security roles specifies the roles with respect to security that the TSF recognises.

FMT_SMR.2 Restrictions on security roles specifies that in addition to the specification of the roles, there are rules that control the relationship between the roles.

FMT_SMR.3 Assuming roles, requires that an explicit request is given to the TSF to assume a role.

Klassenbezeichnungen Teil 3

(in Klammern die Anzahl der Familien)

<i>Vertrauenswürdigkeitsklasse</i>	Sicherheitsanforderung
ACM (3)	Konfigurationsmanagement
ADO (2)	Auslieferung und Betrieb
ADV (7)	Entwicklung
AGD (2)	Handbücher
ALC (4)	Lebenszyklus-Unterstützung
ATE (4)	Testen
AVA (4)	Schwachstellenbewertung
AMA (4)	Erhaltung der Vertrauenswürdigkeit

Beispiel aus ISO 15408-3

Class ACM:Configuration management

Configuration management (CM) helps to ensure that the integrity of the TOE is preserved, by requiring discipline and control in the processes of refinement and modification of the TOE and other related information. CM prevents unauthorised modifications, additions, or deletions to the TOE, thus providing assurance that the TOE and documentation used for evaluation are the ones prepared for distribution.

CM automation (ACM_AUT)

Configuration management automation establishes the level of automation used to control the configuration items.

CM capabilities (ACM_CAP)

Configuration management capabilities define the characteristics of the configuration management system.

CM scope (ACM_SCP)

Configuration management scope indicates the TOE items that need to be controlled by the configuration management system.

Protection Profiles (PP) / Schutzprofile (SP)

Implementierungsunabhängige Menge von Sicherheitsanforderungen für eine Kategorie von Produkten oder Systemen, die bestimmte Benutzeranforderungen erfüllen (müssen).

Firewalls, Datenbaken, IDS, Smart Card Devices, VPN Devices,...

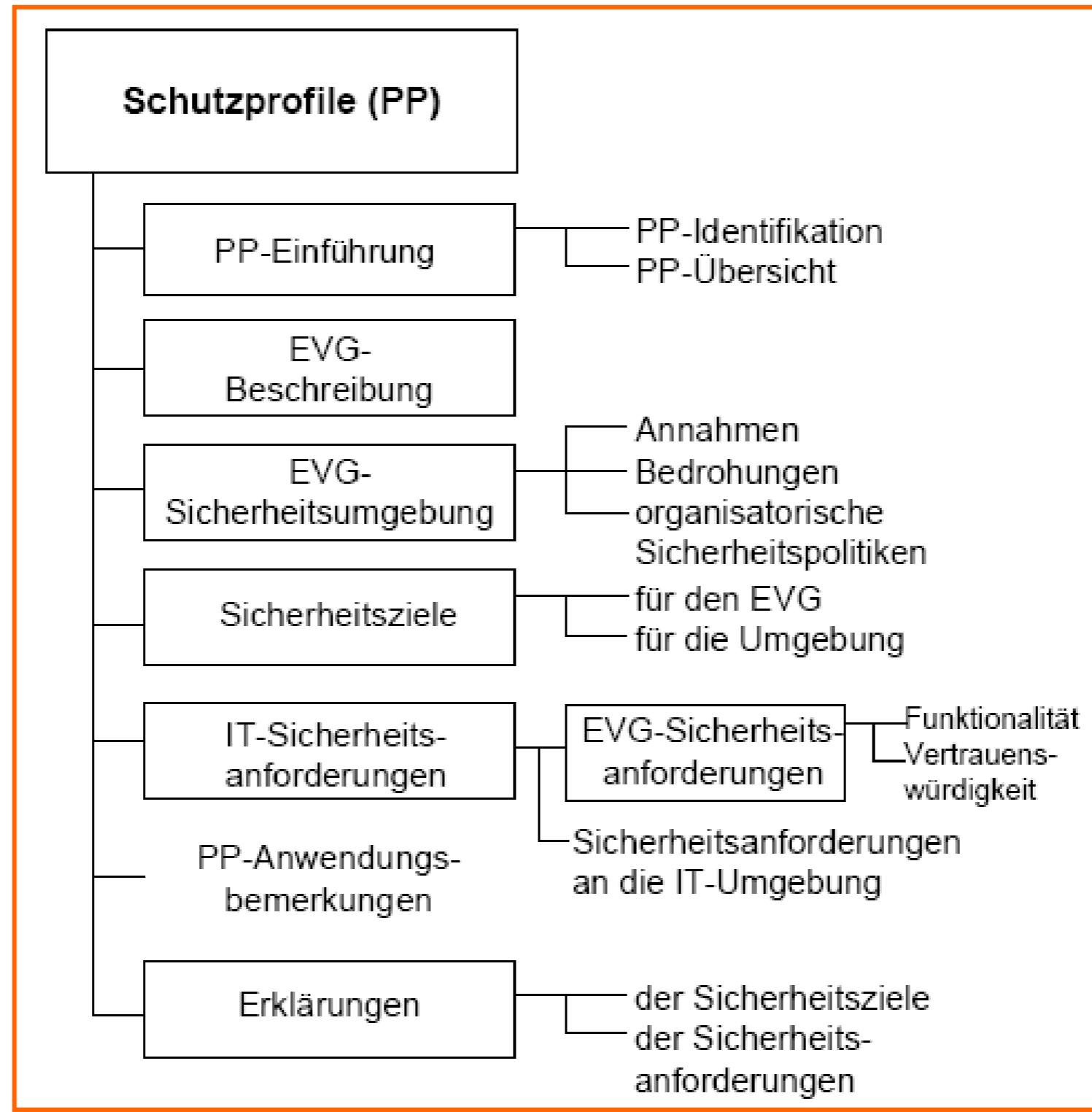
Liste der PPs unter: <http://www.commoncriteriaportal.org/pps/>

Protection Profiles (PP) / Schutzprofile (SP)

Mit Schutzprofilen ist Anwendergruppen und Herstellern die Möglichkeit gegeben, produktklassentypische und dienstleistungsspezifische Sicherheitsanforderungen festzulegen.

Die Berücksichtigung von Schutzprofilen bei der Produktentwicklung erleichtert deren Evaluierung und führt zu Produkten, die in besonderem Maße den anwenderspezifischen Anforderungen entsprechen. Auch Schutzprofile können evaluiert und zertifiziert werden.

CC Schutzprofile - Struktur



Common Criteria / ISO 15408 Prüfarten

Die CC / ISO 15408 sehen drei mögliche Arten der Prüfung und Bewertung vor:

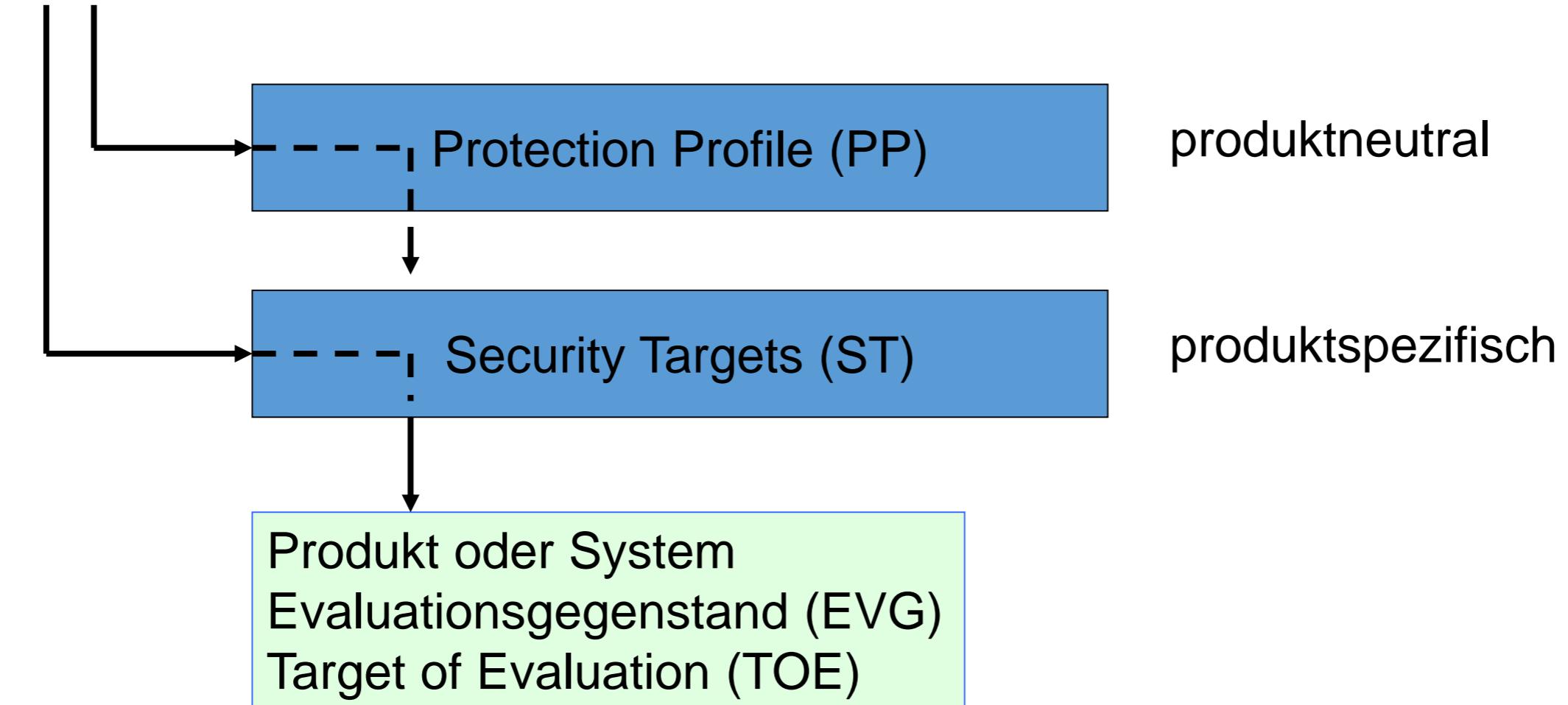
Prüfung und Bewertung eines Protection Profiles (PP) anhand der Evaluationskriterien für Schutzprofile

Prüfung und Bewertung von Sicherheitsvorgaben (Security Target, ST) für den EVG anhand der Evaluationskriterien für Sicherheitsvorgaben

Prüfung und Bewertung eines EVG anhand der Evaluationskriterien basierend auf einem bereits evaluierten ST oder PP

Common Criteria / ISO 15408 Prüfarten

Evaluierung nur gegen existente, vor-
gegebene Sicherheitsanforderung möglich



CC EAL 1 (evaluation assurance level)

funktionell getestet;

Grundstufe an unabhängig geprüfter Sicherheit

- **Liefert eine Grundstufe an Vertrauenswürdigkeit durch**

- Testen einer funktionalen Spezifikation und einer Schnittstellenspezifikation
- Überprüfung der Handbücher
- Unabhängiges Testen der TOE-Sicherheitsfunktionen

- **EAL1-Evaluation ist ohne Hilfestellung durch den Entwickler des TOE möglich**

- **Ziel der EAL1-Evaluation:**

TOE funktioniert wie in der Dokumentation beschrieben und bietet Schutz gegenüber identifizierten Bedrohungen

CC EAL 2

strukturell getestet, niedrige bis mittlere Stufe an unabhängig geprüfter Sicherheit

● schafft Vertrauenswürdigkeit durch

- Testen einer funktionalen Spezifikation und einer Schnittstellenspezifikation
- Erstellung eines Handbuchs
- Unabhängiges Testen der TOE-Sicherheitsfunktionen
- Analyse des Entwurfs des TOE auf hoher Ebene (High-level-Design)
- Nachweis der Entwicklertests auf Grundlage der funktionalen Spezifikation
- Selektive unabhängige Bestätigung der Entwicklertestergebnisse
- Analyse der Stärke der Funktionen
- Nachweis der Suche des Entwicklers nach offensichtlichen Schwachstellen
- Konfigurationsverzeichnis für den TOE
- Nachweis der Sicherheit der Auslieferungsprozeduren

CC EAL 2

- **EAL2-Evaluation ist nur mit Hilfestellung durch den Entwickler des TOE möglich:**
Lieferung von Entwurfsinformationen und Testergebnissen
- **Verbesserung gegenüber EAL1:**
Forderung nach Entwicklertests, Schwachstellenanalyse und unabhängigen Testen auf Grundlage detaillierter TOE-Spezifikationen

CC EAL 3

methodisch getestet und überprüft; mittlere Stufe an unabhängig geprüfter Sicherheit und gründliche Untersuchung des TOE sowie dessen Entwicklung

- schafft Vertrauenswürdigkeit zusätzlich zu EAL 2 durch
 - Nachweis der Entwicklertests auf Grundlage der funktionalen Spezifikation und des Entwurfs auf hoher Ebene
 - Konfigurationsmanagement für den TOE
 - Kontrollen der Entwicklungsumgebung
- EAL3-Evaluation ist nur in Zusammenarbeit mit Entwickler des TOE möglich
- Verbesserung gegenüber EAL2: Forderung nach vollständiger Testabdeckung der Sicherheitsfunktionen und nach Mechanismen, die Vertrauen darin schaffen, dass der TOE während der Entwicklung nicht manipuliert wird

CC EAL 4

methodisch entwickelt, getestet und durchgesehen;
mittlere oder hohe Stufe an unabhängig geprüfter Sicherheit
für konventionelle, marktübliche TOE;
Entstehung zusätzlicher sicherheitsspezifischer Entwicklungskosten

- **schafft Vertrauenswürdigkeit zusätzlich zu EAL 3 durch**
 - Testen einer funktionalen Spezifikation und einer **vollständigen Schnittstellenspezifikation**
 - Analyse des Entwurfs des TOE auf hoher Ebene und **auf niedriger Ebene**
 - **Analyse einer Teilmenge der Implementierung**
 - **Informelles Modell der TOE-Sicherheitspolitik**
 - Nachweis der Suche des Entwicklers nach offensichtlichen Schwachstellen und **durch eine unabhängige Schwachstellenanalyse**, welche den **Schutz vor Angreifern mit niedrigen Angriffspotential nachweist**
 - **Zusätzliches Konfigurationsmanagement einschließlich Automatisierung** für den TOE

CC EAL 4

- **Verbesserung gegenüber EAL3:** Forderung nach umfassender Entwurfsbeschreibung, einer Teilmenge der Implementierung und nach verbesserten Mechanismen, die Vertrauen darin schaffen, dass der TOE während der Entwicklung nicht manipuliert wird

CC EAL 5

semiformal entworfen und getestet; hohe Stufe an unabhängig geprüfter Sicherheit; basiert auf scharfen betrieblichen Entwicklungstechniken für ein TOE mit gezielter EAL5-Einstufung; begrenzter Einsatz Sicherheits-Spezialtechniken zur Entwicklung

- **schafft Vertrauenswürdigkeit zusätzlich zu EAL 4 durch**
 - Analyse der gesamten Implementierung
 - formales Modell der TOE-Sicherheitspolitik
 - Semiformale Darstellung der funktionalen Spezifikation und des Entwurfs auf hoher Ebene sowie einen semiformalen Nachweis der Übereinstimmung untereinander
 - Modularer TOE-Entwurf
 - Nachweis der Entwicklertests auf Grundlage der funktionalen Spezifikation und des Entwurfs auf hoher Ebene und **auf niedriger Ebene**
 - Nachweis der Suche des Entwicklers nach offensichtlichen Schwachstellen und durch eine unabhängige Schwachstellenanalyse, welche den Schutz vor Angreifern mit **mittleren Angriffspotential** nachweist
 - Validierung der Entwickleranalyse der verdeckten Kanäle

CC EAL 5

- **Verbesserung gegenüber EAL4:** Forderung nach semiformaler Entwurfsbeschreibung sowie eine stärker strukturierte Architektur und einer Analyse der verdeckten Kanäle

CC EAL 6

**semiformal verifizierter Entwurf und getestet; sehr hohe Stufe an unabhängig geprüfter Sicherheit; basiert auf streng kontrollierter Entwicklungsumgebung für ein erstklassiges TOE zum Schutz hoher Werte gegen signifikante Risiken;
Sicherheits-Spezialtechniken mit hohen gerechtfertigten Zusatzkosten**

- **schafft Vertrauenswürdigkeit zusätzlich zu EAL 5 durch:**

- **Strukturierte Darstellung** der gesamten Implementierung
- Semiformale Darstellung der funktionalen Spezifikation und des Entwurfs auf hoher und niedriger Ebene sowie einen semiformalen Nachweis der Übereinstimmung untereinander
- Modularer und **mehrschichtiger** TOE-Entwurf
- Nachweis der Entwicklertests auf Grundlage der funktionalen Spezifikation und des Entwurfs auf hoher Ebene und auf niedriger Ebene

CC EAL 6

- Nachweis der Suche des Entwicklers nach offensichtlichen Schwachstellen und durch eine unabhängige Schwachstellenanalyse, welche den Schutz vor Angreifern mit **hohem Angriffspotential** nachweist
- Validierung der **systematischen** Entwickleranalyse der verdeckten Kanäle
- **Anwendung eines strukturierten Entwicklungsverfahrens**
- Umfassendes Konfigurationsmanagement einschließlich **vollständiger** Automatisierung für den TOE

● Verbesserung gegenüber EAL5:

Forderung nach umfassenderen Analysen, einer strukturierten Darstellung der Implementierung sowie einer stärkeren Strukturierung der Architektur, nach einer umfassenden unabhängigen Schwachstellenanalyse, einer systematischen Identifikation der verdeckten Kanäle und einem verbesserten Konfigurationsmanagement sowie Kontrollen der Entwicklungsumgebung

CC EAL 7

CC EAL 7 – formal verifizierter Entwurf und getestet; absolut unabhängige geprüfte Sicherheit; basiert auf sehr streng kontrollierter Entwicklungsumgebung für ein TOE mit hochkonzentrierter Sicherheitsfunktionalität zum Schutz hoher Werte gegen extrem hohe Risiken; Sicherheits-Spezialtechniken mit sehr hohen gerechtfertigten Kosten

- **schafft Vertrauenswürdigkeit durch**
 - Testen einer funktionalen Spezifikation und einer vollständigen Schnittstellenspezifikation; Überprüfung der Handbücher; Unabhängiges Testen der TOE-Sicherheitsfunktionen
 - Analyse des Entwurfs des TOE auf hoher und niedriger Ebene
 - Strukturierte Darstellung der gesamten Implementierung
 - formales Modell der TOE-Sicherheitspolitik
 - **Formale** Darstellung der funktionalen Spezifikation und des Entwurfs **auf hoher Ebene** und eine semiformale Darstellung des Entwurfs auf niedriger Ebene sowie einen semiformalen Nachweis der Übereinstimmung untereinander, **wie jeweils angemessen**

CC EAL 7

- Modularer, mehrschichtiger und **einfacher** TOE-Entwurf
 - Nachweis der Entwicklertests auf Grundlage der funktionalen Spezifikation und des Entwurfs auf hoher und niedriger Ebene sowie der **Darstellung der Implementierung**
 - Unabhängige Bestätigung der Entwicklertestergebnisse und Analyse der Stärke der Funktionen
 - Nachweis der Suche des Entwicklers nach offensichtlichen Schwachstellen und durch eine unabhängige Schwachstellenanalyse, welche den Schutz vor Angreifern mit hohem Angriffspotential nachweist
 - Validierung der **systematischen** Entwickleranalyse der verdeckten Kanäle
 - Anwendung eines strukturierten Entwicklungsverfahrens
 - Kontrollen der Entwicklungsumgebung und Nachweis der Sicherheit der Auslieferungsprozeduren
- **Verbesserung gegenüber EAL6:** Forderung nach umfassenden Analysen unter Verwendung formaler Darstellungen und formaler Übereinstimmung sowie umfassenden Testens

SOF (Strength of Function)

SOF-Niedrig: Schutz gegen zufälliges Brechen,
Angreifer mit geringem Angriffspotential

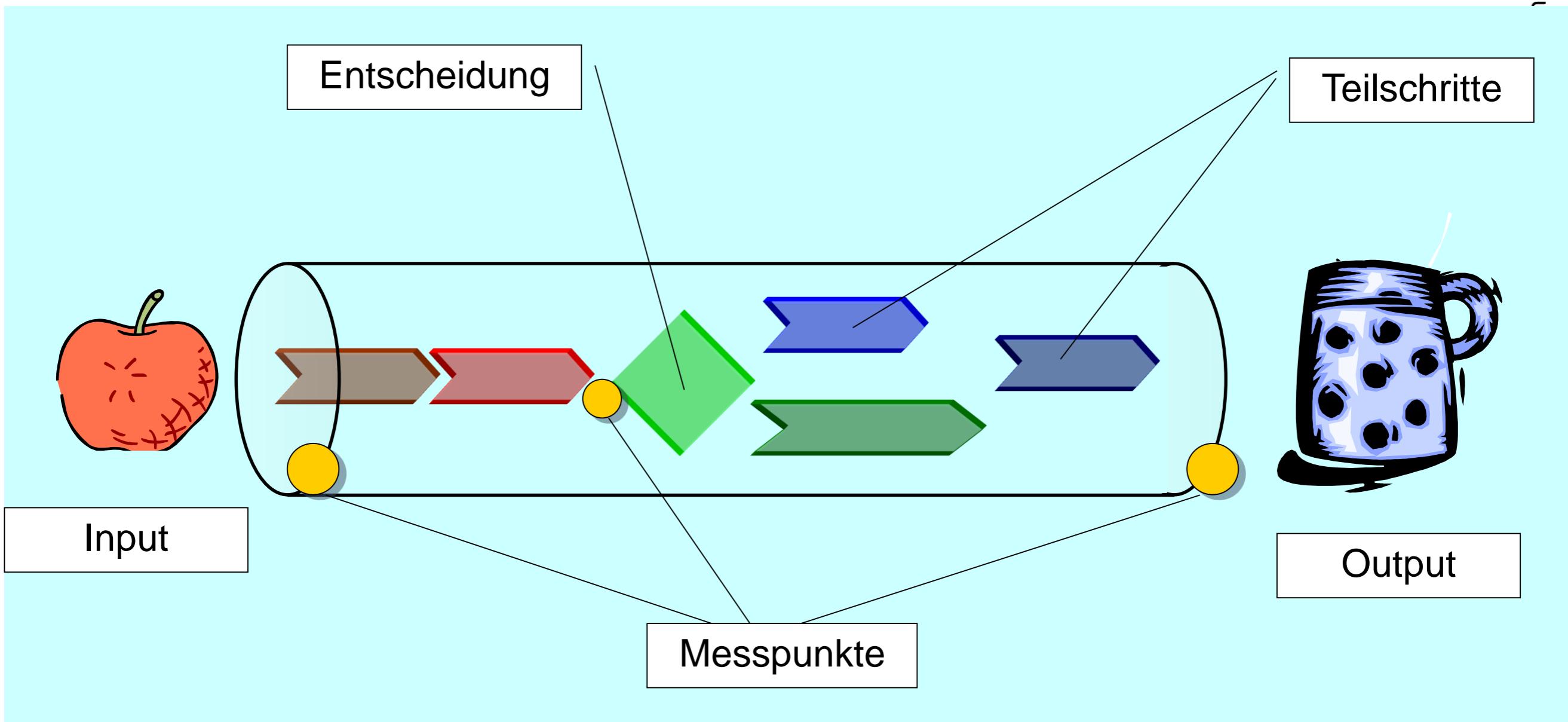
SOF-Mittel: Schutz gegen naheliegendes oder
absichtliches Brechen,
Angreifer mit mittlerem Angriffspotential

SOF-Hoch: Schutz gegen geplantes oder
organisiertes Brechen,
Angreifer mit hohem Angriffspotential

CC – Vorgehen bei Änderungen am TOG

- Ein Zertifikat nur gültig für eine bestimmte Version
- Assurance Continuity Verfahren bei geringfügigen Änderungen am Produkt, sonst Re-Evaluierung
- Zertifizierungsstellen entscheiden über Anwendbarkeit und stimmen sich über Kriterien ab
- International abgestimmtes und anerkanntes Verfahren
- 2006: 25 Assurance Continuity Verfahren hauptsächlich im SmartCard-Umfeld

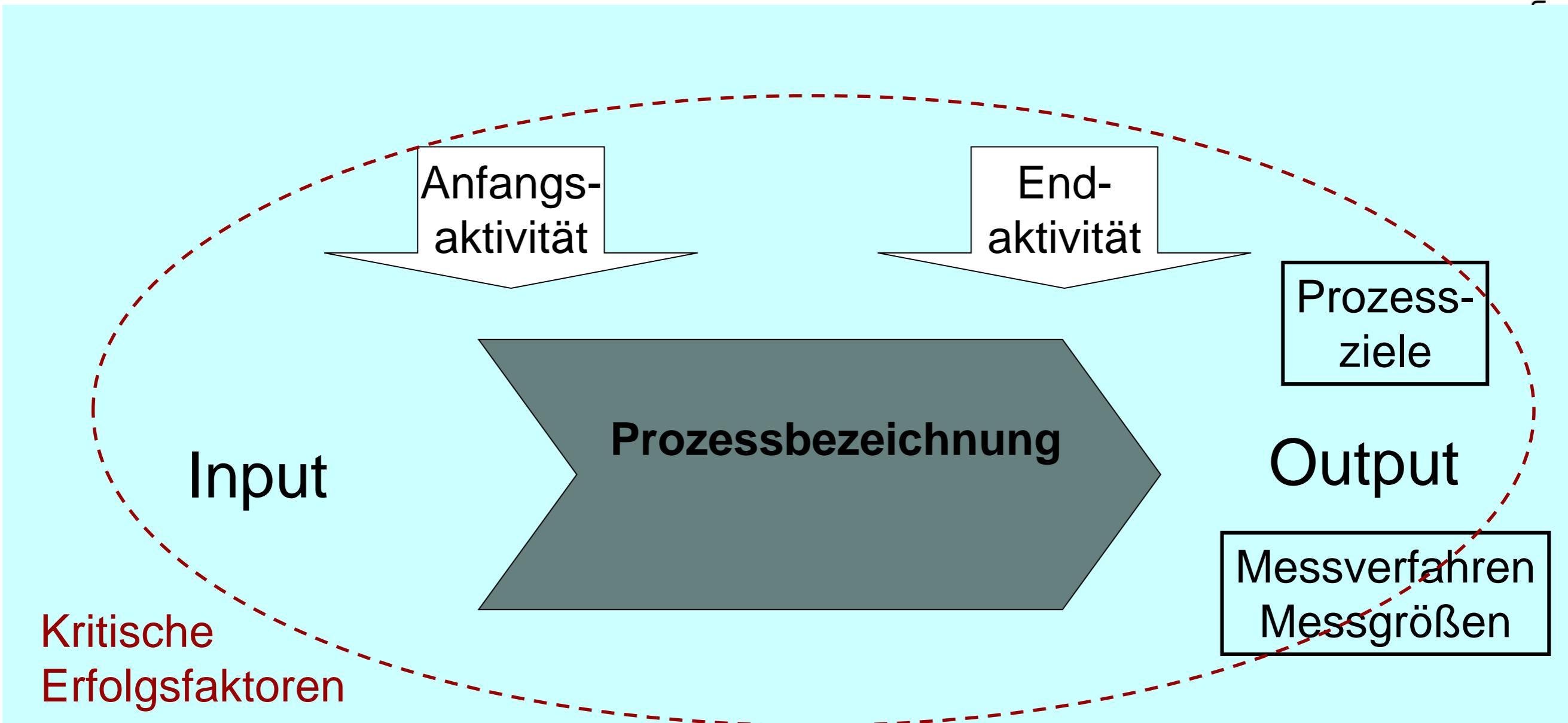
Was ist ein Prozess?



Anforderungen im Themenumfeld „Prozess“ (lt. ISO 9001:2008)

- Festgelegte Abläufe und Interaktionen
- Definierte Kriterien und Methoden für Betrieb und Steuerung
- Sicherstellen der nötigen Ressourcen
- Überwachen, messen und analysieren
- Definierte Planung
- Gesteuerte Ablaufbedingungen
- Bewertung
- Verbesserung

Abgrenzung eines Prozesses

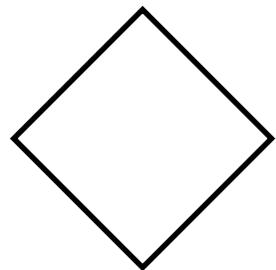


Möglichkeiten zur Prozessdarstellung (1)

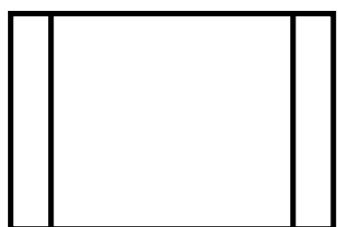
Ablaufdiagramm nach ISO 5807



Prozess(schritt): Beschreibt eine definierte Einzelaktion oder abgestimmte definierte Aktionen die ein konkretes Ergebnis erzielen. (Änderung in Wert, Form oder Ort der Information)



Entscheidung: Beschreibt eine Aktion, die in einer Entscheidung mündet, es gibt einen Eingang und mehrere mögliche Ausgänge.



Subprozess: Übergibt den Prozessablauf an einen bereits definierten Subprozess, das Ergebnis steht dem aufrufenden Prozess zur Verfügung.

Möglichkeiten zur Prozessdarstellung (2)

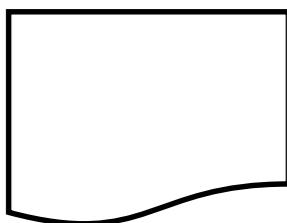
Ablaufdiagramm nach ISO 5807

1

Verbinde: Bezeichnet einen Sprung zu oder von einem anderen Punkt im selben Flowchart. Achtung: eindeutig kennzeichnen!



Terminator: Kennzeichnet Prozessanfangs- oder Endpunkt(e)



Information: Repräsentiert Daten/Informationen in welcher Form auch immer (Papier, elektronisch, fernaltional,...)