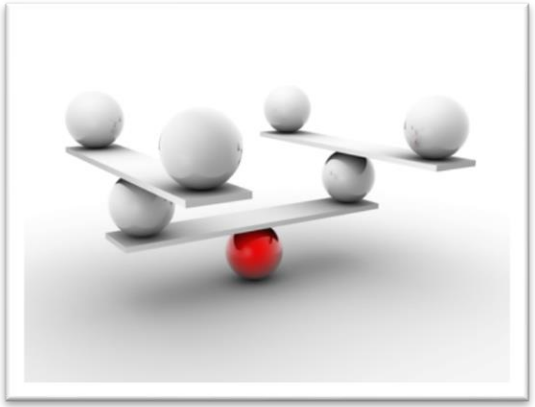
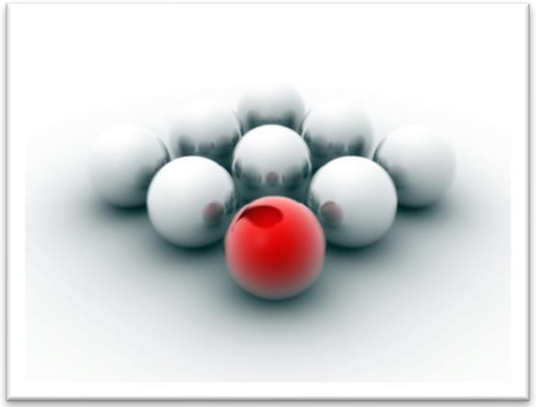
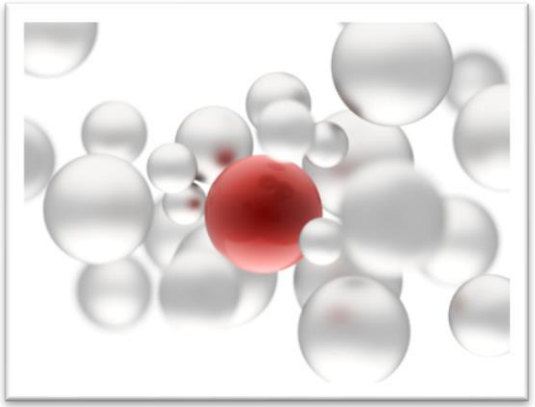
CETUS
Health · IT · Leadership







IT-Sicherheitsmanager für medizinische IT-Netzwerke

Risiken ohne Nebenwirkungen.

Agenda

Tag 4

- ✓ BSIG
- ✓ Normen ISO 27001, IT-Grundschutz und ISO 2700x-Familie
- ✓ ISO 27001
- ✓ B3s

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)

Zuletzt geändert durch Art. 1 G v. 23.6.2017 I 1885

§ 1 Bundesamt für Sicherheit in der Informationstechnik

Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) als Bundesoberbehörde. Das Bundesamt ist zuständig für die Informationssicherheit auf nationaler Ebene. Es untersteht dem Bundesministerium des Innern.

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(3) Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen

BSiG

§ 8b Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) Das Bundesamt ist die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik.

(3) Die Betreiber Kritischer Infrastrukturen haben dem Bundesamt binnen sechs Monaten nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 eine Kontaktstelle für die von ihnen betriebenen Kritischen Infrastrukturen zu benennen. Die Betreiber haben sicherzustellen, dass sie hierüber jederzeit erreichbar sind. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Kontaktstelle.

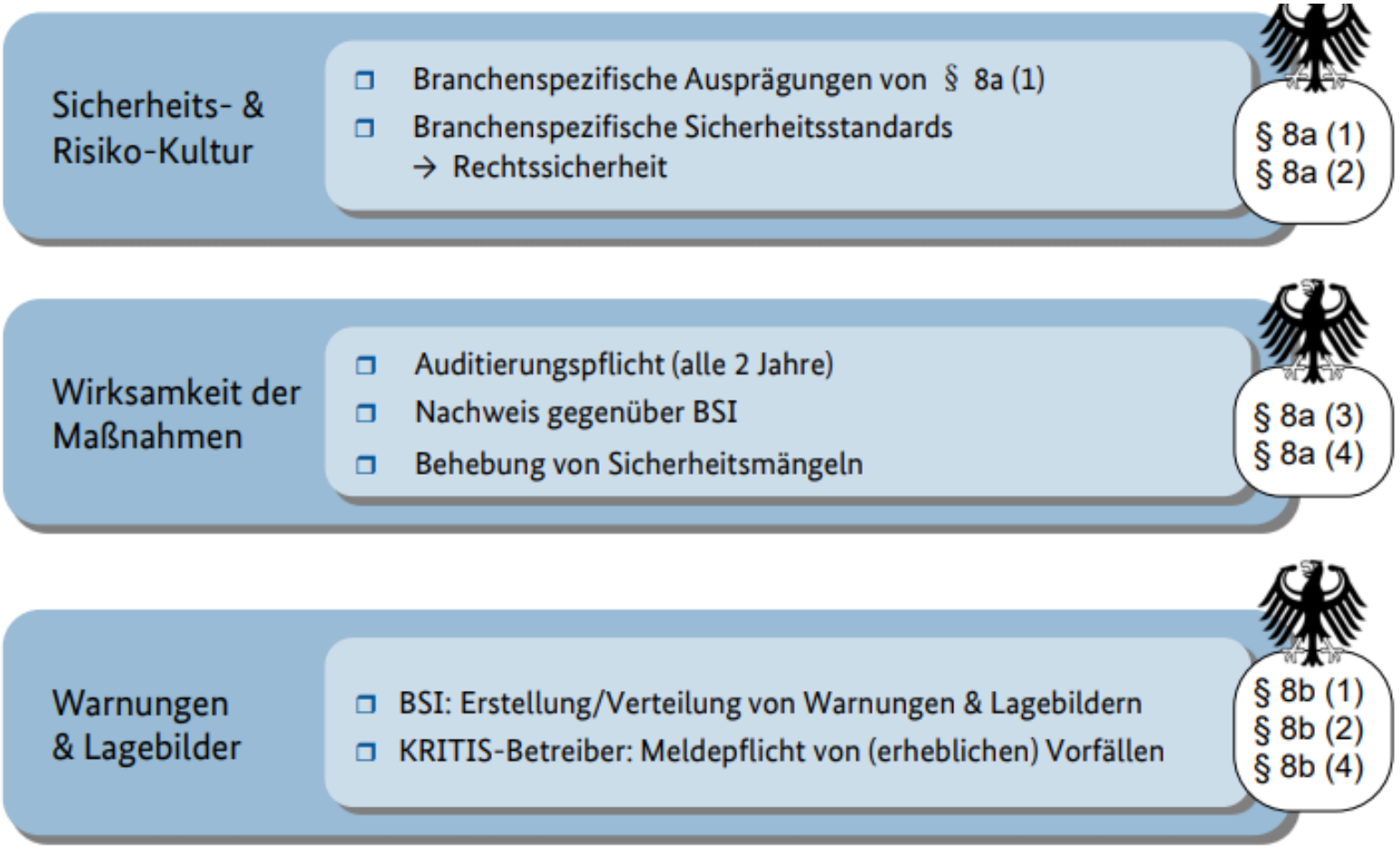
§ 8b Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(4) Betreiber Kritischer Infrastrukturen haben die folgenden Störungen unverzüglich über die Kontaktstelle an das Bundesamt zu melden:

1.Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben,

2. erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können.

BSIG Schutz Kritischer Infrastrukturen



BSiG – Definition „Kritische Infrastrukturen“

Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden

Sektoren	Branchen
Gesundheit	Medizinische Versorgung Arzneimittel und Impfstoffe Labore

Der Schwellenwert zur Identifikation kritischer Infrastrukturen wurde auf 30.000 vollstationäre Behandlungsfälle festgelegt. Gemäß BSI-KritisV haben Krankenhäuser künftig jeweils zum 31. März zu prüfen, ob sie diesen Schwellenwert erreichen oder überschreiten.

Ein Übergangszeitraum ist ausdrücklich nicht vorgesehen.

BSiG – Anforderungen

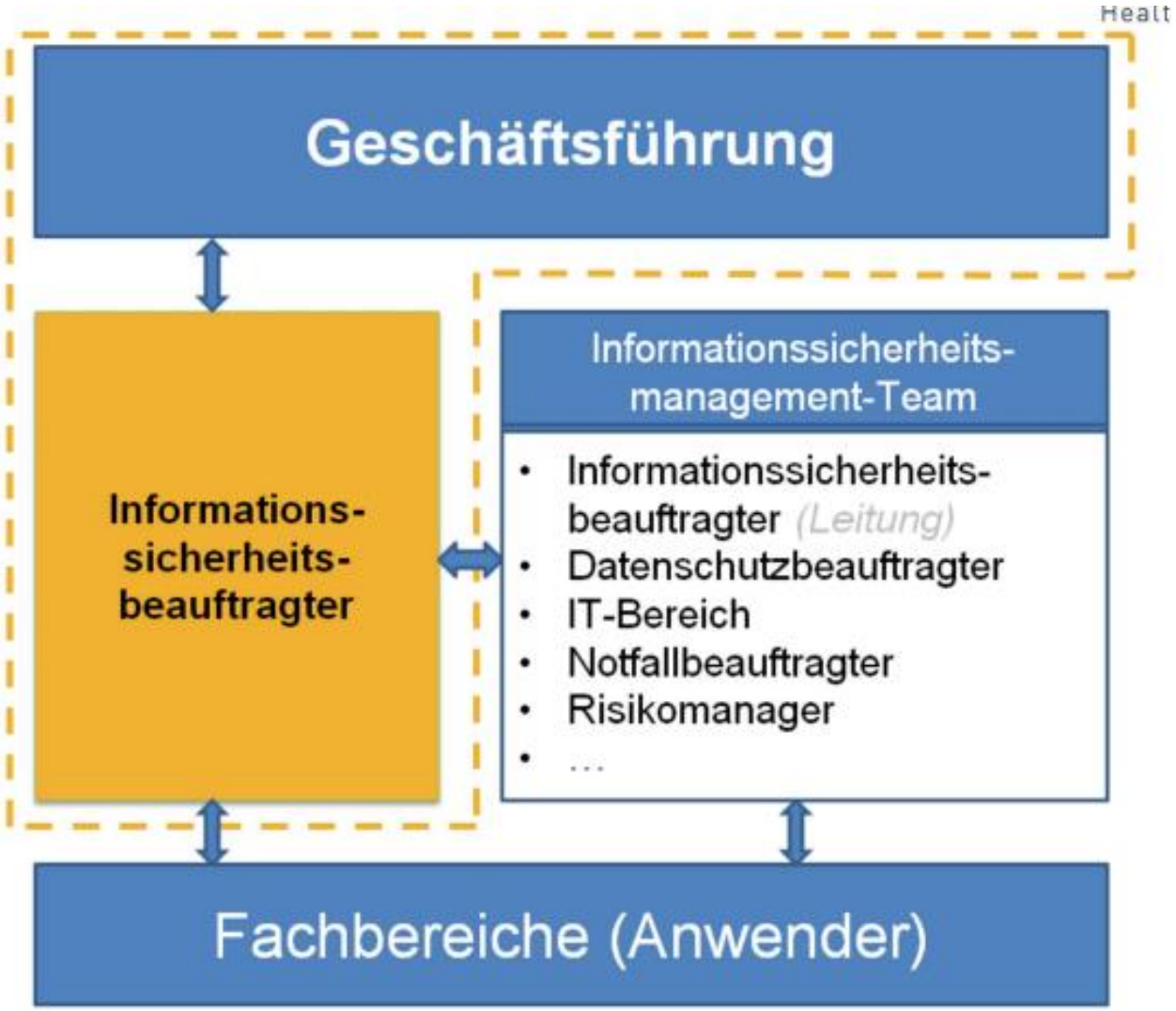
Maßnahmen bei Überschreitung des Schwellenwertes

- ✓ Registrierung als kritische Infrastruktur und Einrichtung Kontaktstelle
- ✓ Meldung von IT-Störungen an das BSI
- ✓ Umsetzung von Maßnahmen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse
- ✓ Die Schritte sind sofort umzusetzen, diese gelten ab dem 1.4. des Jahres, das auf die Überschreitung des Schwellenwertes folgt
- ✓ Der Nachweis der Umsetzung ist spätestens 2 Jahre nach Feststellung der Schwellenwertüberschreitung zu erbringen
- ✓ Ist der Schwellwert nur knapp unterschritten, sollten vorbereitende Maßnahmen getroffen werden, um ggf. im Folgejahr die dann sofort greifende Verpflichtung zur Umsetzung realisieren zu können

BSiG – Definition „Kritische Infrastrukturen“

- ✓ Für Krankenhäuser, welche die Kriterien kritischer Infrastruktur zwei Jahre in Folge erfüllen, entsteht eine Nachweispflicht zur Umsetzung geeigneter organisatorischer und technischer Vorkehrungen zur Vermeidung von Störungen der informationstechnischen Systeme.
- ✓ Wesentliches Ziel der festgelegten Informationspflichten ist der Austausch von für IT-Sicherheit relevanten Informationen zwischen den Betreibern kritischer Infrastrukturen und dem BSI.
- ✓ Es muss ein Prozess beschrieben werden, wie mit Vorfällen im Bereich der IT-Sicherheit umgegangen wird und wann eine Meldung sinnvoll bzw. notwendig ist.
- ✓ §10 (2) BSiG stellt es Betreibern kritischer Infrastrukturen sowie deren Branchenverbänden frei, „branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1“ vorzuschlagen
- ✓ Der Aufbau eines ISMS wird als Basis für die Umsetzung angesehen

BSiG – Umsetzung Aufbauorg. IT-Sicherheit



BSiG - Anforderungen

Technische und organisatorische Schutzmaßnahmen

- ✓ Absicherungsmaßnahmen, wenn IT Einfluss auf die Dienstleistung hat
- ✓ Erhalt von Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit
- ✓ Prävention
- ✓ Untersuchung und Behebung von Störungen

BSiG - Anforderungen

„Der Stand der Technik“

- ✓ Keine Legaldefinition (Flexibilität) = Unbestimmter Rechtsbegriff
- ✓ „Soll-“Vorschrift
- ✓ Erarbeitung durch die Betreiber selbst oder deren Branchenverbände
- ✓ Zweijährlich Audit / Prüfung / Zertifizierung
- ✓ Nachweispflicht gegenüber dem BSI

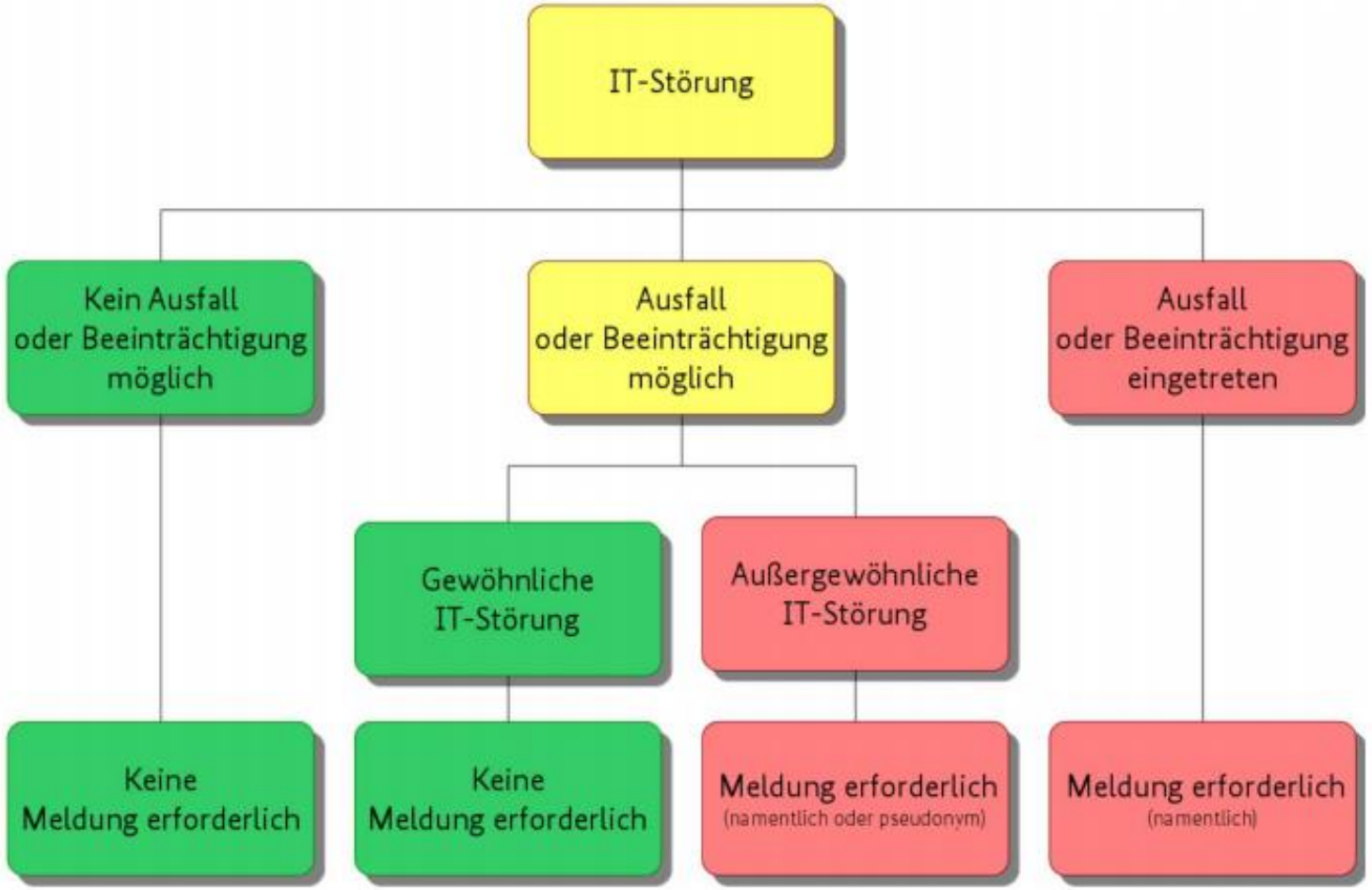
BSiG - Anforderungen

Warn-, Hinweis- und Meldepflichten

- ✓ Erhebliche Störungen IT-System, Komponenten oder Prozesse, erheblich sind:
  - Gezielte Angriffe
  - Neuer Modus Operandi
  - Unerwartete Vorkommnisse
  - Deutlich erhöhter Ressourcenaufwand
- ✓ „Störung“ = eingesetzte Technik kann ihre Funktion nicht mehr oder nicht mehr vollständig erfüllen (auch: erfolglose Angriffe)

BSiG – Meldepflichtige Störungen

Health · IT · Leadership



§ 14 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 8a … eine dort genannte Vorkehrung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig trifft,
2. einer vollziehbaren Anordnung nach § 8a Absatz 3 Satz 5 zuwiderhandelt,
3. entgegen § 8b Absatz 3 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine Kontaktstelle nicht oder nicht rechtzeitig benennt,
4. entgegen § 8b Absatz 4 Satz 1 Nummer 2 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
5. entgegen § 8c Absatz 1 Satz 1 eine dort genannte Maßnahme nicht trifft,
6. entgegen § 8c Absatz 3 Satz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vornimmt oder

§ 14 Bußgeldvorschriften

7. einer vollziehbaren Anordnung nach § 8c Absatz 4

a) Nummer 1 oder

b) Nummer 2

zuwiderhandelt.

(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 2 Buchstabe b mit einer Geldbuße bis zu hunderttausend Euro, in den übrigen Fällen des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

GRUNDLAGEN DER NORMEN

Zielsetzungen

- ✓ Erhöhung der Informationssicherheit einer Organisation durch strukturiertes Management
- ✓ Kalibrierungsgrundlage für Vergleichbarkeit und Zertifizierung
- ✓ **ISO 2700X:** Framework zur Umsetzung von Informationssicherheitsmanagement im Unternehmen – **Anwendbarkeit** global und flexibel
- ✓ **IT-Grundschutz / BSI-Standard:** leicht anwendbare und erprobte Systematik mit Maßnahmenempfehlungen und integrierter Gefährdungsanalyse – **Zielgruppe:** typische Einsatzszenarien und Systeme

Die ISO 2700X-Familie

Norm	Bedeutung
ISO/IEC 27001:2017	Zertifizierungsnorm, d.h. Basis auf der der Auditor die Zertifizierung durchführt.
ISO/IEC 27002	Leitfaden zur besseren Interpretation des Anhang A der ISO 27001:2017
ISO/IEC 27003	Implementierungsleitfaden.
ISO/IEC 27004	Information Security Management Measurement
ISO/IEC 27005	Information Security Risk Management
ISO/IEC 27006- 27008	Leitfäden für Zertifizierer und Auditoren
ISO/IEC 27011	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

Die ISO 2700X-Familie

Norm	Bedeutung
ISO/IEC 27013	Guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001
ISO/IEC 27034	Guidelines for application security

- Die Familie der ISO 2700x wird ständig weiter entwickelt.
- Grundlage bleibt die ISO 27001 als Zertifizierungsnorm

AUFBAU UND ANWENDBARKEIT

Aufbau der ISO 27001:2017

Kapitel	Beschreibung
0 – 3	Allgemeine Kapitel und informative Hinweise zur Wortwahl und zur Nutzung der Norm.
Kapitel 4 – Kontext der Organisation (Sicherheitslinie)	Bezug zur ISO 31000:2009 – jeder Anwender der Norm legt in diesem Schritt fest, welche Einflussfaktoren sich auf das ISMS auswirken.
Kapitel 5 – Führung (Unterstützung und Bereitstellung von Personal und Geld durch die GF)	Beschreibt die Aufgaben des Managements / der Führungsebene im Rahmen des ISMS.
Kapitel 6 – Planung (Risikomanagement Richtlinie, Richtlinie DIN 80001 Risikomanagement)	Beschreibt, welche planerischen Maßnahmen der Anwender umsetzen muss, um Chancen und Risiken miteinander in Einklang zu bringen.

Aufbau der ISO 27001:2017

Kapitel	Beschreibung
Kapitel 7 – Unterstützung (Richtlinie Dokumentenlenkung, SOAs)	Beschreibt die notwendigen Unterstützungsaspekte für ein funktionierendes ISMS sowie Vorgaben zur Dokumentenlenkung und Dokumentation.
Kapitel 8 – Einsatz (Einsatzplanung und Kontrolle, Informationssicherheits- Einschätzung und -Risikobehandlung)	Beschreibt die notwendigen Managementabläufe zur Implementierung von Sicherheitsmaßnahmen und deren Dokumentation.
Kapitel 9 – Leistungsauswertung (Leitlinie Kennzahlen, interne Audits)	Beschreibt, welche Kennzahlen zur Überwachung und Steuerung des ISMS zu ermitteln sind und welche Auditverfahren eingesetzt werden müssen.

Aufbau der ISO 27001:2017

Kapitel	Beschreibung
Kapitel 10 – Verbesserung (PDCA-Zyklus)	Beschreibt, wie auf Fehler und Verbesserungspotenziale zu reagieren ist.
Anhang A – Referenz-Maßnahmenziele und Maßnahmen	Enthält die umzusetzenden Sicherheitsmaßnahmen in abstrakter Formulierung. Konkretisierung in der ISO 27002:2014.
Literaturhinweise	

Was ist ein ISMS überhaupt?

ISMS bedeutet

Informations-

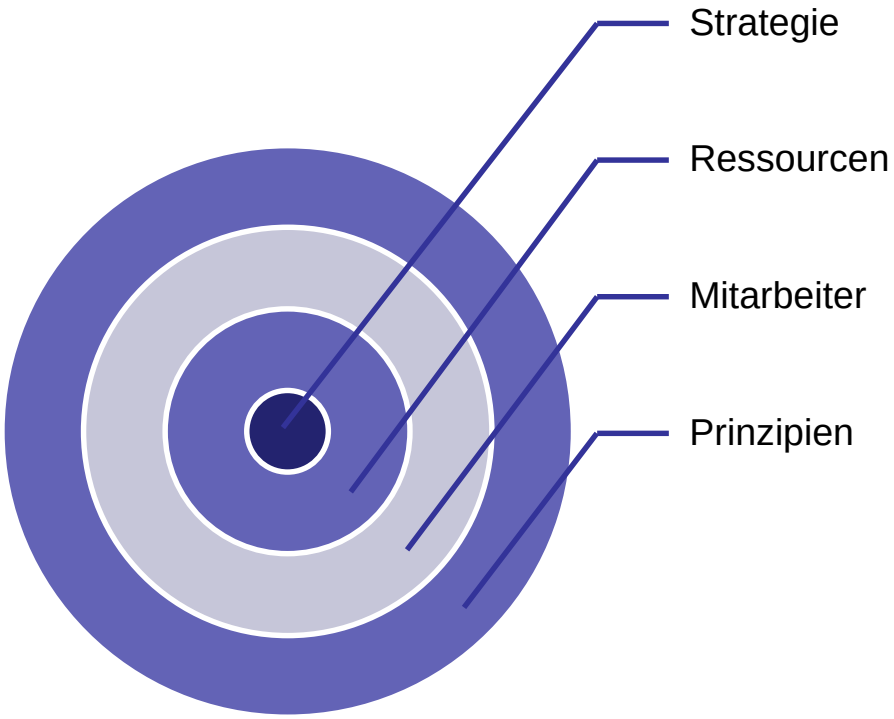
Sicherheits-

Management-

System

- Klarer Fokus auf Informationsverarbeitung.
- Technik ist nachrangig, Führung und Steuerung steht im Vordergrund.
- Regelmäßige Aktualisierung notwendiger Schritt.
- Betrachtet wird das ganze Unternehmen, nicht nur die IT.

Wichtige Bestandteile des ISMS



- **Strategie als Bekenntnis zur Sicherheit.**
- **Ressourcen, um die gesetzten Ziele zu erreichen.**
- **Mitarbeiter als Stütze der Sicherheitsbemühungen.**
- **Prinzipien des Managements als Anker der Strategie.**

Schutzziele der ISO 27001:2013

Verfügbarkeit Availiability	• Informationen zu rechten Zeit am rechten Ort
Vertraulichkeit Confidentiality	• Informationen nur für Berechtigte
Integrität Integrity	• Informationen unverfälscht und nachvollziehbar

Unterschiede zu anderen Normen

BSI-Standards zur IT-Sicherheit
- Bereich IT-Sicherheitsmanagement -

BSI Standard 100-1:
ISMS: Managementsysteme für Informationssicherheit

BSI Standard 100-2:
IT-Grundschutz-Vorgehensweise

BSI Standard 100-3:
Risikoanalyse auf der Basis von IT-Grundschutz

BSI Standard 100-4:
Notfallmanagement

Internationale Standards
- Bereich IT-Sicherheitsmanagement -

ISO 27001 – Information Security Management Systems

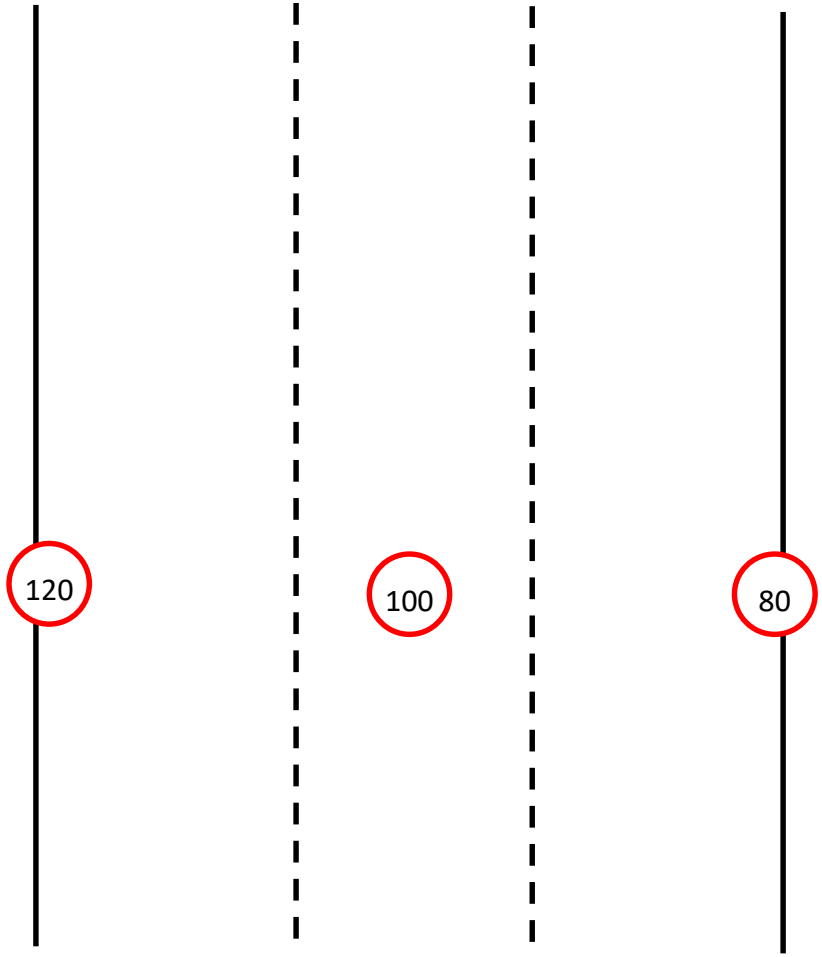
ISO 27002 – Information Security Management Controls

ISO 27005 – Information Security Risik Management

BS 25999 – Business Continuity Management

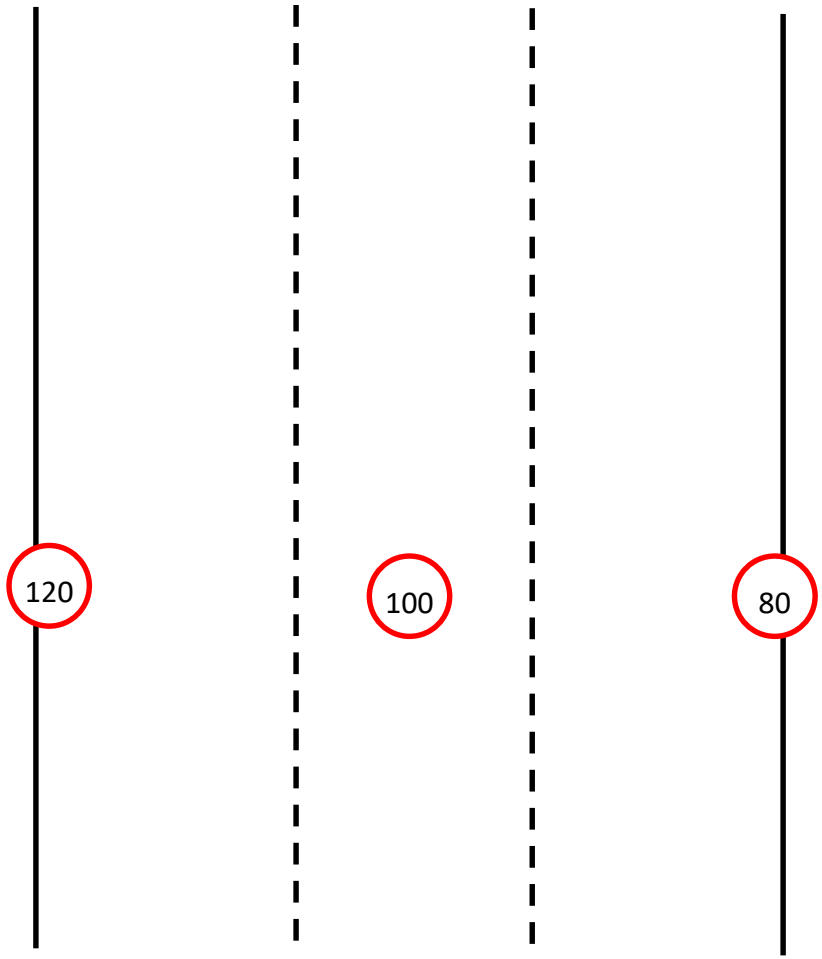
Die Ausrichtung der ISO 27001

- Die ISO 27001 lässt freie Auswahl, welche Geschwindigkeit auf der Straße gefahren wird.
- Die ISO 27001 bietet die Leitplanken, die Fahrspur wählt das Unternehmen selbst aus.
- Das Risiko, ob zu schnell gefahren wird, wird selbst eingeschätzt.



Die Ausrichtung des IT-Grundschutz

- Der IT-Grundschutz schreibt vor, auf welcher Spur wie schnell gefahren wird.
- Die Risikobewertung ist vorweggenommen.
- Die Flexibilität der Risikobewertung ist eingeschränkt.



Vorgehen, Phasen und Zeitplanung

EINFÜHRUNG EINES ISMS

Unterschiedliche Schutzziele

Medizintechnik

- **Safety** = Patientensicherheit
- **Effectiveness** = zur rechten Zeit in rechter Qualität am rechten Ort
- **Security** = Datenschutz & Datensicherheit

Der Patient steht im Mittelpunkt!

IT / Informationssicherheit

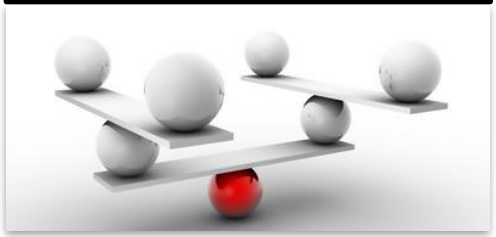
- **Integrität** = unverfälschte und korrekte Informationen
- **Verfügbarkeit** = zur Rechten Zeit am Rechten Ort
- **Vertraulich** = Zugang nur für Berechtigte

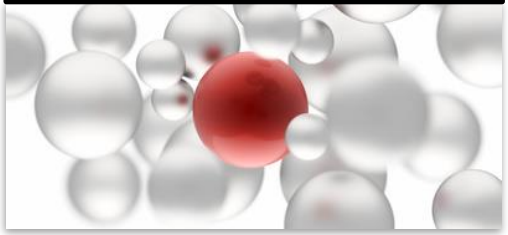
Die Information / der Prozess steht im MIttelpunkt

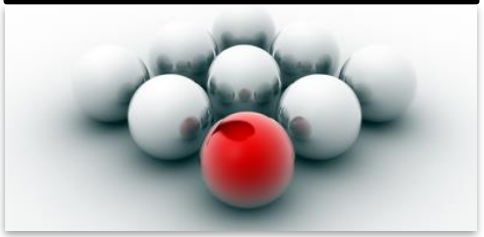
Konfliktpotenzial aufgrund unterschiedlicher Denkrichtungen.

Ähnliche Abläufe (1/2)

Policydesign	Dokumentation	Risikoanalyse
IEC 80001-1:2010 Risk Management Policy **ISO 27001:2013** Security Policy Risk Management Policy	**IEC 80001-1:2010** Risk Relevant Asset Description **ISO 27001:2013** Inventory of critical assets	**Risk Analysis** **Risk Evaluation** **Risk Control**

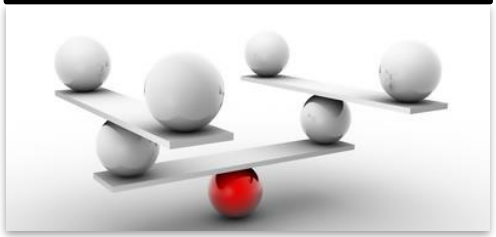


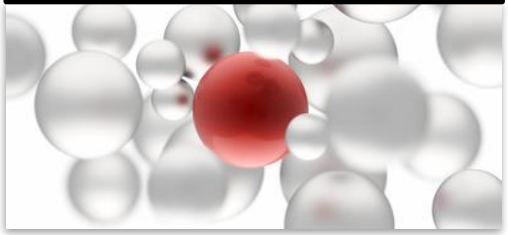


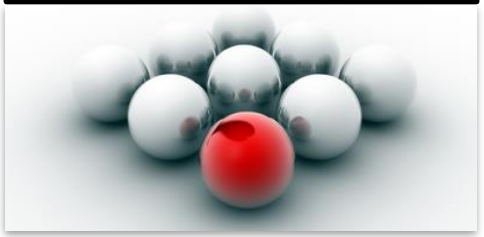


Ähnliche Abläufe (2/2)

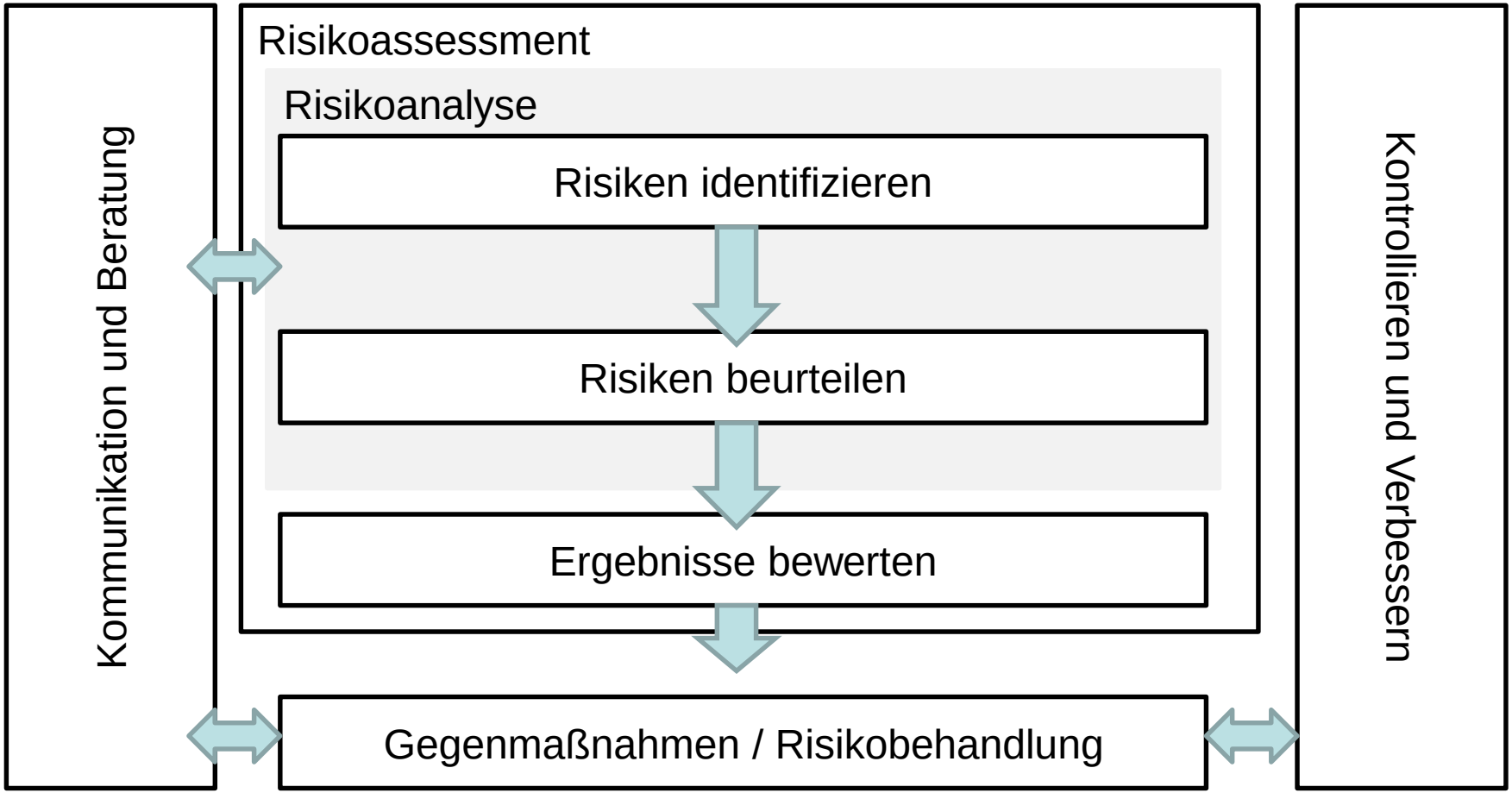
Dokumentation & Kontrolle	Lenkung & Input	Verbesserung
IEC 80001-1:2010 Medical Risk Management File **ISO 27001:2013** Statement of Applicability	**IEC 80001-1:2010** Document Control Procedure **ISO 27001:2013** Control of Documents	**IEC 80001-1:2010** Risk Management Process **ISO 27001:2013** Corrective Action Preventive Action



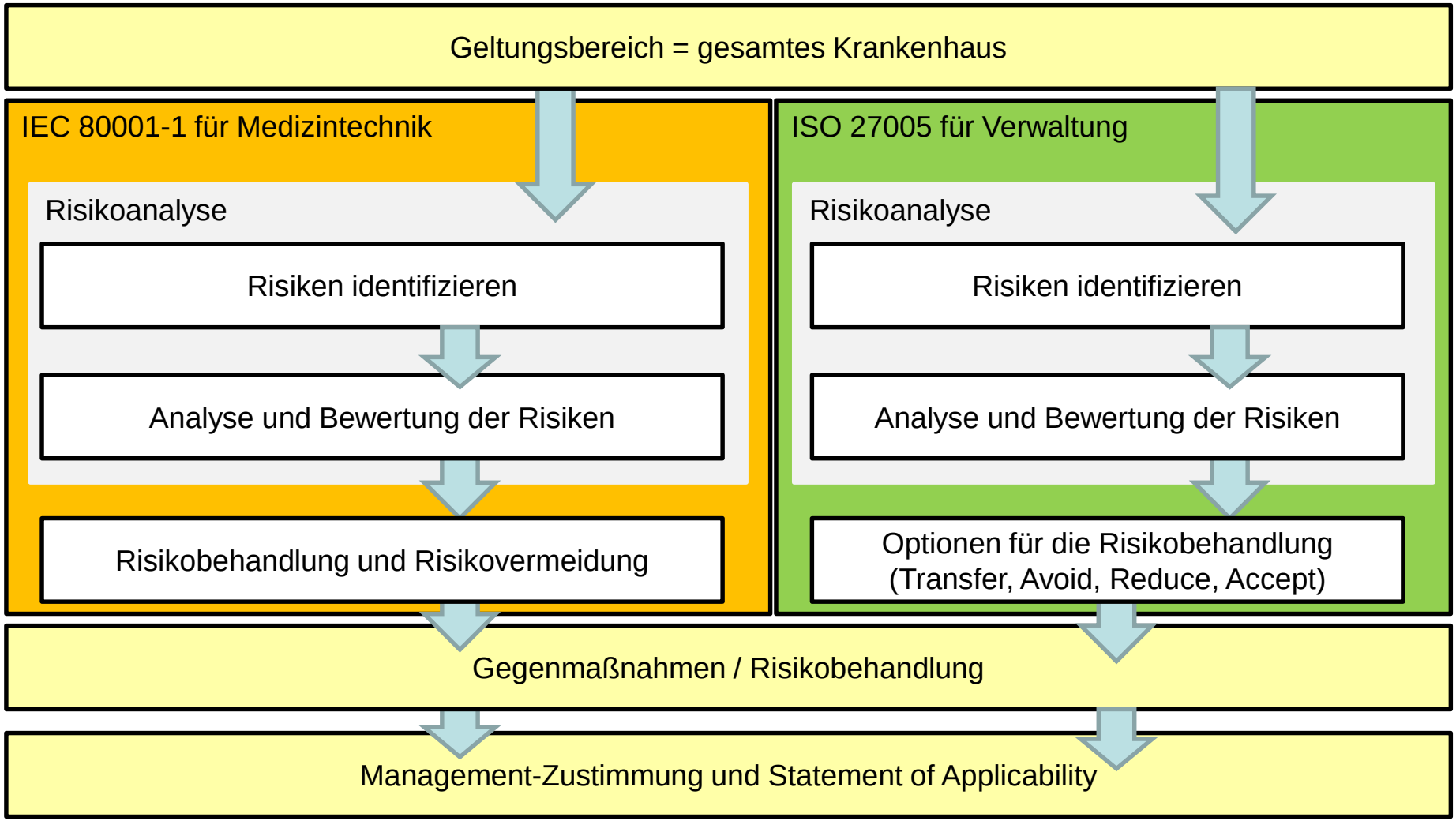




Ablauf einer Risikoanalyse



IEC 80001-1 und ISO 27001 als Team



Aufbau eines ISMS

Geschäftsführung

Informationssicherheitslinie

← delegiert Umsetzung an

← berichtet an

IS-Sicherheitsbeauftragter

Risikobehandlungsplan

IT-Sicherheitskonzept

← unterstützt

IT-Sicherheitsboard optional

Zentrale Richtlinien

Dokumentenlenkung

Richtlinie Risikomanagement (Forderung ISO 27001)
(Schnittstelle zum Konzernrisikomanagement)

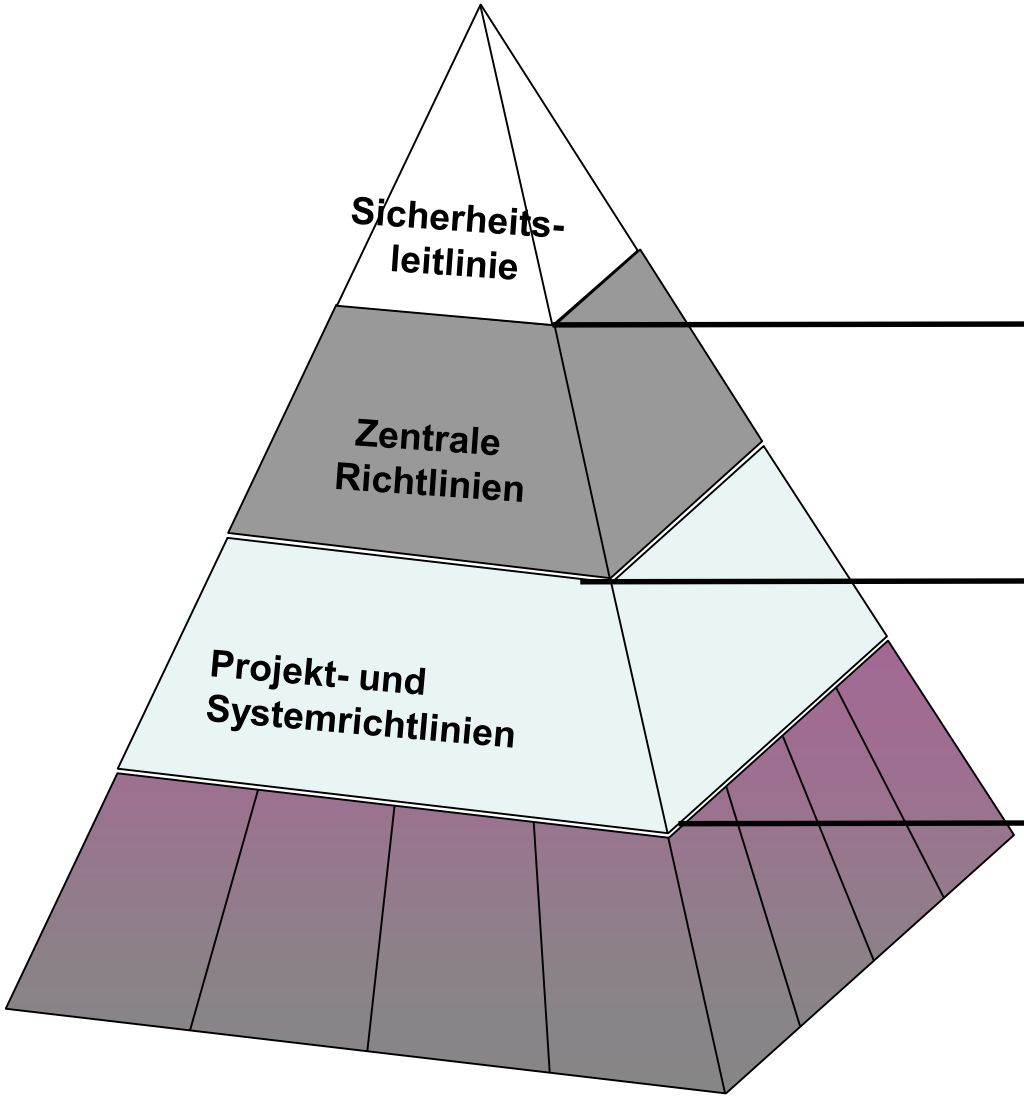
Richtlinie Erfolgsmessung
(Steuerungsinstrument mit Kennzahlen)

Richtlinie Durchführung interner Audits **(Bezug zu QM)**
(ISMS Bestandteil, spezielle Vorgaben für IT-Revision und Audits)

Richtlinie Korrektur- und Vorbeugemaßnahmen
(ISMS Bestandteil – spezielle Vorgaben für ISMS)

RL Risikomanagement gem. DIN 80001
(ISMS Bestandteil – Schnittstelle zur Medizintechnik)

Mehrstufige Dokumentenpyramide



- ✓ Strategisches Dokument – Detailarm – Basisdokument liegt vor
- ✓ Vorgaben für Bereiche und Prozesse – Basisdokumente liegen vor
- ✓ Regelungen für konkrete Prozesse und Projekte
- ✓ Arbeitsanweisungen – einzelne Arbeitsschritte

AUDIT UND ZERTIFIZIERUNG

Audit und Zertifizierung

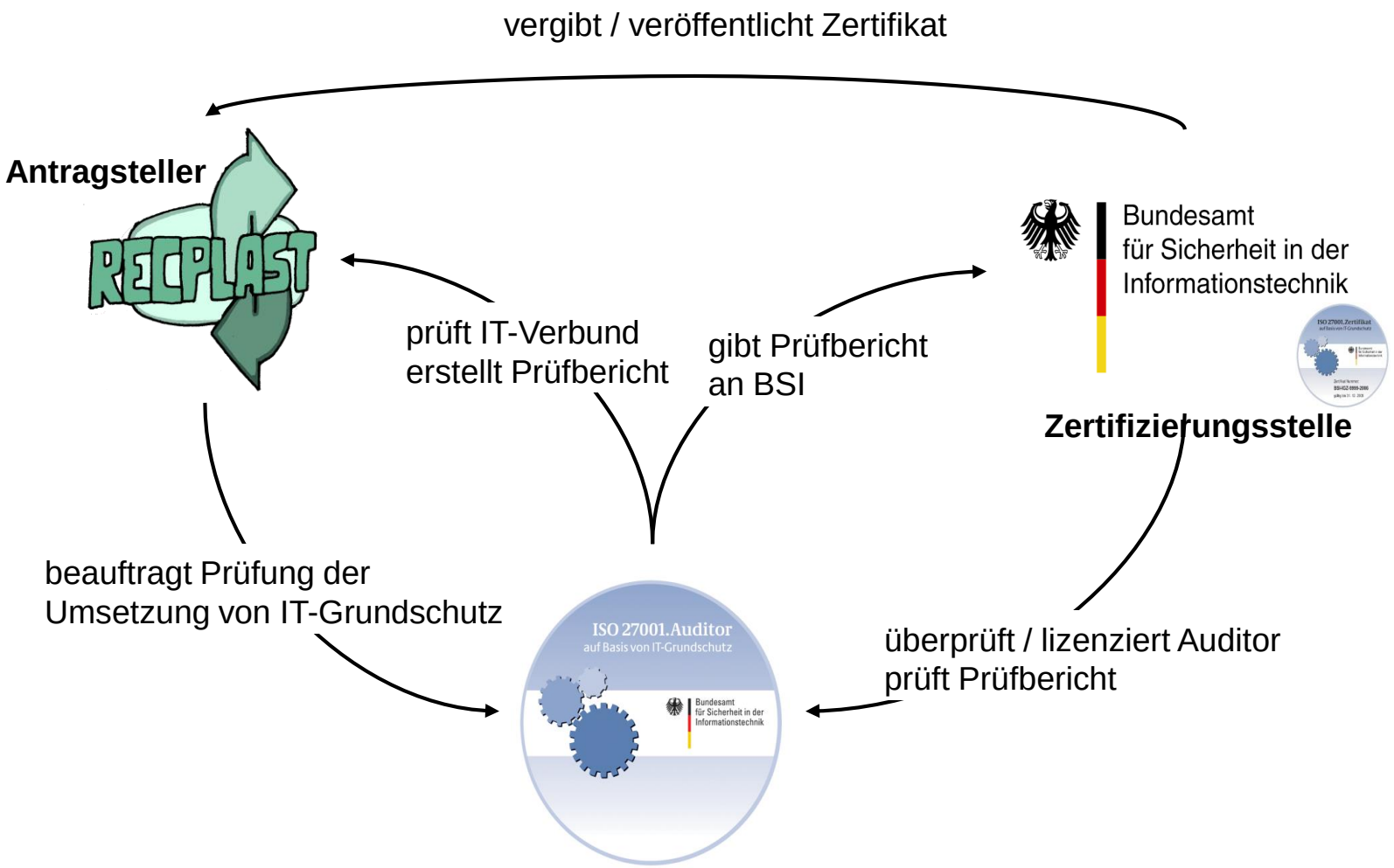
- ✓ **Zertifizierungsnormen:** ISO 27001:2017 und IT-Grundschutz als Gesamtkonzept

- ✓ **Unterschiede:**
  - ISO 27001:2017 zertifiziert das Managementsystem ohne Detailprüfung von Maßnahmen
  - IT-Grundschutz zertifiziert das Managementsystem und stichprobenhaft umgesetzte Maßnahmen
  - Jede Norm hat unterschiedliche Anforderungen an das Audit und die Auditoren
  - IT-Grundschutz wird durch das BSI zertifiziert, ISO 27001:2017 durch anerkannte Zertifizierungsstellen (z.B. QM-Zertifizierer wie DQS, TÜV o.ä.)

Zertifizierungsprozess ISO 27001:2008

- ✓ Organisation beauftragt Zertifizierungsgesellschaft mit Durchführung des Zertifizierungsaudits
- ✓ Die ZertG beauftragt einen oder mehrere Auditoren mit der Durchführung der Audits
- ✓ Der ZertG erteilt nach Prüfung des Auditberichtes auf Empfehlung des Auditors das Zertifikat
- ✓ Auditor ist entscheidende Stelle bei der Zertifikatsvergabe

Zertifizierungsprozess IT-Grundschutz



ISO-27001 Auditor auf Basis von IT-Grundschutz

ISMS-Normen und Qualitätsmanagement

SCHNITTSTELLE QUALITÄT

Schnittstellen Qualitätsmanagement

Allgemeine Anforderungen, Dokumentenlenkung,
Schulung, Sensibilisierung und Weiterbildung

BSI-Standard 100-1
Betrieb des ISMS
BSI-Standard 100-2
Sicherheitskonzept
BSI-Standard 100-3
Risikoanalyse

ISO 27001:2017
Information Security Management Systems

Betrieb des ISMS

ISO 9001
Quality Management Systems

Betrieb des QMS

Internes Audit, Management Berichte, Kontinuierliche Verbesserung,
Korrektur- und Vorbeugemaßnahmen

Welche Synergien existieren

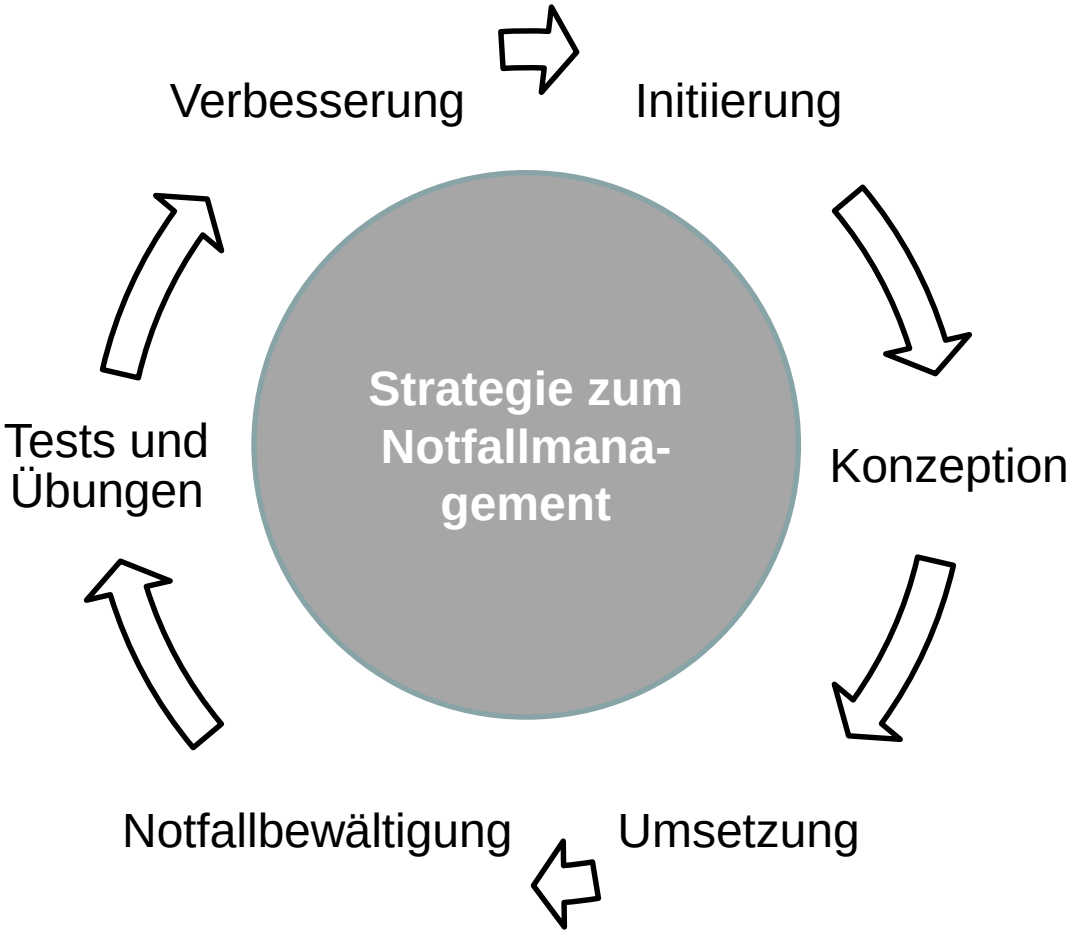
- ✓ Ein funktionierendes ISO 9001 konformes QM-System bringt viele Zertifizierungsanforderungen für IT-Grundschutz mit.
- ✓ Die wichtigsten sind:
  - Dokumentenlenkung
  - Freigabeprozesse
  - Prozessdenken
  - Interner Auditplan mit Managementreport
  - Sensibilität für Korrektur- und Vorbeugemaßnahmen
- ✓ Durch die Privatisierung der IT-GS Zertifizierung sind möglicherweise zukünftig auch Kombizertifikate möglich.

Ein ISMS nach Grundschutz in ein funktionierendes QM zu integrieren spart circa 40% Aufwand.

Schnittstellen zwischen ISMS und Business Continuity

BCM UND ISMS

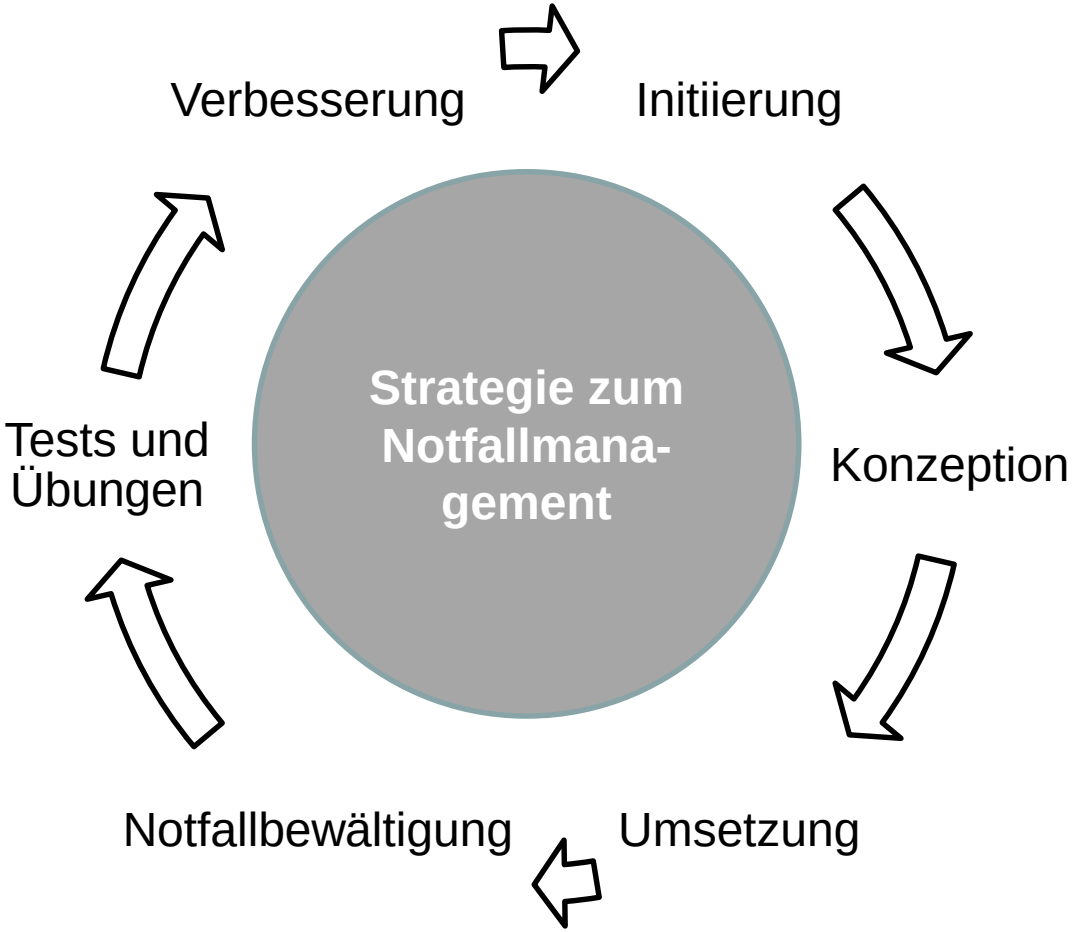
Der Business-Continuity Management Prozess



Die Normen zum BCM

- ✓ International: BS 25999 – Business Continuity Management
  - ➢ Part 1: Code of Practice
  - ➢ Part 2: Specification
- ✓ Generell zertifizierfähig durch lizenzierte Auditoren und Zertifizierungsgesellschaften.
- ✓ Deutsche Norm: BSI-Standard 100-4 – Notfallmanagement

Schnittstellen zum ISMS-Prozess



Schnittstelle zum ISMS ergibt sich aus:

- Leitlinie zur Initiierung nötig
- Konzeption verlangt eine Risikoanalyse
- Umsetzung verlangt konkreten Maßnahmenplan
- BCM nutzt den Dokumentenüberba u

Bezug zur ISO 27001, Anhang A14

A.14.1 Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs(Business Continuity Management)

- ✓ **Ziel:**
  Schutz vor Unterbrechungen von Geschäftsaktivitäten, und um kritische Geschäftsprozesse vor den Auswirkungen größerer Störungen von Informationssystemen oder vor Katastrophen zu schützen und ihre rechtzeitige Wiederaufnahme sicherzustellen.

- ✓ Diese Anforderungen erfüllt ein Business Continuity Management System.

Zusammengefasst

- ✓ Informationssicherheit umfasst nicht nur den Schutz der **Vertraulichkeit**, sondern auch der **Verfügbarkeit** und **Integrität**
- ✓ Somit ist ein integriertes ISMS und ein integriertes BCM alternativlos.
- ✓ Korrektes BCM geht über die eigentliche Norm des IT-Notfallmanagements hinaus.
- ✓ BCM entwickelt ganzheitliche Strategien zur Geschäftsfortführung

SCHNITTSTELLE DATENSCHUTZ

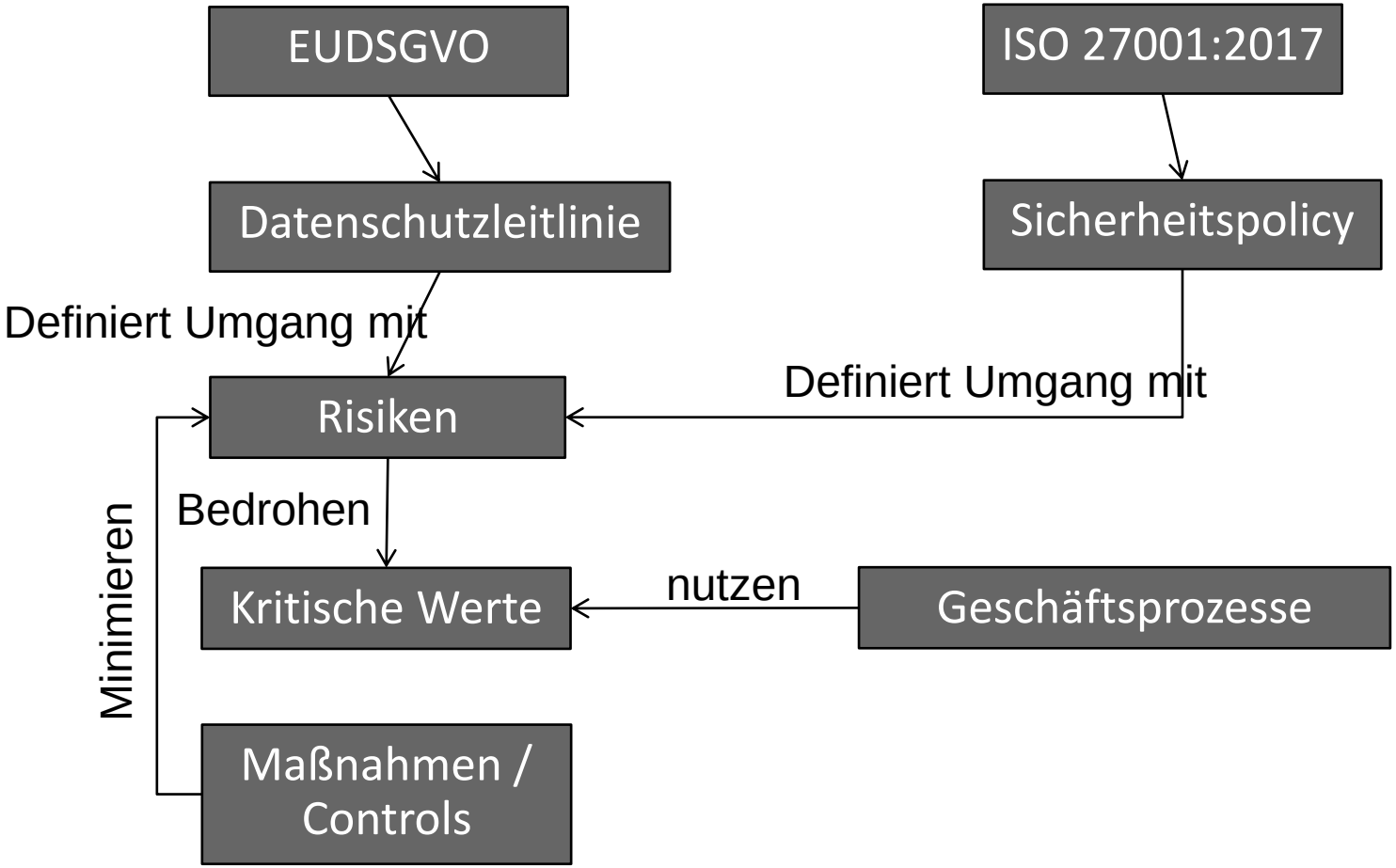
Allgemeines

- ✓ Datenschutz und Informationssicherheit ergänzen sich.
- ✓ Datenschutz bezieht sich auf den Schutz der personenbezogenen Daten **natürlicher** Personen. Er ist gesetzlich normiert.
- ✓ Informationssicherheit bezieht sich auf den Schutz **aller Daten und Informationen natürlich und juristischer Personen**.
- ✓ **Es gilt:** Kein Datenschutz ohne Informationssicherheit, keine Informationssicherheit ohne Datenschutz.
- ✓ Das ISMS legt in jedem Fall einen guten Grundstein für funktionierenden Datenschutz.

Die Rechte der Aufsichtsbehörden

- ✓ Datenschutz und seine Einhaltung wird durch den zuständigen Landesbeauftragten für den Datenschutz geprüft.
- ✓ Aufsichtsbehörden können jederzeit die Einhaltung der Datenschutzgesetze prüfen.
- ✓ Die Datenschutzbehörden werden meist tätig auf Antrag oder Anzeige einer Person, die sich in Ihrer informationellen Selbstbestimmung beeinträchtigt fühlt.
- ✓ Die Datenschutzbehörden können Unternehmen nicht stilllegen, aber empfindliche Strafen verhängen.

Datenschutz und das ISMS - Zusammenhänge



ISO 20000 – Entwicklung und Bezug zu ISO 27001 und IT-GS

ISMS UND IT-MANAGEMENT

Grundlagen der ISO 20000-1:2005

- ✓ Basis der ISO 20000 ist der PDCA-Zyklus
- ✓ Scope ist die strukturierte Leistungserbringung einer IT-Service Organisation
- ✓ Enger Bezug zur ISO/IEC 27001
- ✓ Hilfsmittel zur Umsetzung von Maßnahmen (auch IT-GS)

ISO 20000-1:2005
Service management - Specification

ISO 20000-2:2005
Service management – Code of Practice

Zusammenhang einzelner Kapitel

ISO 20000-1	IT-Grundschutz (11. EL)
Service Level Management	B 1.16 – Anforderungsmanagement
Capacity Management	Spezielle Maßnahmen der einzelnen Bausteine
Information Security Management	Gesamte Norm
Incident Management	B 1.8 – Behandlung von Sicherheitsvorfällen
Problem Management	B 1.9 – Hard- und Softwaremanagement
Configuration Management	B 1.10 - Standardsoftware
Change Management	B 1.14 – Patch- und Änderungsmanagement
Release Management	B 1.10 - Standardsoftware

Ein funktionierendes Managementsystem nach IT-Grundschutz unterstützt und ergänzt ein IT-Servicemanagement und umgekehrt.

UMSETZUNGSPLANUNG

Erfolgskriterien der Umsetzung

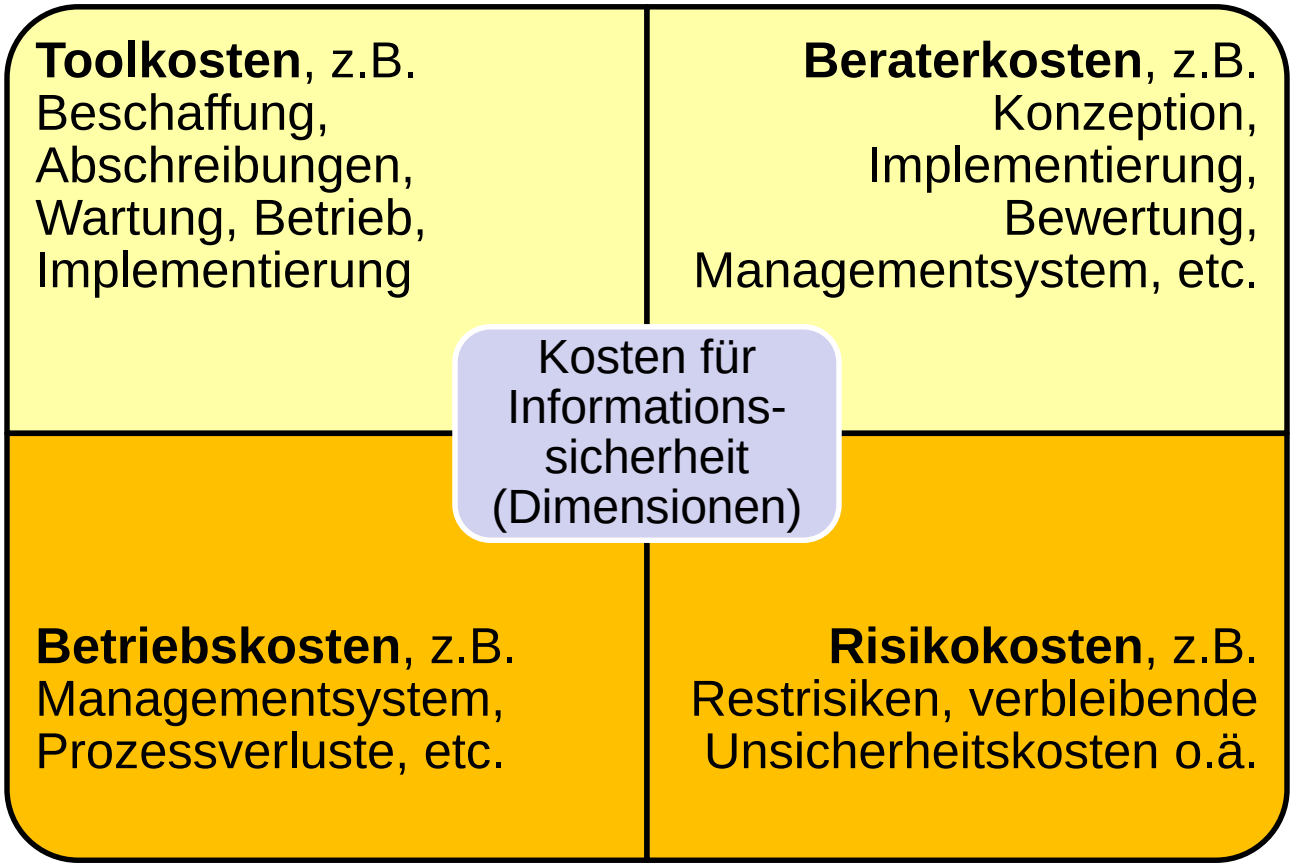
- ✓ Jede Umsetzung von Informationssicherheit scheitert, wenn **Kosten und Nutzen sich nicht die Waage** halten.
- ✓ Jede Umsetzung scheitert, wenn **Ziele nicht im Vorfeld klar definiert** sind.
- ✓ Jede Umsetzung ist multidimensional strukturiert, Abhängigkeiten müssen beachtet werden, zum Beispiel
  - ➢ Auswirkungen auf die Strategie
  - ➢ Auswirkungen auf die Produktion
  - ➢ Auswirkungen auf das Betriebsklima
  - ➢ Auswirkungen auf Prozesse

Informationssicherheit darf nie unwirtschaftlich werden und soll die Geschäftsziele unterstützen.

Daher: Sicherheitskostencontrolling

- ✓ Wichtiger Faktor, um kaufmännische Auswirkungen und reale Ergebnisse gegenüberzustellen.
- ✓ Zu berücksichtigen sind indirekte und direkte Kosten und Nutzen der Informationssicherheit
- ✓ Idealerweise wird ein Vier-Dimensionen-Modell angewendet, um die Kosten zu überwachen.
- ✓ Ferner sollten auch positive Effekte mit hineinkalkuliert werden.
- ✓ **Wirtschaftlichkeit ergibt sich immer aus mehreren Faktoren!**

Beispiel: Kostendimensionen



Direkte Kosten

Indirekte Kosten durch externe Effekte

Beispiel: positive und negative Effekte

ISMS-Auswirkungen	Positive Effekte	Negative Effekte
Produktion	• Verringerung von Ausfällen der IT • Minimierung von Ausfällen wg. Integritätsfehlern	• Verringerung der Produktivität durch Sicherheitsmaßnahmen
Verwaltung	• Verhinderung von Wissensabfluss • Geringere Schäden durch unsichere IT-Nutzung	• Verschlechterungen des Betriebsklimas • Juristische Schwierigkeiten bei Eingriffen in die Arbeitswelt
Externe Parteien	• Erhöhung des Vertrauens in das Unternehmen • Potenziell bessere Finanzierungs-konditionen	• Erhöhtes Ziel für externe Angreifer

Zusammenfassung

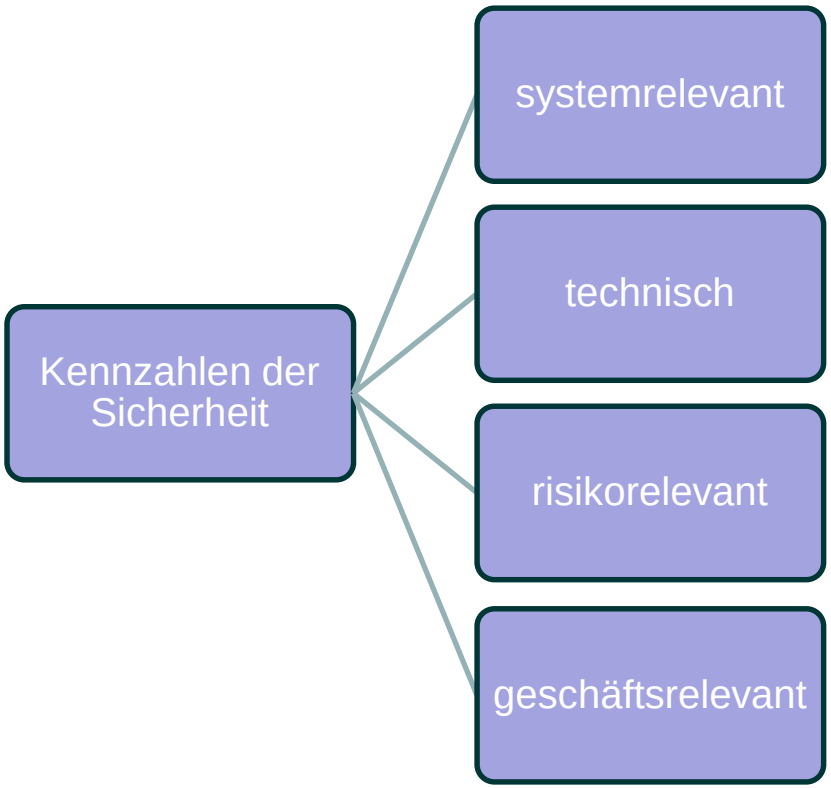
- ✓ Informationssicherheit verursacht Kosten- und Nutzeneffekte (positive und negative Effekte)
- ✓ Um die Wirksamkeit und den Aufwand gegenüberzustellen, sollten alle Dimensionen einbezogen werden.
- ✓ **Informationssicherheit wandelt sich vom technischen Konzept hin zu einer strategischen Aufgabe, die auch im Controlling ihre Berechtigung hat.**

KPI UND REIFEGRADE

KPI-Definitionen – Was ist ein KPI?

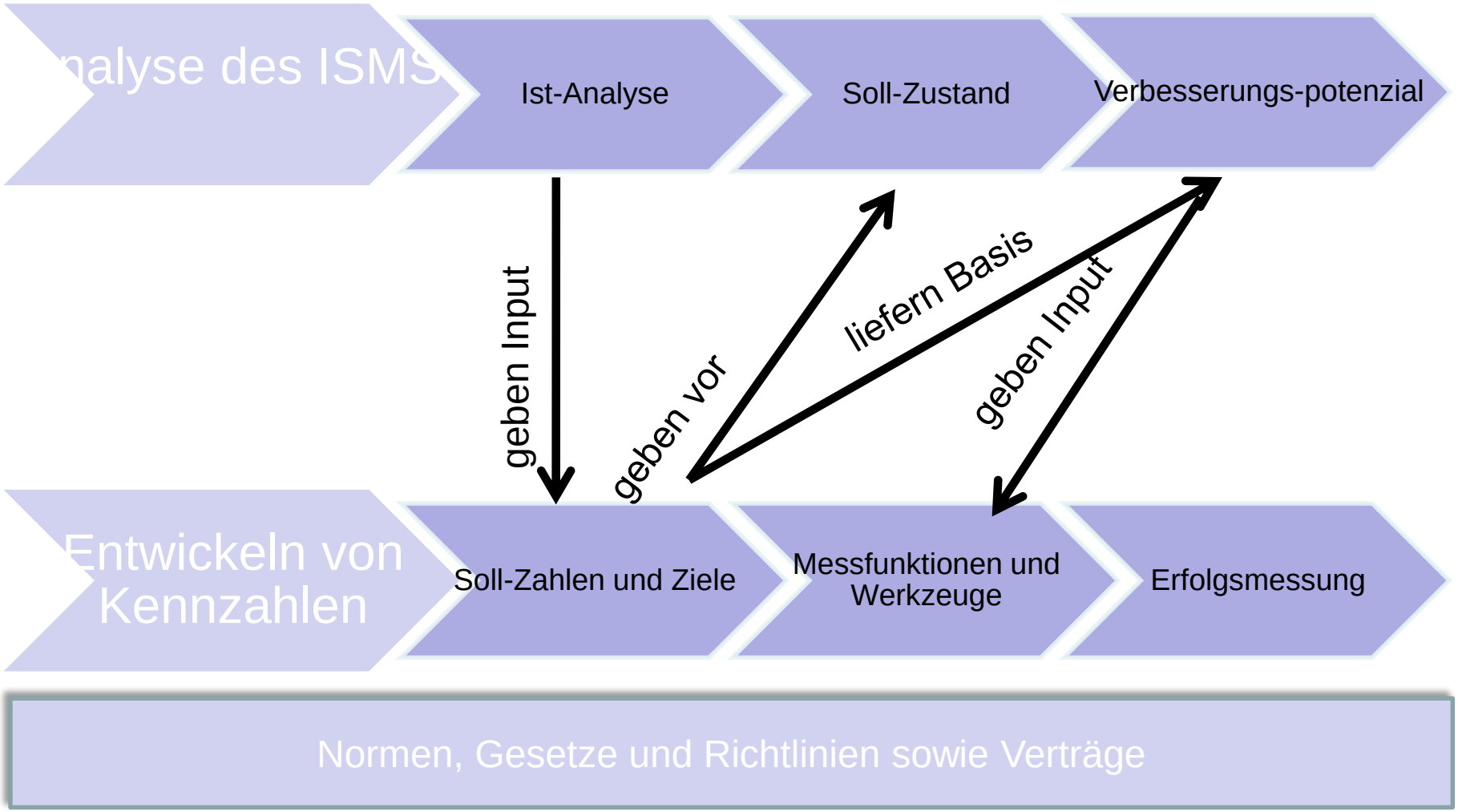
- ✓ KPI = Key Performance Indikator
- ✓ Ziel: Steuerung der Informationssicherheit mittels Kennzahlensystematik
- ✓ Herausforderung: Wie soll Sicherheit aussagekräftig gemessen werden?
- ✓ Welche Dimensionen sind bei der Kennzahlenentwicklung zu berücksichtigen?

Kennzahlendimensionen



- ✓ Berücksichtigen aller relevanten Eingabedimesionen
- ✓ Verlassen der Ebene „Primat der Technik“
- ✓ Analystisch – strukturierter Ansatz zum Finden von Kennzahlen

Kennzahlenentwicklung - Ablauf



Kennzahlenbeispiele

- ✓ Prozentualer Anteil der geschulten Mitarbeiter an der Gesamtheit der Mitarbeiter
- ✓ Absolute Menge der Informationssicherheitsverstöße durch Stakeholder
- ✓ Prozentualer Anteil der geschulten Lieferanten und Dienstleister an der Gesamtheit der Lieferanten und Dienstleister
- ✓ Absolute Höhe der Kosten durch Informationssicherheitsvorfälle
- ✓ Prozentualer Anteil des Verbrauchs des genehmigten Budgets für Informationssicherheit
- ✓ Absolute Anzahl von meldepflichtigen Informationssicherheitsvorfällen
- ✓ Kritische Prozesse und Systeme sind durch ein Risikomanagement abgedeckt
- ✓ Die geplanten internen Audits wurden vollständig durchgeführt

Reifegradermittlung

- ✓ Kennzahlen ermöglichen, die „Reife“ der Informationssicherheit festzustellen und zu steuern.
- ✓ Ein Reifegrad beschreibt die Fähigkeit, ein bestimmtes Management-Modell wiederholbar umzusetzen.
- ✓ Reifegrade sind in verschiedenen Normen definiert: CoBIT, CMMI, usw.
- ✓ Der Reifegrad eines ISMS beschreibt die Fähigkeit, Informationssicherheit so definiert und dokumentiert zu haben, dass Sie für neue Mitarbeiter in der Organisation lebbar ist.

Zusammenfassung

- ✓ Kennzahlen für die Erfolgsmessung der Informationssicherheit zu definieren ist ein Prozess
- ✓ Audits allein genügen nicht als Messer für die Reife eines Managementsystems – das ist nicht das Ziel
- ✓ Mit aussagekräftigen Kennzahlen kann der Reifegrad gemessen werden.
- ✓ Ein Reifegradmodell ermöglicht die Steuerung des Managementsystems und die kontinuierliche Verbesserung.

INTERNES AUDITING

Internes Auditing - Vorbereitung

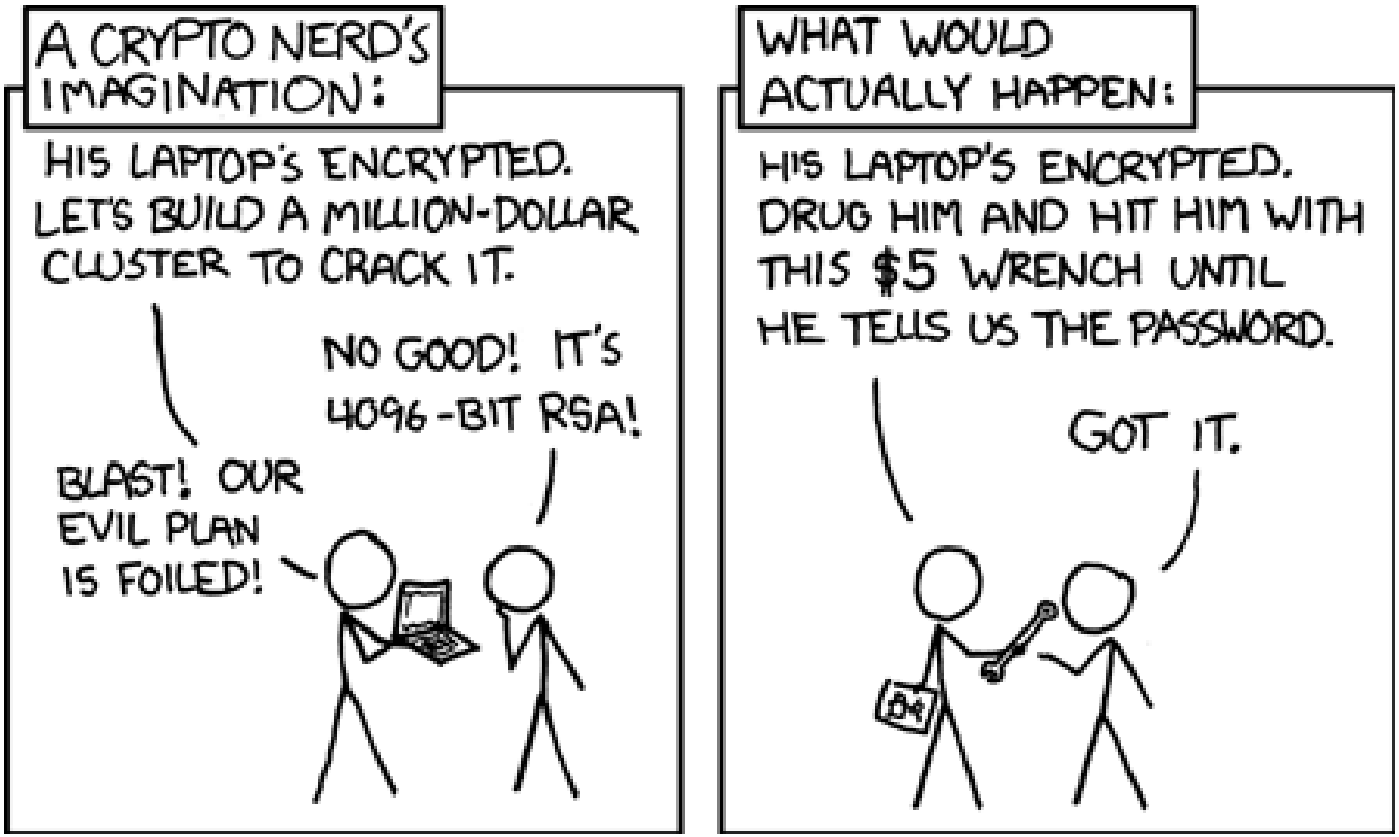
- ✓ **Bei bestehendem QM-System:** Abstimmung mit QM-Leitung und einbinden in den Auditplan
- ✓ Ermitteln von Schwachstellen oder neu eingeführten Maßnahmen
- ✓ Zusammenstellen eines Auditablaufes und Fragenkataloges
- ✓ Interviewpartner ermitteln
- ✓ Vorgaben für Auditbericht mit QM-Leitung abstimmen

Internes Auditing - Ablauf

- ✓ **Wie bei externem Audit – Vorankündigung**
- ✓ Vorstellung und Auftaktgespräch mit Abteilungs- oder Standortleitung
- ✓ Begehung von Abteilung und Standort mit Begleiter
- ✓ Durchführen der Audithandlungen
- ✓ Tagesfeedback an Standortleiter
- ✓ Berichtserstellung

Interne Audits sind Bestandteil eines funktionierenden PDCA-Zyklus. Ohne Managementbericht ist niemals eine Auditreife da.

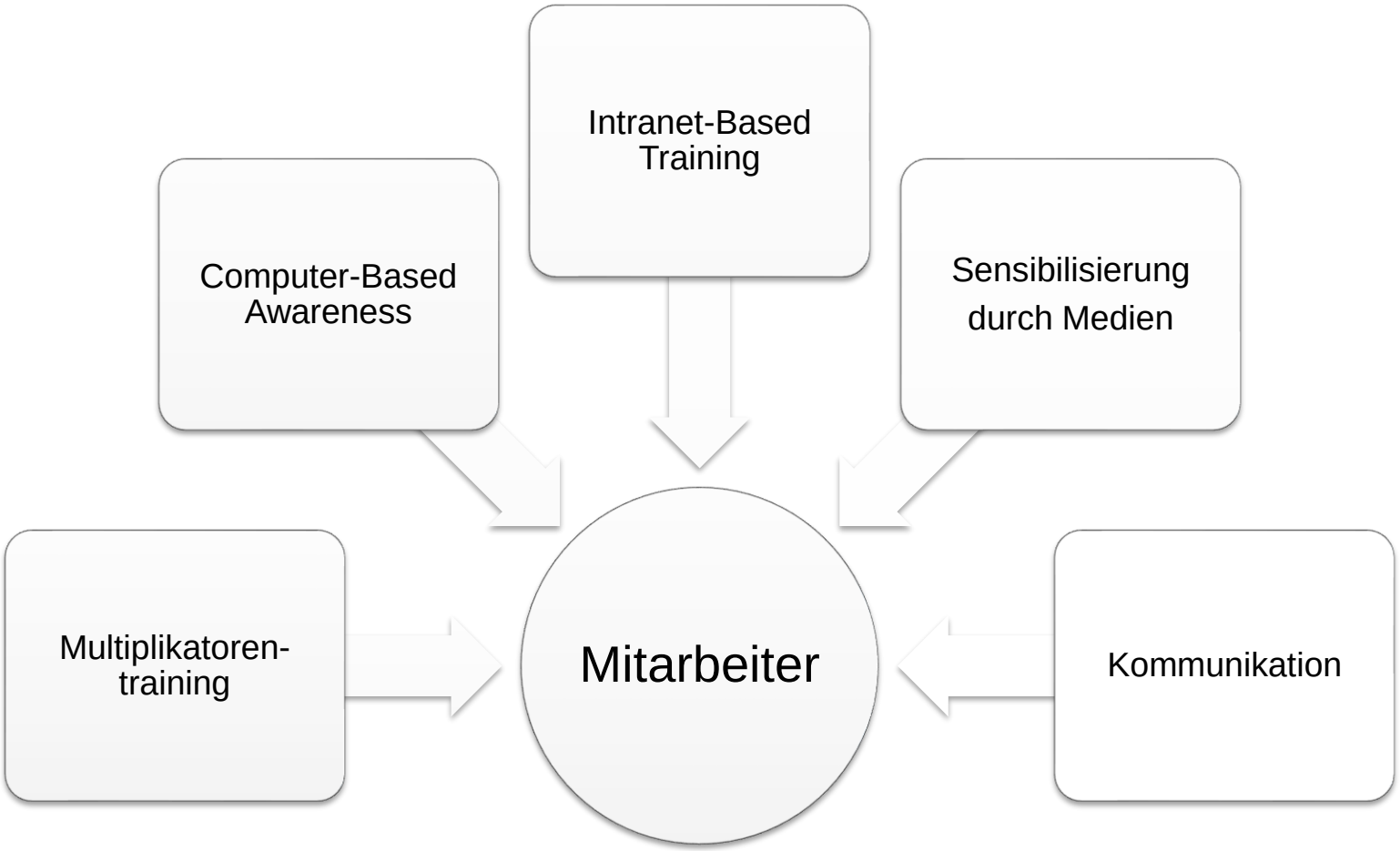
AWARENESS UND ISMS-BETRIEB


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Zielsetzung

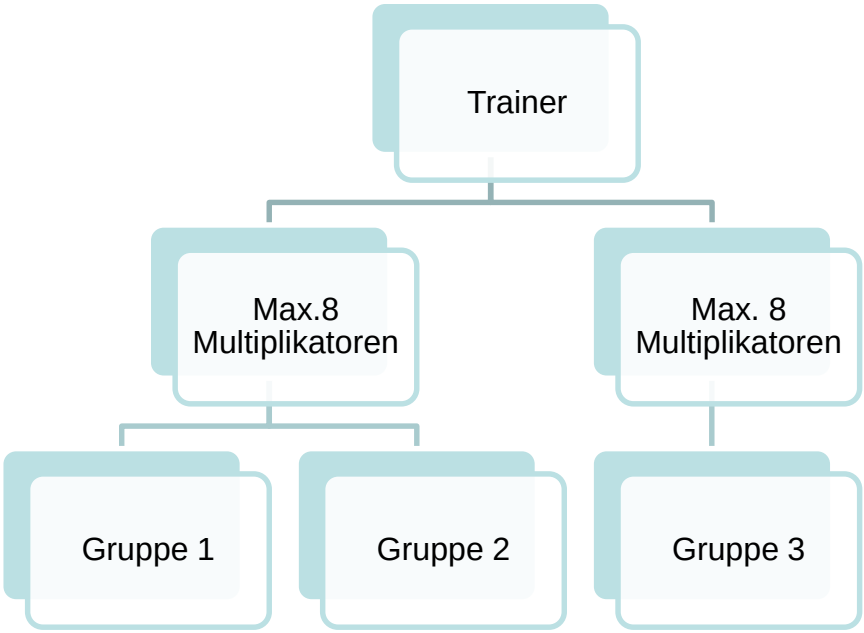
- ✓ Schließen der Sicherheitslücke Mensch durch Schulung und Sensibilisierung
- ✓ Erhöhen des Sicherheitsniveaus des Unternehmens jenseits der Technik
- ✓ Einbeziehen aller Mitarbeiter in die Sicherheitsstrategie
- ✓ Prävention gegen Social Engineering

Methodenauswahl



Multiplikatorentraining

- Untergliedern der Belegschaft in kleine Gruppen
- Schulung von maximal acht „Gruppensprechern“ (Multiplikatoren) in einer Gruppe
- Schulen der Multiplikatoren auf Themen und Umgang mit Schulungsmaterial
- Entwickeln von Schulungsmaterial



Computer-/ Intranet-Based-Awareness

- Einbinden der Maßnahme in den IT-gestützten Arbeitsalltag
- Nutzung von Medien, Figuren oder einfachen Informationen
- Einbindung in klassische CBT-Software oder vorhandenes Intranet

- Vorteile:
  - Direkte Wirkungskontrolle z.B. bei Fragenkatalogen o.ä.
  - Kein Medienbruch
  - Schnelle Aktualisierungsmöglichkeiten
  - Hohe Verbreitung
- Nachteile:
  - Hoher Grad an Freiwilligkeit
  - Gefahr der Nicht-Nutzung aufgrund von zuviel Tagesgeschäft

Sensibilisierung durch Medien

- Integration der Sensibilisierung in den täglichen Alltag
- Häufige Wiederkehr, z.B. auf Arbeitsmitteln wie Blocks, etc.
- Ansprechen des eigenen Alltags, z.B. im Video
- Bezug zum Privaten, z.B. beim Virenschutz

Plakataktion der Deutschen Post AG

B3S

- ✓ Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus
- ✓ B3S ist in 9 Abschnitte aufgeteilt

Aufbau des B3S

Kapitel	Beschreibung
0 – 3	Allgemeine Kapitel und informative Hinweise. Einführung Branchenspezifischer Sicherheitsstandart
Kapitel 4 – Risikomanagement in der Informationssicherheit	Bezug zur ISO 27001. Management Anforderungen, Risikoidentifikation und Bewertung. Kritikalität
Kapitel 5 – Branchenspezifischer Geltungsbereich	Beschreibt wie der Geltungsbereich definiert werden muss.
Kapitel 6 – Bedrohungsszenarien	Beschreibt die Gefährdungen Kritischer Branchenspezifischer Technik und Software. Bezug zur DIN EN 80001-1

Aufbau des B3S

Kapitel	Beschreibung
Kapitel 7 – Angemessene Maßnahmen zur Umsetzung	Beschreibt die Maßnahmenempfehlungen nach Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik Und Orientiert sich an dem Anhang A von der ISO 27001 (172 Maßnahmen)
Kapitel 8 – Übersicht der referenzierten Normen und Standards	
Kapitel 9 – Glossar	

Welche Dokumente sind notwendig?

Das B3S erfordert die Folgenden Dokumente in Schriftlicher Form

- Anwendungsbereich des ISMS
- IT-Sicherheitspolitik und -ziele
- Methodologie zu Risikoeinschätzung und Risikobehandlung
- Erklärung zur Anwendbarkeit
- Plan zur Risikobehandlung
- Bericht zur Risikoeinschätzung
- Aufzeichnungen zu Schulungen, Fähigkeiten, Erfahrung und Qualifikationen
- Ergebnisse der Überwachung und Messung
- Programm für interne Audits
- Ergebnisse der internen Audits
- Ergebnisse der Managementbewertung
- Ergebnisse der Korrekturmaßnahmen
- Logs zu Nutzeraktivität, Ausnahmen und Sicherheitszwischenfällen
- Definition von Sicherheitsrollen und Verantwortlichkeiten
- Inventar der Werte
- Tolerierbare Nutzung der Werte
- Zugangssteuerungsrichtlinie
- Durchführungsverfahren für das IT-Management
- Prinzipien für die Entwicklung sicherer Systeme
- Sicherheitspolitik für Zulieferer
- Verfahren für Vorfallmanagement
- Verfahren für betriebliches Kontinuitätsmanagement

Nachweisen gemäß $8a (3)