



Workshop
Notfallvorsorge + IT-Sicherheit
9.-10. September 2008, Fulda

Normen - Standards - Richtlinien



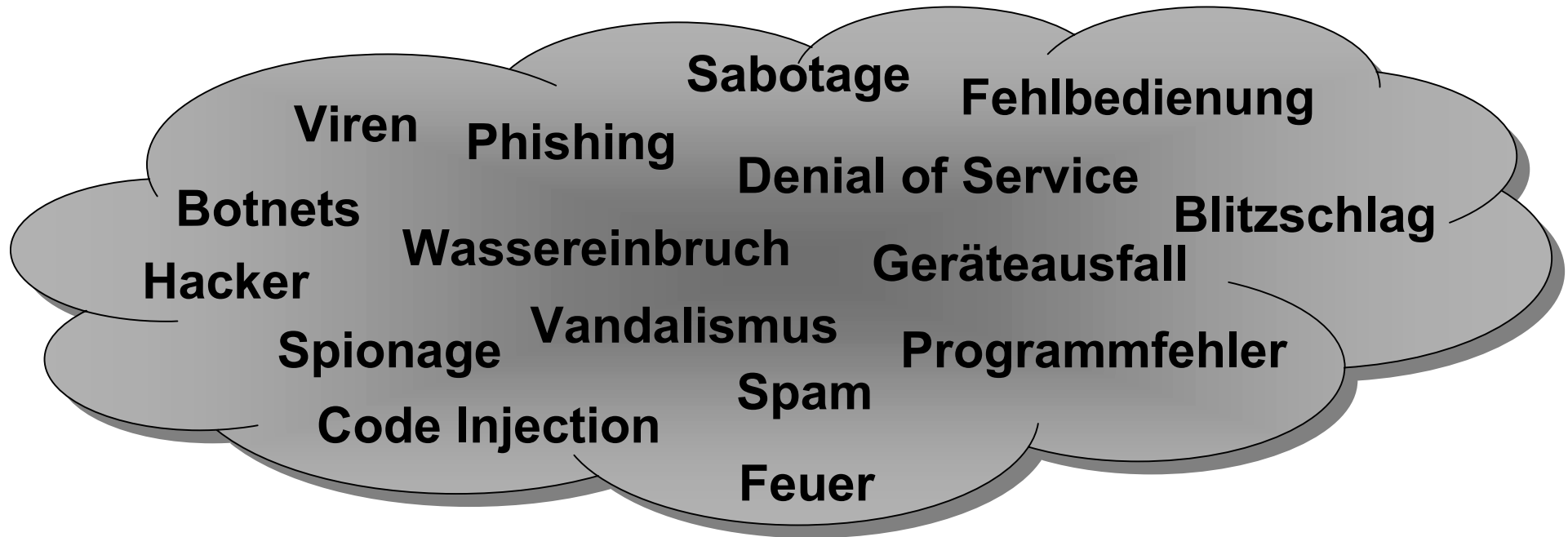


Agenda

- IT Sicherheit - Einführung
- Gesetze
- Richtlinien



IT-Sicherheit: Bedrohungen





Verantwortlichkeiten

- Informationseigentümer
 - Bereichsleiter

- Ressourceneigentümer
 - IT-Leiter für zentrale Ressourcen
 - (Bereichsleiter für Dokumente)



Kriterien der Informationssicherheit

Verfügbarkeit

Schutz vor ungewollter
Vorenthaltung von
Informationen

Vertraulichkeit

Schutz vor unbefugter
Preisgabe von Informationen

Integrität

Schutz vor unbefugter Veränderung von Informationen



Bedrohungen für die IT-Sicherheit

- Verlust der **Verfügbarkeit** z.B. bei
 - technischen Ausfällen von IKT-Systemen
 - Zerstörung von Daten durch Ausfälle oder Anwendungsfehler
- Verlust der **Vertraulichkeit** z.B. bei
 - unberechtigtem Lesen von Daten von Speichermedien und bei der Netzübertragung
- Verlust der **Integrität** z.B. bei
 - unbefugter Eingabe oder Änderung von Daten
 - Abspeichern fehlerhafter Daten durch Eingabe- oder Anwendungsfehler



Schutzbedarfsklassen

Schutzbedarfs- klasse	niedrig	mittel	hoch	sehr hoch
Schadensbetrachtung				
Beeinträchtigung des Geschäftsablaufs	geringfügige Betriebsbehinderung	Betriebsbehinderung	deutliche Einschränkung	existenzbedrohende Handlungsunfähigkeit
negative Außenwirkung/ Wettbewerbsnachteile	vernachlässigbare Beschwerden	Beschwerden, evtl. Kundenverluste	erhebliche Kundenverluste	existenzbedrohende Marktverluste
direkte finanzielle Auswirkungen	vernachlässigbare Beträge	Geringe - spürbare Beträge	erhebliche Bilanzauswirkung	existenzbedrohend / Konkurs
Verstoß gegen Gesetze / Vorschriften / Verträge	keine	geringe - spürbare Strafen u. Haftungs- schäden	hohe Strafen u. Haftungsschäden	existenzbedrohende Strafen u. Haftungsschäden
Anforderungen				
Verfügbarkeit - Hardwareausfälle - im täglichen Betrieb	Mittlere Ausfallzeit > 48h max. Datenverlust >= 24h	Mittlere Ausfallzeit <= 48h max. Datenverlust >= 24h	Mittlere Ausfallzeit <= 24h max. Datenverlust 24h	Mittlere Ausfallzeit <= 4h ohne Datenverlust
Vertraulichkeit	Technische und organisatorische Grundschutzmaßnahmen		Erweiterte Schutzmaßnahmen	Technische und organisa- torische Maximalmaß- nahmen auf Grundlage einer detaillierten Risiko- analyse
Integrität				



Beispiel-Maßnahmen

	Verfügbarkeit	Vertraulichkeit	Integrität		
sehr hoch		elektromagnetische Schirmung		indiv. Risikoanalyse	
		Personenschleusen / videoüberwachte Unterbringung 24/7			
		Abschirmung durch interne Firewall			
		proaktive 24/7 Überwachung der IT-Systeme			
		geographisch verteilter Failover Cluster mit synchr. Datenspiegelung	Intrusion Detection System		
			sicher verschlüsselte Datenspeicherung & -übertragung		
hoch	Notstromaggregat	starke 2-Faktor Authentisierung		+	
	Notfall-Liefervertrag	erweitertes / abgesichertes Logging mit Auswertung			
	redundante Komponenten (z.B. RAID, NIC, Netz)	verschlüsselte Datenübertragung über unsichere Medien			
	lokale Vorhaltung von Ersatzkomponenten	USV-gesteuerter Shut-Down			
mittel	Wartungsvertrag	verschlüsselte UserID / Passwort Authentisierung		Grundschutz	
		differenzierte Zugangsrechte			
		einfaches Logging			
		Malware-Schutz / Internet Firewall			



Treiber für IT-Sicherheit

- Gesetze
(KonTraG, BDSG, TKG)
- Prüfungsbestimmungen
(IDW RS FAIT 2/ PS330)
- Normen – Richtlinien
(CobiT, ITIL ISO/IEC 27001/2,
BSI-Standard 100-1, 100-2, 100-3)

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

Inhalt: Veränderungen von anderen Gesetzen

- Handelsgesetzbuch
- Aktiengesetz
- GmbH - Gesetz
- Gesetz über Kapitalanlagegesellschaften
- Genossenschaftsgesetz
- Wertpapierhandelsgesetz
- Börsenzulassungsverordnung
- Publizitätsgesetz
- Wirtschaftsprüferordnung
- Gesetz über Angelegenheiten der freien Gerichtsbarkeit

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich Artikel 2: Änderung des **Handelsgesetzbuchs**

6. § 317 wird wie folgt gefasst:

„§ 317 **Gegenstand und Umfang der Prüfung**

(2) Der Lagebericht und der Konzernlagebericht sind darauf zu prüfen, ob der Lagebericht mit dem Jahresabschluss und der Konzernlagebericht mit dem Konzernabschluss sowie mit den bei der Prüfung gewonnenen Erkenntnissen des Abschlussprüfers in Einklang stehen und ob der Lagebericht insgesamt eine zutreffende Vorstellung von der Lage des Unternehmens und der Konzernlagebericht insgesamt eine zutreffende Vorstellung von der Lage des Konzerns vermittelt. Dabei ist auch zu prüfen, ob die **Risiken der künftigen Entwicklung zutreffend dargestellt** sind.“

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

Artikel 1: Änderung des Aktiengesetzes

...

9. § 91 wird wie folgt geändert:

...

a) Die Überschrift wird wie folgt gefasst: "Organisation; Buchführung".

b) Der bisherige Text wird Absatz 1.

c) Folgender Absatz wird angefügt:

„(2) Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“

...

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich Artikel 2: Änderung des **Handelsgesetzbuchs**

6. § 317 wird wie folgt gefasst:

„§ 317 Gegenstand und Umfang der Prüfung

...

(4) Bei einer Aktiengesellschaft, die Aktien mit amtlicher Notierung ausgegeben hat, ist außerdem im Rahmen der Prüfung zu beurteilen, ob der Vorstand die ihm nach § 91 Abs. 2 des Aktiengesetzes obliegenden Maßnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann.“

...

9. § 321 wird wie folgt gefasst:

„§ 321 Prüfungsbericht

...

(4) Ist im Rahmen der Prüfung eine Beurteilung nach § 317 Abs. 4 abgegeben worden, so ist deren Ergebnis in einem besonderen Teil des Prüfungsberichts darzustellen. Es ist darauf einzugehen, ob Maßnahmen erforderlich sind, um das interne Überwachungssystem zu verbessern.“



Auswirkungen des KonTraG

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
Auswirkungen: Ausstrahlung auf alle Organisationsformen

- **direkt Aktiengesellschaften**
- **indirekt Gesellschaften im Rahmen von Konzernen mit AGen**
- **Bundesdrucksache (Gesetzesbegründung, kein Gesetz)
Nr. 13/9712, S.15 erweitert Geltungsbereich auf GmbHs, KGs und OHGs, wenn sie mittelgroß oder groß sind**

Orientierung der Größenklassen an §267 HGB:

Größenklasse	Bilanzsumme	Umsatzerlöse	Arbeitnehmer
Kleine Kapitalgesellschaft	maximal 4,015 Mio. Euro	maximal 8,030 Mio. Euro	maximal 50
Mittelgroße Kapitalgesellschaft	maximal 16,060 Mio. Euro	maximal 32,120 Mio. Euro	maximal 250
Große Kapitalgesellschaft	ab 16,060 Mio. Euro	ab 32,120 Mio. Euro	ab 250
Ein Unternehmen steigt in die höhere Größenklasse auf, wenn zwei der drei Merkmale am Abschlußstichtag zweier aufeinander folgender Geschäftsjahre zutreffen			



BDSG Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

...

3. zu gewährleisten, ... dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können ... (Weitergabekontrolle),

...

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

...



TKG § 90 Auskunftsersuchen der Sicherheitsbehörden

(1) Wer geschäftsmäßig Telekommunikationsdienste anbietet, ist verpflichtet, Kundendateien zu führen

(2) Die aktuellen Kundendateien sind von dem Verpflichteten nach Absatz 1 verfügbar zu halten, so dass die Regulierungsbehörde einzelne Daten und Datensätze in einem von ihr vorgegebenen automatisierten Verfahren abrufen kann. Der Verpflichtete hat durch technische und organisatorische Maßnahmen sicherzustellen, dass ihm Abrufe nicht zur Kenntnis gelangen können.



BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), Version 1.0

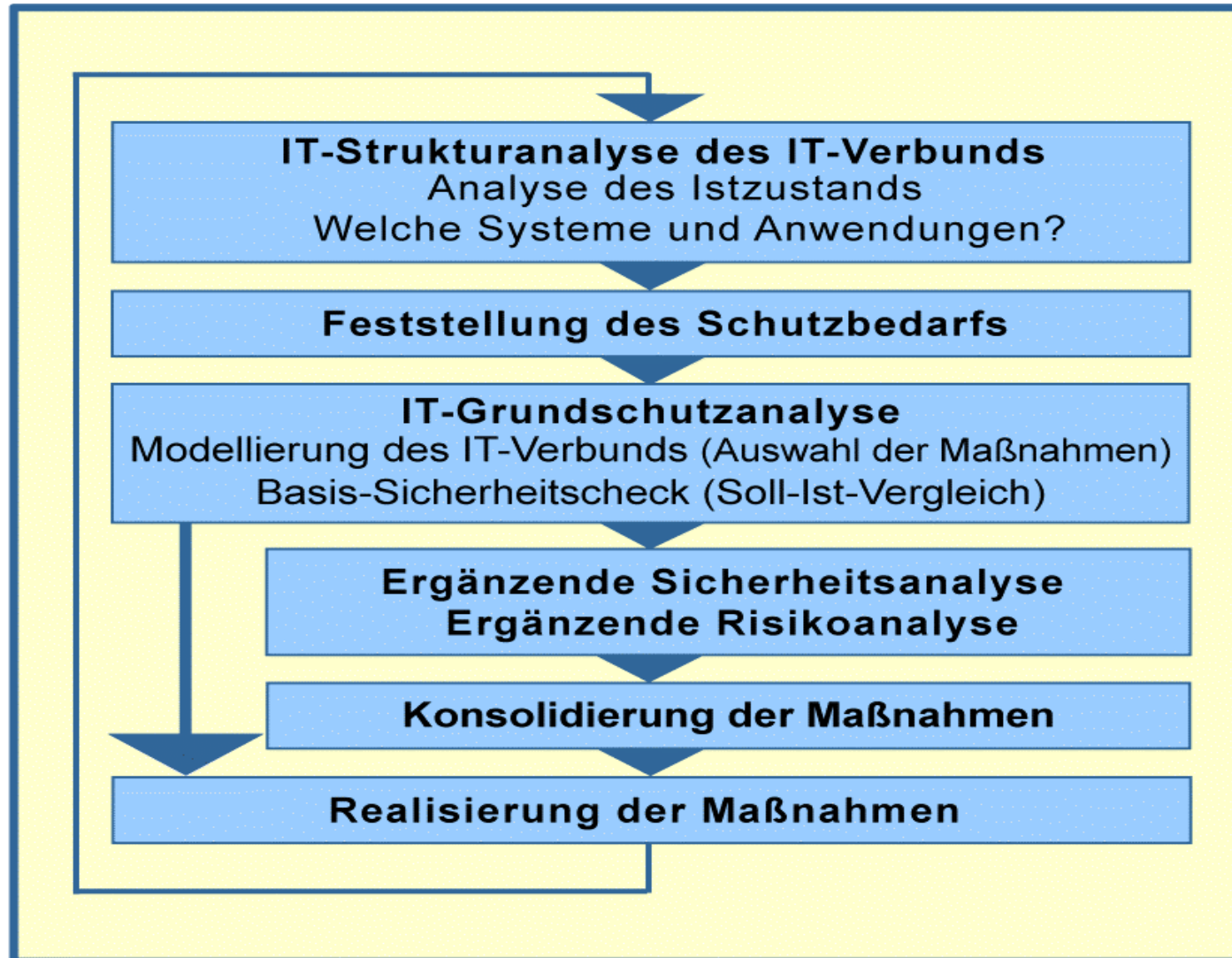
Informationssicherheit hat als Ziel den Schutz von Informationen. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. IT-Sicherheit beschäftigt sich vordringlich mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung. Hierbei sind die klassischen Grundwerte der IT-Sicherheit Vertraulichkeit, Integrität und Verfügbarkeit die Grundlagen für ihren Schutz.

ISO/IEC 27001/27002 Information technology - Security techniques - Information security management systems - Requirements

Erhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen; zusätzlich können auch weitere Eigenschaften mit betrachtet werden wie Authentizität, Verantwortlichkeit, Unleugbarkeit und Funktionssicherheit



ISM - BSI 100-2 IT-Grundschutz-Vorgehensweise



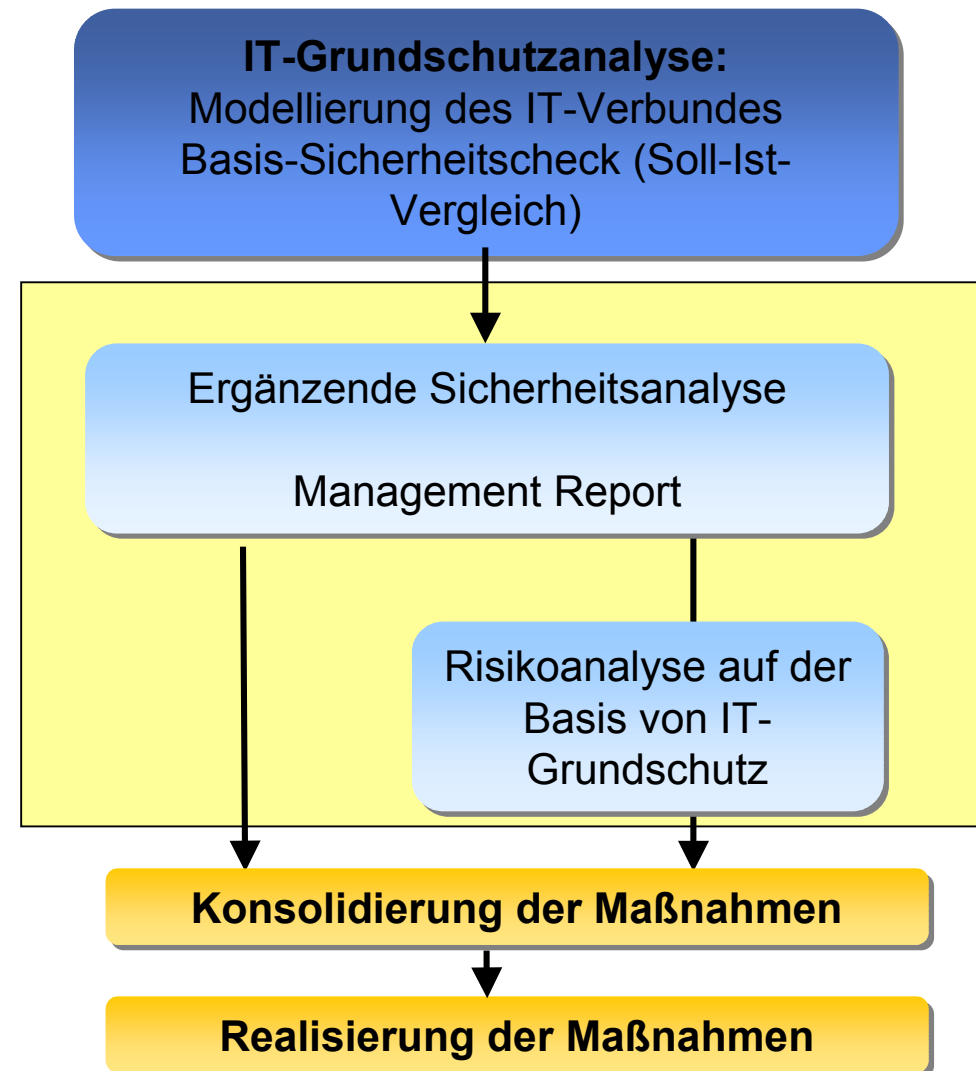
Quelle: BSI



ISM - Anforderung Risikoanalyse BSI (100-2)

BSI Standard 100-2, IT-Grundschutz-Vorgehensweise, Kap. 4.5

- IT-Grundschutz für typische IT-Anwendungen und IT-Systeme mit normalem Schutzbedarf
- Ergänzende Sicherheitsanalyse für Zielobjekte, wenn
 - erhöhter Schutzbedarf bei Vertraulichkeit, Integrität oder Verfügbarkeit
 - keine hinreichende Abbildung mit IT-Grundschutz-Bausteinen möglich
 - Betrieb in Einsatzszenarien (Umgebung, Anwendung), die im Rahmen des IT-Grundschutzes nicht vorgesehen sind
- Begründung der Entscheidung in Management Report



Quelle: BSI



BSI Standards und Grundschutzkataloge

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

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**



BSI 100-3 Übersicht

Ziele

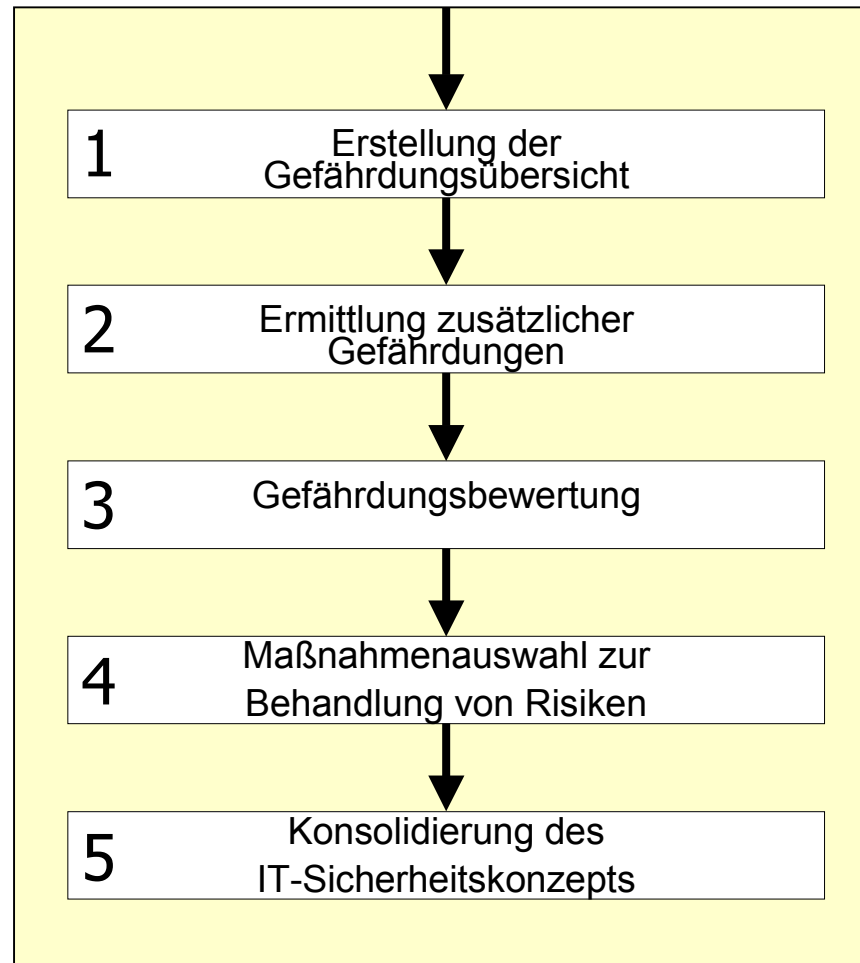
- Analyse von IT-Risiken mit Gefährdungen aus den IT-Grundschieutzkatalogen

Charakteristika

- setzt aufwändige Schritte aus dem Grundschieutz in Inhalt **und Form** voraus
 - IT-Strukturanalyse
 - Schutbedarfsfeststellung
 - Modellierung
 - Basis-Sicherheitsscheck I
- dann erst ergänzende Sicherheitsanalyse nach 100-3
- zwingend, wenn Grundschieutzzertifikat angestrebt wird
- keine Eintrittswahrscheinlichkeiten



BSI 100-3 Risikoanalyse Überblick



Quelle: BSI 2007



BSI 100-3 Bewertung

- nur für IT-Risiken / nicht für BCM anwendbar
- aufwendig
- Darstellung nicht Management-kompatibel
- starke Einbindung in Grundschatz
- keine Eintrittswahrscheinlichkeiten



ISM - Anforderung Risikoanalyse ISO/IEC 27001

Definition der Strategie für die Risiko-Analyse

- Auswahl einer Methode
- Festlegen der Kriterien für die Akzeptanz von Risiken und die akzeptierbaren Risikograde



Identifizierung der Risiken

- Identifizierung der Assets und ihrer Eigner
- Identifizierung der Bedrohungen für die Assets
- Identifizierung der Schwachstellen
- Identifizierung der Auswirkungen auf die Assets



Analyse und Auswertung der Risiken

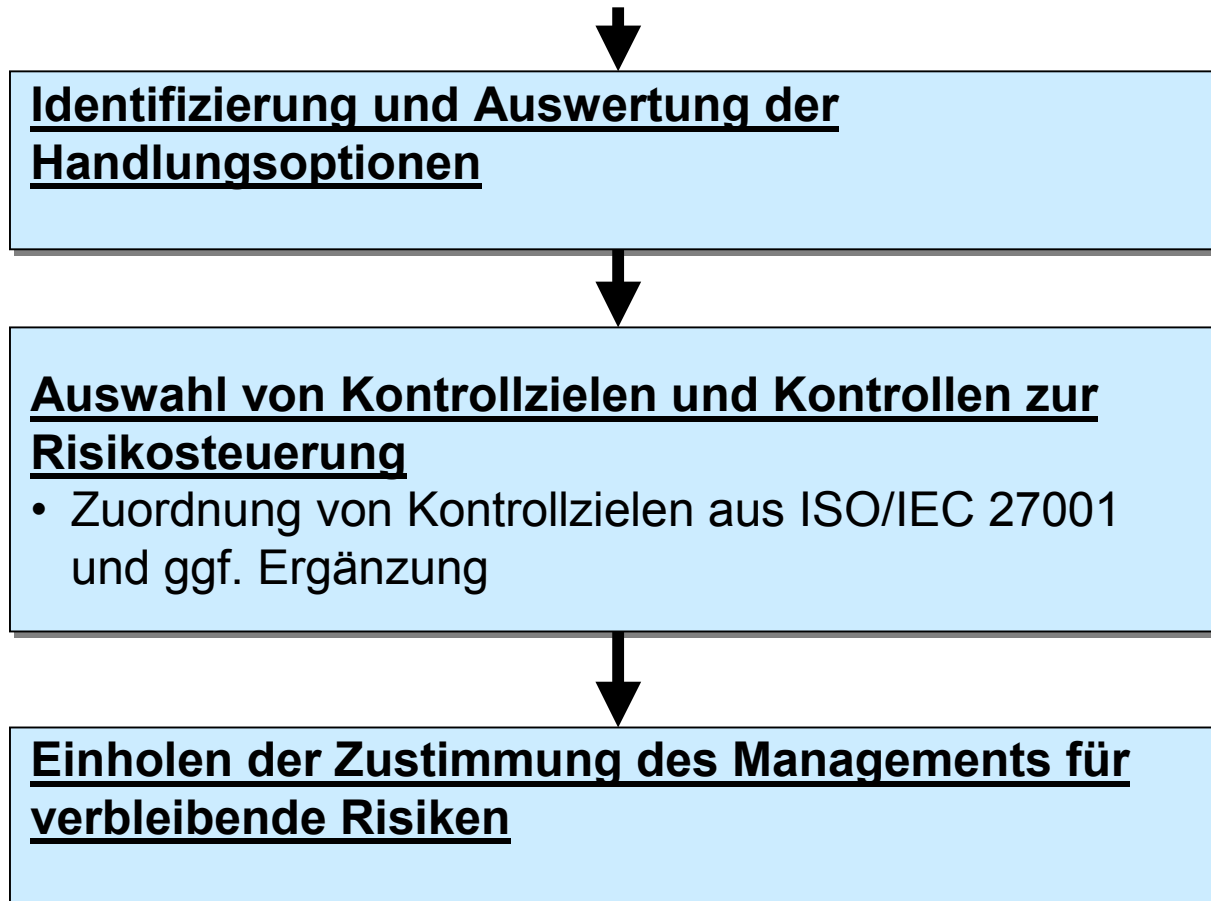
- Festlegung der Geschäftsauswirkungen
- Festlegen der Wahrscheinlichkeiten
- Schätzung der Risikohöhe
- Ableitung des Handlungsbedarfs



Weiter geht's auf der nächsten Folie



ISM - Anforderung Risikoanalyse ISO/IEC 27001



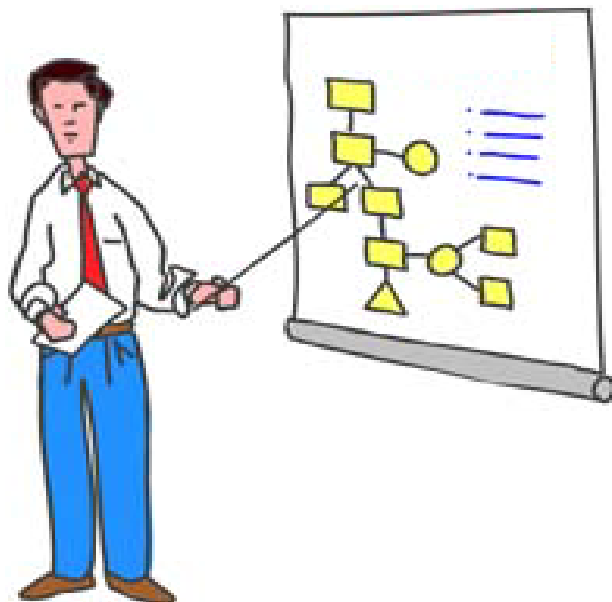


ISO 27001 – Beispiel für Kontrollziele

A.9 Physical and environmental security		
A.9.1 Secure areas		
<i>Objective:</i> To prevent unauthorized physical access, damage and interference to the organization's premises and information.		
A.9.1.1	Physical security perimeter	<i>Control</i> Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.
A.9.1.2	Physical entry controls	<i>Control</i> Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
A.9.1.3	Securing offices, rooms and facilities	<i>Control</i> Physical security for offices, rooms, and facilities shall be designed and applied.



Vielen Dank für Ihre Aufmerksamkeit!



Dipl.-Math.

Lothar Goecke

Geschäftsführer

consequa GmbH
Süderstraße 73
20097 Hamburg
www.consequa.de

Tel.: 040 / 78 89 70 62
Fax: 040 / 78 89 70 66
Mob: 0171 / 863 50 17
lothar.goecke@consequa.de