TEM04 Zusammenfassung

Security Management

Alexander Hauck

Wirtschaftsinformatik, Frühlingssemester 2016

Inhalt

ISMS und Informationssicherheitsstandards

Grundwerte Informationssicherheit:

- Vertraulichkeit (Schutz vor unberechtigtem Zugriff)
- Integrität (Informationen und Daten sind richtig und vollständig)
- Verfügbarkeit (Informationen und Daten sind dann abrufbar, wenn sie benötigt werden)

Einführung ISMS

Ein ISMS 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.
- Vermögenswerte und Informationen der Unternehmung („Assets“) schützen.
- Rechtliche und regulatorische, Branchen- und Marktanforderungen erfüllen.

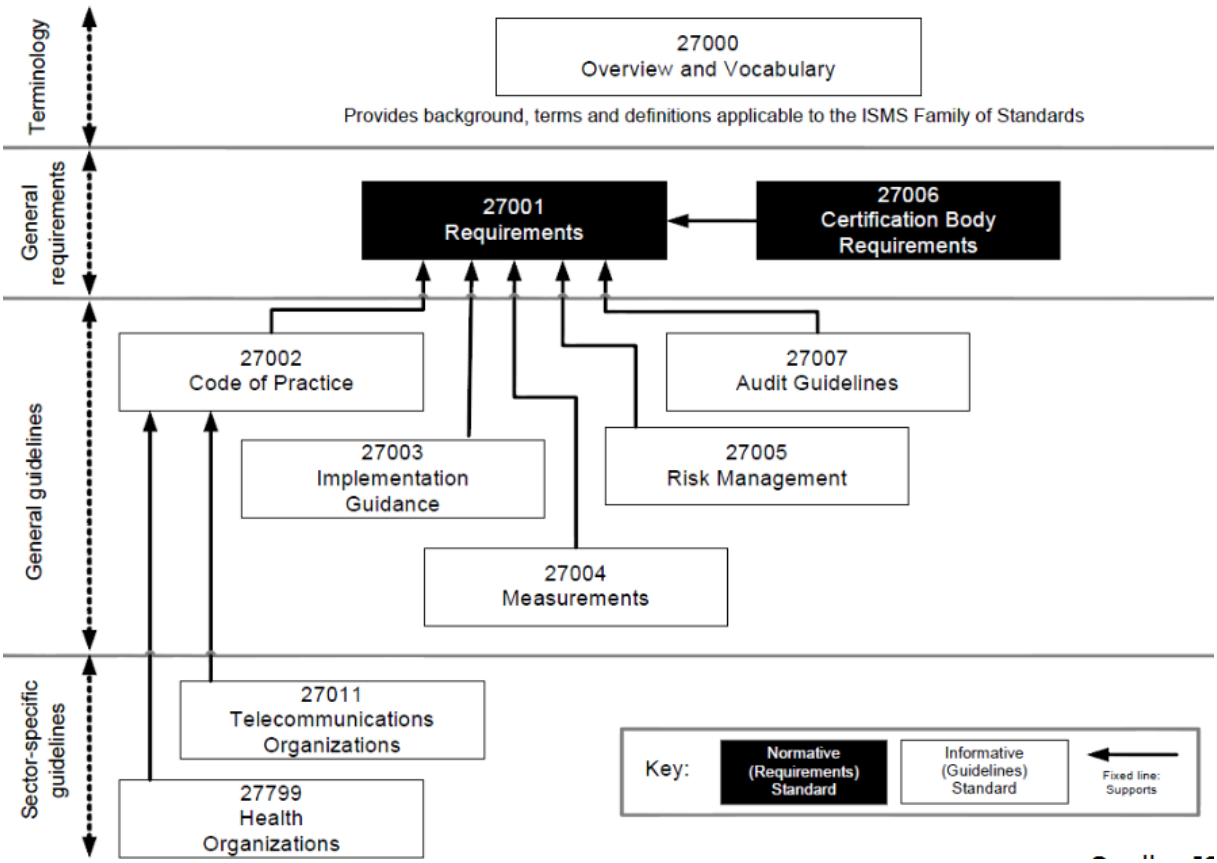
Nutzen von Standards

- **Kostensenkungen:**
  - Nutzungung vorhandener und praxiserprobter Vorgehensmodelle
  - Vereinheitlichung, Nachvollziehbarkeit
- **Einführung eines angemessenen Sicherheitsniveaus:**
  - Orientierung am Stand der Technik und Wissenschaft
  - Gewährleistung der Aktualität
  - Zyklische Bewertung, dadurch Verbesserung der Sicherheit
- **Wettbewerbsvorteile:**
  - Zertifizierung
  - Verbesserung des Unternehmensimages
  - Stärkung der Rechtssicherheit

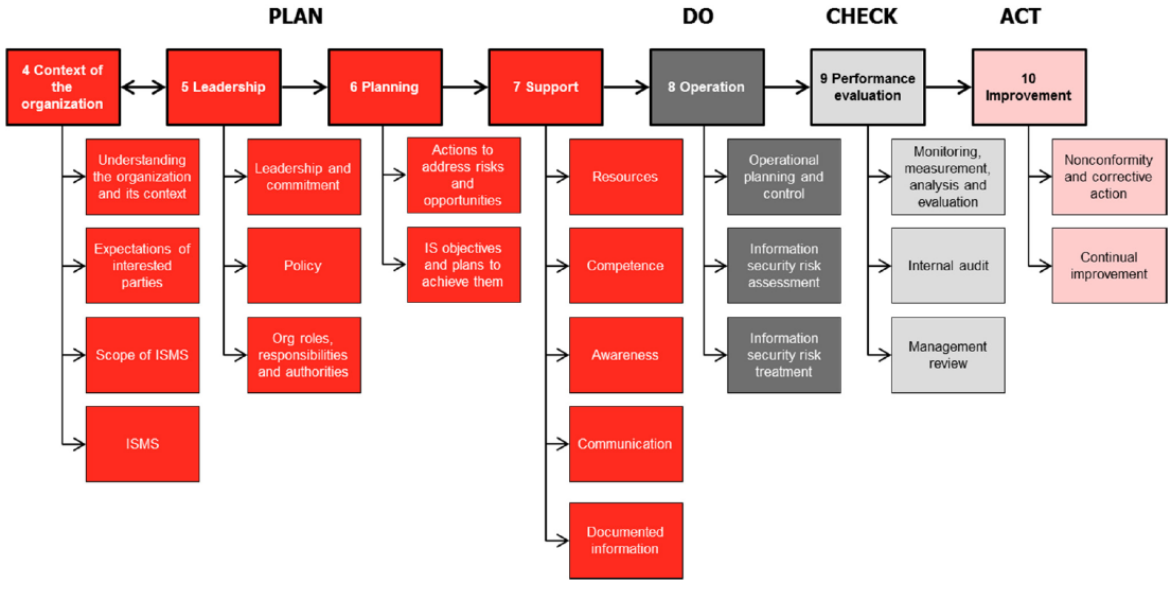
Übersicht über die ISO Standards

- ISO 27000:2009 ISMS – Overwiew and Vocabulary
- ISO 27001:2013 ISMS – Requirements (= Anforderungen für Zertifikation)
- ISO 27002:2013 Code of practice for information security controls (wie mans macht)
- ISO 27003:2010 ISMS implementation guidance
- ISO 27004:2009 Information security management – Measurement (Kontrolle)
- ISO 27005:2011 Informaton security risk management

Weitere ISO Standards sind vorhanden, jedoch sind diese Branchenspezifisch.



- 27000: Begriffsdefinitionen, Erklärung von „Plan – Do – Check – Act“, Überblick über ISO
- 27001:
  - Definiert Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten ISMS.
  - Definiert Ziele und Massnahmen zur Verbesserung der Informationssicherheit.
  - Eine Firma kann sich nach ISO 27001 zertifizieren lassen.
  - Freiheitsgrade („Scope“): Ganze Firma, Abteilung, Standort etc.
  - Kontrollziele und Kontrollen („Statement of Applicability“, SOA)
  - Scope und SOA definieren den Umfang einer Zertifizierung nach ISO 27001.
  - PDCA-Zyklus abgebildet auf die **Kapitelstruktur** von ISO 27001:



- 27002:
  - Beinhaltet 114 Steuerungsmassnahmen
  - Buch ist in 14 Domänen aufgeteilt, darunter: Organisatorische, physische und logische Sicherheit, Anwendungsentwicklung und –unterhalt, Notfallvorsorge, Einhaltung und Überprüfung der Sicherheit, etc.
  - Umsetzungsangaben beinhalten keine Details (nur **„Sollte" – Formulierungen**). Deshalb ist auch keine Zertifizierung nach ISO 27002 möglich.
  - Eignet sich sehr gut zur Umsetzung eines **Grundschutzes**.
- 27003: Anleitung für die Entwicklung eines Implementierungsplans, Enthält nur Empfehlungen, jedoch keine Anforderungen.
- 27004: Anleitung für die Implementation eines Messsystems und der damit verbundenen Kontrollen gemäss ISO 27002.
- 27005: Framework für ein Information Security Risk Management ohne Spezifikation einer Risiko Management Methode.

Weitere, alternative Standards:

- IT Grundschutz-Kataloge und BSI-Standards vom Bundesamt für Sicherheit in der Informationstechnik.
- Standard of Good Practice for Information Security (Information Security Forum ISF)
- Control Objectives for Information and Related Technology (COBIT): Framework zur IT-Governance (z.B. nur 1 Hersteller für PC und Laptops)

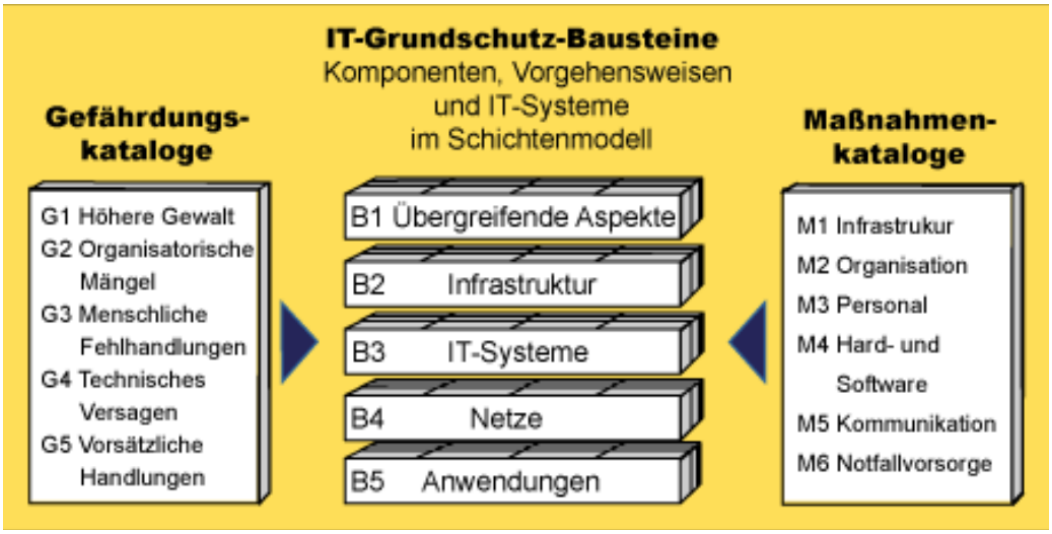
Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Unabhängige und neutrale Stelle für Fragen der Informationssicherheit in der Informationsgesellschaft.
- **BSI Standards:**
  - Beschreiben die Vorgehensweise nach IT-Grundschutz
  - Enthalten Ausführungen zum Informationssicherheitsmanagement und zur Risikoanalyse
  - „Betty Bossi" Rezepte
- **IT-Grundschutz-Kataloge:**
  - Baustein- , Massnahmen- und Gefährdungskataloge
  - 79 Bausteine, 1225 Massnahmen, 4101 Seiten.
  - Sind einfacher verständlich als ISO, jedoch ohne Zertifizierung.

Idee des IT-Grundschutzes

- Abläufe und IT-Komponenten sind **überall ähnlich**:
  - Typische Gefährdungen, Schwachstellen und Risiken
  - Typische Geschäftsprozesse und Anwendungen
  - Typische IT-Komponenten
- Dies erlaubt die Errichtung eines Gerüsts für das Sicherheitsmanagement
- Zentrale Aspekte: Wiederverwendbarkeit, Anpassbarkeit, Erweiterbarkeit
- Standard-Sicherheitsmassnahmen helfen, ein **Standard-Sicherheitsniveau** aufzubauen

IT-Grundschutz nach BSI



- Beispiel **Gefährdungskatalog** Vorsätzliche Handlungen: „Missbrauch von Administratorrechten bei Windows-Betriebssystem." → Sehr konkret, bis auf OS-Ebene.
- **Massnahmenkataloge** enthalten praxisnahe und detailliert beschriebene Massnahmen. Beispiel Massnahmenkatalog Hard- und Software: „Änderung voreingestellter Passwörter".
- **Grundschutz-Bausteine**: Bilden Klammer zwischen Gefährdungs- und Massnahmenkatalogen. Jeder Baustein enthält relevante Gefährdungen und entsprechende Massnahmen. Beispiel für Baustein B 3.201: Allgemeiner Client
  - Gefährdungen: Unerlaubte Ausübung von Rechten, Gefährdung durch Reinigungs- oder Fremdpersonal, Verlust gespeicherter Daten uvm.
  - Massnahmen: Bildschirmsperre, Einsatz von Viren-Schutzprogrammen, Herausgabe einer PC-Richtlinie, Einsatz angemessener Sicherheitsprodukte für IT-Systeme etc.
- Aufwand für die Entwicklung eines Sicherheitskonzepts wird dank den Bausteinen reduziert.
- I.d.R. genügt es, die Massnahmen der Bausteine einzuplanen und konsequent umzusetzen.
- **Unterschied Grundschutzkatalog und ISO:** Konkret vs. Allgemein, keine Zertifizierung vs. Zertifizierung

B 2.4	Zyklus	Siegel	G 1.4	G 1.5	G 1.7	G 1.16	G 2.1	G 2.6	G 4.1	G 4.2	G 4.6	G 5.1	G 5.2	G 5.3	G 5.4	G 5.5
M 1.3	PK	A	X						X	X	X					
M 1.7	PK	A	X							X						
M 1.10	PK	Z	X					X				X	X	X	X	X
M 1.15	BT	A	X	X	X		X	X				X	X	X	X	X
M 1.18	PK	Z	X	X				X	X	X		X		X	X	X
M 1.23	BT	A					X	X				X	X	X	X	X
M 1.24	PK	C		X					X	X						
M 1.26	PK	W	X	X					X							
M 1.27	PK	B			X											
M 1.28	PK	B							X	X	X	X				
M 1.31	PK	Z	X	X	X				X	X		X		X	X	
M 1.52	PK	Z	X	X	X				X	X		X			X	X
M 1.58	PK	A	X	X				X				X	X			
M 1.62	PK	C	X			X										
M 2.17	UM	A	X				X	X				X	X	X	X	X
M 2.21	UM	A	X				X									

Abbildung 1 Kreuzreferenztabelle

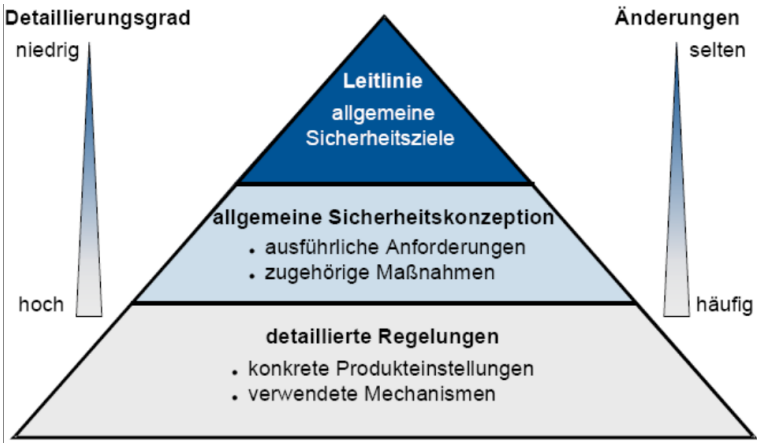
- G = Gefährdung, M = Massnahme
- B 2.4 = Baustein 2.4
- Siegel A = Unbedingt

BSI-Standards

- **BSI-Standard 100-1:** Managementsysteme für Informationssicherheit (ISMS)
  - Zielgruppe: Management
  - Definiert allgemeine Anforderungen an ein ISMS
  - Berücksichtig Empfehlungen aus ISO, ist auch kompatibel mi ISO
  - Leicht verständlich
- **BSI-Standard 100-2:** IT-Grundschutz-Vorgehensweise
  - Konkretisiert den Standard 100-1.
  - Beschreibt Aufgaben des IT-Sicherheitsmanagements und den Aufbau von Organisationsstrukturen für die Informationssicherheit.
  - Gibt Anleitung zur Erstellung eines Sicherheitskonzepts, zur Auswahl angemessener Sicherheitsmassnahmen und zum Aufrechterhalten und Verbessern der Informationssicherheit.
- **BSI-Standard 100-3:** Risikoanalyse auf der Basis von IT-Grundschutz
  - Für spezielle Objekte mit besonders hohen Sicherheitsanforderungen oder solche, die nicht in den IT-Grundschutzkatalogen enthalten sind.
- **BSI-Standard 100-4:** Notfallmanagement

Sicherheitspolicy und –konzepte

Sicherheitspyramide



Informationssicherheits-Policy (ISP)

- Die Policy sollte vom Top-Management ausgearbeitet werden und klare Statements beinhalten.
- Gilt **langfristig** (3-5 Jahre)
- Fokus: Sicherstellung der Geschäftsfortführung (**Continuity Management**)
- Sie muss schriftlich fixiert sein, innerhalb des Unternehmens kommuniziert werden und für Interessierte zugänglich sein.
- Die ISP ist Bezugspunkt für die gesamte Informationssicherheit.
- **Infos / Vorlagen** für die Informationssicherheits-Policy sind u.a. an folgenden Orten zu finden:
  - ISO 27001, Kap. 5.2 „Policy“
  - ISO 27001, Kap. 7.5 „Documented Information“
  - ISO 27002, Kapitel 5 „Information security policies“
  - BSI 100-1, Kapitel 7 “Der Informationssicherheit-Prozess”
  - BSI 100-2 Kapitel 3.3 „Erstellung einer Leitlinie zur Informationssicherheit“
  - BSI IT-Grundschutz-Kataloge, M 2.192 „Erstellung einer Leitlinie zur Informationssicherheit“
- **Grundlagen:**
  - Unternehmens-Policy
  - Unternehmenskultur
  - Organisation des Unternehmens
  - Gesetze / Verträge
  - Anforderungen an Sicherheit des Unternehmens → Verhältnismässigkeit zwischen Risiko und Wirtschaftlichkeit beachten.

- **Checkliste / Inhalte:**
  - Vorwort / Einordnung / Motivation
  - Geltungsbereich und Abgrenzung
  - Grundlagen (Gesetze, übergeordnete Dokumente, Verträge)
  - Ziel und Zweck ISP (Sicherstellen Geschäftsvorgang)
  - Informationssicherheitsziel und –strategie
  - Rollen und Verantwortlichkeiten
  - Umgang mit Risiken, Wirtschaftlichkeitsaspekte
  - Zuwiderhandlungen
  - Life Cycle
  - Unterschrift
  - Lesbarkeit / Aufmachung / Umfang / Publizierung
  - Umsetzbarkeit / Realisierbarkeit

Informationssicherheitskonzepte (ISK)

- Enthalten taktische Aussagen → Rahmenbedingungen für Teilbereiche festlegen
- Basiert auf der ISP
- Definiert den Umgang mit verschiedenen zentralen Elementen der Informationssysteme
- Mittelfristige Geltungsdauer (1-3 Jahre)
- Beispiele:
  - Datensicherungs-Konzept (z.B. Was sind die Verantwortlichkeiten? Wer Kontrolliert die Datensicherung? Wie werden die Mitarbeiter geschult? Wann werden die Sicherungen durchgeführt? Welche Daten werden gesichert?) → Eher Allgemein
  - Virenschutz-Konzept
  - Firewall-Konzept
  - Notfallkonzept
  - Verschlüsselungs-Konzept
  - …
- Zu behandelnde Aspekte:
  - Security Management
  - Critical Business Application
  - Computer Installation
  - Networks
  - System Development
  - End User Environment

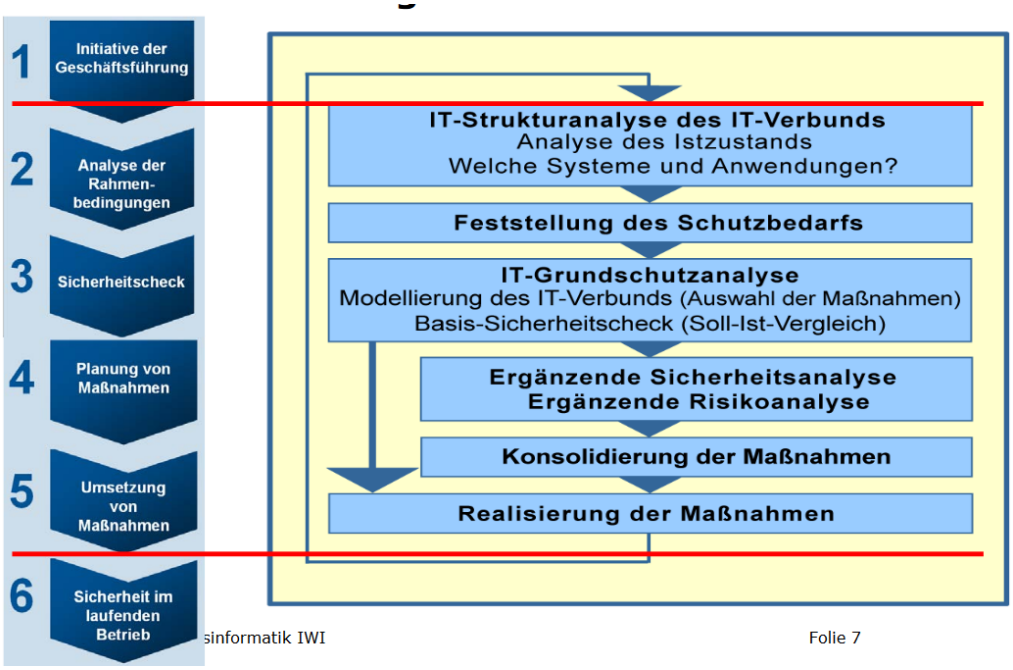
Regelwerk / Massnahmenkatalog

- Detailziele, welche regelmässig angepasst werden müssen
- Abgeleitet von den Konzepten
- Oft auf Standardwerken basierend (ISO, Grundschutzkataloge, Whitepapers etc.)
- Beispiele:
  - Richtlinien für den sicheren Betrieb von Datenbanken
  - Richtlinien für Remote-Access
  - Richtlinien für die Entsorgung von IT-Equipment
  - Richtlinien für Dokumentation
  - …

Vorgehen IT-Grundschutz

Rückblick BSI-Standards

- BSI-Standard 100-1: Managementsysteme für Informationssicherheit (sehr grundlegend):
  - Welches sind die **Erfolgsfaktoren** beim Management von Informationssicherheit?
  - Wie kann der **Sicherheitsprozess** vom verantwortlichen Management gesteuert und überwacht werden?
  - Wie werden **Sicherheitsziele** und eine angemessene **Sicherheitsstrategie** entwickelt?
  - Wie kann ein einmal erreichtes **Sicherheitsniveau** dauerhaft aufrechterhalten und verbessert werden?
- BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
  - Wie etabliere ich ein **ISMS**?
  - Wie erarbeite ich ein **IT-Sicherheitskonzept**?
  - Welche **Objekte** muss ich schützen?
  - Welches **Mass** an Sicherheit ist angemessen?
  - Wie bestimmte ich die anzuwendenden **Massnahmen**?
  - Wie führe ich eine **Standortbestimmung** durch? (**Soll/Ist**-Vergleich)
  - Worauf ist bei der **Umsetzung** zu achten?
- BSI-Standard 100-3: Risikoanalyse auf Basis von IT-Grundschutz. Die IT-Grundschutz-Vorgehensweise ist zweistufig:
  - **Stufe 1: Für normalen Schutzbedarf**, übliche Einsatzszenarien und existierende Grundschutz-Bausteine:
    - Qualitative Methode zur Risikoanalyse und –bewertung ist vorhanden → Anwendung von Standard-Sicherheitsmassnahmen
    - Idee: Ähnliche IT-Umgebungen = Ähnliche Bedrohungen
  - **Stufe 2: Für höheren Schutzbedarf.** Es wird eine Risikoanalyse und –bewertung nach BSI-Standard 100-3 durchgeführt.



Rückblick IT-Grundschutz-Kataloge

- Anwendungen für einen **angemessenen Schutz**.
- Massnahmenbündel für bestimmte IT-Schutzobjekte (=Bausteine)
- Zeigen Gefahren für bestimmte IT-Schutzobjekte auf und wie man sich vor diesen schützt.
- Die Inhalte des Katalogs haben **Empfehlungscharakter** (d.h. Verantwortung wird nicht abgenommen!)
- Die Massnahmen müssen gegebenenfalls individuell angepasst werden.
- Das Management als zentraler Bereich: Von ihm geht die Initiative aus und es trägt auch die Verantwortung. Nur wenn es sich um Informationssicherheit bemüht wird sie auch wahrgenommen.

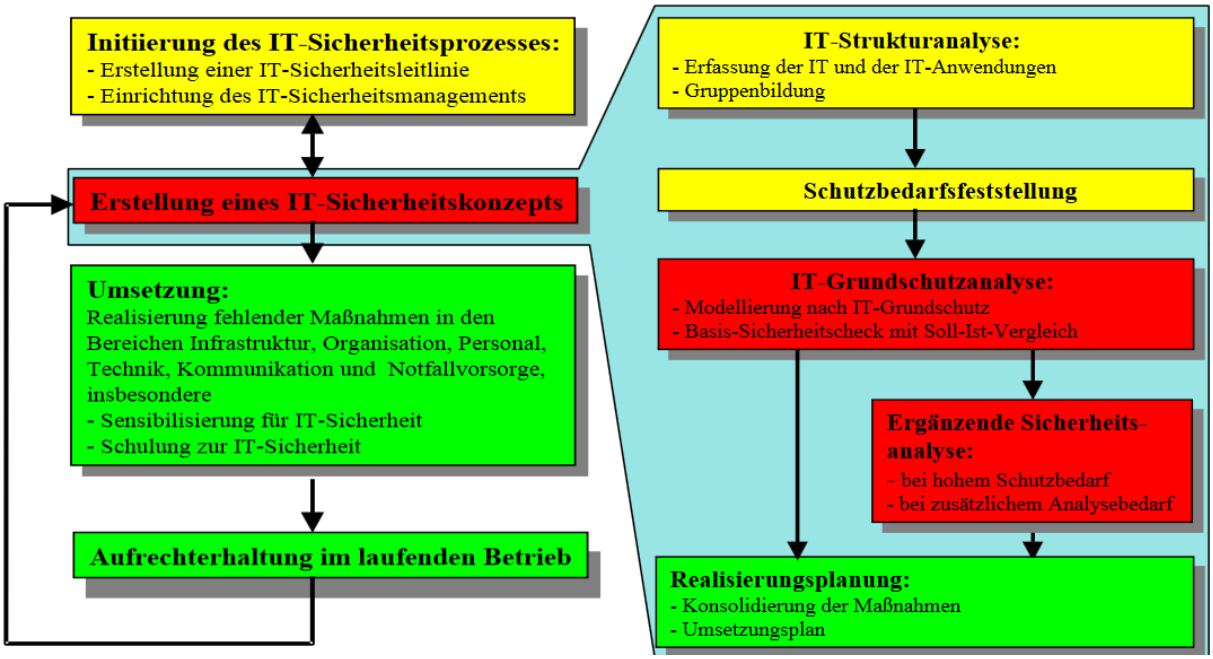
Kreuzreferenztabellen

- Tabellen, welche angeben, welche Gefährdungen mit welchen Massnahmen begegnet werden können. Die Massnamen werden mit sogenannten Siegelstufen priorisiert (A = Essenziel, B=Besonders wichtig, C=wichtig, Z=Ergänzend)
- Wieso gibt es eine Kategorie Z? → Könnte ggf. in Zukunft oder für gewisse Bereiche plötzlich wichtig werden.
- Optimalerweise wird für eine Gefahr eine Massnahme ausgewählt, welche gleichzeitig viele andere Gefahren abdeckt.

B 3.106	Zyklus	Siegel	G 1.2	G 2.7	G 2.18	G 3.9	G 3.48	G 4.10	G 4.23	G 4.35	G 5.7	G 5.23	G 5.52	G 5.71	G 5.79	G 5.83	G 5.84	G 5.85
M 2.227	PK	A		X		X	X						X			X		X
M 2.228	PK	A		X		X							X					X
M 2.232	PK	C		X						X				X			X	X
M 2.233	PK	B				X	X			X	X	X	X	X		X	X	X
M 4.48	UM	A		X											X			
M 4.56	BT	C		X	X									X				
M 4.75	UM	A											X		X			
M 4.136	UM	A	X	X		X		X	X	X	X	X	X	X	X	X	X	X
M 4.137	UM	A		X		X	X	X	X	X	X	X	X	X		X	X	X
M 4.139	UM	A		X		X	X	X	X	X	X	X	X	X		X		X
M 4.140	UM	A		X			X		X	X			X	X				X
M 4.141	UM	A		X			X			X	X		X					X
M 4.142	UM	B		X			X		X	X			X					X
M 4.143	UM	B		X			X		X	X			X					X
M 4.144	UM	B		X									X	X		X	X	X

PK: Planung und Konzeption, BE: Beschaffung, UM: Umsetzung, BT: Betrieb, AU: Aussonderung, NV: Notfallvorsorge.

Erstellung eines IT-Sicherheitskonzepts



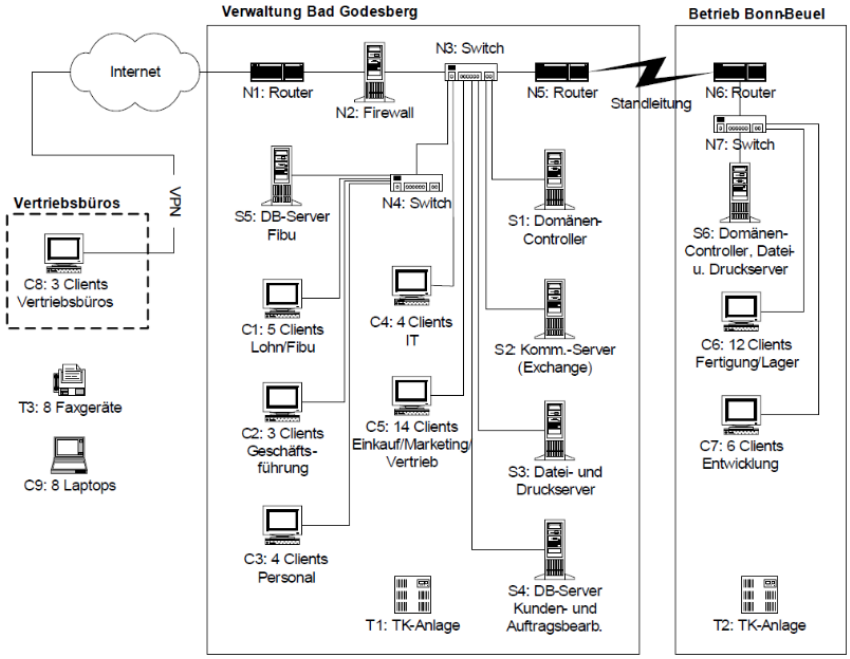
Input	Vorgang	Output
• Netzwerkplan • Inventar	**IT-Strukturanalyse**	• Bereinigter, verdichteter Netzwerkplan • Objektlisten • Abhängigkeiten von Systemen und Anwendungen
• Objektlisten • Schutzbedarfskategorien	**Schutzbedarfs-feststellung**	• Objektlisten mit zugeordnetem Schutzbedarf • Entscheidungsgrundlage für ergänzende Sicherheitsanalyse
• Objektlisten • Grundschutz-Bausteine • Interviews, Überprüfungen	**IT-Grundschutzanalyse**	• Grundschutzmodell • Umsetzungsstati der Sicherheitsmass-nahmen (Soll-Ist-Vergleich)
• Objekte mit Schutzbedarf „hoch“ oder „sehr hoch“	**Ergänzende Sicherheitsanalyse**	• Zusätzliche Sicherheitsmassnahmen mit Umsetzungsstati
• Massnahmen mit Umsetzungsstati „teilweise“ oder „nein“ • Budget • Personelle Ressourcen	**Realisierungsplanung**	• Projektplanung • Auftragslisten

Zu beachten: Der Output eines Vorgangs dient beim nächsten Vorgang u.U. als Input. Im Folgenden wird auf die verschiedenen Vorgänge im Detail eingegangen.

IT-Strukturanalyse

Netzwerkplan

- **Aktualisieren**: Netzwerkpläne sind möglichst aktuell zu halten, entsprechende Infos sind bei IT-Verantwortlichen, Administratoren etc. einzuholen.
- **Auswerten**: Welche IT-Systeme gibt es (Clients, Server etc.), welche Verbindungen existieren zwischen diesen Systemen (sehr wichtig!) und nach aussen (ebenfalls sehr wichtig!)
- Gleichartige Komponenten werden zu **Gruppen** zusammengefasst (=Komplexitätsreduktion). Z.B. Systeme vom gleichen Typ, gleicher Netzwerkanbindung, gleiche Aufgaben etc. Wichtig: Keine Komponenten mit unterschiedlichem Schutzbedarf zusammenfassen (z.B. Clients der GL mit den „normalen“ Clients oder Clients Buchhaltung mit Clients Personalabteilung).
- Diese Gruppen werden fortan **wie einzelne Objekte** behandelt.



Nr.	Beschreibung	Plattform	Standort	Anzahl	Status	Benutzer/Administrator
S1	Domänen-Controller	Windows Server 2003	BG, R. 1.02 (Serverraum)	1	in Betrieb	alle IT-Benutzer/ IT-Administration
S4	DB-Server Kunden- und Auftragsbearbeitung	Windows Server 2003	BG, R. 1.02 (Serverraum)	1	in Betrieb	Marketing und Vertrieb, Fertigung, Lager/ IT-Administration
C5	Clients Kunden- und Auftrags-bearbeitung	Windows Vista	BG, R. 2.03 – 2.09	14	in Betrieb	Einkauf, Marketing und Vertrieb/ IT-Administration

Zuordnung von Systemen und Anwendungen

- Schutzbedarf eines IT-Systems hängt vom Schutzbedarf der Anwendungen ab.
- IT-Systeme und Anwendungen werden einander deshalb zugeordnet.

Nr.	Beschreibung	Personenbezogene Daten	C2	C5	C6	C8	C9	S1	S3	S4	S6
A4	Auftrags- und Kundenverwaltung	X	X	X	X	X	X			X	
A5	Benutzerauthentisierung	X						X			X
A9	Druckservice BG								X		
A10	Druckservice Beuel										X
A13	Application Gateway										

A: Anwendung, C: Client, S:Server

- Für den Schutzbedarf eines Systems ist **diejenige Anwendung mit den höchsten Sicherheitsanforderungen** (bezüglich Vertraulichkeit, Integrität und Verfügbarkeit) relevant.
- Es gilt das **Maximumprinzip**.

Schutzbedarfsfeststellung

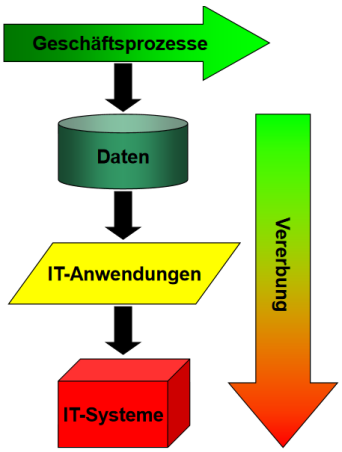
Bestimmung des Schutzbedarfs des betrachteten Informationsverbundes:

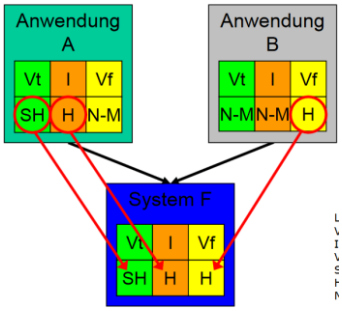
- Wie viel Schutz benötigen die identifizierten Objekte?
- Wie kommt man zu einer begründeten und nachvollziehbaren Einschätzung des Schutzbedarfs (notwendig, da die Einführung einer Massnahme u.U. viel Geld kostet)
- Welche Objekte haben einen erhöhten Schutzbedarf?

Vorgehen:

1. Definition von **Schutzbedarfskategorien**. Individuell, z.B. niedrig bis mittel, hoch und sehr hoch. Typische Schadenszenarien: Verstoss gegen Gesetze, Beeinträchtigung der persönlichen Unversehrtheit, Beeinträchtigung der Aufgabenerfüllung, Imageschäden, finanzielle Auswirkungen.
2. **Schutzbedarfsfeststellung** von IT-Anwendungen, Daten, IT-Systemen, Verbindungen.
3. **Dokumentation und Interpretation** der Ergebnisse (Begründung!)

Auch hier ist das Maximumprinzip zu beachten. Z.B. sind in einem Programm Kundendaten gespeichert welche einen hohen Schutzbedarf haben. So hat auch der Server, auf welchem die Daten liegen, einen erhöhten Schutzbedarf. Zweites Beispiel: Auf dem Server laufen 5 Anwendungen. Der Server erbt denjenigen Schutzbedarf von der Software mit dem höchsten Schutzbedarf.





Vt: Vertraulichkeit, I: Integrität, Vf: Verfügbarkeit, SH: Sehr hoch, H: Hoch, N-M: Niedrig bis mittel

Es existieren verschiedene Regeln:

- **Maximumprinzip**: Höchster Schutzbedarf der Anwendung gilt für das ganze System
- **Kumulationseffekt**: System hat höheren Schutzbedarf als die zugeordneten Anwendungen (höherer Schaden aufgrund von **gleichzeitigem Ausfall von mehreren Anwendungen**).
- **Verteilungseffekt**: System hat niedrigeren Schutzbedarf als die zugeordnete Anwendung (z.B. durch Redundanz oder Backup an externem Ort)

Schutzbedarfsfeststellung			
Nr.	**Bezeichnung**	**Schutzbedarf**	**Begründung**
A1	Personaldaten-verarbeitung	Vertraulichkeit: hoch	Personaldaten sind besonders schutzbedürftige Daten, deren Missbrauch die Betroffenen erheblich beeinträchtigen kann.
		Integrität: normal	Fehler werden rasch erkannt und können entweder aus der Datensicherung eingespielt oder durch Eingabe korrigiert werden.
		Verfügbarkeit: normal	Ausfälle bis zu einer Woche können mit manuellen Verfahren überbrückt werden.
A5	Benutzerauthen-tisierung	Vertraulichkeit: normal	Die Passwörter sind verschlüsselt gespeichert und damit praktisch nicht zugänglich.
		Integrität: hoch	Der hohe Schutzbedarf ergibt sich daraus, dass sich alle Mitarbeiter hierüber identifizieren.
		Verfügbarkeit: hoch	Bei Ausfall dieser Anwendung ist keine Identifizierung und damit keine Ausführung von IT-Verfahren möglich. Ein Ausfall ist allenfalls bis zu 24 Stunden tolerabel.

S1	Domänen-Controller	Vertraulichkeit: normal	Maximumprinzip gemäß Anwendung A5 (Benutzerauthentisierung)
		Integrität: hoch	Maximumprinzip gemäß Anwendung A5 (Benutzerauthentisierung)
		Verfügbarkeit: normal	Gemäß Anwendung A5 (Benutzerauthentisierung) wäre der Schutz-bedarf hoch. Er wurde als normal festgelegt, weil die Benutzer aus Bad Godesberg sich auch über den Domänen-Controller S6 in Beuel anmel-den können. Ein Ausfall bis zu drei Tagen ist hinnehmbar (Vertei-lungseffekt).

- Beurteilung bezüglich Vertraulichkeit, Integrität und Verfügbarkeit.
- Grundlage: Schutzbedarf der verarbeiteten Daten.
- Die Schadensszenarien sind dabei aus Sicht der Nutzer der Anwendungen zu betrachten.
- Auch die Schutzbedarfskategorien müssen begründet und dokumentiert werden.

IT-Räume

- Die Vererbung ist bis auf die IT-Räume anzuwenden. Evtl. Kumulationseffekte beachten.

Raum				Schutzbedarf		
Bezeichnung	**Art**	**Lokation**	**IT-Systeme**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**
BG, R. 1.01	Technikraum	Verwaltungsgebäude	TK-Anlage T1	normal	normal	hoch
BG, R. 1.02	Serverraum	Verwaltungsgebäude	S1 bis S5 N1 bis N5	hoch	hoch	hoch

Kommunikationsverbindungen

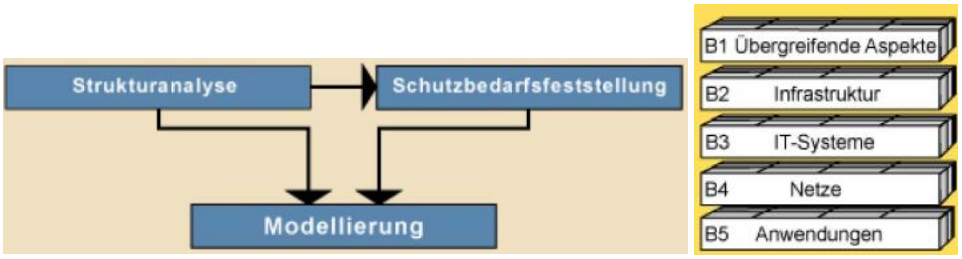
- **Kritisch sind Verbindungen in ein öffentliches Netz**, Verbindungen welche besondere schützenswerte Informationen übertragen und Verbindungen, über die vertrauliche Informationen NICHT übertragen werden dürfen.
- Der Schutzbedarf leitet sich von den angeschlossenen Systemen ab.

Interpretation

- Schutzbedarf normal bis mittel → Standard-Sicherheitsmassnahmen
- Schutzbedarf hoch → Standard-Sicherheitsmassnahmen + evtl. ergänzende Sicherheitsanalyse
- Schutzbedarf sehr hoch → Standard-Sicherheitsmassnahmen + zwingend ergänzende Sicherheitsanalyse (Vergleiche Grafik zu Beginn dieses Kapitels).

Modellierung nach IT-Grundschutz

- Die in den vorherigen zwei Schritten gewonnen Ergebnisse werden nun mit den vorhandenen IT-Grundschutz-Bausteinen abgeglichen.
- Ergebnis: IT-Grundschutz-Modell



- Total gibt es **85 Bausteine**.
- Schichtenweise werden diejenigen Bausteine ausgewählt, welche für die Sicherheit des IT-Verbunds notwendig sind.
- Die ausgewählten Bausteine werden dem jeweiligen Zielobjekt zugeordnet.
- Bei Bedarf werden die Bausteine modifiziert (z.B. zusätzliche Massnahmen)
- Wichtig: **Abschliessende Prüfung auf Vollständigkeit** durchführen. Sind alle IT-Systeme, Verbindungen und Anwendungen einbezogen? Wurden alle Objekte angemessen modelliert?

Baustein	Zielobjekt	Hinweise
B 1.4 *Datensicherungskonzept*	Gesamte Organisation	Gilt einheitlich für alle Betriebsteile.
B 2.1 *Gebäude*	Verwaltungsgebäude	Der Baustein muss auf beide Gebäude getrennt angewendet werden.
B 2.1 *Gebäude*	Produktionshalle	
B 2.4 *Serverraum*	Serverraum BG, R. 1.02	Der Baustein muss auf beide Serverräume getrennt angewendet werden.
B 2.4 *Serverraum*	Serverraum Beuel, R. 2.05	
B 3.203 *Laptop*	C9	Die Laptops in den Vertriebsbüros, in Bad Godesberg und in Beuel werden von den Vertriebsmitarbeitern benutzt und sind in einer Gruppe zusammengefasst.
B 5.7 *Datenbanken*	A3 Finanzbuchhaltung	Die Datenbanksysteme unterscheiden sich bezüglich ihrer Server, ihrer Benutzer und ihres Schutzbedarfs. Der Baustein ist daher getrennt auf beide Anwendungen anzuwenden.
B 5.7 *Datenbanken*	A4 Auftrags- und Kundenverwaltung	

Basis-Sicherheitscheck

- Soll folgende Fragen beantworten:
  - Sind meine Informationen hinreichend geschützt?
  - Was bleibt noch zu tun?
- Vorgehen: Bereits umgesetzte Massnahmen mit den Empfehlungen der IT-Grundschutz-Kataloge vergleichen (Soll- Ist Vergleich). So werden bestimmte Massnahmen nicht doppelt umgesetzt und man sieht, was noch fehlt. Schlussendlich hat es einen finanziellen Hintergrund.
- Organisatorische Vorarbeiten: Vorhanden Dokumente sichten, Inventar, Budget, Projektleiter / Key Personen aus mehreren Abteilungen definieren, Beizug externer Stellen abklären / organisieren, Interviewpartner suchen, Termine planen.

Maßnahme (erforderlich ab Siegelstufe)	ent-behrl.	ja	teil-weise	nein	Bemerkung/Begründung bei Nicht-Umsetzung
M 1.3 *Angepasste Aufteilung der Stromkreise* (A)				X	Bislang wurde die Elektroinstallation nicht geprüft.
M 1.7 *Handfeuerlöscher* (A)			X		Die betroffenen Mitarbeiter wurden nicht im Umgang mit den vorhandenen CO_2-Löschern geschult.
M 1.10 *Verwendung von Sicherheits-türen und -fenstern* (C)			X		Der Raum hat kein Sicherheitsfenster, nur eine Sicherheitstür.

Ergänzende Sicherheitsanalyse

- (Prüfungsfrage!) Sie ist durchzuführen, wenn für einzelne Zielobjekte
  - Die Schutzbedarfskategorie „hoch“ oder „sehr hoch“ in mindestens einem der drei Grundwerte (Vertraulichkeit, …) vorliegt.
  - Kein geeigneter Baustein im Katalog zu finden ist oder
  - Objekte in untypischer Weise oder Einsatzumgebung betrieben werden (z.B. ein Server in einem U-Boot).

Das Ergebnis ist eine Festlegung, ob Grundschutzmassnahmen für das Objekt genügen oder weitergehende Untersuchungen notwendig sind. Beispiele für diese Untersuchungen:

- Klassische Risikoanalyse: Bedrohungen und Schwachstellen ermitteln, Eintrittswahrscheinlichkeiten und Schadenshöhen schätzen.
- Penetrationstest: Verhalten eines Angreifers simulieren, **Blackbox- und Whitebox-Ansatz**
  - Blackbox → nicht von Interesse WIE das System ausschaut → „ausprobieren was geht“.
  - Whitebox → System, Struktur, Geräte müssen bekannt sein → diese Kenntnisse ausnutzen.

Realisierungsplan

- Fehlende Sicherheitsmassnahmen zusammenstellen
- Massnahmen definieren und Umsetzungsreihenfolge festlegen
- Aufwand schätzen, Verantwortliche und Termine bestimmen
- Ergebnis: Realisierungsplan aka. Roadmap.

Zielobjekt: BG R. 1.02 Serverraum				
Baustein: B 2.4 Serverraum				
Maßnahme (erforderlich ab Siegelstufe)	**Umsetzung bis**	**Verantwortlich**	**Budget**	**Bemerkungen**
M 1.3 (A) *Angepasste Aufteilung der Stromkreise*	38. KW	Umsetzung: M. Wachsam Kontrolle: P. Muster	a) 0,- € b) 0,3 PT c) 0,- € d) 0 PT/Jahr	Die Elektro-Installation wird von der Haustechnik geprüft. Eine mindestens jährliche Überprüfung wird festgelegt.

Z = Zusatzmassnahme, PT = Personentage, a) einmalige Investition, b) einmaliger Personalaufwand, c) wiederkehrende Kosten, d) wiederkehrender Personalaufwand

Zusammenfassung IT Grundschutz

Argumente „Pro“:

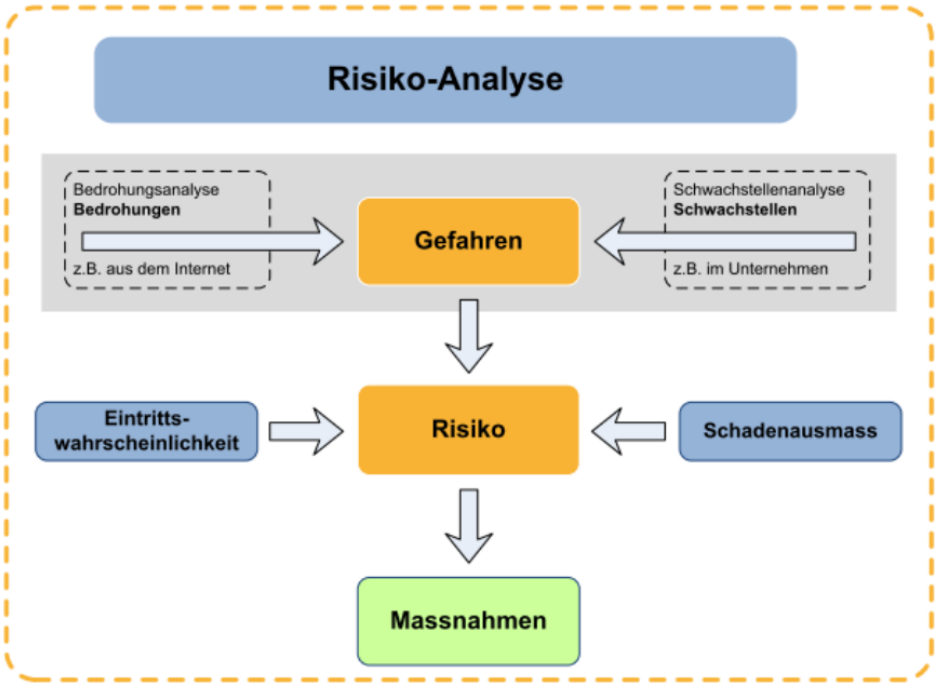
- Standardbasierend
- Vollständig
- Keine detaillierte Risikoanalyse notwendig
- Gleichmässiger, umfassender Schutz auf allen Objekten
- Einfach und schnell anwendbar
- Definierte Basis für weitergehende Schutzmassnahmen (ergänzte Analysen)

Aufpassen bei:

- Ungenügender Schutz bei erhöhten Risiken oder besonderem Schutzbedarf
- Mögliche Einschränkungen der Funktionalität durch Überschutz.
- Begründung von Massnahmen schwierig.
- Je nach Detaillierungsgrad, Anspruch an Aktualität und Vollständigkeit des Massnahmenkatalogs aufwändig.
- Vorteile des Grundschutzvorgehens nicht durch administrativen „Overkill“ zunichtemachen.

Vorgehen Risikoanalyse

- Risikoanalyse anwenden wenn Objekte hohen oder sehr hohen Schutzbedarf aufweisen.
- Potentielle Risiken im IT-Bereich: Nicht autorisierte Zugriffe, fehlende Fachkompetenz von Mitarbeitern, Datendiebstahl, veraltete Softwarelösungen, mangelhafte Backups, fehlender Notfallplan, mangelhafte Dokumentation etc.
- Risikomanagement-Stile:
  - Risiken ignorieren („Cowboy“)
  - Risiken scheuen („Maus“)
  - Risiken eingehen, diese aber kontrollieren („Kontrolliert handelnder Unternehmer“)
  - Risiken scheuen, aber trotzdem viel kontrollieren („Bürokrat“).
- Operationelle Risiken: Risiken, welche in einer Unternehmung Schäden verursachen können.
- **Risiko = Eintrittswahrscheinlichkeit * Schadensausmass**
- Qualitative Risikoanalyse: Die beteiligten Grössen werden nur eingeschätzt (z.B. 1 bis 5).
- Quantitative Risikoanalyse: Die beteiligten Grössen sollen numerisch korrekt berechnet werden.

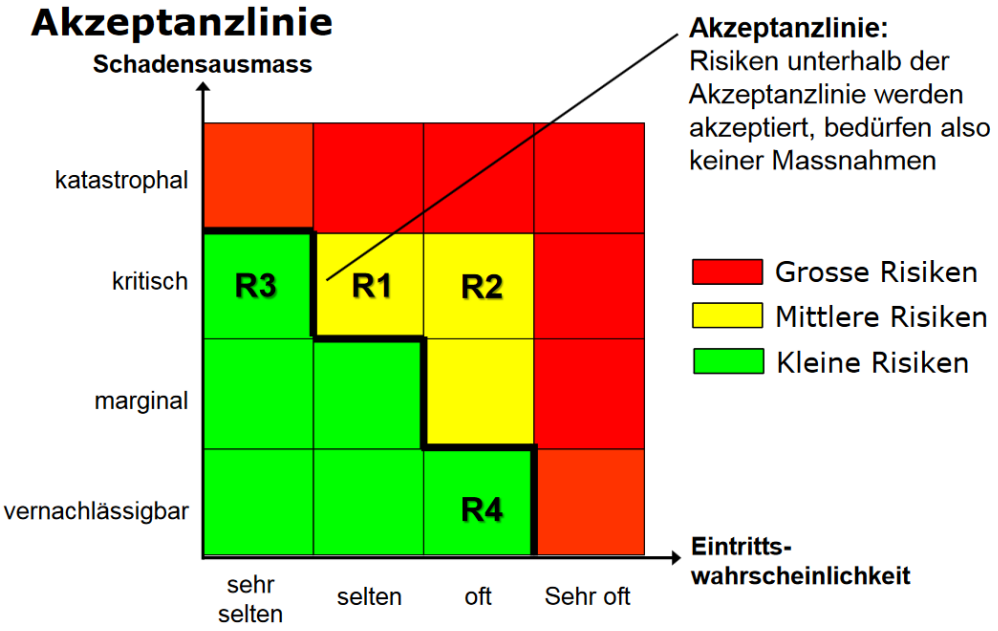


- Gefahren nach ISO sind z.B. Physische Schäden (Feuer, Wasser etc.), Naturereignisse, Verlust wichtiger Dienste (kein Strom mehr), Kompromittieren von Informationen (Diebstahl, ausspionieren, …), Technisches Versagen, unautorisierte Aktionen.
- **Die grösste Gefahr stellt jedoch der Mensch an sich dar**: Social engineering, hacking, spoofing, Terrorismus, Informationsdiebstahl, verkauf persönlicher Infos, Systemsabotage etc.

Definition Schadensausmass und Eintrittswahrscheinlichkeit

- Empfohlen wird eine 3- bis 5-stufige Skala.
  - Z.B. Vernachlässigbar, marginal, kritisch, katastrophal für Schadensausmass
  - Z.B. sehr selten, selten, oft, sehr oft für Eintrittswahrscheinlichkeit
- Die Stufen sind im Detail zu definieren, z.B. bedeutet selten: alle 5 Jahre, oft = jährlich, katastrophal = Sachschäden > 500‘000.- CHF, Schwerverletzte oder grosser Imageschaden.

Risiko-Landkarte



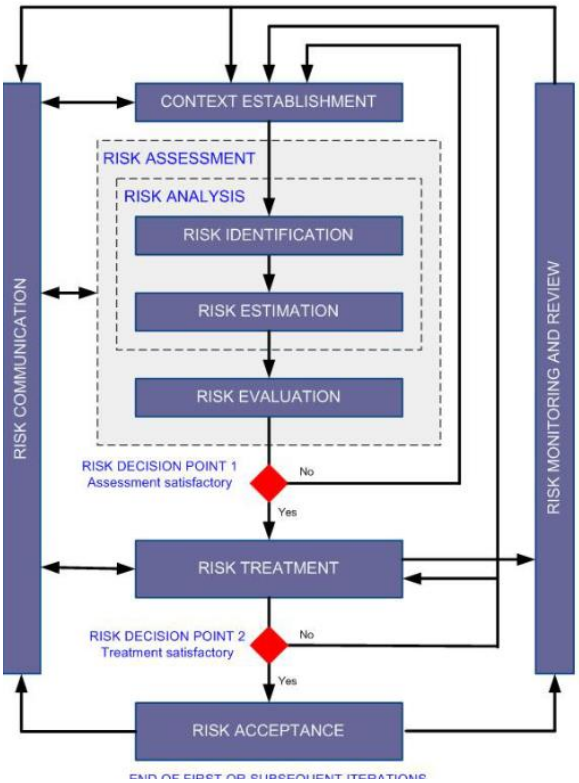
- Beispiel für ein Risiko welches nicht verhindert werden kann: Das man Konkurs geht.
- **Risikobewältigung**
  - Risiken vermeiden: Geschäftsprozesse aufgeben oder anpassen.
  - Risiken vermindern: Sicherheitsmassnahmen einsetzen, um Schadensausmass oder Eintrittswahrscheinlichkeit zu reduzieren.
  - Risiken übertragen: Überwälzen finanzieller Schäden auf Versicherungen
  - Risiken tragen: Akzeptieren von (Rest-)Risiken (= Selbstbehalt bei Versicherung)
- Der Entscheid, wie mit Risiken umgegangen werden soll, muss dokumentiert und von der Geschäftsleitung genehmigt werden.

Risiko-Katalog

Nr	Risiko	Auswirkungen	W	A	Massnahmen	W	A
			vor Mass-nahmen			nach Mass-nahmen	
1	Viren	Integrität, Verfügbar-keit, Vertraulichkeit	4	3	Virenscanner, Fire-wall etc.	1	1
2	Diebstahl Note-book	Datenverlust	3	2	Sensibilisierung, Verschlüsselung	3	1

- Dienen der Buchführung über identifizierte Risiken.
- Übrig gebliebene Risiken nach dem Durchführen der Massnahmen = Restrisiken, welche dokumentiert und von der GL genehmigt werden müssen.

Risiko-Management Prozesse



Ein professionelles Unternehmensrisiko-Management muss als Prozess organisiert werden

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 Folie 38

- Context Establishment: Gegenstand, Zweck, Absichten, Ziele, Fokus und relevante Einflüsse, Randbedingungen und Abgrenzungen aus externer und interner Sicht festlegen.
- Risk Identification: Objekte, Bedrohungen, Schwachstellen und bereits existierende Massnahmen erfassen.
- Risk Estimation: Häufigkeit und Schadensausmass einschätzen.
- Risk Evaluation: Bewertung der identifizierten Risiken.
- Risk Treatment: Definition, Konzeption, Planung und Umsetzung von Massnahmen.
- Risk Acceptance: Akzeptanz des risk treatments und Restrisiko-Einschätzung durch GL
- Risk Communication: Information der direkt Beteiligten und Betroffenen in jedem Prozess.
- Risk Monitoring and Review: Situation bezüglich allfälliger Veränderungen überwachen.

Kriterien für die Prozess**wiederholung**:

- Externe Trigger: Ändernde Umgebungsbedingungen, inakzeptable Restrisiken, neue Anforderungen.
- Periodische Durchführung: Synchron mit anderen Management-Prozessen (z.B. Strategieprozesse).

Notfallplanung, Notfallorganisation

Englischer Begriff: Business Continuity Management

Beispiele für Notfälle:

- DDoS Attacke auf Firmenwebsite (Bank für 48h offline → bankrott)
- Feuer, Wasserschaden
- Stromausfall für längere Zeit
- Datenverlust, z.B. Malware verschlüsselt Daten
- Phising Angriff: Kunden melden leere Bankkonten.

Ziele der Notfallvorsorge:

- Sicherstellen des Geschäftsfortganges. Dafür sind die wichtigsten Geschäftsprozesse, Applikationen, Systeme und Netzwerke zu identifizieren.
- Schadensminimierung

Grundlagen / Vorgaben zum Notfall-Management finden sich in:

- ISO 27002
- BSI Standard 100-4
- Informationssicherheitshandbuch

Phasen:

1. Planung der Notfallvorsorge
    a. Analyse der Bedürfnisse
    b. Zu schützende Geschäftsprozesse und die dazu nötige Infrastruktur identifizieren
    c. Mögliche Notfallszenarien
2. Umsetzung der den IT-Betrieb begleitenden Notfallvorsorge-Massnahmen (z.B. Notfallgenerator in Betrieb nehmen).
3. Durchführung von Notfallübungen.
4. Umsetzung geplanter Massnahmen nach Eintreten eines Notfalls.
5. Rückkehr zum Normalzustand.

Business Impact Analysis (BIA)

- **Unterschied zu Risikoanalyse:** Man geht hier davon aus, dass ein Vorfall bereits passiert ist.
- BIA: Ermitteln der Wichtigkeit (Kritikalität) der Geschäftsprozesse resp. Applikationen.
- In den Spalten werden Ausfallzeiten, in den Reihen Prozesse/Applikationen eingetragen.
- Pro Feld wird anschliessend die Beeinträchtigung auf die Unternehmung ermittelt (z.B. klein, mittel, gross, existenziell) → Ähnlich Schutzbedarfskategorie nach BSI

Umsetzung

Notfallmanagement

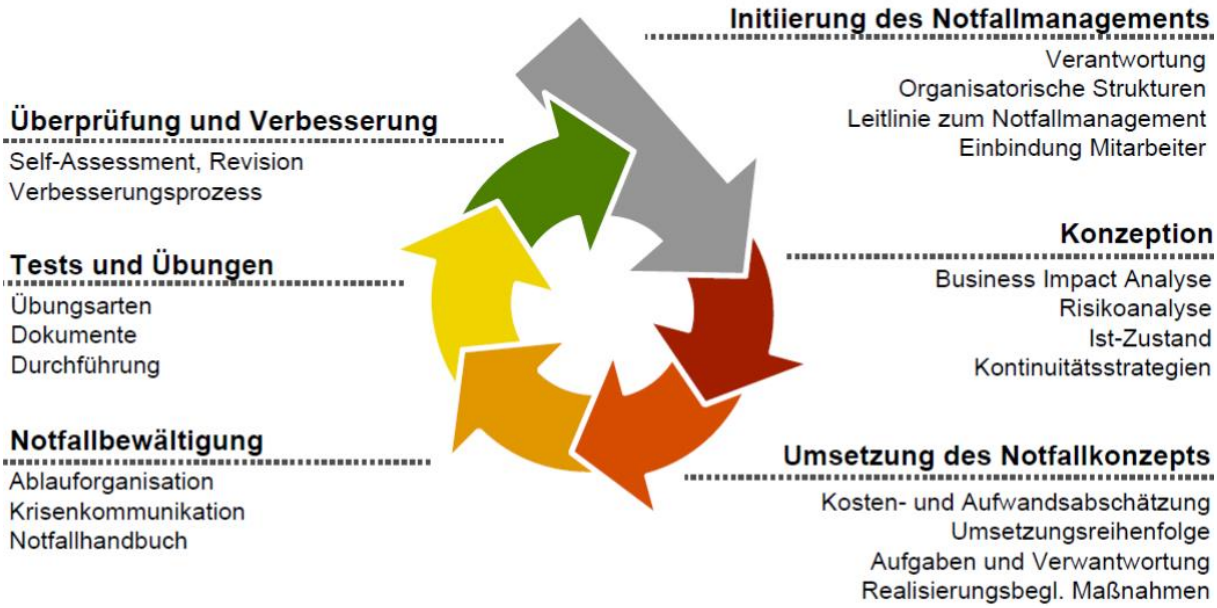


Bild 1 Notfallmanagement gemäss BSI-Standard 100-4

Notfallmanagement ist ein rekursiver Prozess!

Notfallorganisation

- Definition der Stäbe (Militär)
- Festlegen der Rollen
- Pflichtenheft der einzelnen Aufgaben
- Klären der Verantwortlichkeiten / Kompetenzen
- Definition der Entscheidungswege / Erreichbarkeit
- Festlegen der Stellvertretung

Notfallhandbuch

- Einfache Anleitung zur Bewältigung eines Notfalls
  - Notfallorganisation
  - Alarmierung (wer muss alarmiert werden?)
  - Sofortmassnahmen
  - Vorbehaltene Entschlüsse
- Charakteristik: KISS, Checklistenartig, muss ständig aktualisiert werden
- Das **Handbuch** dient als Unterstützung (Überblick in Paniksituation behalten) und sollte auch von jemand anderen angewendet werden können, falls die zuständige Person nicht da ist.
- Das Handbuch ist an einem sinnvollen Ort, möglichst extern, zu deponieren.

Vorbehaltene Entschlüsse

Vorgängig erarbeitete Massnahmen für einen bestimmten Fall. Die Lösungen sind nicht nur IT-bezogen, sondern kommen auch aus den Fachabteilungen.

Informationspolitik bei einem Vorfall

Wer wird wann worüber informiert?

- Mitarbeitende
- Kunden
- Öffentlichkeit
- Briefing Mitarbeiter bezüglich der Weitergabe von Informationen

Notfallübungen

- Zur Festigung der Kompetenzen in der Krisenbewältigung
- Training für Stellvertreter
- Alarmierungstest
- Erkennen von Schwächen in der Notfallvorsorge

Häufige Schwächen bei der Notfallvorsorge

- Doku nicht aktuell
- Nie eingeübt
- Beschreibung zu kompliziert
- Vorgehen zu aufwendig
- Im Notfall nicht verfügbar

Prüfungsvorbereitung:

- BSI-Standard 100-4, Kap. 3 (S. 10 bis 14) lesen
- IT-Grundschutz-Katalog Baustein „B 1.3 Notfallmanagement“ lesen.

Awareness

Awareness = Bewusstsein. Die gängige Meinung lautet: „Sicherheitsmassnahmen hemmen nur die bekannten Abläufe und stören die Effizienz der Arbeit.“ Informationssicherheit sollte jedoch zur Selbstverständlichkeit und Bestandteil der Firmenkultur werden.

- Informationssicherheit wird erreicht durch Technik (kaufen), Prozesse (definieren) und die Mitarbeiter, welche sensibilisiert und ausgebildet werden müssen.
- Der Mensch kann den grössten Schutz bieten und gleichzeitig auch das grösste Risiko darstellen → Das Potential der Mitarbeiter muss eingebunden werden.
- Awareness muss vom obersten Management unterstützt werden!

Risiken durch Mitarbeiter:

- Lässt Sachen rumliegen
- Verwendet ein schwaches Passwort
- Falscher Umgang mit E-Mail / Internet
- Gibt interne Infos nach aussen weiter
- Mangelhafte Datenablage (Backup, Struktur)

Gegenmassnahmen:

- Technischer Art: Content Filter, Überwachung, Berechtigungen
- Organisatorischer Art: Weisungen, Awareness, Schulungen, Kultur
- Die Einsicht durch den Mitarbeiter sollte im Vordergrund stehen, nicht das Verbot. „Wenn du ein Schiff bauen willst, so trommle nicht Menschen zusammen, um Holz zu beschaffen, Werkzeuge vorzubereiten, Aufgaben zu vergeben und die Arbeit einzuteilen, sondern lehre die Menschen die Sehnsucht nach dem weiten, endlosen Meer“.
- Verständnis schaffen → Verhalten ändern → zur Gewohnheit werden.

Weisungen/Richtlinien:

- Verhaltensregeln definieren
- Do and don’ts festlegen
- Mögliche Inhalte einer Benutzerrichtlinie: Internet (Inhalte, Download → verantwortungsvoll), Installation Software, Passwort, private Hardware (BYOD), E-Mail, Zutritt (Extern, Büro), Clear-Desk, Sanktionen.
- Eine Richtlinie alleine nützt nichts, wenn sie nicht angewandt wird!

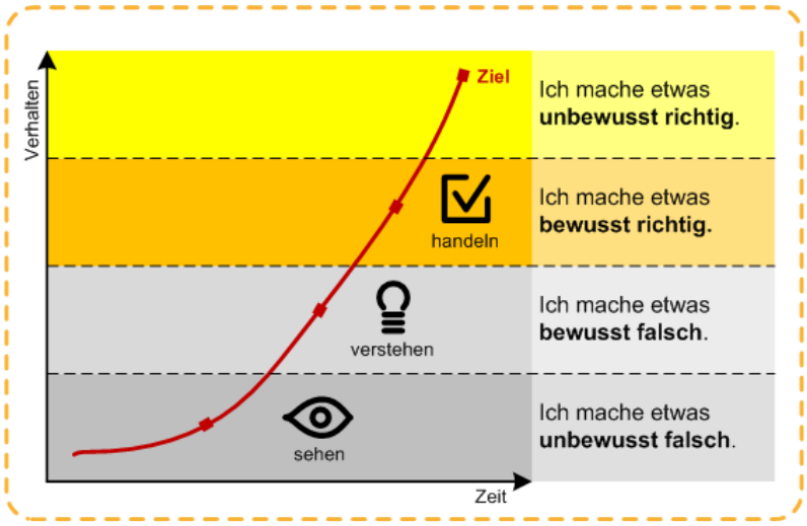
Warum «Awareness»?

- Mensch = grösste Chance UND grösstes Risiko
- Fachkompetenz bilden
- Berücksichtigung der «Mündigkeit» der Betroffenen.

Sanktionen

- Sind zu definieren und anzuwenden (Unterstützung durch das Management)
- Ein „verbindliches Regelwerk“ muss vorhanden sein und die Mitarbeiter müssen Kenntnis von diesem und es auch verstanden haben.
- Nicht Härte, sondern Konsequenz.

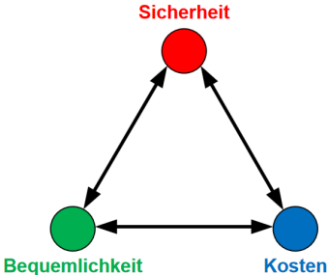
Prozess der Verhaltensänderung:



Awareness und deren Bedeutung im Unternehmen:

- Muss vom obersten Management unterstützt werden (Ressourcen bereitstellen, Vorbildfunktion)
- Ist stufengerecht zu schulen (normaler Benutzer, IT-Mitarbeiter, Management)
- Schon kleine Massnahmen erhöhen die Informationssicherheit wesentlich.

Informationssicherheit im Spannungsfeld:



Awareness-Programm

- Sollte auf Zielpublikum zugeschnitten, verständlich und verdaubar sein.
- Aha-Erlebnis
- Aufforderung zur Tat
- Nachhaltigkeit

Begriffe

BIA *Business Impact Analysis*
BSI *Bundesamt für Sicherheit in der Informationstechnik*
COBIT *Control Objectives for Information and Related Technology*
DDoS *Distributed Denial of Service*
ISF *Information Security Forum*
ISK *Informationssicherheitskonzept*
ISMS *Informationssicherheitsmanagementsystem*
ISO *International Organization for Standardization*
ISP *Informationssicherheits-Policy, Siehe*
SOA *Statement of Applicability*