Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

Information Security Management
01 Standards & Frameworks I (ISO, BSI)

HSLU – Informatik

Mathias Bücherl (M.Sc.)

Tel. +41 79 746 10 98

mathias.buecherl@hslu.ch

Material von Prof. Dr. Fischer, Prof. Armand Portmann und Oliver Hirschi

Ziele

- Sie kennen die wichtigsten Standards der Informationssicherheit
- Sie finden sich in den Standards ISO 27001 und 27002 zurecht
- Sie kennen die Grundzüge der BSI-Standards (BSI=Bundesamt für Sicherheit in der Informationstechnik, Deutschland)

AGENDA

1. **Kurze Einführung ISMS**
2. ISMS nach ISO 27001
3. Best Practise nach ISO 27002
4. Ergänzende Standards ISO 27003 und 27004
5. Risikoanalyse nach ISO 27005
6. Die BSI-Standards 200-x
7. Kombinierte Risiko-Analyse nach BSI 200-3

Informationssicherheit: Womit?
Die drei Säulen der Informationssicherheit

Technik

kaufen
konfigurieren

Prozesse

definieren
kontrollieren

Menschen

sensibilisieren
ausbilden

Verantwortung

- Fehlende Informationssicherheit kann den Geschäftsfortgang stören oder verunmöglichen
- Der Schutz der Informationen gehört zur Sorgfaltspflicht des Managements
- Verantwortung kann nicht delegiert werden!

  „Wer die Erfüllung einer Aufgabe befugterweise einem anderen Organ überträgt, haftet für den von diesem verursachten Schaden, sofern er nicht nachweist, dass er bei der Auswahl, Unterrichtung und Überwachung die nach den Umständen gebotene Sorgfalt angewendet hat.“
  (OR Art. 754 Absatz 2)

Die Überwachung der Informationssicherheit ist Chefsache!

Ohne Management-Support geht gar nichts!

- Keine Ressourcen (Zeit und Geld)
- Keine Kompetenzen (Befehls- und Umsetzungsgewalt)
- Keine Priorität

Das Management trägt die Risiken und entscheidet über die eingesetzten Ressourcen!

Oft gehörte Sicht des Managements

- Was bringt uns Informationssicherheit?
  …ausser Kosten?
- Wir haben ja schon eine Firewall, …oder wie das Ding auch immer heisst?
- Unser Unternehmen ist kein lohnendes Ziel für Hacker!
- Bei uns ist noch nie etwas passiert!
- Unsere Mitarbeiter sind 100% loyal!
- Wir können auf unsere Computer problemlos einige Tage verzichten!

Was passiert, wenn wir nichts machen?

- Kompletter Datenverlust führt in über 50% der Fälle zum Konkurs innert 24 Monaten
- Die Beschaffung und der Aufbau eines Standard-Ersatzsystems dauert mindestens 36h (falls kein Ersatzsystem direkt vor Ort verfügbar)
- Datendiebstahl (wird in den wenigsten Fällen bemerkt)
- Kommen vertrauliche Daten an die Öffentlichkeit, ist der Image-Verlust bei den Kunden je nach Unternehmen immens
- Verletzung gesetzlicher Vorgaben kann strafrechtliche Folgen haben
- Verletzung der Sorgfaltspflicht

Einführung ISMS

- Definition

  Ein *Information Security Management System* beschreibt Regeln und Verfahren für eine Unternehmung, welche den Zweck haben, Informationssicherheit mithilfe eines Prozesses zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und kontinuierlich zu verbessern
- Motivation, Zweck
  - Sicherheit erhalten, dass Vermögenswerte und Informationen der Unternehmung („Assets“) angemessen geschützt sind
  - Rechtliche und regulatorische, aber auch Branchen- und Marktanforderungen erfüllen

Einführung ISMS

Vorgehen

- Einen Prozess unterhalten, mit dem Informations-sicherheitsrisiken identifiziert und bewertet, sowie Kontrollen bestimmt, eingeführt und kontinuierlich verbessert werden können
- Dies setzt voraus, dass der Schutzbedarf von Vermögenswerten bestimmt, Schutzmassnahmen eingeführt und Kontrollen definiert werden
- Verschiedene Standards machen Vorgaben für den Aufbau eines ISMS

Nutzen von Standards

- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____

AGENDA

1. Kurze Einführung ISMS
2. **ISMS nach ISO 27001**
3. Best Practise nach ISO 27002
4. Ergänzende Standards ISO 27003 und 27004
5. Risikoanalyse nach ISO 27005
6. Die BSI-Standards 200-x
7. Kombinierte Risiko-Analyse nach BSI 200-3

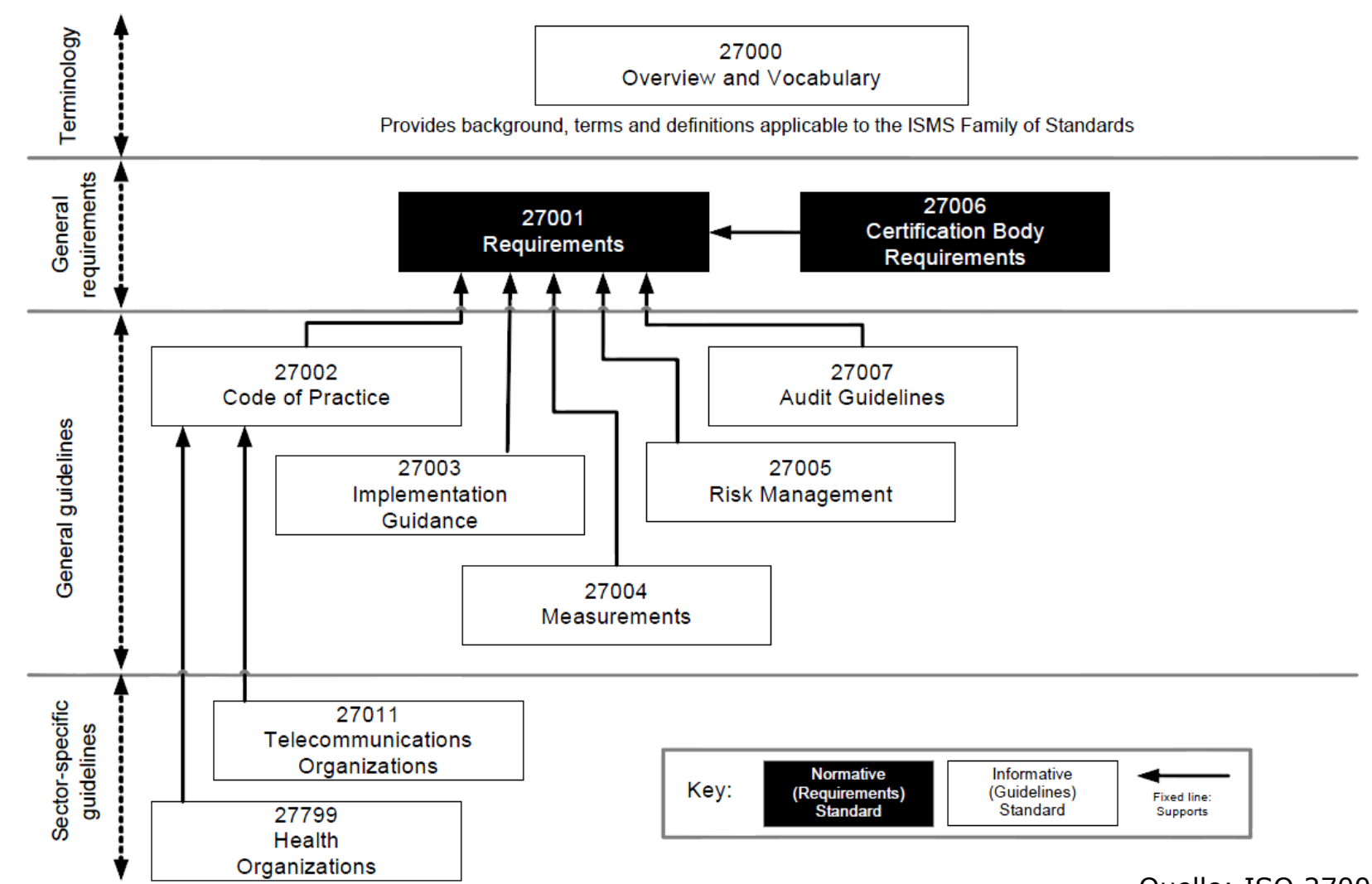
Übersicht über die wichtigsten ISO-Standards

Es gibt über 50!

- **ISO 27000:2018**
  ISMS – Overview and vocabulary
- **ISO 27001:2015**
  ISMS – Requirements
- **ISO 27002:2013**
  Code of practice for information security controls
- **ISO 27003:2017**
  ISMS implementation guidance
- **ISO 27004:2016**
  Information security management - Measurement
- **ISO 27005:2018**
  Information security risk management

http://www.iso27001security.com/

Überblick über die ISO 27000 Standard-Reihe



Quelle: ISO 27000

ISO 27000
ISMS – Overview and vocabulary

- Definiert Begriffe, welche in der ISO 27000 Standard-Reihe verwendet werden
- Definiert und erläutert kurz, was ein Information Security Management System (ISMS) ist
- Erklärt den dazu verwendeten Prozess-Ansatz „Plan – Do – Check – Act“
- Gibt einen Überblick über die ISO 27000 Standard-Reihe

Video-Teaser

- Aufbau: https://youtu.be/wbg9-ybqCIo

ISO 27001
ISMS – Requirements

- Definiert Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems
- Wurde aus dem britischen Standard BS 7799-2:2002 entwickelt und als ISO-Norm im Jahr 2005 veröffentlicht
- Definiert den Sicherheitsprozess nach dem Prozess-Ansatz „Plan – Do – Check – Act“ (PDCA)
  - Dieses Vorgehensmodell wird in ISO 27001:2013 nicht mehr explizit erwähnt, da es auch andere Ansätze gibt, um einen Sicherheitsprozess zu modellieren
  - Stellvertretend für solche Ansätze wird der PDCA-Ansatz in der Vorlesung aber trotzdem vorgestellt

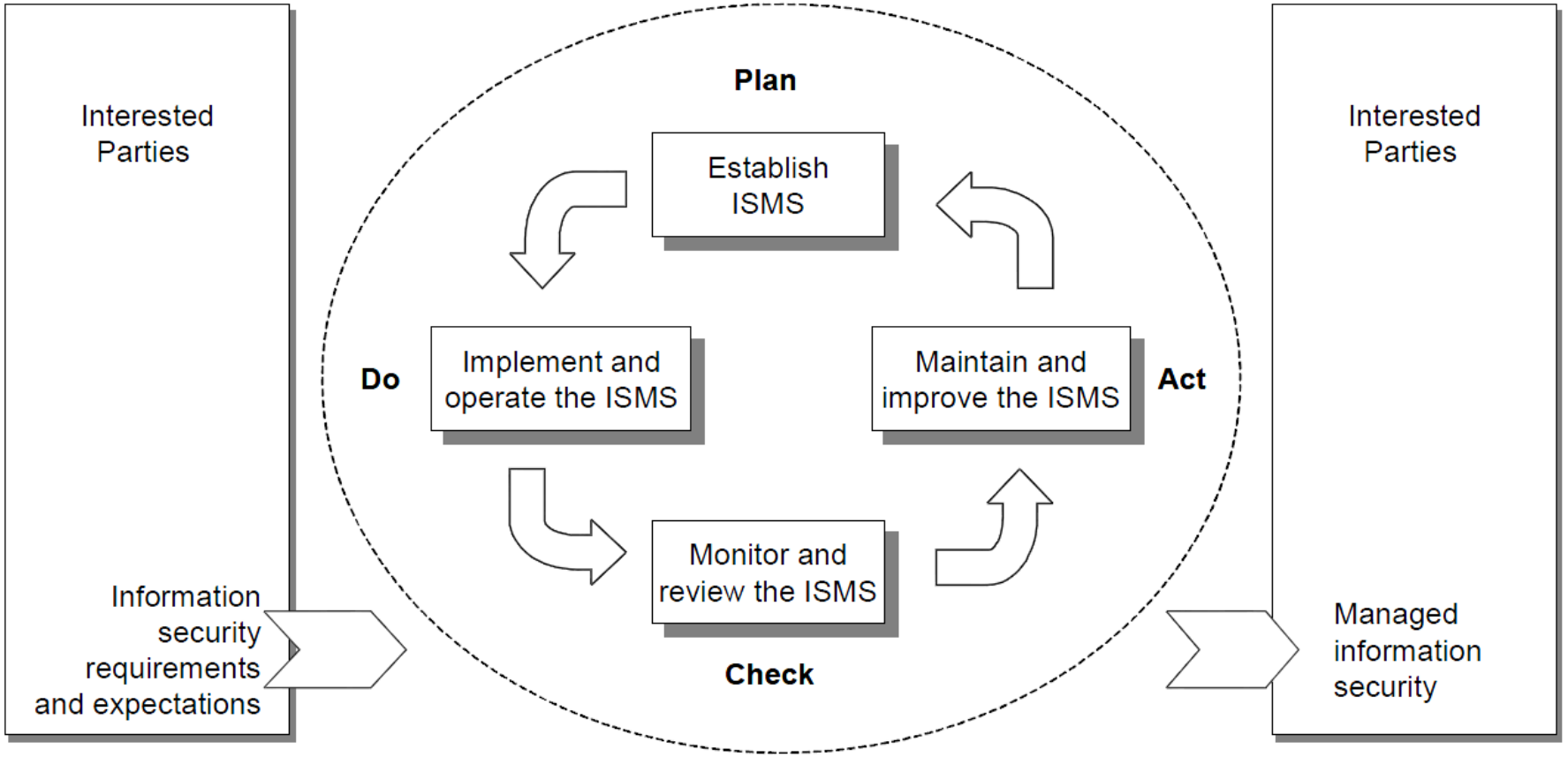
ISO 27001
ISMS – Requirements

- Definiert in Anhang A Ziele und Massnahmen zur Verbesserung der Informationssicherheit (die Ziele und Massnahmen sind aus ISO 27002 entlehnt)
- Eine Firma kann sich nach ISO 27001 zertifizieren lassen

ISO 27001
ISMS – Requirements

- Freiheitsgrade beim Aufbau eines ISMS
  - „Scope“: Bereich, über den sich das ISMS erstreckt
    - Ganze Firma
    - Eine Abteilung
    - Ein Standort
    - Ein Teil der Infrastruktur: z. B. die DMZ
    - Etc.
  - Kontrollziele und Steuerungen («Controls» aus ISO 27002), welche vom ISMS berücksichtigt werden („Statement of Applicability“, SOA)
- „Scope“ und „Statement of Applicability“ definieren den Umfang einer Zertifizierung nach ISO 27001

Prozess ISMS nach ISO 27001

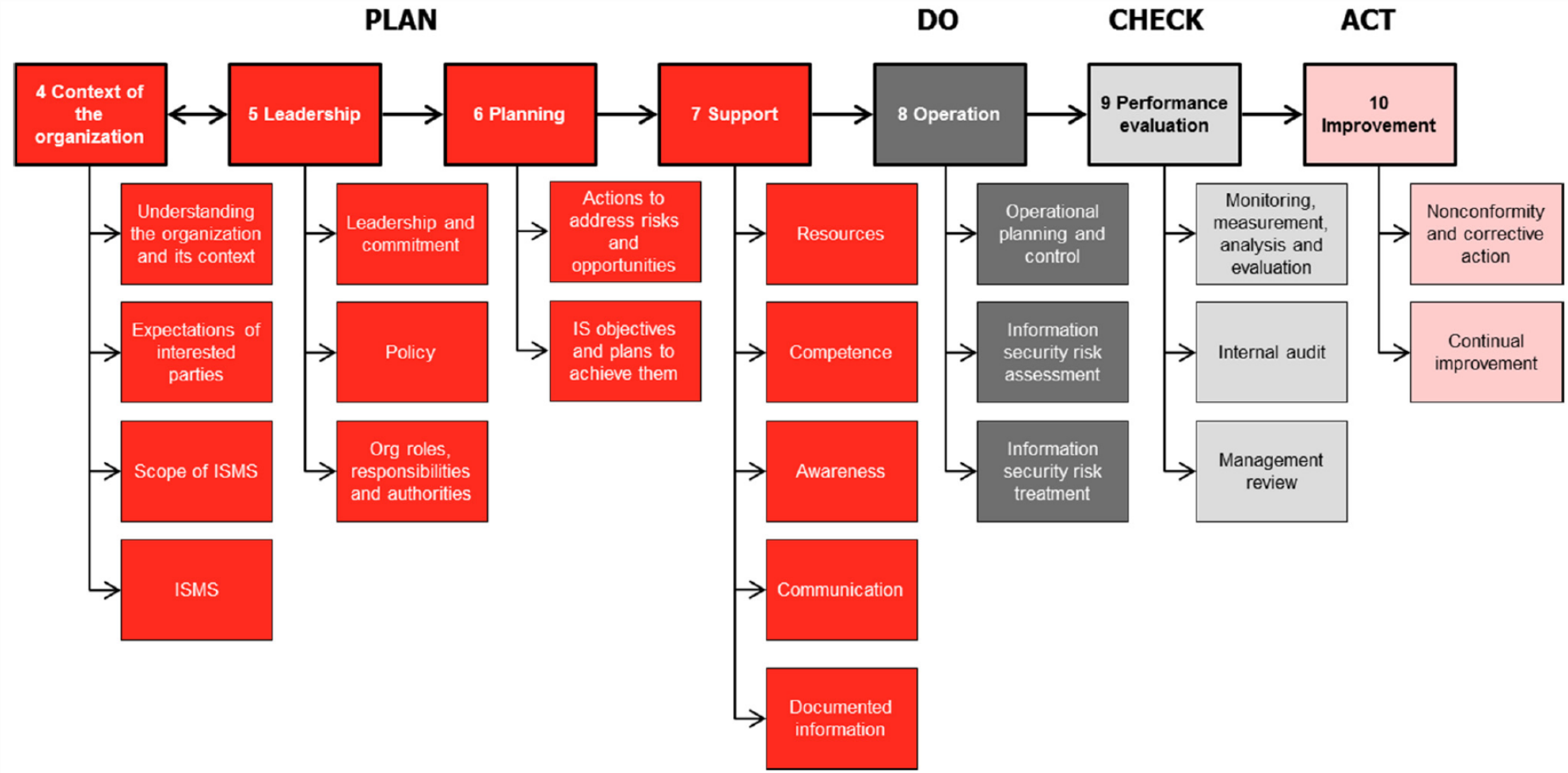


Quelle: ISO 27001

Plan-Do-Check-Act nach ISO 27001

- **Planen (Erstellung des ISMS)**
  Erstellung der jeweils für das Risikomanagement und zur Informationssicherheitsverbesserung relevanten ISMS-Richtlinien, Zielsetzungen, Prozesse und Prozeduren zur Erzielung von Ergebnissen gemäss den Gesamtrichtlinien und -zielsetzungen einer Organisation.
- **Machen (Einführung und Durchführung des ISMS)** Einführung und Durchführung der ISMS-Richtlinien, -Steuerungsmassnahmen, -Prozessen und -Prozeduren.
- **Prüfen (Überprüfung und Revision des ISMS)**
  Beurteilung und, wo massgebend, Messung des Prozesserfolgs gegenüber den ISMS-Richtlinien, -Zielsetzungen und praktischen Erfahrungen, sowie Berichterstattung über die Ergebnisse an das Management zwecks Revision.
- **Handeln (Wartung und Verbesserung des ISMS)**
  Ergreifung korrigierender und vorbeugender Massnahmen, basierend auf den Ergebnissen des ISMS-Audits und der Management-Revision oder anderen relevanten Informationen zur Erzielung einer laufenden Verbesserung des ISMS.

PDCA-Zyklus abgebildet auf Kapitelstruktur von ISO27001



Quelle: Präsentation zum bsi ISO/IEC 27001 Launch Event, London, 27 November 2013

Video-Teaser

- Zusammenfassung: https://youtu.be/MmHO4apXCW8

AGENDA

1. Kurze Einführung ISMS
2. ISMS nach ISO 27001
3. **Best Practise nach ISO 27002**
4. Ergänzende Standards ISO 27003 und 27004
5. Risikoanalyse nach ISO 27005
6. Die BSI-Standards 200-x
7. Kombinierte Risiko-Analyse nach BSI 200-3

ISO 27002
Code of practice for information security mgmt.

- Standardwerk zum Thema Informationssicherheit, kurz oft CoP genannt
- Definiert 114 Steuerungsmassnahmen*) für den sicheren Umgang mit Informationen
- Zu jeder Massnahme sind Umsetzungsanleitungen angegeben, allerdings jeweils mit nur wenig Detailgrad
- Eine Zertifizierung nach ISO 27002 ist nicht möglich, da es keine harten Forderungen gibt (nur „sollte“-Formulierungen)
- Der Standard eignet sich sehr gut zur Umsetzung eines sog. Grundschutzes (Mindestanforderungen im Sicherheitsbereich)

*) auch Massnahmen oder Prüfpunkte genannt, engl. Controls

ISO 27002
Code of practice for information security mgmt.

- Ursprung: British Standard BS 7799-1:1999
- Später: Übernahme durch ISO als Norm ISO 17799:2000 und Überarbeitung im Jahr 2005 ➔ ISO 17799:2005
- 2007: Umbenennung zu ISO 27002:2007 (Wortgleich zu ISO 17799:2005)
- 2013: Überarbeitung ➔ ISO 27002:2013
- Adressierte Themen
  - Organisatorische, physische und logische Sicherheit
  - Anwendungsentwicklung und -unterhalt
  - Notfallvorsorge
  - Einhaltung und Überprüfung der Sicherheit
  - Etc.

Kapitel in ISO 27002

5. **Information security policies**
6. **Organization of information security**
7. **Human resource security**
8. **Asset management**
9. **Access control**
10. **Cryptography**
11. **Physical and environmental security**
12. **Operations security**
13. **Communications security**
14. **System acquisition, development and maintenance**
15. **Supplier relationships**
16. **Information security incident management**
17. **Information security aspects of business continuity management**
18. **Compliance**

14 Domänen

Kapitelstruktur von ISO 27002

9 Access control ← Eine von 14 Domänen

Eines von 35 Steuer.-zielen (engl. Control Objectives)

9.1 Business requirements of access control

Objective: To limit access to information and information processing facilities.

9.1.1 Access control policy

Control ← Eine von 114 Steuerungsmassnahmen, Prüfpunkte

An access control policy should be established, documented and reviewed based on business and information security requirements.

Implementation guidance

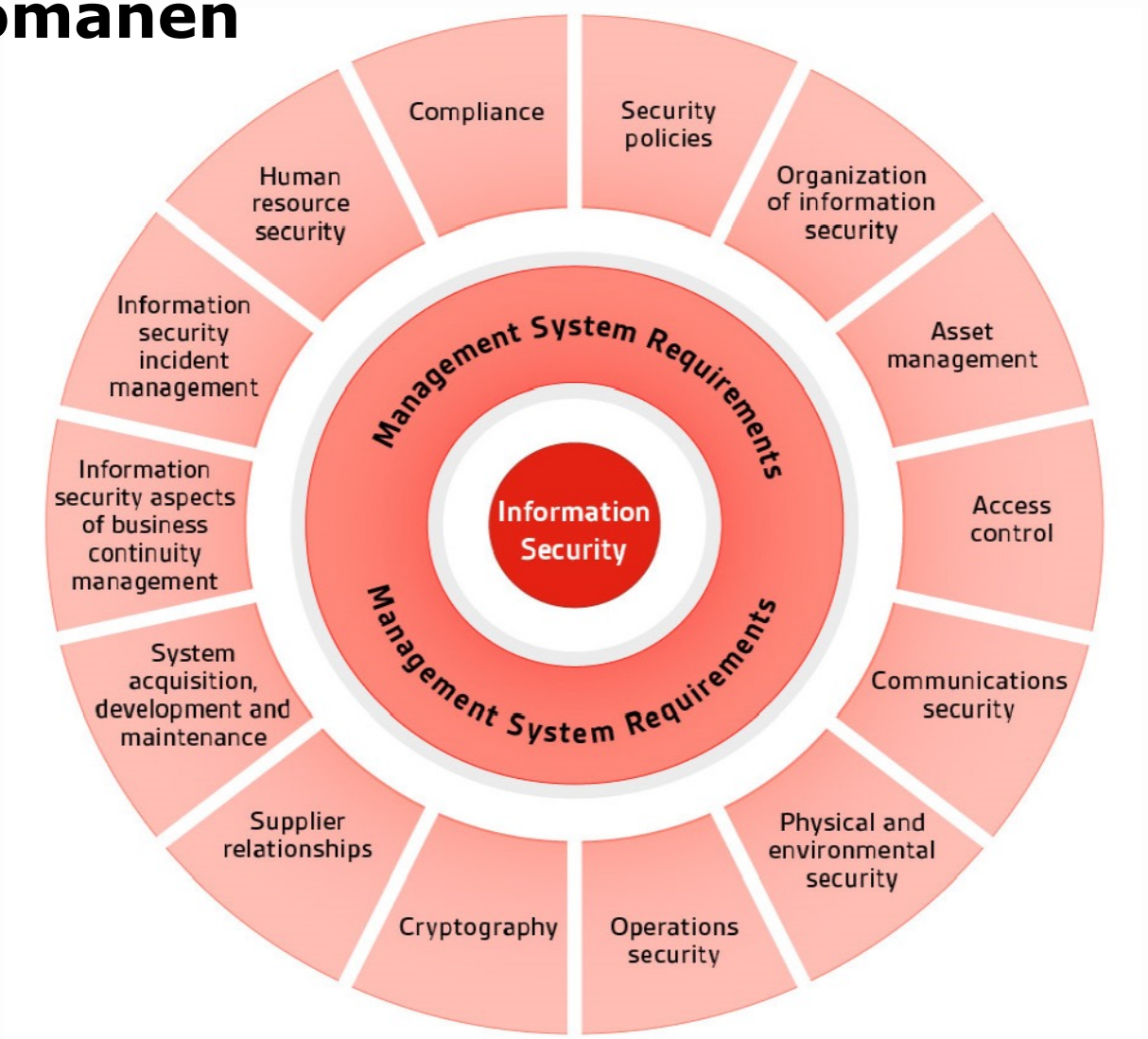
Asset owners should determine appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the associated information security risks.

Access controls are both logical and physical (see Clause 11) and these should be considered together. Users and service providers should be given a clear statement of the business requirements to be met by access controls.

The policy should take account of the following:

a) security requirements of business applications;

14 Domänen



Quelle: Präsentation zum bsi ISO/IEC 27001 Launch Event, London, 27 November 2013

AGENDA

1. Kurze Einführung ISMS
2. ISMS nach ISO 27001
3. Best Practise nach ISO 27002
4. **Ergänzende Standards ISO 27003 und 27004**
5. Risikoanalyse nach ISO 27005
6. Die BSI-Standards 200-x
7. Kombinierte Risiko-Analyse nach BSI 200-3

ISO 27003
ISMS implementation guidance

- Anleitung für die Entwicklung eines Implementierungsplans für ein ISMS nach ISO 27001
- Der Standard enthält nur Empfehlungen, jedoch keine Anforderungen
- Aufwand für den Aufbau eines ISMS in einer Firma mittlerer Grösse (ca. 250 Mitarbeitende)
  - 12 – 18 Monate
  - Mehrere hunderttausend Franken

ISO 27004
Information security management - Measurement

- Anleitung für die Implementation eines Messsystems für die Beurteilung der Effektivität eines ISMS und der damit verbundenen Steuerungsmassnahmen gemäss ISO 27002
- Der Standard enthält Empfehlungen zu folgenden Aktivitäten
  - Entwicklung von Messkriterien
  - Implementation eines Information Security Measurement Programme (ISMP)
  - Analyse von Messresultaten und Reporting an die Stakeholders
  - Nutzung der Resultate, um das ISMS und die zugehörigen Massnahmen, sowie Kontrollen zu verbessern
  - Nutzung der Resultate, um das ISMP zu verbessern

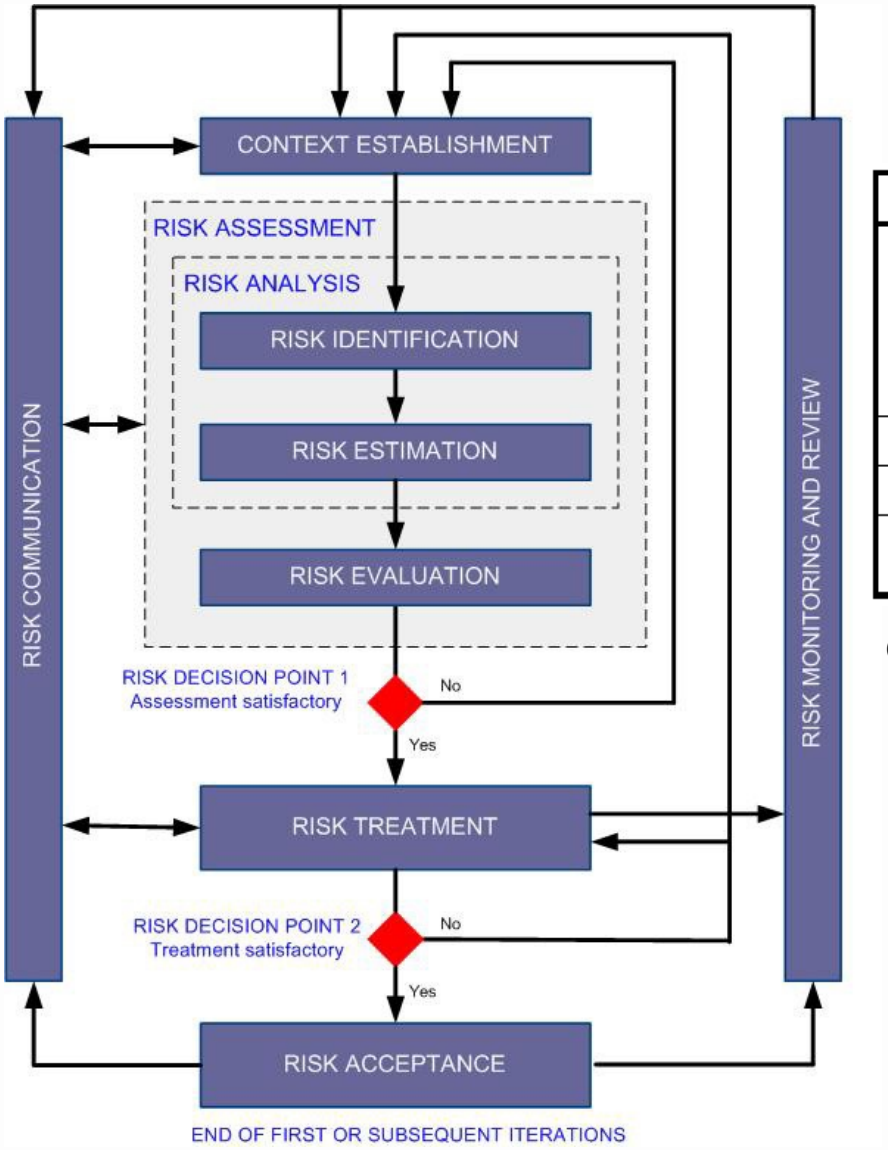
AGENDA

1. Kurze Einführung ISMS
2. ISMS nach ISO 27001
3. Best Practise nach ISO 27002
4. Ergänzende Standards ISO 27003 und 27004
5. **Risikoanalyse nach ISO 27005**
6. Die BSI-Standards 200-x
7. Kombinierte Risiko-Analyse nach BSI 200-3

ISO 27005
Information security risk management

- Anleitung für ein Information Security Risk Management ohne Spezifikation einer Risiko Management Methode
- Beliebige Risiko Management Methoden können unter dem vorgegebenen Framework angewendet werden
- Der Standard basiert auf ISO 27001 und ISO 27002 und setzt deshalb für die Anwendung die Kenntnis dieser beiden Standards voraus
- Er spezifiziert den ganzen Risiko Management Prozess beginnend mit der Risiko Analyse bis zum Plan für den Umgang mit den identifizierten Risiken

Information security risk mgmt. process



ISMS Process	Information Security Risk Management Process
Plan	Establishing the context Risk assessment Developing risk treatment plan Risk acceptance
Do	Implementation of risk treatment plan
Check	Continual monitoring and reviewing of risks
Act	Maintain and improve the Information Security Risk Management Process

Quelle: ISO 27005

Aufgabe zu ISO 27002

Nennen Sie 5 Steuerungselemente und die zugehörigen Domänen, welche für die Überprüfung des Objekts *Serverraum* relevant sind.

AGENDA

1. Kurze Einführung ISMS
2. ISMS nach ISO 27001
3. Best Practise nach ISO 27002
4. Ergänzende Standards ISO 27003 und 27004
5. Risikoanalyse nach ISO 27005
6. **Die BSI-Standards 200-x**
7. Kombinierte Risiko-Analyse nach BSI 200-3

Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Unabhängige und neutrale Stelle für Fragen der Informationssicherheit in der Informationsgesellschaft
- Gründung 1991 per Gesetz als nationale Behörde für IT-Sicherheit
- Jahresbudget: geschätzt € 64 Mio.
- Mitarbeiter: > 650
- Standort: Bonn
- Kunden: Bundesverwaltung, Wirtschaft, Wissenschaft, Bürger

BSI-Standards, IT-Grundschutz-Kompendium

- Die **BSI-Standards** beschreiben die Vorgehensweise nach IT-Grundschutz und enthalten Ausführungen zum Informations-sicherheitsmanagement und zur Risikoanalyse

- Das **IT-Grundschutz-Kompendium** beinhaltet die Bausteine, Gefährdungen und Umsetzungshinweise (statt Massnahmen)
  - 8 Domainen, über 80 Bausteine
  - Umsetzung in den Bausteinen enthalten
  - 816 statt vorher über 4000 Seiten

BSI-Standards, IT-Grundschutz-Kompendium

BSI-Standards zur Informationssicherheit

Informationssicherheit und IT-Grundschutz

BSI-Standard 200-1
Managementsysteme für Informationssicherheit (ISMS)

BSI-Standard 200-2
IT-Grundschutz-Methodik

BSI-Standard 200-3
Risikoanalyse auf der Basis von IT-Grundschutz

BSI-Standard 100-4
Notfallmanagement

IT-Grundschutz-Kompendium

Kapitel 1	Vorspann
Kapitel 2	Schichtenmodell und Modellierung

Elementare Gefährdungen

Schichten

Prozess-Bausteine:

- ISMS (Sicherheitsmanagement)
- ORP (Organisation & Personal)
- CON (Konzepte & Vorgehensweise)
- OPS (Betrieb)
- DER (Detektion & Reaktion)

System-Bausteine:

- IND (Industrielle IT)
- APP (Anwendungen)
- SYS (IT-Systeme)
- NET (Netze & Kommunikation)
- INF (Infrastruktur)

Quelle: BSI-Standard und Grundschutz nach heise.de

Vergleich BSI 100-1 vs. 200-1

BSI Standard 100-1	BSI Standard 200-1
1. Initiierung des Sicherheits-prozesses	1. Initiierung des Sicherheits-prozesses
2. Erstellung einer Sicherheits-konzeption	2. Erstellung der Leitlinie zur Informationssicherheit
3. Umsetzung der Sicherheits-konzeption	3. Organisation des Sicherheits-prozesses
4. Aufrechterhaltung und Verbesserung	4. Erstellung einer Sicherheits-konzeption
	5. Umsetzung der Sicherheits-konzeption
	6. Aufrechterhaltung und Verbesserung

Vergleich BSI 100-2 vs. 200-2

BSI Standard 100-2	BSI Standard 200-2
Schicht 1 – Übergreifende Aspekte Schicht 2 – Infrastruktur Schicht 3 – IT-Systeme Schicht 4 – Netze Schicht 5 – Anwendungen	**Prozessorientierte Bausteinschicht:** • ISMS (Managementsysteme für Informationssicherheit) • ORP (Organisation und Planung) • CON (Konzepte) • OPS (Betrieb) • DER (Detektion und Reaktion) **Systemorientierte Bausteinschicht:** • INF (Infrastruktur) • NET (Netze und Kommunikation) • SYS (IT-Systeme) • APP (Anwendungen) • IND (Industrielle IT)

BSI-Standard 200-1: Managementsysteme für Informationssicherheit

- Zielgruppe: Management
- Definiert allgemeine Anforderungen an ein ISMS
- Kompatibel mit den entsprechenden Standards der ISO 2700x Reihe
- Berücksichtigt insbesondere Empfehlungen aus ISO 13335 und ISO 27002
- Didaktisch sehr gut aufbereitet (leicht verständlich)
- Enthält diverse Hinweise zur Zusammenarbeit Sicherheitsmanagement und Datenschutz

BSI-Standard 200-2: IT-Grundschutz-Vorgehensweise

- Konkretisiert die Darstellung des ISMS nach BSI-Standard 200-1
- Beschreibt Aufbau und Betrieb eines ISMS in der Praxis
  - Aufgaben des IT-Sicherheitsmanagements
  - Aufbau von Organisationsstrukturen für die Informationssicherheit
- Gibt Anleitung
  - Zur Erstellung eines Sicherheitskonzepts
  - Zur Auswahl von angemessenen Sicherheitsmassnahmen
  - Zum Aufrechterhalten und verbessern der Informationssicherheit

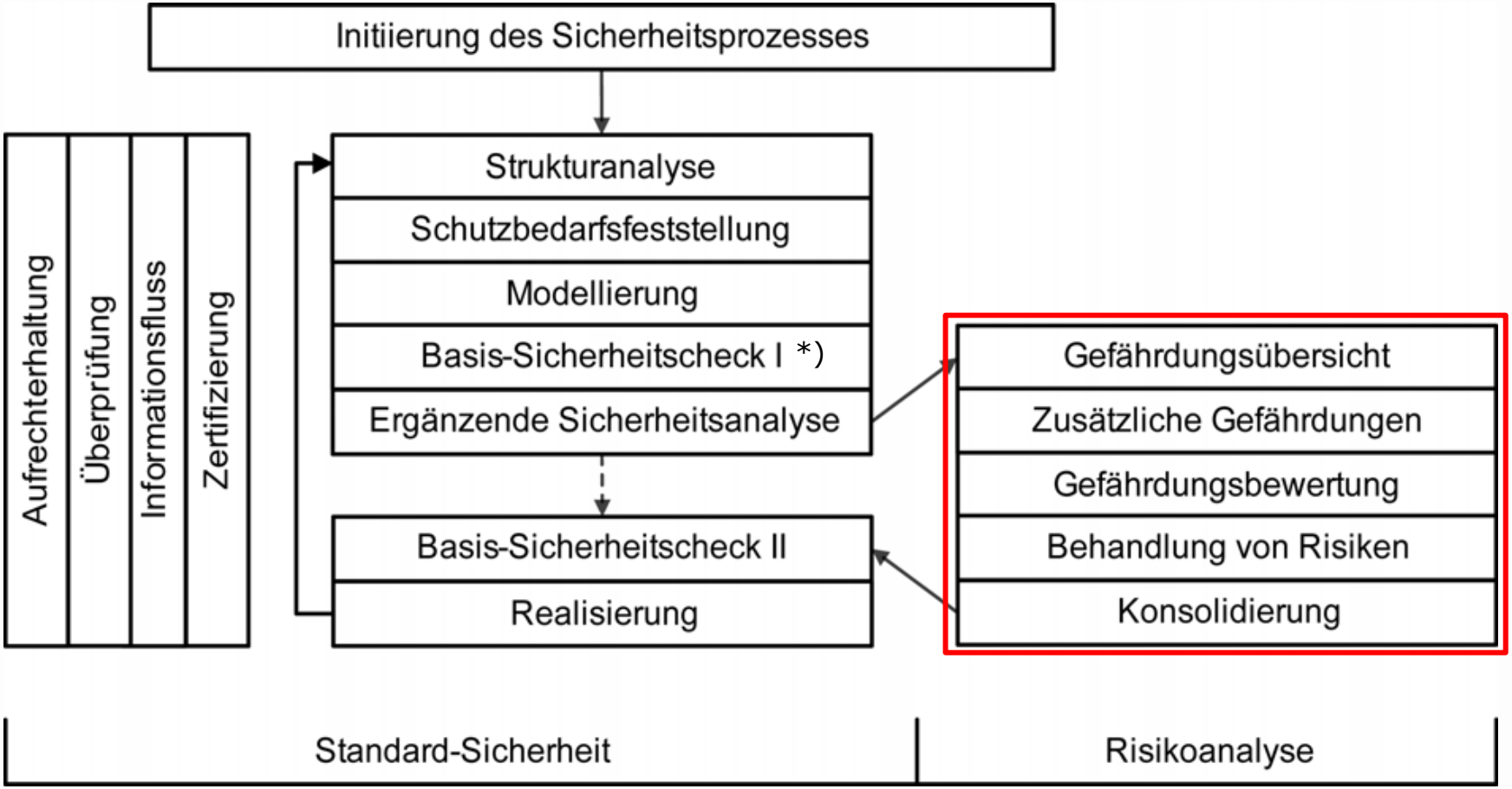
AGENDA

1. Kurze Einführung ISMS
2. ISMS nach ISO 27001
3. Best Practise nach ISO 27002
4. Ergänzende Standards ISO 27003 und 27004
5. Risikoanalyse nach ISO 27005
6. Die BSI-Standards 200-x
7. **Kombinierte Risiko-Analyse nach BSI 200-3**

BSI-Standard 200-3: Risikoanalyse auf Basis von IT-Grundschutz

- Die Standard-Sicherheitsmassnahmen der IT-Grundschutzkataloge sind in der Regel ausreichend
- Es gibt allerdings auch Ausnahmen
  - Objekte mit besonders hohen Sicherheitsanforderungen
  - Objekte, welche in den IT-Grundschutzkatalogen nicht behandelt werden
  - Objekte, welche in Einsatzszenarien betrieben werden, die im Rahmen des IT-Grundschutz nicht vorgesehen sind
- In diesen Fällen muss eine Risikoanalyse auf der Basis von IT-Grundschutz durchgeführt werden

BSI-Standard 200-3: Risikoanalyse auf Basis von IT-Grundschutz



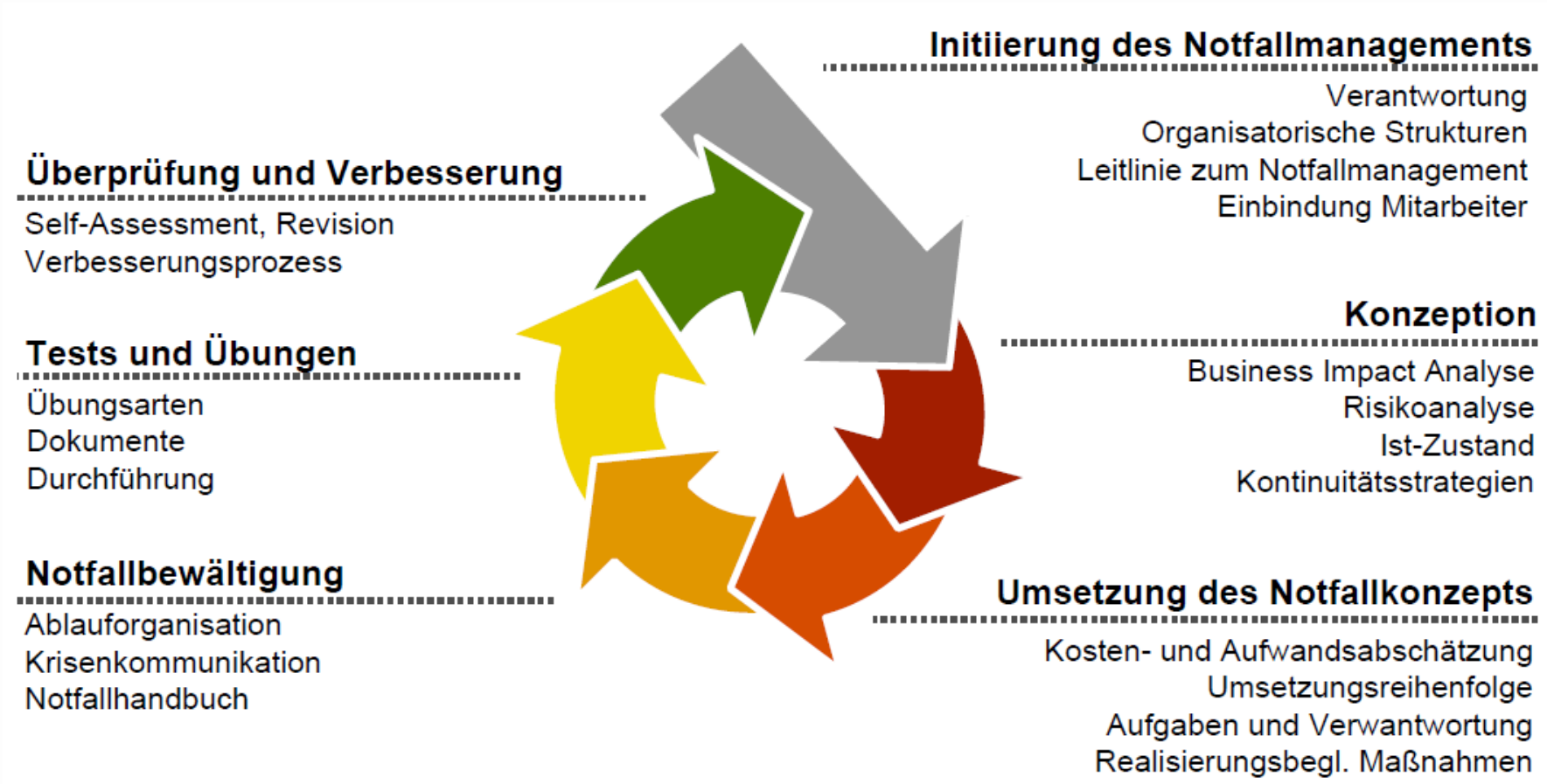
*) Basis-Sicherheitscheck = Soll-Ist-Vergleich

Quelle: BSI-Standard 100-3, Version 2.5

BSI-Standard 100-4: Notfallmanagement

- Methodik zur Etablierung und Aufrechterhaltung eines unternehmensweiten, internen Notfallmanagements
- Führt zu einem eigenständigen Managementsystem für die Geschäftsfortführung und Notfallbewältigung
- Baut auf der IT-Grundschutzvor-gehensweise auf (BSI-Standard 100-2)

BSI-Standard 100-4: Notfallmanagement



Quelle: Vortrag „IT-Grundschutz – Informationssicherheit ohne Risiken und Nebenwirkungen“, Isabel Münch, 19.10.09

ISO 27001 Zertifikat auf der Basis von IT-Grundschutz

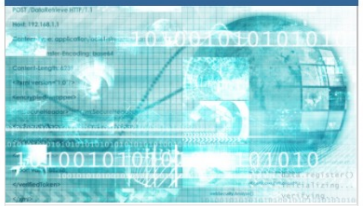
- Umfasst sowohl eine Prüfung des ISMS als auch der konkreten IT-Sicherheitsmassnahmen auf Basis von IT-Grundschutz
- Beinhaltet **immer** eine offizielle ISO-Zertifizierung nach ISO 27001
- Ist aber aufgrund der zusätzlich geprüften technischen Aspekte wesentlich **aussagekräftiger** als eine reine ISO-Zertifizierung

Aufgabe zu BSI-Standards

Recherchieren Sie auf der BSI Website, welche Dienste das BSI anbietet.

Aufgabenfelder BSI Deutschland

Cyber-Sicherheit



Cyber-Sicherheit erweitert das Aktionsfeld der klassischen IT-Sicherheit auf den gesamten Cyber-Raum. ›

Digitale Gesellschaft

Digitalisierung und Vernetzung verändern die Gesellschaft und ziehen neue Chancen ebenso wie Risiken nach sich. ›

IT-Grundschutz

Der BSI IT-Grundschutz ermöglicht es, notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen. ›

Kritische Infrastrukturen

Kritische Infrastrukturen (KRITIS) wie Energie- und Wasserversorgung haben eine wichtige Bedeutung für das staatliche Gemeinwesen. ›

Industrial Control System

Industrial Control System (ICS) Security befasst sich mit der IT-Sicherheit in den Bereichen Fabrikautomation und Prozesssteuerung. ›

Kryptografie und Kryptotechnologie

IT-Sicherheit erfordert eine kontinuierliche Entwicklung und Evaluierung von kryptografischen Verfahren und Kryptotechnologie. ›

Sicherheitsberatung

Die zentrale Anlaufstelle für alle Anfragen zur Beratung und Unterstützung bei Fragen zur Informationssicherheit. ›

Standards und Kriterien

BSI-Standards enthalten Empfehlungen zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen ... ›

Plus: Zertifizierung und Anerkennung

Quelle: www.bsi.de