

Security Management

Inhaltsverzeichnis

1 Kapitel 1 – Einführung.....	3
1.1 Information.....	3
1.1.1 Was gefährdet die Information (Bedrohungen)?.....	3
1.1.2 Mögliche Täter	3
1.1.3 Bedrohungskategorien	4
1.2 Verantwortung.....	4
1.2.1 Management Grundregeln	4
1.2.2 Was passiert wenn wir nichts machen?	5
1.3 Informationssicherheit.....	5
1.3.1 Sicherheit.....	5
1.3.2 Informationssicherheit	5
1.3.3 Nutzen der Informationssicherheit	5
1.3.4 Wie anpacken?	5
1.3.5 Vorgehen Informationssicherheit	6
1.3.6 Grundziele der Informationssicherheit	6
1.3.7 Zeitpunkt der Entdeckung eines Grundzielverlustes	6
1.4 Identität / Authentizität	6
1.4.1 Identität.....	6
1.4.2 Authentizität.....	7
1.5 Risiko	7
1.5.1 Risiko/Sicherheit	7
1.5.2 Abwägen von Risiko- und Massnahmenkosten	7
1.6 Integrale Sicherheit.....	8
1.7 Informationssicherheit: Womit?	8
1.8 Informationssicherheit VS IT-Sicherheit.....	8
1.9 Datensicherheit VS Datenschutz	9
1.10 Datenschutzgesetz (DSG)	9
1.11 Zutritts-, Zugangs- und Zugriffskontrolle	9
2 Kapitel 2 – ISMS und Informationssicherheitsstandards.....	10
2.1 ISMS (Information Security Management System)	10
2.1.1 Motivation, Zweck.....	10
2.1.2 Vorgehen	10
2.1.3 Komponenten eines ISMS	10
2.2 Überblick der ISO-Standards	11
2.2.1 Nutzen von Standards	11
2.2.2 ISO 27000 (ISMS – Overview and vocabulary).....	11
2.2.3 ISO 27001 (ISMS – Requirements)	12
2.2.4 ISO 27002 (Code of practice for information security mgmt)	13
2.2.5 ISO 27003 (ISMS implementation guidance)	13
2.2.6 ISO 27004 (Information security management – Measurement).....	14
2.2.7 ISO 27005 (Information security risk management).....	14
2.2.8 Aufgabe zu den ISO-Standards	15
2.3 BSI-Standards und IT-Grundschutzkataloge	15
2.3.1 Idee des IT-Grundschutzes.....	15
2.3.2 Inhalt der IT-Grundschutzkataloge	16
2.3.3 Nutzen der IT-Grundschutzkataloge	17
2.3.4 Aufgaben zu IT-Grundschutzkatalogen	17
2.3.5 BSI-Standard 100-1 (Managementsysteme für Informationssicherheit)	18
2.3.6 BSI-Standard 100-2 (IT-Grundschutz-Vorgehensweise)	18
2.3.7 BSI-Standard 100-3 (Risikoanalyse auf Basis von IT-Grundschutz)	19
2.3.8 BSI-Standard 100-4 (Notfallmanagement)	19
2.4 ISO 27001 Zertifikat auf der Basis von IT-Grundschutz	20
2.5 Information Security Forum (ISF) - Standard of Good Practice for Information Security	20
3 Kapitel 3 - Sicherheitspolitik und –Konzepte	21
3.1 Sicherheitspyramide nach SiBH	21
3.2 Sicherheitspyramide nach BSI	21
3.3 Dokumentstruktur nach BSI	21

3.4	Sicherheitspyramide	22
3.5	Checkliste Informationssicherheitspolitik	23
3.6	Informationssicherheitspolitik (ISP) – 1. Stufe	24
3.6.1	<i>Definition</i>	24
3.7	Informationssicherheitskonzepte (ISK) – 2. Stufe	24
3.7.1	<i>Definition</i>	24
3.7.2	<i>Ziele</i>	25
3.7.3	<i>Vorlagen zu Sicherheitskonzepten</i>	25
3.7.4	<i>Beispiele von Sicherheitskonzepten</i>	25
3.7.5	<i>Weitere Sicherheitskonzepte</i>	25
3.8	Regelwerk / Massnahmenkatalog - 3. Stufe	26
3.8.1	<i>Beispiele von Richtlinien</i>	26
3.9	Zusammenspiel ISP und ISK	26
4	Kapitel 4 – Vorgehen IT-Grundschutz	28
4.1	BSI-Standard 100-2: IT-Grundschutz Vorgehensweise	28
4.2	BSI-Standard 100-3: Risikoanalyse auf Basis von IT-Grundschutz	28
4.2.1	<i>Stufe 1</i>	28
4.2.2	<i>Stufe 2:</i>	28
4.3	Kreuzreferenztabellen	28
4.4	Bemerkungen zum IT-Grundschutz	29
4.5	IT-Grundschutz Wirkprinzip	29
4.6	Grundregeln	29
4.7	Erstellung IT-Sicherheitskonzept	30
4.7.1	<i>IT-Strukturanalyse</i>	31
4.7.2	<i>Schutzbedarf feststellung</i>	32
4.7.3	<i>IT-Grundschutzanalyse</i>	34
4.7.4	<i>Ergänzende Sicherheitsanalyse</i>	36
4.7.5	<i>Realisierungsplan</i>	36
4.8	IT-Grundschutz – Aufpassen	36
5	Kapitel 5 – Risikoanalyse	37
5.1	Vorgehen	37
5.2	Risiken in Unternehmen	37
5.2.1	<i>Risiken im Bereich der IT-Organisation</i>	38
5.2.2	<i>Bedrohungen / Gefahren</i>	38
5.3	Risiko Ermittlung	38
5.4	Risiko Analyse	38
5.4.1	<i>Vorgehen</i>	38
6	Kapitel 6 – Notfallplanung	42
6.1	Ziele	42
6.1.1	<i>Themen</i>	42
6.2	Fokus	42
6.3	Phasen	42
6.4	Business Impact Analysis (BIA)	42
6.5	Notfallvorsorge für grösste Risiken	43
6.6	Umsetzung	43
1.	<i>Notfallmanagement</i>	43
2.	<i>Notfallorganisation</i>	43
3.	<i>Notfallhandbuch</i>	43
4.	<i>Vorbehaltene Entschlüsse</i>	44
5.	<i>Informationspolitik / Kommunikationspolitik</i>	44
6.	<i>Notfallübungen</i>	44
6.7	Schwächen der Notfallvorsorge	44
7	Kapitel 7 – Awareness	45
7.1	Risiken durch Mitarbeiter	45
7.2	Weisungen / Richtlinien	45
7.2.1	<i>Beispiel Benutzerrichtlinien (mögliche Inhalte)</i>	45
7.3	Awareness und deren Bedeutung für Unternehmen	45
7.4	Wie anpacken?	45
7.4.1	<i>Zeitlicher Ablauf eines Awareness Programms</i>	45
7.4.2	<i>Comments</i>	46
8	Glossar	47

1 Kapitel 1 – Einführung

1.1 Information

Information ist die Verknüpfung von Daten in Form von Zahlen, Worten und Fakten zu interpretierbaren Zusammenhängen. Durch die Vernetzung von Informationen entsteht Wissen, das zunächst personenbezogen ist.

Informationen müssen vor Missbrauch geschützt werden!



1.1.1 Was gefährdet die Information (Bedrohungen)?

- **Nicht vorsätzliche (Zufällige) Gefährdungen**
 - Naturgefahren (Blitz, Hagel und Unwetter...)
 - Ausfall von Strom oder Telekommunikation
 - Technische Pannen oder Fehler von Hard- und Software
 - Bedienerfehler / Fahrlässigkeit der Mitarbeitenden
- **Vorsätzliche Gefährdungen**
 - Bösartiger Code (Viren, Würmer, Trojaner etc.)
 - Informationsdiebstahl
 - Angriffe (von Skript-Kiddies bis Hacker)
 - Wirtschaftsspionage („was die Konkurrenz wissen möchte“)
 - Missbrauch der IT-Infrastruktur

1.1.2 Mögliche Täter

- Mitarbeitende (z.B. enttäuschte)
- Geheimdienste (Echelon, Onyx, ...)
- Industriespionage
- Hacker/Cracker
- Whistleblower (ein Hinweisgeber oder ein Informant)
- Softwareentwickler (Back Doors)
- Fremdpersonal
- Administratoren

1.1.3 Bedrohungskategorien

Höhere Gewalt	Feuer, Blitz, Sturm, Überschwemmung, Personalabgang, Krankheit, Stromausfall.....
Menschliches Versagen	Fahrlässigkeit, Gleichgültigkeit, Unwissenheit, Leichtgläubigkeit, Fehlmanipulation, fehlende Sensibilisierung, Übermüdung, Unwissen, falsches Verhalten....
Gesetzliche und vertragliche Mängel	Nicht einhalten von Gesetzen, Reglementen etc. (Compliance), juristische Konsequenzen bei Vertragsverletzungen...
Organisatorische Schwachstellen	Fehlendes Sicherheits-verständnis des Managements, Unklare Verantwortlichkeiten, Ungenaue oder fehlende Abläufe / Prozesse, Mangelhafte Richtlinien, Keine Strategie und Konzepte, Mangelhafte Awareness der Mitarbeitenden, Fehlende Kontrollen usw...
Technisches Versagen	Ungenügende Wartung, Keine präventive Überwachung (Managed Security missing), Falsch dimensionierte Systeme, Fehlerhafte Konfiguration, Fehlerhafte Applikationen /Betriebssysteme /Firmware / Treiber usw...

1.2 Verantwortung

Fehlende Informationssicherheit kann den Geschäftsfortgang stören oder verunmöglichen. Der Schutz der Informationen gehört zur Sorgfaltspflicht des Managements! Die 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)

1.2.1 Management Grundregeln

- Die **Verantwortung** für die Informationssicherheit liegt beim Management und kann nicht delegiert werden. Es entscheidet über den Umgang mit den Risiken, stellt die notwendigen Mittel zur Verfügung und trägt das Risiko.
- Informationssicherheit muss in **alle Prozesse und Projekte** integriert werden, bei denen Informationen übertragen, verarbeitet und genutzt werden.
- Der IS-Prozess muss vom Management überwacht werden.
- Für den IT-Betrieb und die Informationssicherheit müssen ausreichend **Ressourcen** bereitgestellt werden.
- Es müssen die organisatorischen **Rahmenbedingungen** für die Informationssicherheit geschaffen werden.
- Die Umsetzung muss wirtschaftlich sein. IS darf nicht mehr kosten als die damit erreichte Risikominderung.
- Die IS muss in sinnvoller Relation zum Schutzbedarf stehen (**Angemessenheit**).
- Die Schutzmassnahmen müssen realisierbar sein und dürfen die Sicherheitslage nicht verschärfen (**Praktikabilität**). Sie müssen nachweisbar Bedrohungen abwehren bzw. Risiken mindern (**Wirksamkeit**).

1.2.2 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 können strafrechtliche Folgen haben
- Verletzung der Sorgfaltspflicht

1.3 Informationssicherheit

1.3.1 Sicherheit

Sicherheit bezeichnet einen Zustand, der frei von unvertretbaren Risiken der Beeinträchtigung ist oder als gefahrenfrei angesehen wird.

1.3.2 Informationssicherheit

Als **Informationssicherheit** bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden Systemen, die die **Vertraulichkeit**, **Verfügbarkeit** und **Integrität** sicherstellen.

Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von Schäden und der Minimierung von Risiken. In der Praxis orientiert sich die Informationssicherheit heute unter anderem an der ISO/IEC Standard-Reihe 2700x aber auch zunehmend an ISO/IEC 15408.

Die Informationssicherheit ist gewährleistet, wenn die Informationen ausschliesslich dem autorisierten Personenkreis zugänglich sind (**Vertraulichkeit**), in einer kontrollierten, konsistenten und nachvollziehbaren Art und Weise erzeugt, mutiert oder ergänzt werden (**Integrität und Authentizität**) und innerhalb nützlicher Frist zur Verfügung stehen (**Verfügbarkeit**).

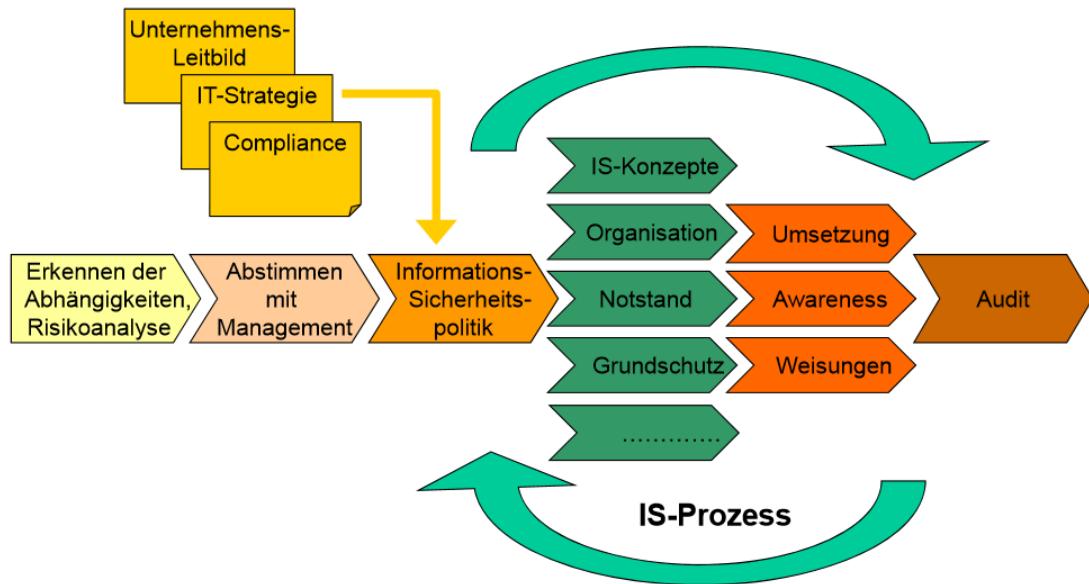
1.3.3 Nutzen der Informationssicherheit

Sicherheitsmanagement-Ziele	Nutzen
Etablierter Sicherheitsprozess	Geringere Verwundbarkeit Bessere Verfügbarkeit
Sensibilisierung der Mitarbeiter	Wettbewerbsvorteil Kundenzufriedenheit
Gesetzliche/vertragliche Verpflichtungen	Reduktion Haftungsrisiko (Sorgfaltspflicht)
Notfallplanung	Sicherung des Geschäftsfortgangs
Messbarkeit und Kontrolle der Sicherheit	Transparenz bringt Existenzberechtigung

1.3.4 Wie anpacken?

- Management ins Boot holen
- Prozess der Informationssicherheit etablieren
- Verantwortlichkeiten festlegen
- Sicherheit allumfassend betrachten
- Schrittweise und stetig umsetzen

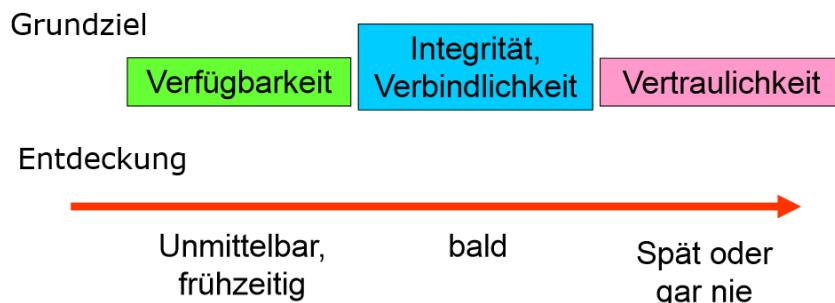
1.3.5 Vorgehen Informationssicherheit



1.3.6 Grundziele der Informationssicherheit

Vertraulichkeit	Vertraulichkeit ist gegeben, wenn sichergestellt werden kann, dass Informationen nicht durch unautorisierte Personen, Instanzen oder Prozesse eingesehen werden können. (Confidentiality)
Integrität	Integrität ist gewährleistet, wenn Daten oder Systeme nicht unautorisiert oder zufällig manipuliert werden können. (Integrity)
Verfügbarkeit	Verfügbarkeit ist gewährleistet, wenn in der vom Benutzer gewünschten Zeit auf Dienste oder Informationen zugegriffen werden kann. (Availability)
Verbindlichkeit	Verbindlichkeit liegt vor, wenn eine Handlung eindeutig einer Person zugeordnet und von dieser nicht geleugnet werden können. (Non-Repudiation)

1.3.7 Zeitpunkt der Entdeckung eines Grundzielverlustes



1.4 Identität / Authentizität

1.4.1 Identität

Beim Menschen bezeichnet Identität (lateinisch *idem*, *derselbe*, *dasselbe*, *der Gleiche*) die ihn kennzeichnende und als Individuum von anderen Menschen unterscheidende Eigentümlichkeit seines Wesens.

1.4.2 Authentizität

In der Informationssicherheit bezeichnet **Authentizität** die Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit. Die Überprüfung einer behaupteten Eigenschaft wird als Authentifikation bezeichnet. Durch Authentifikation des Datenursprungs wird nachgewiesen, dass Daten einem angegebenen Sender zugeordnet werden können, was durch digitale Signaturen ermöglicht werden kann.

1.5 Risiko

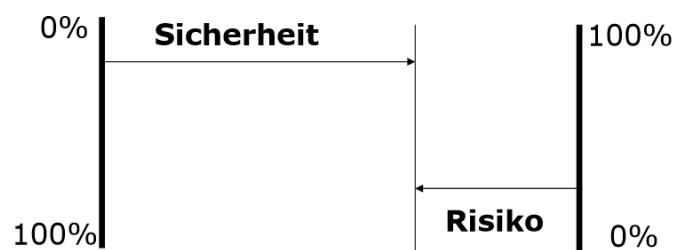
Möglicher negativer Ausgang bei einer Unternehmung, mit dem Nachteile, Verlust, Schäden verbunden sind; mit einem Vorhaben, Unternehmen o.Ä. verbundenes Wagnis.

→ Wahrscheinlichkeit, dass eine Gefährdung über eine Schwachstelle zu einem Schaden von bestimmtem Ausmass führt.

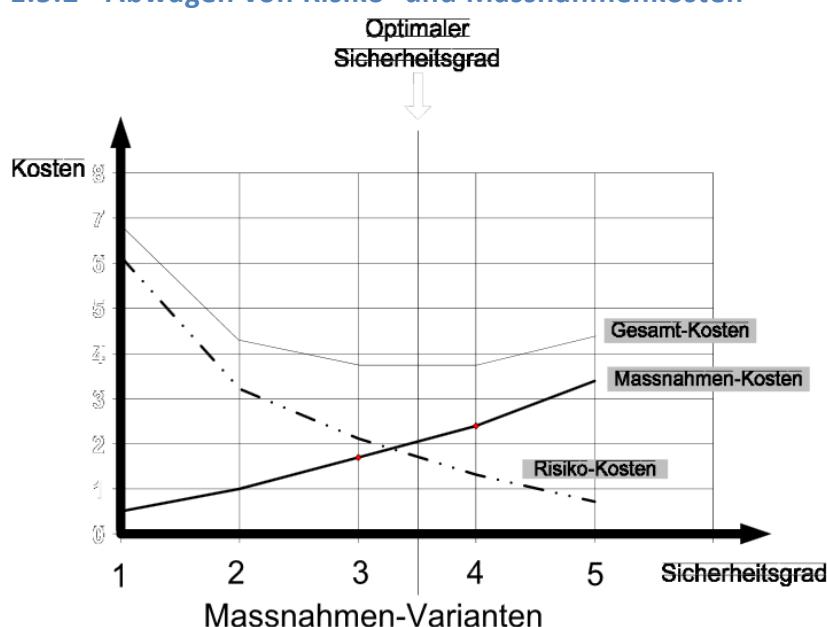
$$\boxed{\text{Risiko} = \text{Eintrittswahrscheinlichkeit} * \text{Schadenausmass}}$$

1.5.1 Risiko/Sicherheit

Die Eintrittswahrscheinlichkeit und die negative Zielabweichung können bewertet werden. Sicherheit und Risiko sind voneinander abhängig!



1.5.2 Abwägen von Risiko- und Massnahmenkosten

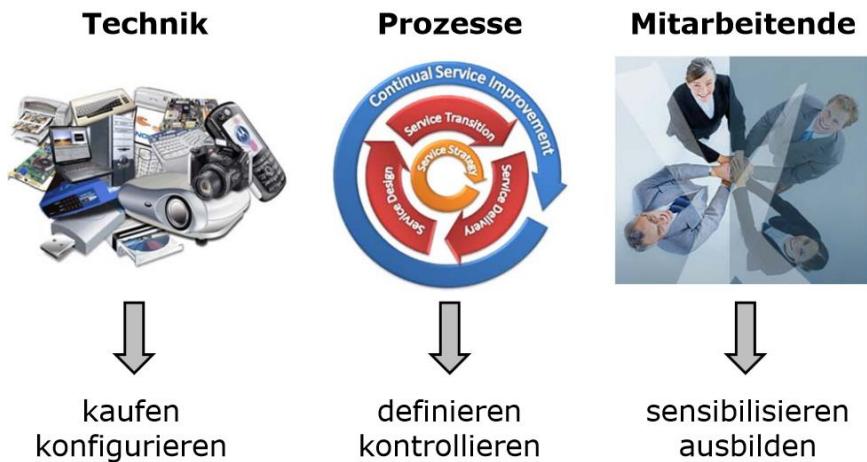


1.6 Integrale Sicherheit



→ Umfassende Betrachtung aller Sicherheitsaspekte einer Organisation

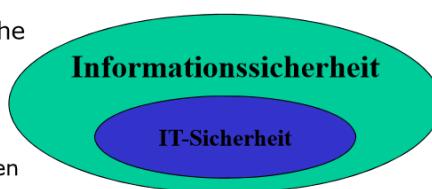
1.7 Informationssicherheit: Womit?



1.8 Informationssicherheit VS IT-Sicherheit

Informationssicherheit

- Schutz der Information als solche
- Medien unabhängig
 - Elektronische Datenträger
 - Papier
 - In den Köpfen der Mitarbeitenden



IT-Sicherheit / ICT-Sicherheit

- Schutz der Information in ICT Systemen
- Medien sind ausschliesslich ICT Systeme
 - Server / Hosts
 - Clients / Notebooks
 - Mobile Datenträger (SmartPhones, USB-Sticks, DigiCams etc.)

1.9 Datensicherheit VS Datenschutz

Datensicherheit (≈Informationssicherheit)

- Schutz von Daten und Informationen

Datenschutz

- Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden

1.10 Datenschutzgesetz (DSG)

- Art. 1 Zweck
 - Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.
- Art. 4 Grundsätze
 1. Personendaten dürfen nur rechtmässig bearbeitet werden.
 2. Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.
 3. Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.
 4. Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein.
 5. Ist für die Bearbeitung von Personendaten die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung erst gültig, wenn sie nach angemessener Information freiwillig erfolgt. Bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die Einwilligung zudem ausdrücklich erfolgen.

1.11 Zutritts-, Zugangs- und Zugriffskontrolle

Zutrittskontrolle

- gerätebezogen
- Schutz des physischen Systems

Zugangskontrolle

- personenbezogen
- Schutz des logischen Systems

Zugriffskontrolle

- «Daten»-bezogen
- Schutz der Operationen



2 Kapitel 2 – ISMS und Informationssicherheitsstandards

2.1 ISMS (Information Security Management System)

Das **Information Security Management System (ISMS)**, engl. für „Managementsystem für Informationssicherheit“) ist eine Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

2.1.1 Motivation, Zweck

- Sicherheit erhalten, dass Vermögenswerte und Informationen der Unternehmung («Assets») angemessen geschützt sind
- Rechtliche und regulatorische, aber auch Branchen- und Marktanforderungen erfüllen

2.1.2 Vorgehen

- Einen Prozess unterhalten, mit dem Informationssicherheitsrisiken identifiziert, 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 (ISO 27001):**
- **ISO 27000:2009**
ISMS – Overview and vocabulary
- **ISO 27001:2008**
ISMS – Requirements
- **ISO 27002:2007**
Code of practice for information security management
- **ISO 27003:2010**
ISMS implementation guidance
- **ISO 27004:2009**
Information security management - Measurement
- **ISO 27005:2011**
Information security risk management

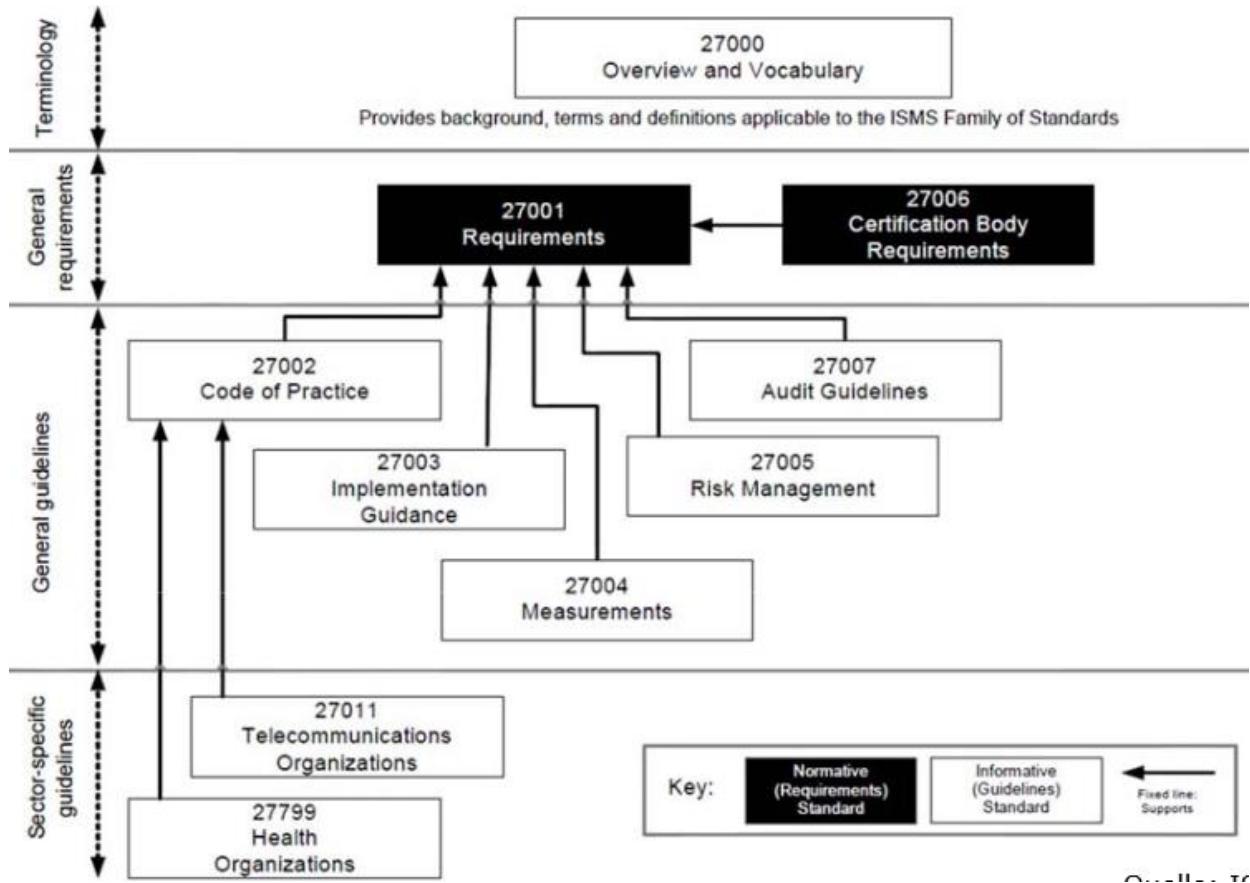
2.1.3 Komponenten eines ISMS

Zu einem ISMS gehören folgende Komponenten:

- Management-Prinzipien
- Ressourcen
- Mitarbeitende
- Sicherheitsprozess bestehend aus:
 - Sicherheitspolitik, in der die Sicherheitsziele und die Strategie zu deren Umsetzung dokumentiert sind
 - Sicherheitsorganisation
 - Sicherheitskonzept

→Kapitel 2 des Buches durchlesen!!! Wird hier nicht weiter behandelt...

2.2 Überblick der ISO-Standards



2.2.1 Nutzen von Standards

Kostensenkung	Nutzung vorhandener und praxiserprobter Vorgehensmodelle Methodische Vereinheitlichung und Nachvollziehbarkeit Ressourceneinsparung durch Kontinuität und einheitliche Qualifikation Interoperabilität
Einführung eines angemessenen Sicherheitsniveaus	Orientierung am Stand der Technik und Wissenschaft Gewährleistung der Aktualität Verbesserung des Sicherheitsniveaus durch die Notwendigkeit der zyklischen Bewertung
Wettbewerbsvorteile	Zertifizierung des Unternehmens sowie von Produkten Nachweisfähigkeit bei öffentlichen und privatwirtschaftlichen Vergabeverfahren Verbesserung des Unternehmensimage Stärkung der Rechtssicherheit

2.2.2 ISO 27000 (ISMS – Overview and vocabulary)

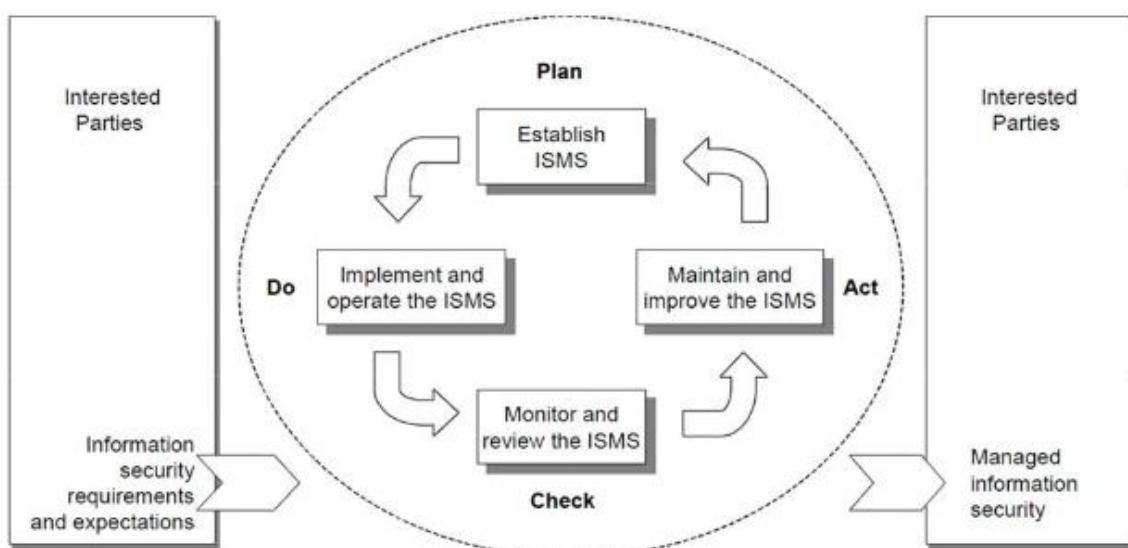
- Definiert Begriffe, welche in der ISO 27000 Standard-Reihe verwendet werden
- Erläutert kurz, was ein Information Security Management System (ISMS) ist
- Erklärt den dazu verwendeten Prozess-Ansatz «Plan –Do – Check – Act»
- Gibt einen Überblick über die ISO 27000 Standard-Reihe

2.2.3 ISO 27001 (ISMS – Requirements)

- Definiert Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems
- Definiert den Sicherheitsprozess nach dem Prozess-Ansatz «Plan – Do – Check – Act»
- Definiert in Anhang A Ziele und Massnahmen zur Verbesserung der Informationssicherheit (die Ziele und Massnahmen sind aus ISO 27002 entlehnt)
- Eine Zertifizierung nach ISO 27001 ist möglich
- 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 Kontrollen (aus ISO 27002), welche vom ISMS berücksichtigt werden («Statement of Applicability»)

«Scope» und «Statement of Applicability» definieren den Umfang einer Zertifizierung nach ISO 27001

2.2.3.1 ISMS-Prozess nach ISO 27001 (Plan-Act-Check-Do)



- **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, -Kontrollen, -Prozesse 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.

2.2.4 ISO 27002 (Code of practice for information security mgmt)

- Standardwerk zum Thema Informationssicherheit, kurz oft CoP genannt
- Definiert 133 Kontrollen für den sicheren Umgang mit Informationen
- Zu jeder Kontrolle 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)

2.2.4.1 Kapitel des ISO 27002

1. Anwendungsbereich
2. Begriffe
3. Aufbau dieser Norm
4. Risikoeinschätzung und -behandlung
5. **Sicherheitsleitlinie**
6. **Organisation der Informationssicherheit**
7. **Management von organisationseigenen Werte**
8. **Personalsicherheit**
9. **Physische und umgebungsbezogene Sicherheit**
10. **Betriebs- und Kommunikationsmanagement**
11. **Zugangskontrolle**
12. **Beschaffung, Entwicklung und Wartung von Informationssystemen**
13. **Umgang mit Informationssicherheitsvorfällen**
14. **Sicherstellung des Geschäftsbetriebs**
15. **Einhaltung von Vorgaben (Compliance)**

→ 11 Domänen

Kapitelstruktur von ISO 27002

10 Betriebs- und Kommunikationsmanagement

Eine von 11 Domänen

10.1 Verfahren und Verantwortlichkeiten

Eines von 39 Kontrollzielen
(engl. Control Objectives)

Ziel: Sicherstellung des korrekten und sicheren Betriebs der informationsverarbeitenden Einrichtungen.

Für das Management und den Betrieb von informationsverarbeitenden Einrichtungen sollten Verantwortlichkeiten und Verfahren definiert sein. Dies beinhaltet die Entwicklung angemessener Betriebsprozesse.

Die Aufteilung von Pflichten (4-Augen-Prinzip) sollte bei Bedarf umgesetzt werden, um so das Risiko von fahrlässigem oder vorsätzlichem Missbrauch zu verringern.

10.1.1 Dokumentierte Betriebsprozesse

Maßnahmen ← Eine von 133 Kontrollen (Massnahmen, Prüfpunkte, engl. Controls)
Betriebsprozesse sollten dokumentiert und gepflegt sein und den Benutzern bei Bedarf bereitgestellt werden.

Anleitung zur Umsetzung

Im Zusammenhang mit dem Betrieb von Einrichtungen für Informations- und Kommunikationsdienste sollten dokumentierte Betriebsprozesse erstellt werden. Solche Betriebsprozesse beinhalten z. B. Anlaufen und Abschalten von Computern, Backup, Wartung, Medienhandhabung, Computerraumverwaltung und Postzustellung sowie Arbeitsschutz.

2.2.5 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

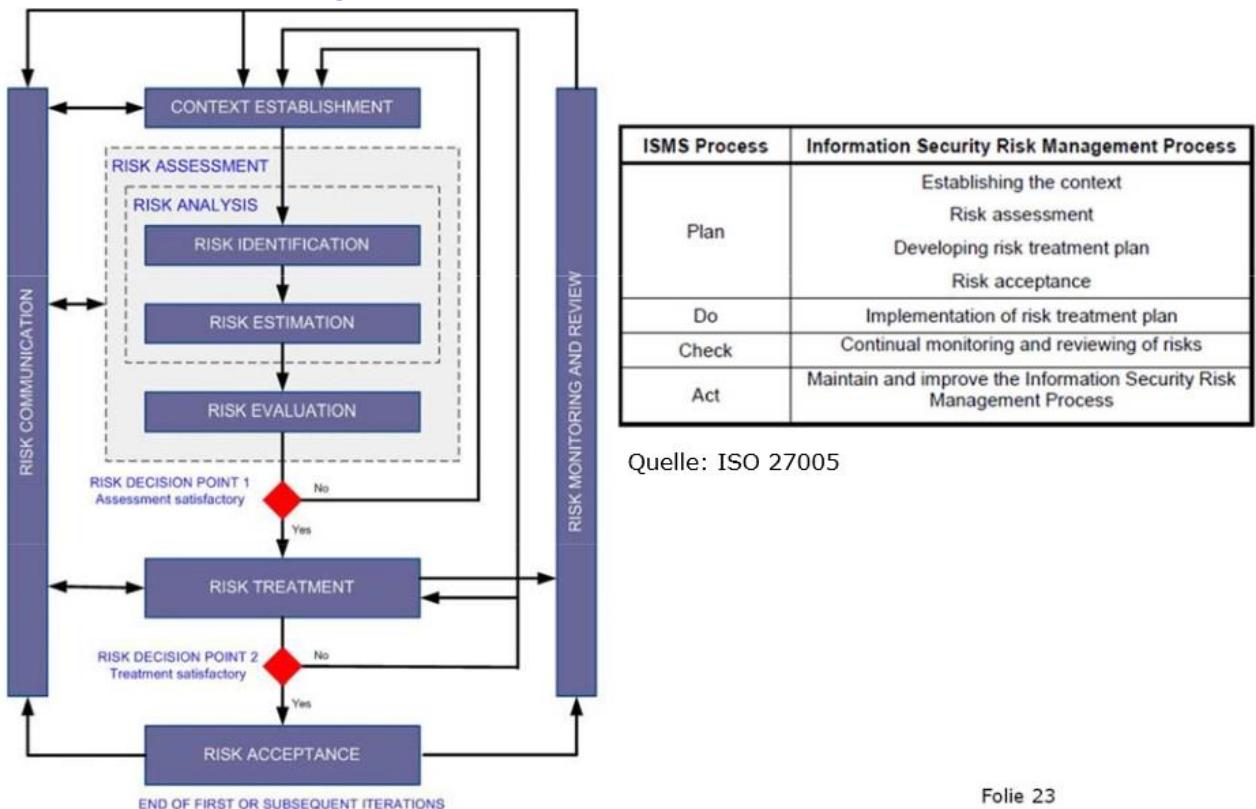
2.2.6 ISO 27004 (Information security management – Measurement)

- Anleitung für die Implementation eines Messsystems für die Beurteilung der Effektivität eines ISMS und der damit verbundenen Kontrollen 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 Kontrollen zu verbessern
 - Nutzung der Resultate, um das ISMP zu verbessern

2.2.7 ISO 27005 (Information security risk management)

- Anleitung für ein Information Security Risk Management ohne Spezifikation einer Risiko Management Methode
- 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

2.2.7.1 ISMS-Risikomanagement Prozess



2.2.8 Aufgabe zu den ISO-Standards

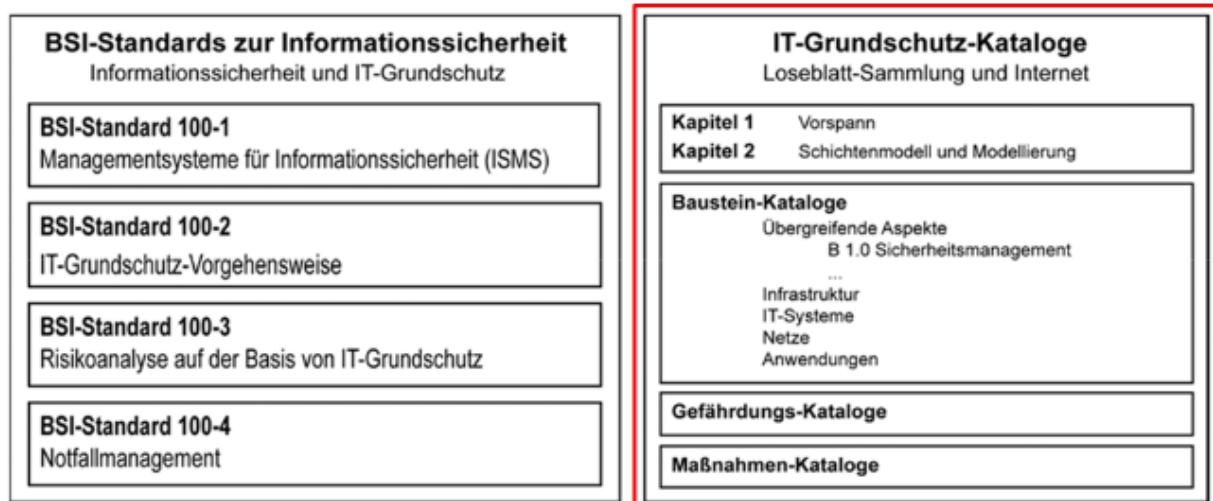
Nennen Sie 5 Kontrollen und die zugehörigen Domänen, welche für die Überprüfung des Objekts **Serverraum** relevant sind:

5 Kontrollen und zugehörige Domänen, welche für die Überprüfung des Objekts **Serverraum** relevant sind (Aufzählung nicht abschliessend).

- 6.2.1 Identifizierung von Risiken in Zusammenhang mit Externen (Organisation der Informationssicherheit)
- 7.1.1 Inventar der organisationseigenen Werte (Management von organisationseigenen Werten)
- 9.1.1 Sicherheitszonen (Physische und umgebungsbezogene Sicherheit)
- 9.1.2 Zutrittskontrollen (dito)
- 9.1.4 Schutz vor Bedrohungen von Aussen und aus der Umgebung (dito)
- 9.2.1 Platzierung und Schutz von Betriebsmitteln (dito)
- 9.2.2 Unterstützende Versorgungseinrichtungen (dito)
- 9.2.3 Sicherheit der Verkabelung (dito)
- 9.2.4 Instandhaltung von Gerätschaften (dito)
- 11.1.1 Regelwerk zur Zugangskontrolle (Zugangskontrolle)
- 11.6.2 Isolation sensibler Systeme (dito)

2.3 BSI-Standards und IT-Grundschutzkataloge

Die **BSI-Standards** beschreiben die Vorgehensweise nach IT-Grundschutz und enthalten Ausführungen zum Informationssicherheitsmanagement und zur Risikoanalyse. Die **IT-Grundschutz-Kataloge** beinhalten die Baustein-, Massnahmen- und Gefährdungskataloge (79 Bausteine, 1225 Massnahmen, 4101 Seiten).

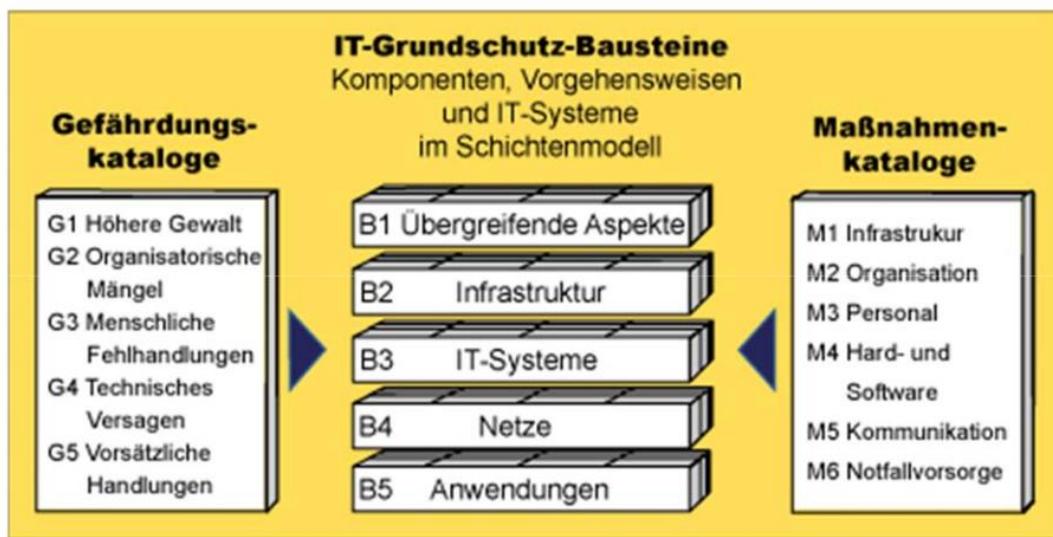


2.3.1 Idee des IT-Grundschutzes

Infrastrukturelle, organisatorische, personelle und technische Standard-Sicherheitsmaßnahmen helfen, ein Standard-Sicherheitsniveau aufzubauen, um geschäftsrelevante Informationen zu schützen!

- Abläufe und IT-Komponenten sind überall ähnlich (Wiederverwendbarkeit, Anpassbarkeit, Erweiterbarkeit)
- Darauf aufbauend kann ein Gerüst für das Sicherheitsmanagement erstellt werden

2.3.2 Inhalt der IT-Grundschutzkataloge



2.3.2.1 Gefährdungskataloge

Enthält die wesentlichen Gefährdungen für die Informationssicherheit. Zu jeder Kategorie (G1 – G5) ist eine Vielzahl von Gefährdungen definiert. Die Gliederung erfolgt entlang möglicher Ursachen:

- G 1: Höhere Gewalt
- G 2: Organisatorische Mängel
- G 3: Menschliche Fehlhandlungen
- G 4: Technisches Versagen
- G 5: Vorsätzliche Handlungen

2.3.2.2 Massnahmenkataloge

Detailliert beschriebene und praxisnahe Massnahmen, um Gefährdungen für die Informationssicherheit zu begegnen. Zu jeder Kategorie (M 1 – M 6) ist eine Vielzahl von Massnahmen definiert. Aufbau:

- M 1: Infrastruktur
- M 2: Organisation
- M 3: Personal
- M 4: Hard- und Software
- M 5: Kommunikation
- M 6: Notfallvorsorge

2.3.2.3 Baustein kataloge (Klammer zwischen Gefährdungs- und Massnahmenkatalogen)

Ein Baustein beschreibt einen Teilespekt der Informationssicherheit (z. B. ein techn. System, ein organisatorischer Sachverhalt, eine Anwendung etc.). Zu jedem Baustein werden relevante Gefährdungen und empfohlene Schutzmassnahmen beschrieben. Gliederung in die folgenden Schichten:

- B 1: Übergreifende Aspekte
- B 2: Infrastruktur
- B 3: IT-Systeme
- B 4: Netze
- B 5: Anwendungen

2.3.3 Nutzen der IT-Grundschutzkataloge

- Aufwand für die Entwicklung eines Sicherheitskonzepts reduzieren
- In der Regel genügt es, die auf den Einsatzzweck zutreffenden Bausteine auszuwählen und die darin enthaltenen Massnahmen einzuplanen und konsequent umzusetzen

Vorteile	Nachteile
Extrem ausführliche und detaillierte Beschreibung (ca. 3000 Seiten! Vergleich ISO: ca. 250 Seiten)	Ungenügender Schutz bei erhöhten Risiken oder Schutzbedarf
Geht auf spezifische Probleme ein (z.B. Windows Server)	Mögliche Einschränkung der Funktionalität durch Überschutz
Zertifizierung möglich und kostengünstig	Begründung von Massnahmen erschwert
Aufwand der Risikoanalyse wird stark reduziert	Pflege der Aktualität und Vollständigkeit des Massnahmenkataloges aufwändig

2.3.4 Aufgaben zu IT-Grundschutzkatalogen

1. Leiten Sie 5 Massnahmen zum Thema Schutz des Serverraums aus den IT-Grundschutzkatalogen ab. Geben Sie zu jeder Massnahme eine damit mitigierte Gefährdung an.

Vgl. Baustein B 2.4 Serverraum

Massnahmen und Gefährdungen

- M 1.7 Handfeuerlöscher → G 1.4 Feuer
- M 1.24 Vermeidung von wasserführenden Leitungen → G 1.5 Wasser
- M 2.17 Zutrittsregelung und -kontrolle → G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen
- M 1.28 Lokale unterbrechungsfreie Stromversorgung → G 4.1 Ausfall der Stromversorgung
- M 1.23 Abgeschlossene Türen → G 5.1 Manipulation oder Zerstörung von Geräten oder Zubehör

2. Lesen Sie eine Massnahme mit Siegelstufe A (=vorrangig umzusetzen) genau durch, und geben Sie den Initiierungsverantwortlichen an. Wie beurteilen Sie die beschriebene Massnahme bezüglich Detailgrad?

Massnahme der Siegelstufe A und Initiierungsverantwortlicher

- M 1.7 Handfeuerlöscher → Brandschutzbeauftragter, Leiter Haustechnik

Beurteilung der Massnahme bzgl. Detailgrad

- Die Massnahmen sind generell sehr detailliert beschrieben. Je nach Massnahme sind unter Umständen Spezialkenntnisse erforderlich, um sie im Detail zu verstehen und umsetzen zu können (→ Bezüge zu anderen Normen).

3. Versuchen Sie die unten aufgeführte Kreuzreferenz-Tabelle nachzuvollziehen. Welche Aussage macht sie?

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									

Kreuzreferenz-Tabellen stellen einen Zusammenhang zwischen Massnahmen und der damit mitigierten Gefährdungen eines Bausteins dar. Wichtig: Die Bedeutung einer Massnahme misst sich nicht an der Anzahl Gefährdungen, welche damit mitigiert werden.

4. Beschreiben Sie die Unterschiede zwischen den IT-Grundschutzkatalogen und ISO 27002.

IT-Grundschutzkataloge	ISO 27002
<ul style="list-style-type: none"> Detaillierte Beschreibung von Standard-Sicherheitsmassnahmen, welche praktisch für jedes IT-System zu beachten sind («normaler» Schutzbedarf) → Massnahmenkataloge. Darstellung einer pauschal angenommenen Gefährdungslage → Gefährdungskataloge. Beschreibung einer Vielzahl von generischen Bausteinen, welche helfen konkrete Massnahmen (und Gefährdungen) zu identifizieren → Baustein kataloge. 	<ul style="list-style-type: none"> Sehr allgemein formulierte Anforderungen (an Technik, Organisation und Prozesse), welche in einer Unternehmung im Hinblick auf die Sicherstellung des Informationsschutzes umgesetzt werden sollten. Die Umsetzungshinweise sind nur sehr allgemein gehalten. Sie werden nirgends konkret, indem sie z. B. Empfehlungen zu bestimmten Systemen (z. B. ein Windows-Server) geben.

2.3.5 BSI-Standard 100-1 (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

2.3.6 BSI-Standard 100-2 (IT-Grundschutz-Vorgehensweise)

- Konkretisiert die Darstellung des ISMS nach BSI-Standard 100-1
- 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

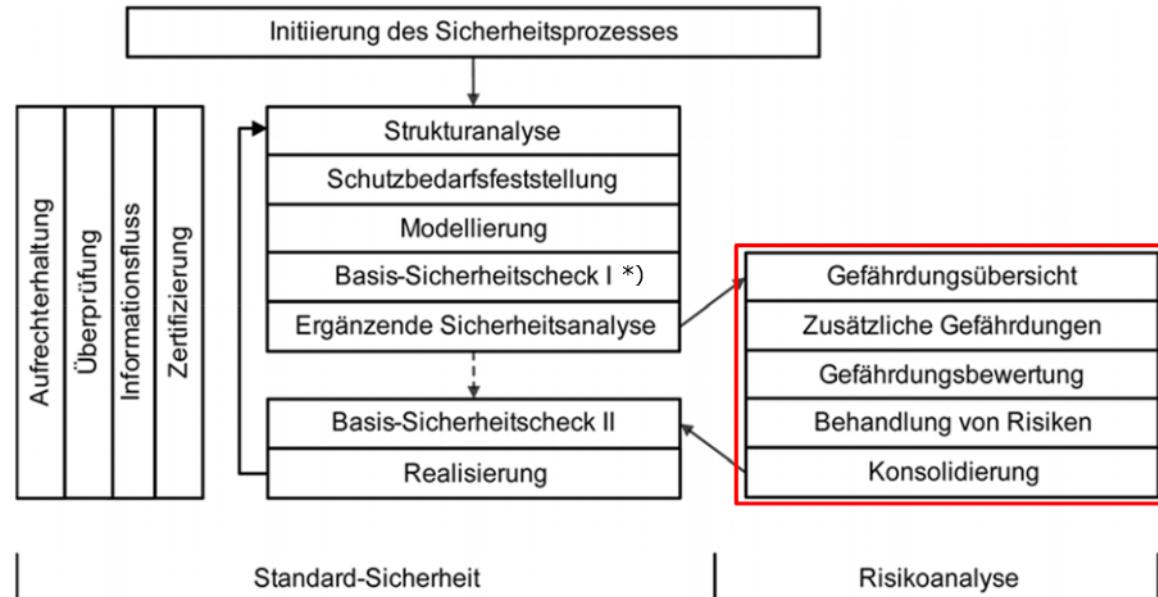
2.3.7 BSI-Standard 100-3 (Risikoanalyse auf Basis von IT-Grundschutz)

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

2.3.7.1 Risikoanalyse nach BSI 100-3



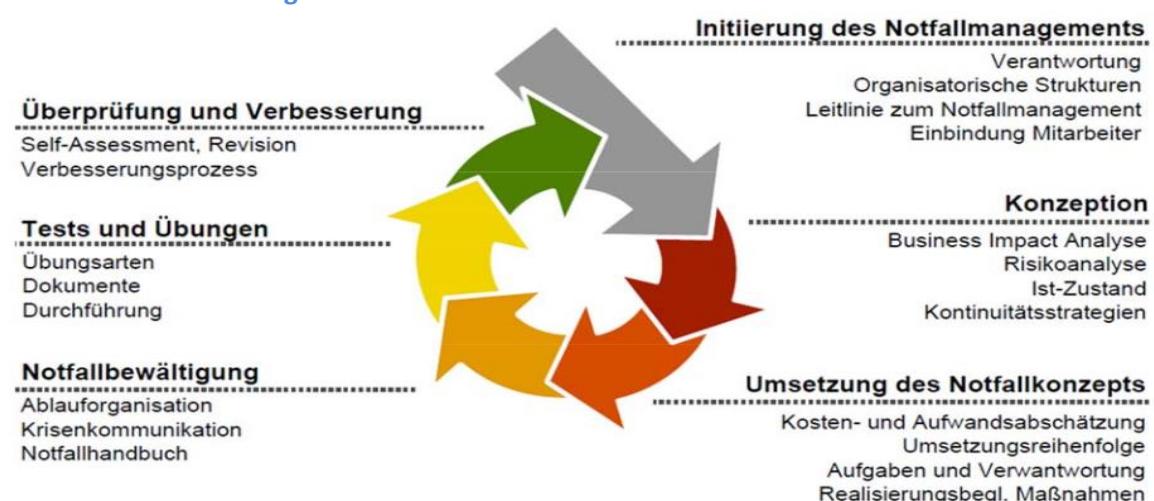
*) Basis-Sicherheitscheck = Soll-Ist-Vergleich

Quelle: BSI-Standard 100-3, Version 2.5

2.3.8 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-Grundschutzvorgehensweise auf (BSI-Standard 100-2)

2.3.8.1 Notfallmanagement



2.4 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!

2.5 Information Security Forum (ISF) - Standard of Good Practice for Information Security

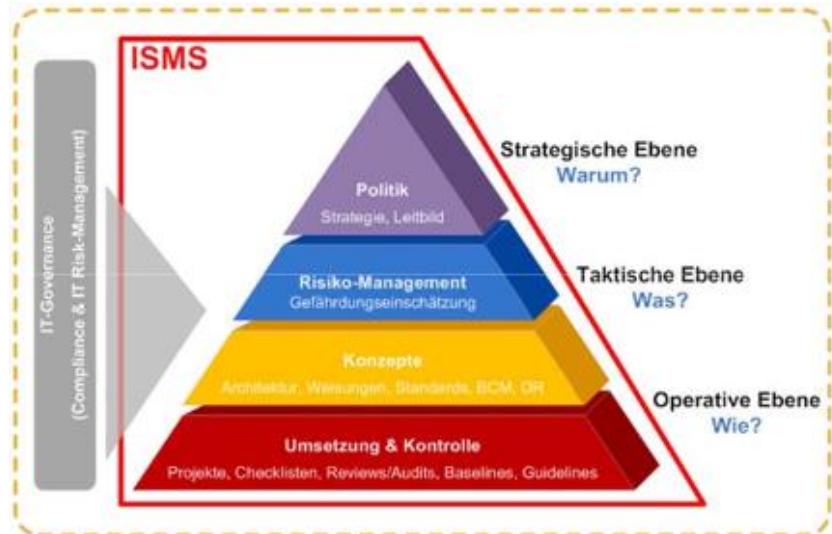
Businessfokussierter Leitfaden zur Identifikation und zum Management von Informationssicherheitsrisiken in Organisationen. Basiert auf Erfahrungen von über 260 grossen, weltweit tätigen Organisationen. Berücksichtigt auch andere Standards (COBIT, PCI DSS, ISO 27001/2, SOX etc.). Kann als Grundlage für den Aufbau eines ISMS dienen...

Aufgebaut nach 6 Kategorien, auch Aspekte genannt:

- Security Management (enterprise-wide)
- Critical Business Applications
- Computer Installations
- Networks
- Systems Development
- End User Environment

3 Kapitel 3 - Sicherheitspolitik und –Konzepte

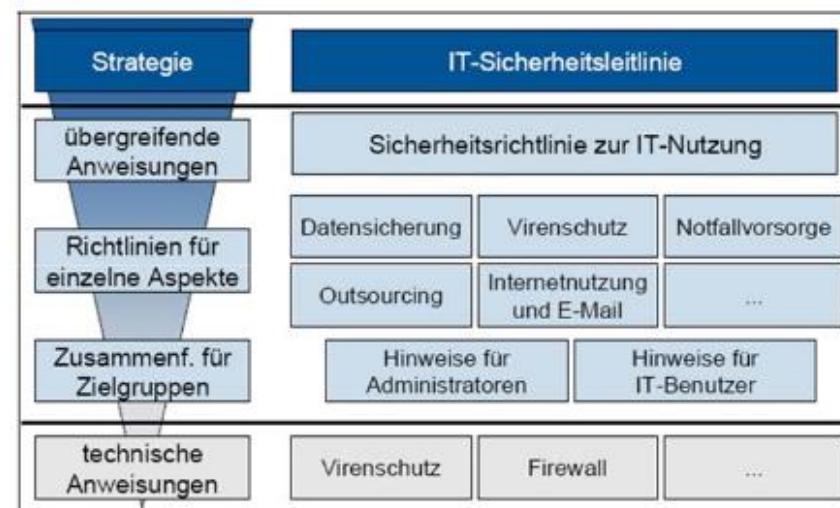
3.1 Sicherheitspyramide nach SiBH



3.2 Sicherheitspyramide nach BSI



3.3 Dokumentstruktur nach BSI



3.4 Sicherheitspyramide



→ Vorgehen: Top-Down-Approach (Vom Generellen zum Detaillierten)

Aufgabe: Wo können Vorlagen für die Informationssicherheitspolitik gefunden werden?

ISO 27001 Kp. 4.2.1b

- Definition der ISMS-Leitlinie unter Berücksichtigung der Eigenschaften des Geschäfts, der Organisation, ihres Standorts, ihrer Werte und ihrer Technologie, die:
 - 1) einen **Rahmen für Zielsetzungen** vorgibt und eine **generelle Richtung** sowie **Grundsätze für Aktionen** hinsichtlich Informationssicherheit festlegt;
 - 2) geschäftliche, gesetzliche oder amtliche Anforderungen und vertragliche Sicherheitsverpflichtungen berücksichtigt;
 - 3) mit dem strategischen Risikomanagementkontext der Organisation abgestimmt ist, in dem die Einrichtung und Instandhaltung des ISMS erfolgen wird;
 - 4) Kriterien festlegt, nach denen Risiken bewertet werden (siehe 4.2.1 c)); und
 - 5) **vom Management genehmigt** wurde.

ISO 27001 Kp. 4.3 «Dokumentationsanforderungen»

- 4.3.1 Allgemeines
 - Die Dokumentation des ISMS sollte Folgendes enthalten:
 - a) eine dokumentierte Erklärung der ISMS-Leitlinie (siehe 4.2.1 b)) und der ISMS-Ziele;
 - ...

ISO 27001 Kp. 5.1 «Verpflichtung des Managements»

- Das Management muss seine Verpflichtung für die Festlegung, Umsetzung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung des ISMS nachweisen, indem es:
 - a) eine ISMS-Leitlinie festlegt;
 - ...

ISO 27002 Kp. 5 «Sicherheitsleitlinie»

- 5.1 Informationssicherheitsleitlinie
 - Ziel: Richtungsvorgabe und Unterstützung des Managements bei der Informationssicherheit, in Übereinstimmung mit Geschäftsanforderungen und geltenden Gesetzen und Regelungen.
Das Management sollte eine klare Richtung der Grundsätze in Einklang mit Geschäftszielen vorgeben und Unterstützung und Engagement für Informationssicherheit durch organisationsweite Veröffentlichung und Aufrechterhaltung einer Informationssicherheitsleitlinie vorgeben.
- 5.1.1 Leitlinie zur Informationssicherheit
 - Das Management sollte eine Informationssicherheitsleitlinie genehmigen, veröffentlichen und alle Angestellten und relevanten Externen davon in Kenntnis setzen.
- 5.1.2 Überprüfung der Informationssicherheitsleitlinie
 - Die Informationssicherheitsleitlinie sollte in regelmäßigen Abständen und immer dann überprüft werden, wenn wesentliche Änderungen erfolgen, um ihre Eignung, Angemessenheit und Wirksamkeit auf Dauer sicherzustellen.

BSI 100-1 Kp. 7 «Der Informationssicherheitsprozess»

- Formulierung von Sicherheitszielen und einer Leitlinie zur Informationssicherheit
 - Es müssen **Sicherheitsziele festgelegt und strategische Vorgaben gemacht** werden, wie die Ziele erreicht werden sollen. Die Kernaussagen werden in einer Leitlinie zur Informationssicherheit (englisch: information security policy oder IT security policy) dokumentiert. Die Sicherheitsleitlinie sollte mindestens Aussagen zu den folgenden Themen enthalten:
 - Sicherheitsziele der Behörde oder des Unternehmens,
 - Beziehung der Sicherheitsziele zu den Geschäftszielen oder Aufgaben der Institution,
 - angestrebtes Sicherheitsniveau,
 - Leitaussagen, wie das angestrebte Sicherheitsniveau erreicht werden soll und
 - Leitaussagen, ob und wodurch das Sicherheitsniveau nachgewiesen werden soll.
 - Die Leitlinie wird vom Management verabschiedet und in der Institution bekannt gegeben.

BSI 100-2 Kp. 3.3 «Erstellung einer Leitlinie zur Informationssicherheit»

- Die Leitlinie zur Informationssicherheit beschreibt allgemeinverständlich, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Institution hergestellt werden soll. Sie beinhaltet die von der Institution angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Die Sicherheitsleitlinie beschreibt damit auch über die Sicherheitsziele das angestrebte Sicherheitsniveau in einer Behörde oder einem Unternehmen. Sie ist somit Anspruch und Aussage zugleich, dass dieses Sicherheitsniveau auf allen Ebenen der Institution erreicht werden soll.
- Schritte zur Erstellung
 - 3.3.1 Verantwortung der Behörden- bzw. Unternehmensleitung für die Sicherheitsleitlinie
 - 3.3.2 Festlegung des Geltungsbereichs und Inhalt der Sicherheitsleitlinie
 - 3.3.3 Einberufung einer Entwicklungsgruppe für die Sicherheitsleitlinie
 - 3.3.4 Bekanntgabe der Sicherheitsleitlinie

BSI IT-Grundschutz-Kataloge

- M 2.192 Erstellung einer Leitlinie zur Informationssicherheit
 - Die Leitaussagen zur Sicherheitsstrategie sollten in einer Leitlinie zur Informationssicherheit zusammengefasst werden, um die zu verfolgenden Sicherheitsziele und das angestrebte Sicherheitsniveau für alle Mitarbeiter zu dokumentieren. Mit der Sicherheitsleitlinie bekennt sich die Behörden- bzw. Unternehmensleitung sichtbar zu ihrer Verantwortung für Informationssicherheit.
 - Bei der Erstellung der Leitlinie zur Informationssicherheit müssen folgende Punkte beachtet werden:
 - Verantwortung der Behörden- bzw. Unternehmensleitung
 - Festlegung des Geltungsbereichs
 - Festlegung von Sicherheitszielen
 - Inhalt der Sicherheitsleitlinie
 - Bekanntgabe der Leitlinie zur Informationssicherheit
 - Aktualisierung der Sicherheitsleitlinie

3.5 Checkliste Informationssicherheitspolitik

- 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
- Zu widerhandlungen
- Life Cycle
- Unterschrift
- Lesbarkeit / Aufmachung / Umfang / Publizierung
- Umsetzbarkeit / Realisierbarkeit

3.6 Informationssicherheitspolitik (ISP) – 1. Stufe

3.6.1 Definition

Im Bereich der IT-Sicherheit oberste Richtlinie einer Organisationseinheit, in der sicherheitsrelevante Bestimmungen zu Verhaltensweisen von Mitarbeitern und von IT-Systemen (Informationstechnologie) festgehalten werden. Aussagen zu:

- IT-Sicherheitsziele
- Bezug IT-Sicherheitsziele -> Geschäftsziele
- Angestrebtes Sicherheitsniveau und wie wird dies erreicht?
- Definition der IT-Sicherheitsorganisation (Bsp. Buch S.43)

Ziele

- Strategische Ebene
- Klares Statement des Management (Vorbild)
- Bezugspunkt für die gesamte Informationssicherheit

(Wichtigste) Rollen der Sicherheitsorganisation

- GL / Management (trägt die Verantwortung / Risiko!)
- Informationssicherheitsbeauftragter (sollte nicht aus dem Bereich IT stammen!)
- Mitarbeitende

Grundlagen

- Unternehmenspolitik
- Unternehmenskultur
- Gesetze / Verträge
- Anforderungen an Vertraulichkeit / Verfügbarkeit
- Organisation der Unternehmens
- Grundsätze (z.B. alles ist erlaubt, was nicht verboten ist)

Checkliste ISP

Ein ISP Dokument sollte folgende Punkte abdecken:

- Vorwort / Einordnung / Motivation
- Geltungsbereich und Abgrenzung
- Grundlagen (Gesetze, übergeordnete Dokumente)
- Ziel und Zweck ISP (Sicherstellen Geschäftsvorgang)
- Sicherheitsziel und –strategie IT
- Rollen und Verantwortlichkeiten
- Umgang mit Risiken, Wirtschaftlichkeitsaspekte
- Zu widerhandlungen
- Life Cycle
- Unterschrift
- Lesbarkeit / Aufmachung / Umfang / Publizierung
- Realisierbarkeit

Compliance (Gesetze / Verträge)

- OR / StGB
- Datenschutzgesetz
- Urheberrecht
- BÜPF / VÜPF (wichtig wegen Internet / Email)
- Verträge mit Kunden, Lieferanten, Mitarbeitenden etc

Richtlinien

- Leitplanken für Informationssicherheit
- Fokus Sicherstellung der Geschäftsführung (!!)
- Generelle Willensäusserung der GL bezüglich Sicherheitslevel
- Widerspiegelt UN-Kultur
- Abgeleitet von UN-Politik
- Muss unbedingt von GL getragen werden
- Wirtschaftliche Aspekte, Kostenfolgen aufzeigen (!!)
- Langfristige Betrachtung (3-5 Jahre)

3.7 Informationssicherheitskonzepte (ISK) – 2. Stufe

3.7.1 Definition

Das projektbezogene Informationssicherheitskonzept enthält alle an das zu entwickelnde System verbindlich gestellten Informationssicherheitsanforderungen und die Informationssicherheitsmaßnahmen zum Schutz der Informationen vor Verlust der Integrität, Vertraulichkeit, Verbindlichkeit und Verfügbarkeit sowie die Informationssicherheitsanforderungen und Informationssicherheitsmaßnahmen zum Schutz der technischen Anlagen zur Informationsverarbeitung und Informationsübermittlung.

3.7.2 Ziele

- Taktische Aussagen
- Rahmenbedingungen für Teilbereiche festlegen
- Übergeordnete Definitionen

3.7.3 Vorlagen zu Sicherheitskonzepten

- Auf hohem Abstraktionsniveau dargestellte Bereiche von Sicherheitsmaßnahmen
- Formuliert die groben, längerfristig geltenden Ziele eines Bereiches der Informationssicherheit
- Basiert auf der Info-Sicherheitspolitik
- Definiert den Umgang mit verschiedenen zentralen Elementen der Informationssysteme
- Mittelfristige Geltungsdauer (1-3 Jahre)

Lebenszyklus des Sicherheitskonzepts

Planung und Konzeption

- Auswahl einer Methode zur Risikobewertung
- Klassifikation von Risiken bzw. Schäden
- Risikobewertung
- Entwicklung einer Strategie zur Behandlung von Risiken
- Auswahl von Sicherheitsmaßnahmen

Umsetzung

- Realisierungsplan für das Sicherheitskonzept
- Umsetzung der Sicherheitsmaßnahmen
- Überwachung und Steuerung der Umsetzung
- Aufbau Notfallvorsorge und Behandlung von Sicherheitsvorfällen
- Schulung und Sensibilisierung der Mitarbeitenden

Erfolgskontrolle, Überwachung

- Erkennen von Sicherheitsvorfällen im laufenden Betrieb
- Überprüfung der Einhaltung von Gesetzen, Vorgaben und Verträgen
- Überprüfung der Eignung und Wirksamkeit von Sicherheitsmaßnahmen
- Überprüfung der Effizienz der Sicherheitsmaßnahmen
- Erstellen von Management-Berichten

Optimierung, Verbesserung

- Beseitigen von Fehlern
- Verbesserung von Sicherheitsmaßnahmen

3.7.4 Beispiele von Sicherheitskonzepten

- Backup-Konzept
- Virenschutz-Konzept
- Firewall-Konzept
- E-Mail- und Internet-Konzept
- Konzept zur Vergabe der Benutzerrechte / Rollen
- Change Management Policy
- Notfallkonzept
- Netzwerk- und Remote-Access-Konzept
- Verschlüsselungs-Konzept
- Mobile Devices (Smart Phones / PDA's / Sticks)
- ...

3.7.5 Weitere Sicherheitskonzepte

- Konzept zur Vergabe der Benutzerrechte/Rollen (Er hat worauf Zugriff? Mitarbeiteraustritt?)
- Change Management Policy (Wie gehe ich mit Veränderungen/neues Release um?)
- Notfallkonzept (Was passiert bei grösseren Ausfällen?)

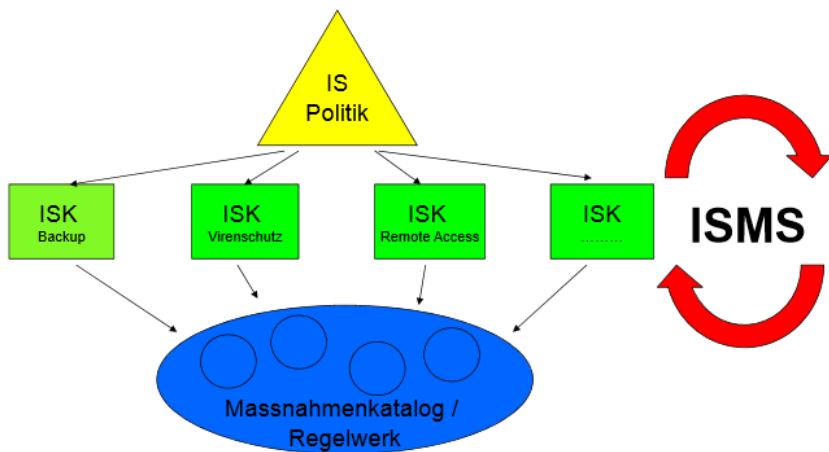
3.8 Regelwerk / Massnahmenkatalog - 3. Stufe

- Bildet die unterste Schicht der Sicherheitspyramide
- Formuliert die Detailziele
- Werden von den Konzepten abgeleitet
- Basieren oft auf den Standardwerken wie ISO oder Grundschutzhandbuch

3.8.1 Beispiele von Richtlinien

- Sicherer Betrieb von Windows Servern (->Betriebshandbuch)
- Sicherer Betrieb von Datenbanken
- Sicherheit am Arbeitsplatz
- Remote-Access (sicherer Zugriff auf Daten z.B. via VPN)
- Entsorgung von IT-Equipment (Daten dürfen nicht in falsche Hände geraten)

3.9 Zusammenspiel ISP und ISK



Jedes Unternehmen ist einem ständigen dynamischen Wandel unterworfen und deshalb muss der IS-Prozess stetig durchgeführt werden!

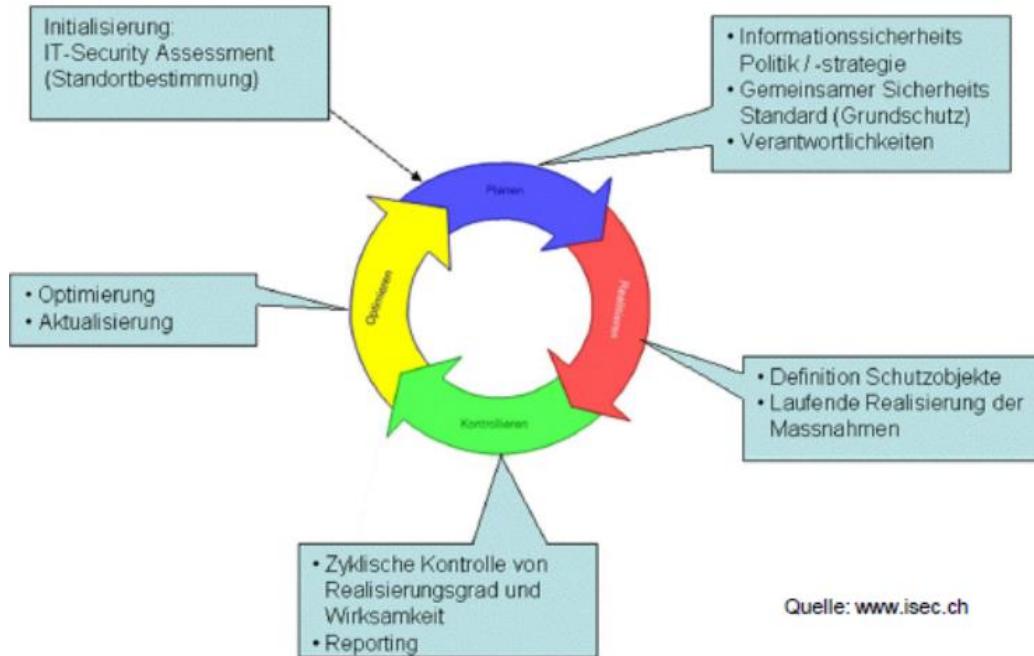
- Veränderung der Infrastruktur
 - Neue Applikationen / Betriebssysteme
 - Neue Systeme (Ausbau / Ersatz)
- Veränderung Umfeld / Rahmenbedingungen
 - Neue Malware (Phishing Attacks, Drive by Infection, Zero Day Attacks, Trojaner, BOTS)
 - Data Leakage (Offene Aufforderung zur Informationsveruntreuung durch Regierungsstellen)
 - Änderungen in der Organisation (Reorg, Spinoff, Fusion, Outsourcing, Insourcing)
 - Rechtliche Veränderungen

Der IS-Prozess kann folgende Elemente beinhalten:

- Risikobeurteilung
- Überzeugung der Unternehmensleitung
- Übersicht über die Prozesse/Mittel/Verbindungen
- ISP's, ISK's, Regelwerk (Massnamen und Weisungen)
- Sicherheitsorganisation
- Verfahren IT-Grundschutz
- Spezifische Risikoanalysen bei erhöhtem Schutzbedarf

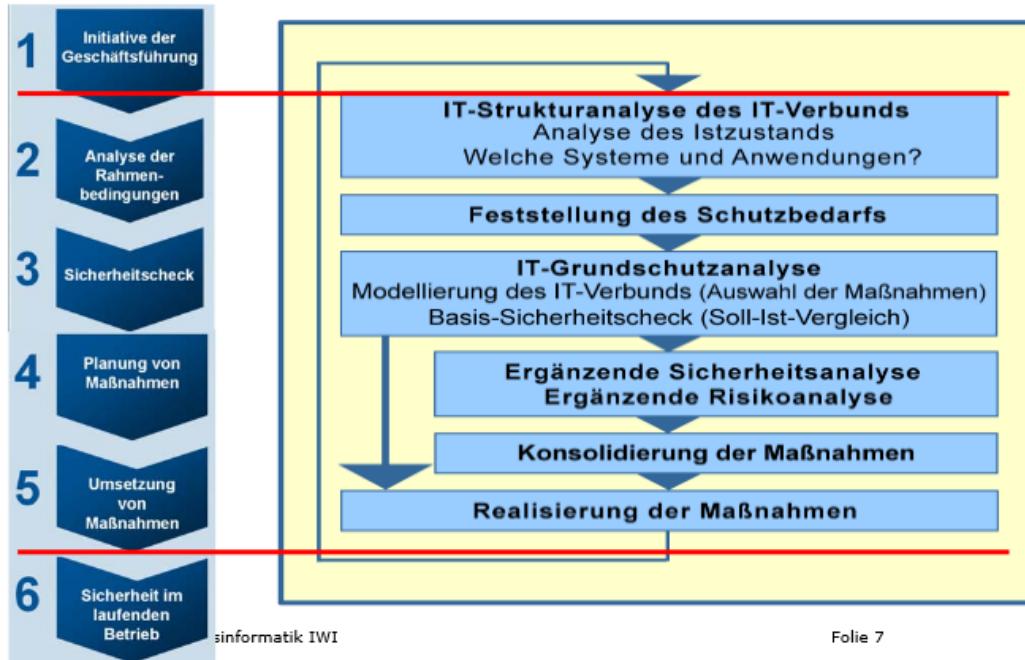
- Audits
- Werkzeuge zur Reduktion des Verwaltungsaufwandes
- Awareness (alle miteinbeziehen!!)
- Notstand (BCP Business Continuity Planning, DRP Disaster Recovery Planning)
- Reporting

Beispiel:



4 Kapitel 4 – Vorgehen IT-Grundschutz

4.1 BSI-Standard 100-2: IT-Grundschutz Vorgehensweise



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

Die IT-Grundschutz-Vorgehensweise ist zweistufig:

4.2.1 Stufe 1

Für normalen Schutzbedarf, übliche Einsatzszenarien und existierende Grundschutz-Bausteine:

- Eine qualitative Methode zur Risikoanalyse und -bewertung ist in der IT-Grundschutz-Vorgehensweise enthalten → keine explizite Risikobewertung notwendig, stattdessen Anwendung von Standard-Sicherheitsmaßnahmen
- Idee: beim Einsatz ähnlicher IT-Umgebungen und vergleichbarer Umfeldbedingungen sind die Bedrohungen sehr ähnlich

4.2.2 Stufe 2:

Für den höheren Schutzbedarf, unübliche Einsatzszenarien, unzureichende Abdeckung mit Bausteinen und durch das Management festgestellten Bedarf: → Es wird eine vereinfachte Risikoanalyse und -bewertung nach BSI-Standard 100-3 durchgeführt

4.3 Kreuzreferenztabellen

Tabellen, welche angeben, welchen Gefährdungen mit welchen Massnahmen begegnet werden kann (bezogen auf einen bestimmten Baustein). Die Massnahmen werden priorisiert (sog. Siegelstufe):

- A: Essenzielle Massnahme, vorrangig umzusetzen
- B: Besonders wichtige Massnahme, zügig umzusetzen
- C: Wichtige Massnahme, verzögerte Umsetzung zulässig
- Z: Ergänzende M., Umsetzung nicht zwingend notwendig

Wichtig:

- Anzahl «X» ist kein Mass für die Wichtigkeit einer M.
- Nur die wichtigsten Gefährdungen sind aufgeführt

Legende für Spalte «Zyklus»:
 PK: Planung und Konzeption
 BE: Beschaffung
 UM: Umsetzung
 BT: Betrieb
 AU: Aussonderung
 NV: Notfallvorsorge

Kreuzreferenztabellen

B 3.106 Server unter Windows 2000

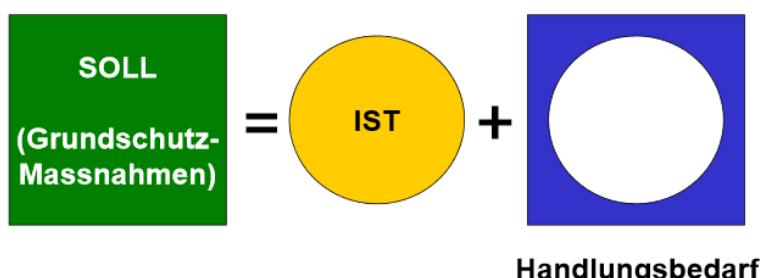
	Zyklus	Siegel	G 1.2	G 2.7	G 2.18	G 3.9	G 3.48	G 4.10	G 4.23	G 4.35	G 5.7	G 5.23	G 5.52	G 5.71	G 5.79	G 5.83	G 5.84	G 5.85
B 3.106				X		X	X				X					X		X
M 2.227	PK	A		X		X						X						X
M 2.228	PK	A		X		X						X						X
M 2.232	PK	C		X						X				X			X	X
M 2.233	PK	B				X	X			X	X	X	X	X		X	X	X
M 4.48	UM	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

4.4 Bemerkungen zum IT-Grundschutz

- Die Beschreibung der Gefährdungen dient lediglich der Sensibilisierung und der Begründung von Massnahmen und hat im Grundschutz-Vorgehen keine weitere Funktion!
- Das BSI macht keine Unterscheidung zwischen Gefahren und Schwachstellen!
- Die Inhalte haben Empfehlungscharakter und sind keine «Gesetze»!
- Es gibt keine Garantie auf Vollständigkeit!
- IT-Grundschutz-Massnahmen müssen gegebenenfalls individuell angepasst und angewendet werden!

4.5 IT-Grundschutz Wirkprinzip

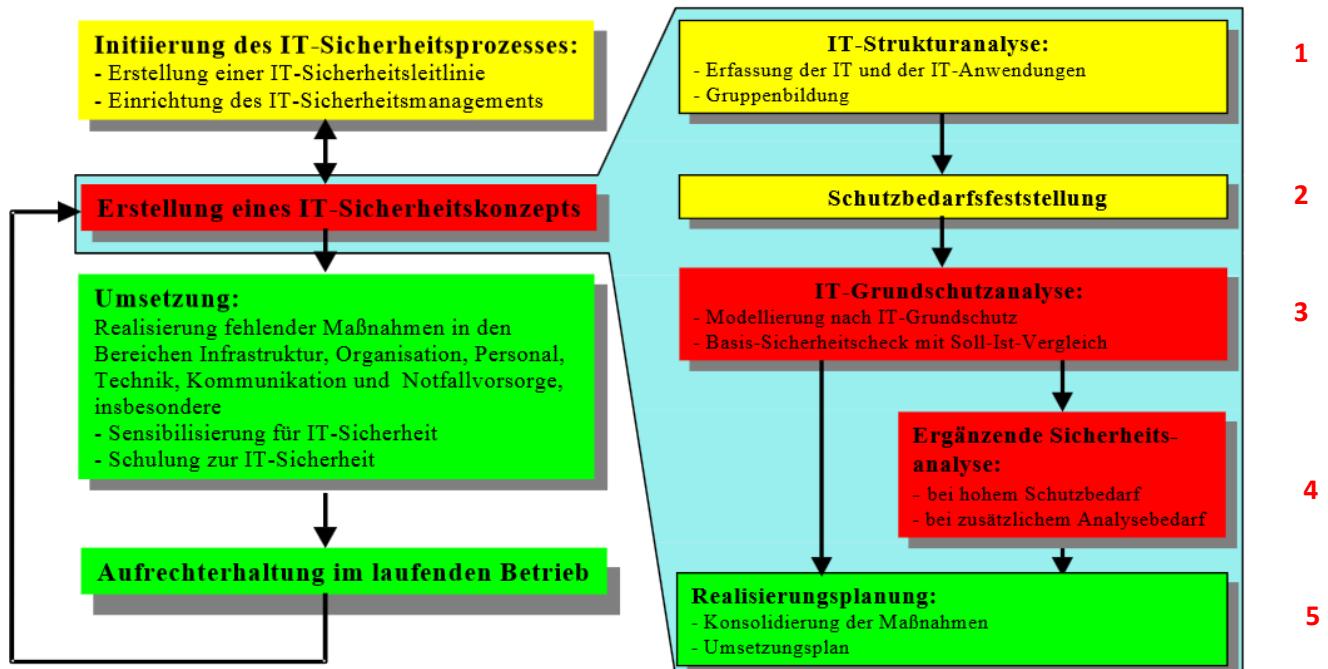
Gilt generell, unabhängig vom angewendeten Standard, also nicht nur für den BSI IT-Grundschutz!



4.6 Grundregeln

- Die Initiative für IT-Sicherheit geht vom Management aus
- Die Verantwortung für IT-Sicherheit liegt beim Management
- Nur wenn sich das Management um Informationssicherheit bemüht, wird die Aufgabe auch wahrgenommen

4.7 Erstellung IT-Sicherheitskonzept



Input	Vorgang	Output
<ul style="list-style-type: none"> Netzwerkplan Inventar 	IT-Strukturanalyse	<ul style="list-style-type: none"> Bereinigter, verdichteter Netzwerkplan Objektlisten Abhängigkeiten von Systemen und Anwendungen
<ul style="list-style-type: none"> Objektlisten Schutzbedarfskategorien 	Schutzbedarfsfeststellung	<ul style="list-style-type: none"> Objektlisten mit zugeordnetem Schutzbedarf Entscheidungsgrundlage für ergänzende Sicherheitsanalyse
<ul style="list-style-type: none"> Objektlisten Grundschutz-Bausteine Interviews, Überprüfungen 	IT-Grundschatzanalyse	<ul style="list-style-type: none"> Grundschutzmodell Umsetzungsstati der Sicherheitsmaßnahmen (Soll-Ist-Vergleich)
<ul style="list-style-type: none"> Objekte mit Schutzbedarf „hoch“ oder „sehr hoch“ 	Ergänzende Sicherheitsanalyse	<ul style="list-style-type: none"> Zusätzliche Sicherheitsmaßnahmen mit Umsetzungsstati
<ul style="list-style-type: none"> Massnahmen mit Umsetzungsstati «teilweise» oder «nein» Budget Personelle Ressourcen 	Realisierungsplanung	<ul style="list-style-type: none"> Projektplanung Auftragslisten

1 4.7.1 IT-Strukturanalyse

4.7.1.1 Erhebung Netzwerkplan

- **Netzwerkplan aktualisieren:**
 - Netzwerkpläne sind meist nicht auf dem aktuellsten Stand
 - Entsprechende Informationen beschaffen bei IT-Verantwortlichen, Administratoren resp. Netz- und Systemmanagement
- **Netzwerkplan auswerten:**
 - Welche IT-Systeme gibt es? (Clients, Server, Netzwerk-Komponenten etc.)
 - Welche Verbindungen zw. diesen Systemen?
 - Welche Verbindungen nach aussen (Einwahl, Internet, VPN etc.)

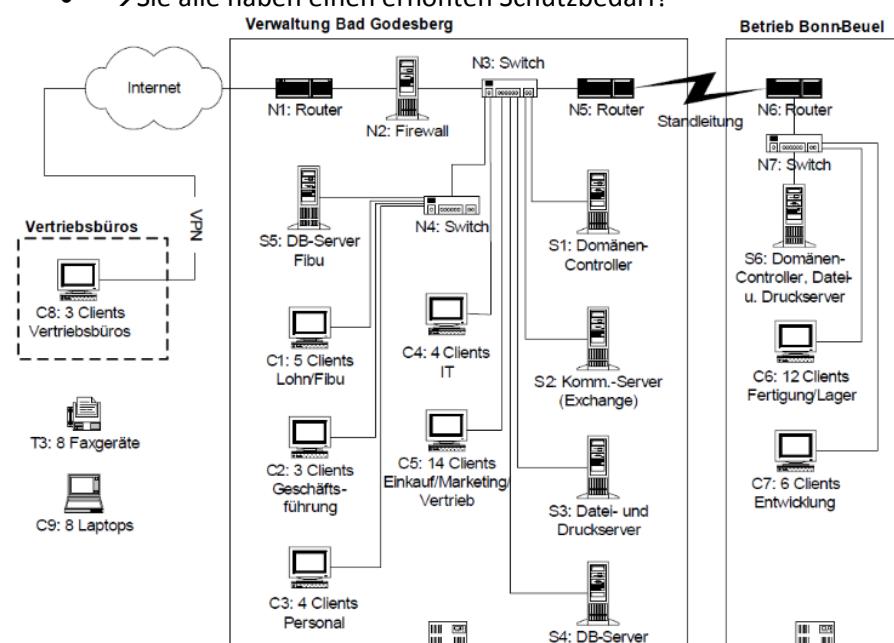
4.7.1.2 Komplexitätsreduktion

Gleichartige Komponenten zu Gruppen zusammenfassen. Mögliche Gruppierungskriterien:

- Systeme von gleichem Typ
- Systeme mit gleicher oder nahezu gleicher Konfiguration
- Systeme mit gleicher oder nahezu gleicher Netzwerkanbindung
- Systeme mit gleichen administrativen und infrastrukturellen Rahmenbedingungen
- Systeme, welche für gleiche Aufgaben genutzt werden
- Systeme, welche den gleichen Schutzbedarf aufweisen

Die bei der Komplexitätsreduktion entstandenen Gruppen werden fortan wie einzelne Objekte behandelt. **Wichtig:** Keine Komponenten mit zu unterschiedlichem Schutzbedarf zusammenfassen, Beispiele:

- Clients der Geschäftsleitung nicht in Gruppe der «normalen» Clients integrieren
- Dito für Clients von Entwicklungsabteilung, Personalabteilung, Buchhaltung und IT-Administration
- → Sie alle haben einen erhöhten Schutzbedarf!



4.7.1.3 Erhebung IT-Systeme

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 Auftragsbearbeitung	Windows Vista	BG, R. 2.03 – 2.09	14	in Betrieb	Einkauf, Marketing und Vertrieb/IT-Administration
C7	Clients in Entwicklungsabteilung	Windows Vista	Beuel, R. 2.14 – 2.20	6	in Betrieb	Entwicklung/IT-Administration

4.7.1.4 Zuordnung von Systemen und Anwendungen

- Erfassung und Zuordnung der Anwendungen
- Konzentration auf Systeme mit
 - Höchsten Bedarf an Vertraulichkeit
 - Höchsten Bedarf an Korrektheit (Integrität)
 - Kürzeste tolerierbare Ausfallzeit (Verfügbarkeit)

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, S = Server, C = Client

Quelle: BSI Webkurs IT-Grundschutz

2 4.7.2 Schutzbedarfsfeststellung

- Begründete und nachvollziehbare Einschätzung des Schutzbedarfs
- Ziel: angemessene Sicherheitsmaßnahmen für verschiedene IT-Komponenten

4.7.2.1 Vorgehen

- Definition der Schutzbedarfskategorien entsprechend der Besonderheiten der Organisation (sog. Individualisierung)

niedrig bis mittel	hoch	sehr hoch	Normal / Niedrig bis mittel Begrenzte und überschaubare Schäden
z. B.:			Hoch Beträchtliche Schäden möglich
			Sehr hoch Existentiell bedrohliche, katastrophale Schäden möglich

- Schutzbedarfsfeststellung:
 - von IT-Anwendungen und Daten
 - davon abgeleitet von IT-Systemen
 - davon abgeleitet von Kommunikationsverbindungen und IT-Räumen
 - Dokumentation und Interpretation der Ergebnisse

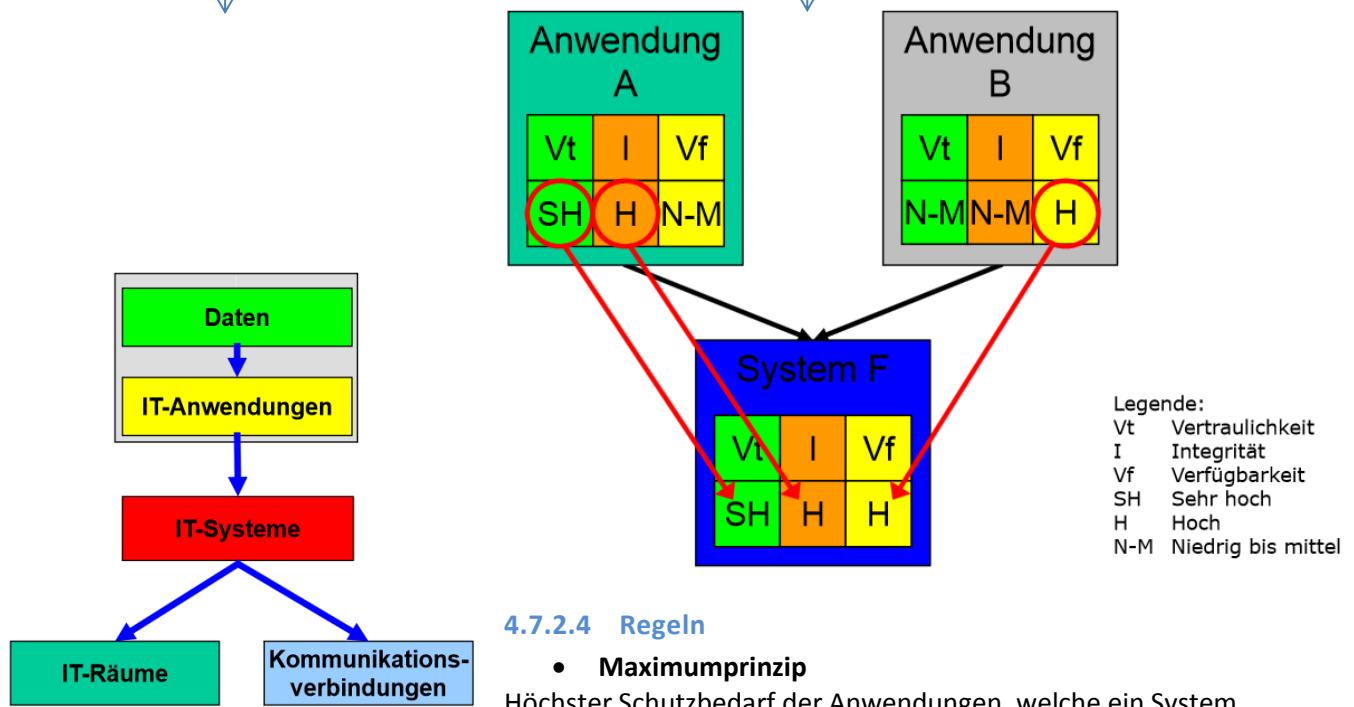
4.7.2.2 Individualisierung der Kategorien

Individualisierung Anhand folgender Schadenszenarien:

- Verstoss gegen Gesetze/Vorschriften/Verträge
- Beeinträchtigung des informationellen Selbstbestimmungsrechts

- Beeinträchtigung der persönlichen Unversehrtheit
- Beeinträchtigung der Aufgabenerfüllung
- Negative Aussenwirkung (Imageschäden)
- Finanzielle Auswirkungen

4.7.2.3 Abhängigkeit/Vererbung von Schutzbedarf und Maximum-Prinzip



nutzen, gilt für das 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 (Anwendung ist auf mehrere Systeme verteilt; auf dem betrachteten System laufen nur weniger wichtige Teile davon)

4.7.2.5 Schutzbedarf von IT-Anwendungen

Für alle IT-Anwendungen muss der Schutzbedarf für die drei Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität bestimmt werden! Beispiel:

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.

4.7.2.6 Schutzbedarf von IT-Systemen

IT-System		Schutzbedarfsfeststellung	
Nr.	Bezeichnung	Schutzbedarf	Begründung
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 Schutzbedarf hoch. Er wurde als normal festgelegt, weil die Benutzer aus Bad Godesberg sich auch über den Domänen-Controller S6 in Beuel anmelden können. Ein Ausfall bis zu drei Tagen ist hinnehmbar (Verteilungseffekt).

Regeln: siehe oben!

4.7.2.7 Schutzbedarf von IT-Räumen

Vererbung und Maximumprinzip berücksichtigen: Schutzbedarf bemisst sich am Schutzbedarf der IT-Systeme und der Informationen, welche im IT-Raum gelagert und verarbeitet werden

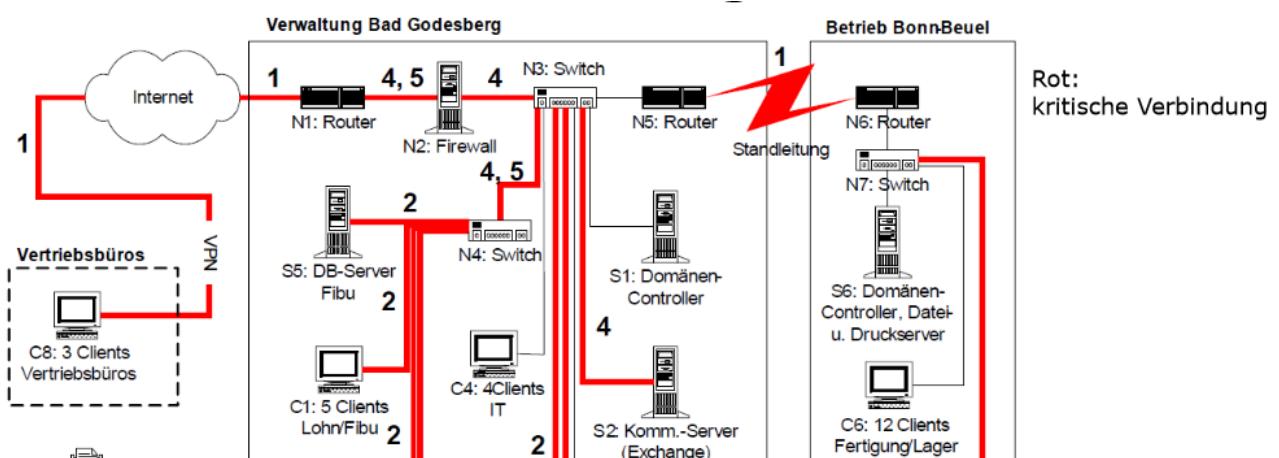
Raum			Schutzbedarf			
Bezeichnung	Art	Lokation	IT-Systeme	Vertraulichkeit	Integrität	Verfügbarkeit
BG, R. 1.01	Technikraum	Verwaltungsgebäude	TK-Anlage T1	normal	normal	hoch
BG, R. 1.02	Serverraum	Verwaltungsgebäude	S1 bis S5 N1 bis N5	hoch	hoch	hoch
Beuel, R. 2.01	Serverraum	Produktionshalle	S6, N6, N7	normal	normal	normal
Beuel, R. 2.10 – 2.13	Büroräume	Produktionshalle	C6, einige mit Faxgeräten	hoch	normal	normal

4.7.2.8 Schutzbedarf von Kommunikationsverbindungen

Folgende Verbindungen sind als kritisch einzustufen:

- Verbindungen in ein öffentliches Netz (Internet, Telefonnetz etc.)
- Verbindungen, über die besonders schützenswerte Informationen übertragen werden
- Verbindungen, über die vertrauliche Informationen nicht übertragen werden dürfen

→ Der Schutzbedarf der übertragenen Informationen leitet sich vom Schutzbedarf der miteinander verbundenen IT-Systeme ab



4.7.2.9 Interpretation der Ergebnisse

- Normal / Niedrig bis mittel

Standard-Sicherheitsmaßnahmen

- Hoch

Standard-Sicherheitsmaßnahmen + evtl. ergänzende Sicherheitsanalyse

- Sehr hoch

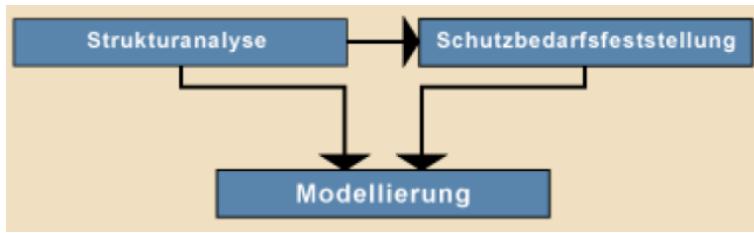
Standard-Sicherheitsmaßnahmen + zwingend ergänzende Sicherheitsanalyse

3

4.7.3 IT-Grundschatzanalyse

4.7.3.1 Modellierung nach IT-Grundschatzanalyse

Ziel der Modellierung gemäß IT-Grundschatzanalyse ist es festzulegen, welche Bausteine des IT-Grundschatzanalysehandbuchs auf welche Zielobjekte der IT einer Organisation anzuwenden sind (Ergebnis: IT-Grundschatzanalysemodell).



4.7.3.2 Vorgehen

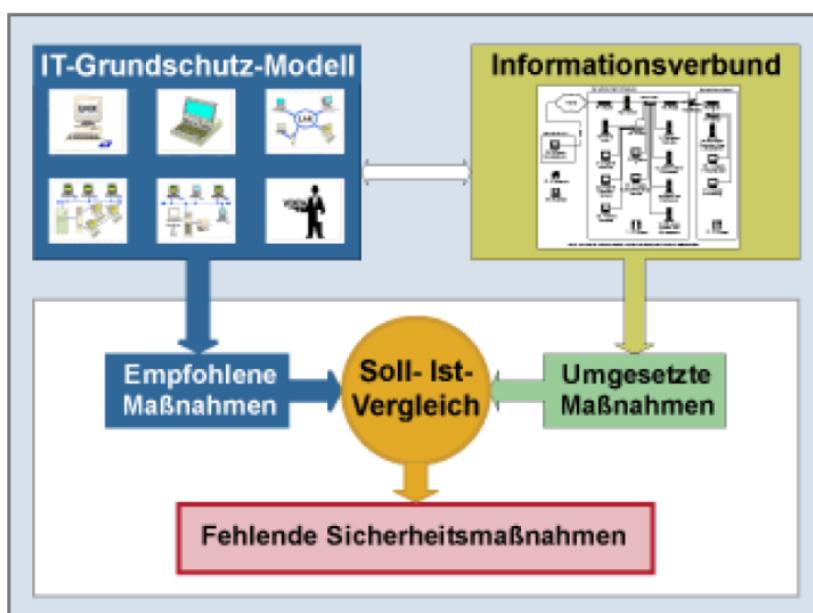
- Die Modellierung erfolgt entsprechend dem Schichtenmodell der IT-Grundschutz-Bausteine (Total 85 Bausteine)
- Schichtweise werden diejenigen Bausteine ausgewählt, welche für die Sicherheit des IT-Verbunds notwendig sind
- Ausgewählte Bausteine werden dem jeweiligen Zielobjekt (IT-Systeme, Räume etc.) zugeordnet
- Bei Bedarf können Bausteine im Rahmen der Modellierung modifiziert werden (z. B. Ergänzung um zusätzliche Massnahmen oder Konkretisierung von technischen Details)

Wichtig: Abschliessende Prüfung auf Vollständigkeit durchführen

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	

4.7.3.3 Basis-Sicherheitscheck

Mit einem Basis Sicherheitscheck ermitteln wir, ob und inwieweit die Massnahmenempfehlungen des IT-Grundschutzhandbuchs für die einzelnen Zielobjekte des betrachteten IT-Verbunds umgesetzt sind.



Vorgehen :

- Im Grundschutzmodell haben wir die anzuwendenden Bausteine ausgewählt, dies stellt nun eine Art Prüfplan dar.

- Nun überprüfen wir für jedes Zielobjekt und für jede Massnahme der entsprechenden Bausteine, ob sie überhaupt auf das Zielobjekt anzuwenden ist und inwieweit sie umgesetzt wurde.

4 4.7.4 Ergänzende Sicherheitsanalyse

Sie ist durchzuführen, wenn für einzelne Zielobjekte

- die Schutzbedarfskategorie «hoch» oder «sehr hoch» in mindestens einem der drei Grundwerte vorliegt,
- kein geeigneter Baustein im Baustein-Katalog zu finden ist, oder
- Objekte in untypischer Weise oder Einsatzumgebung betrieben werden

4.7.4.1 Vorgehensweisen für weitere Untersuchungen

- **Klassische Risikoanalyse**
 - relevante Bedrohungen oder Schwachstellen ermitteln
 - Eintrittswahrscheinlichkeiten und Schadenshöhen schätzen
- **Penetrationstest**
 - Verhalten eines Angreifers simulieren
 - Blackbox- und Whitebox-Ansatz unterscheiden
- **Differenz-Sicherheitsanalyse**
 - Feststellen, welche der Sicherheitsmassnahmen über die Grundschatzmassnahmen hinausgehend realisiert sind
 - Vergleich durchführen, ob die ergriffenen Massnahmen den «Best Practices» entsprechen, die sich in der Praxis für hochschutzbedürftige IT-Bereiche etabliert haben

5 4.7.5 Realisierungsplan

- Ergebnisse sichten (fehlende Sicherheitsmassnahmen zusammenstellen)
- Massnahmen konsolidieren (überfl. M. streichen, verbleibende konkretisieren - >Massnahmenliste)
- Aufwand schätzen (finanziell, personell / einmalig, wiederkehrend)
- Umsetzungsreihenfolge festlegen (zuerst diejenigen, welche Voraussetzung für andere sind)
- Verantwortliche und Termine bestimmen (für Realisierung und Überwachung von jeder Massnahme)
- Begleitende Massnahmen festlegen (Sensibilisierung und Schulung)
- Ergebnis: Realisierungsplan

Beispiel:

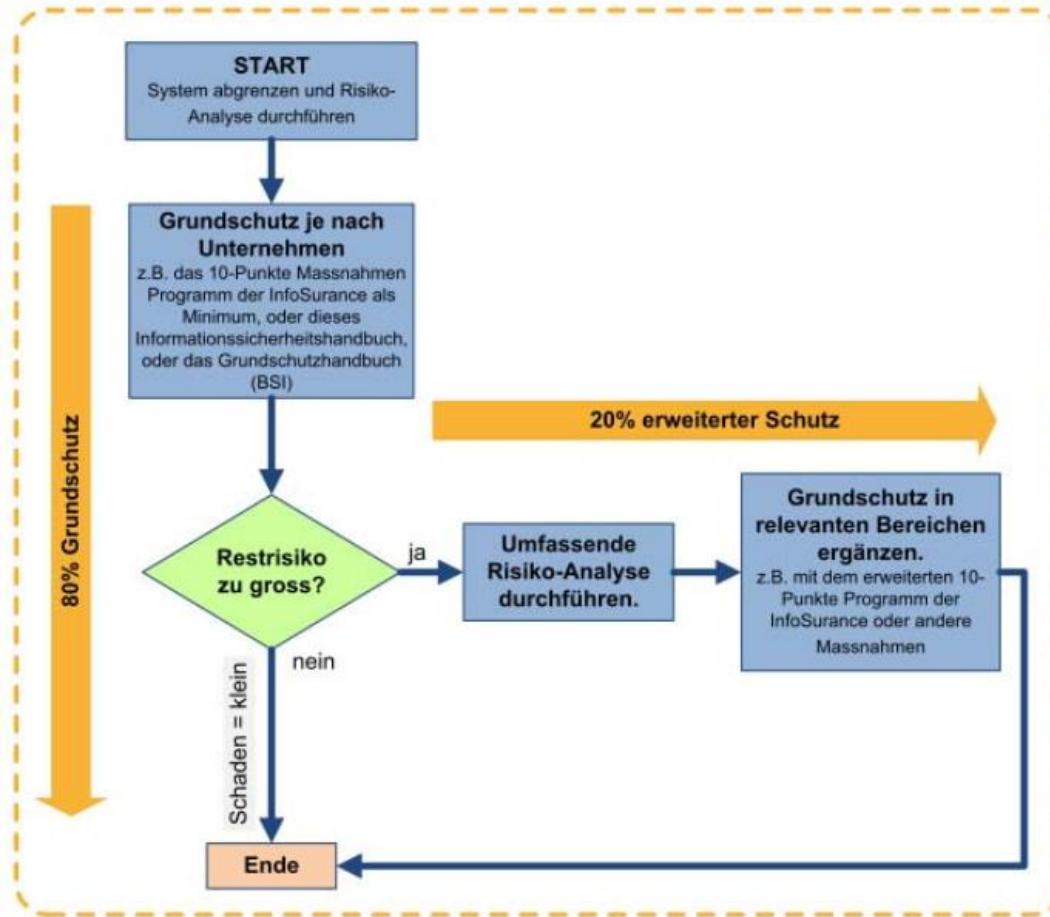
Zielobjekt: BG R. 1.02 Serverraum				
Baustein: B 2.4 Serverraum				
Maßnahme (erforderlich ab Siegelstufe)	Umsetzung bis	Verantwortlich	Budget	Bemerkungen
M 1.3 (A) Angepasste Aufteilung der Stromkreise	38. KW	Umsetzung: M. Wachsam Kontrolle: P. Muster	a) 0,- € b) 0,3 PT c) 0,- € d) 0 PT/Jahr	Die Elektro-Installation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

4.8 IT-Grundschutz – Aufpassen

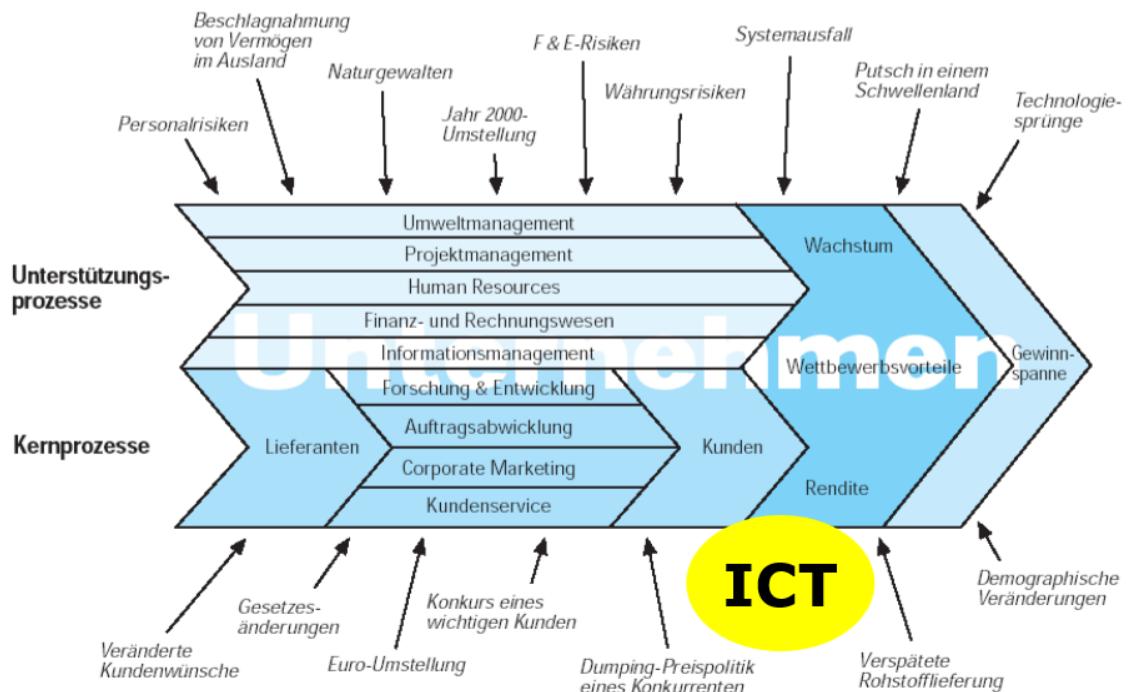
- Ungenügender Schutz bei erhöhten Risiken oder besonderem Schutzbedarf
- Mögliche Einschränkung der Funktionalität durch Überschutz
- Begründung von Massnahmen schwierig
- Je nach Detaillierungsgrad, Anspruch an Aktualität und Vollständigkeit des Massnahmenkataloges aufwändig
- Vorteile des Grundschutzvorgehens nicht durch administrativen «Overkill» zunichte machen

5 Kapitel 5 – Risikoanalyse

5.1 Vorgehen



5.2 Risiken in Unternehmen



5.2.1 Risiken im Bereich der IT-Organisation

- **Organisatorische Risiken**
 - Nicht autorisierte Zugriffe auf Informationen und Applikationen
 - Nicht prozessbezogener Einsatz von Applikationen
 - Fehlende Fachkompetenz von Mitarbeitenden
 - Mangelhafte Testverfahren
 - Datendiebstahl
- **Infrastrukturelle Risiken**
 - IT-Infrastruktur kann den Ansprüchen (z. B. Leistungsfähigkeit) nicht gerecht werden
 - Fehlender Notfallplan
 - Fehlender Wiederanlaufsplan (Business ContinuityManagement)
 - Bauliche oder technische Standards werden nicht erfüllt (Schutz vor Zutritt, Feuer und Energieausfall)
 - Mangelhafte Dokumentation der Systeme, Mangelhaftes Backupkonzept
- **Anwendungs- und prozessbezogene Risiken**
 - Veraltete und nicht integrierte Softwarelösungen (Insellösungen)
 - Fehlende strategische Neuorientierung
- **Kostenbezogene Risiken**
 - Fehlende Kostentransparenz
 - Mangelhafte Projektdefinition und -organisation mit daraus resultierenden Kostenüberschreitungen
- **Projektbezogene Risiken**
 - Run-away-Projekte (Zeit, Kosten und Termine laufen aus dem Ruder)
 - Unprofessionelles Projekt-Management

5.2.2 Bedrohungen / Gefahren

- Gezielte Angriffe von aussen oder innen
- Fahrlässigkeit
- Naturkatastrophen / Elementarschäden
- Politische Instabilität
- Weitere Bedrohungen ISO 27005

5.3 Risiko Ermittlung

Risiko

=

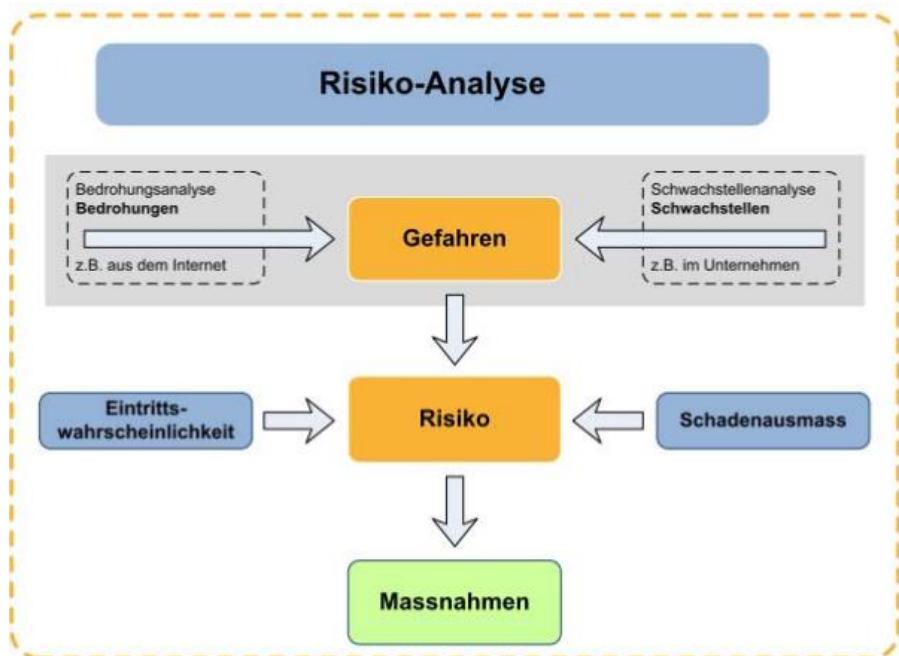
Eintrittswahrscheinlichkeit x Schadensausmass

5.4 Risiko Analyse

- **Quantitative Risikoanalyse**
 - Die an der Risikoanalyse beteiligten Größen sollen numerisch exakt berechnet werden
- **Qualitative Risikoanalyse**
 - Die an der Risikoanalyse beteiligten Größen werden anhand einer mehrstufigen Skala nur eingeschätzt, z. B. Schadensausmass «4» auf einer 5-stufigen Skala

5.4.1 Vorgehen

Zuerst müssen die vorhandenen Bedrohungen aufgelistet und eingestuft werden. Danach müssen die vorhandenen Schwachstellen ermittelt werden. Trifft eine Gefährdung auf eine Schwachstelle, dann entsteht eine Gefahr!



5.4.1.1 Schadenausmass

Auswirkung (A)	Stufe	Beschreibung
Vernachlässigbar	1	Vernachlässigbare Auswirkungen <ul style="list-style-type: none"> Dienstleistungen nicht wesentlich gestört Sachschäden im Bereich von CHF 100.- bis 5'000.-^(*) keine Verletzten kein Imageverlust
Marginal	2	Geringe Auswirkungen <ul style="list-style-type: none"> Die Einhaltung gesetzlicher und vertraglicher Pflichten ist nicht gefährdet Die Dienstleistungen sind nur geringfügig beeinträchtigt Sachschäden im Bereich von CHF 5'000.- bis 50'000.-^(*) keine Verletzten kein Imageverlust
Kritisch	3	Grosse Auswirkungen <ul style="list-style-type: none"> Die Einhaltung gesetzlicher und vertraglicher Pflichten ist gefährdet oder die Dienstleistungen sind beeinträchtigt Sachschäden im Bereich von CHF 50'000.- bis 500'000.-^(*) Keine Verletzten Imageverlust ist klein und von kurzer Dauer
Katastrophal	4	Sehr grosse Auswirkungen <ul style="list-style-type: none"> Die Einhaltung gesetzlicher und vertraglicher Pflichten sind stark gefährdet oder die Dienstleistungen werden verunmöglich Sachschäden im Bereich > CHF 500'000.-^(*) einige Schwerverletzte grosser Imageschaden (Presse)

5.4.1.2 Eintrittswahrscheinlichkeit

Eintrittswahrscheinlichkeit (W)	Stufe	Kriterium
Sehr selten	1	Möglich aber eher unwahrscheinlich z.B. 1-mal in 10 Jahren
Selten	2	Tritt selten ein, aber kann vorkommen z.B. alle 5 Jahre
Oft	3	Tritt gelegentlich ein z.B. jährlich
Sehr oft	4	Kommt öfters vor z.B. monatlich

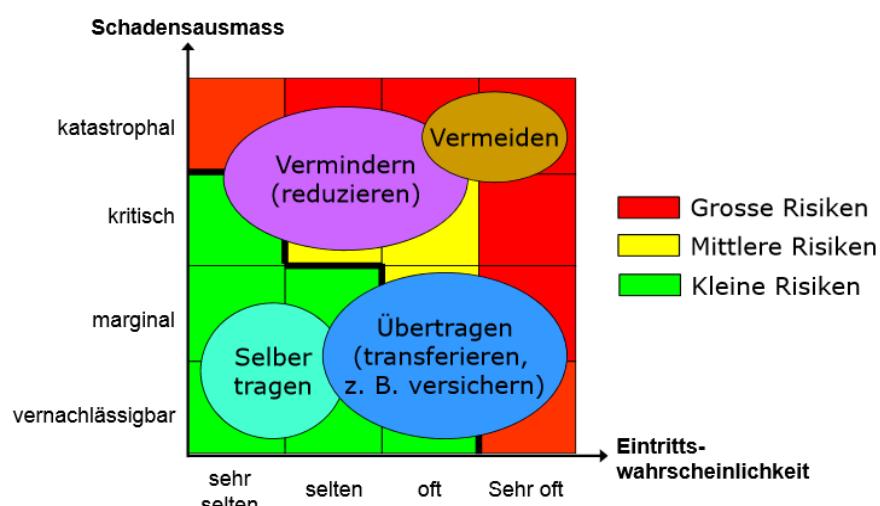
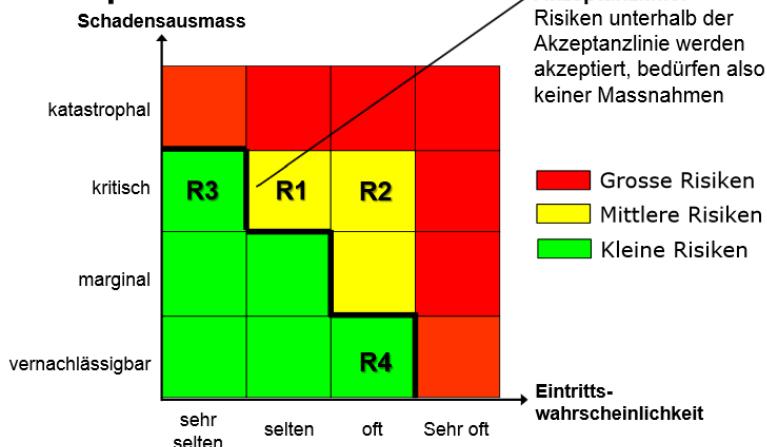
5.4.1.3 Risiko Portfolio

Nr.	Gefahr	W	A	R = W x A
1	Diebstahl (z.B. Notebook etc.)	3	2	6
2	Computer-Viren, Spyware	4	3	12
3	Social Engineering Attacke	3	3	9

W= Eintrittswahrscheinlichkeit (1-4), A= Schadensausmass (1-4), R= Risiko

5.4.1.4 Risikomatrix

Akzeptanzlinie



5.4.1.5 Umgang mit Risiken

- **Risiken vermeiden:**

Anpassen oder Aufgeben von Geschäftsprozessen, sodass die Risiken nicht mehr vorhanden sind

- **Risiken vermindern:**

Mit geeigneten Sicherheitsmaßnahmen das Schadensausmass oder die Eintrittswahrscheinlichkeit reduzieren

- **Risiken übertragen (transferieren):**

Überwälzung finanzieller Schäden auf Versicherungen, Outsourcer oder Benutzer eines Service

- **Risiken tragen:**

Akzeptieren von Risiken (Restrisiken)



5.4.1.6 Risiko Katalog

Nr	Risiko	Auswirkungen	W		A		Massnahmen	W		A	
			vor Massnahmen		nach Massnahmen			nach Massnahmen		nach Massnahmen	
1	Viren	Integrität, Verfügbarkeit, Vertraulichkeit	4	3			Virenschanner, Firewall etc.	1	1		
2	Diebstahl Note-book	Datenverlust	3	2			Sensibilisierung, Verschlüsselung	3	1		
3	Social Engineering Attacke	Know-how Verlust, Diebstahl	3	3			Sensibilisierung	1	1		

W= Eintrittswahrscheinlichkeit (1-4), A= Schadensausmass (1-4), R= Risiko

6 Kapitel 6 – Notfallplanung

6.1 Ziele

- Den Geschäftsfortgang sicherstellen
- Weiteren Schaden verhindern

6.1.1 Themen

- Prioritäten der Geschäftsprozesse festlegen
- Notfall-Organisation
- Alarmierung / Eskalation
- Notfallhandbuch
- Notfallübung
- Informationspolitik/Kommunikation bei einem Vorfall

6.2 Fokus

Sicherstellen des Geschäftsfortganges und somit Sicherstellen:

- der wichtigsten Geschäftsprozesse,
- der dafür erforderlichen Applikationen resp. der dafür erforderlichen Systeme und Netzwerke

6.3 Phasen

1. Planung
 - Analyse der Bedürfnisse
 - Zu schützende Geschäftsprozesse
 - Dazu nötige Infrastruktur
 - Mögliche Notfallszenarien
2. Umsetzung der den IT-Betrieb begleitenden Notfallvorsorge-Massnahmen
3. Durchführung von Notfallübungen
4. Umsetzung geplanter Massnahmen nach Eintreten eines Notfalls
5. Rückkehr zum Normalzustand

6.4 Business Impact Analysis (BIA)

Ermitteln der Wichtigkeit (Kritikalität) der Geschäftsprozesse resp. Applikationen

- Spalten

Ausfallzeiten z.B. 8h, 1 Tag, 3 Tage, 1 Woche

- Reihen

Prozesse / Applikationen

- Pro Feld Beeinträchtigung auf die Unternehmung ermitteln

- Z.B. klein, mittel, gross, existenziell
- Klassifizierung z.B. ähnlich wie die Schutzbedarfskategorien des BSI (Finanzielle Auswirkungen, Verstoss gegen Gesetze / Vorschriften / Verträge, Beeinträchtigung der Aufgabenerfüllung, Imageschäden, etc.)

Applikationen/ Prozesse	Ausfallzeiten			
	8 h	1 Tag	3 Tage	1 Woche
Applikation A / Prozess A	Kleine Beeinträchtigung	Kleine Beeinträchtigung	Mittlere Beeinträchtigung	Grosse Beeinträchtigung

6.5 Notfallvorsorge für grösste Risiken

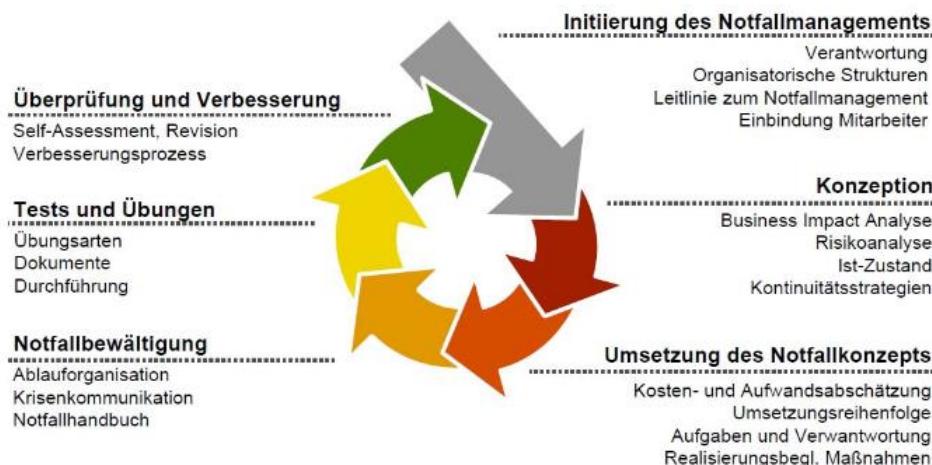
→ Definition von möglichen Szenarien/Gefahren

- **Priorisierung nach:**
 - Übergreifende Folgen
 - Mit grossen Auswirkungen / Schäden
 - Hohe Wahrscheinlichkeit
- **Pro Szenario**
 - Definition der Auslöser des Notfall-Betrieb
 - Ableiten von vorbeugenden Massnahmen (zur Reduktion der Wahrscheinlichkeit resp. Schadenshöhe)
 - Ableiten von Sofortmassnahmen
 - Ableiten von vorbehaltene Entschlüsse
 - Überlegungen zur Rückführung zum Normalfall (z.B. Zusammenführen von Datenbanken nach der Aufteilung für den Notfallbetrieb)
- **Nicht behandelte Szenarien dokumentieren!**

6.6 Umsetzung

1. Notfallmanagement
2. Notfallorganisation
3. Notfallhandbuch
4. Vorbehaltene Entschlüsse
5. Informationspolitik/Kommunikation
6. Notfallübungen

1. Notfallmanagement



2. Notfallorganisation

- Definition der Stäbe
- Festlegen der Rollen
- Erstellen der Pflichtenhefter
- Klären der Verantwortlichkeiten / Kompetenzen
- Definition der Entscheidungswege / Erreichbarkeit
- Festlegen der Stellvertretung

3. Notfallhandbuch

Einfache Anleitung zur Bewältigung des Notfalls:

- Notfallorganisation
- Alarmierung
- Sofortmassnahmen
- Vorbehaltene Entschlüsse

4. Vorbehaltene Entschlüsse

Vorgängig erarbeitete Massnahmen für einen Fall X, resp. Y,. Werden im Notfall zur Unterstützung eingesetzt und bilden Handlungs- und Entscheidungsspielraum. Lösungen sind nicht nur IT-bezogen, sondern kommen auch aus den Fachabteilungen!

5. Informationspolitik / Kommunikationspolitik

Wer wird wann worüber informiert?

- Mitarbeitende (z.B. Intranet)
- Kunden (z.B. Telefon, Schreiben, Webseite)
- Öffentlichkeit (Mediensprecher, Medienkonferenz)
- Briefing Mitarbeitende bezüglich der Weitergabe von Informationen

6. Notfallübungen

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

6.7 Schwächen der Notfallvorsorge

- Dokumentation nicht aktuell
- Nie eingebübt
- Beschreibung zu kompliziert
- Vorgehen zu aufwändig
- Im Notfall nicht verfügbar
- Kein schrittweises Wiederanlaufen geplant (Übergang zurück zum Normalbetrieb)

7 Kapitel 7 – Awareness

Ein grosses Risiko ist oft zwischen Bildschirm und Tastatur zu finden →Der Benutzer!

- Der Mensch kann den grössten Schutz bieten
- Der Mensch kann das grösste Risiko darstellen

Das Potenzial der Mitarbeitenden muss eingebunden werden!

7.1 Risiken durch Mitarbeiter

- Schwache Passwörter
- Unsichere Passwortspicks (unter der Tastatur)
- Ausschalten Virenschutz
- Installation eigener Hard- und Software
- Falscher Umgang mit e-Mail/Internet
- Weitergabe von internen resp. vertraulichen Informationen (Data Leakage)
- Mangelhafte Datenablage (Struktur, Backup)
- Anpassungen an der Konfiguration

7.2 Weisungen / Richtlinien

Verhaltensregeln definieren und Dos and don'ts festlegen

7.2.1 Beispiel Benutzerrichtlinien (mögliche Inhalte)

- Internet (Inhalte, Download, Zeiten)
- Download/Installation Software
- Passwörter
- Private Hardware (BYOD)
- E-Mail (Inhalte, Vertraulich, Umleitung)
- Zutritt (Externe, Büro)
- Mobile Geräte und Datenträger
- Clear-Desk
- Sanktionen

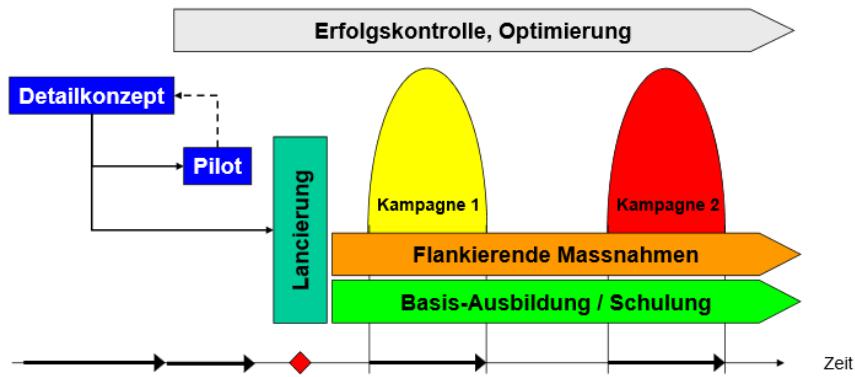
7.3 Awareness und deren Bedeutung für Unternehmen

- «Awareness» muss vom obersten Management unterstützt werden!
- «Awareness» muss stufengerecht gebildet werden:
 - Benutzer/Anwender
 - IT Mitarbeiter
 - Management

7.4 Wie anpacken?

- | | |
|--|--|
| <ul style="list-style-type: none">• Gefahren<ul style="list-style-type: none">• Begreifen• Folgen abschätzen• Schutz<ul style="list-style-type: none">• Know-how aufbauen• Mitarbeitende als Sensor• Überwachung• Motivation<ul style="list-style-type: none">• Mitarbeitende einbeziehen• Verständnis schaffen• Entstehung einer Kultur fördern | <ul style="list-style-type: none">• Zielgruppen<ul style="list-style-type: none">• Management (GL, VR, Projektleiter etc.)• Mitarbeitende• IT-Team• Umsetzung<ul style="list-style-type: none">• Methoden (Schulungen, Kampagnen, flankierende Massnahmen, Goodies etc.)• Erfolgskontrolle durchführen• Nachhaltigkeit sicher stellen |
|--|--|

7.4.1 Zeitlicher Ablauf eines Awareness Programms



7.4.2 Comments

Die Awareness Kampagne sollte auf das Zielpublikum zugeschnitten sein (Verständlichkeit). Dies führt meistens zu AHA-Erlebnissen. Allerdings sollten auch Verstöße geahndet werden → Sanktionen sind zu definieren und anzuwenden!

- Ein verbindliches «Regelwerk» muss vorhanden sein
- Sämtliche Mitarbeitenden müssen dieses Regelwerk kennen und es auch verstanden haben
- Es muss klar ersichtlich sein, was bei einem Verstoss passiert

8 Glossar

Mit **Awareness** („Bewusstsein“ oder „Gewahrsein“) ist im Informatik Bereich gemeint:
das Bewusstsein einer Anwendung eines Computers für alle Eigenschaften ihrer Umgebung.

In der Informationssicherheit bezeichnet **Authentizität** die Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit. Die Überprüfung einer behaupteten Eigenschaft wird als Authentifikation bezeichnet. Durch Authentifikation des Datenursprungs wird nachgewiesen, dass Daten einem angegebenen Sender zugeordnet werden können, was durch digitale Signaturen ermöglicht werden kann.

Information ist die Verknüpfung von Daten in Form von Zahlen, Worten und Fakten zu interpretierbaren Zusammenhängen. Durch die Vernetzung von Informationen entsteht Wissen, das zunächst personenbezogen ist.

Als **Informationssicherheit** bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden Systemen, die die **Vertraulichkeit**, **Verfügbarkeit** und **Integrität** sicherstellen. Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von Schäden und der Minimierung von Risiken. In der Praxis orientiert sich die Informationssicherheit heute unter anderem an der ISO/IEC Standard-Reihe 2700x aber auch zunehmend an ISO/IEC 15408

Sicherheit bezeichnet einen Zustand, der frei von unvertretbaren Risiken der Beeinträchtigung ist oder als gefahrenfrei angesehen wird.