Compliance und IT-Sicherheit

Isabel Münch

Bundesamt für Sicherheit in der Informationstechnik
IT-Sicherheitsmanagement und IT-Grundschutz

Agenda

- Das BSI
- Compliance-Anforderungen und IT-Sicherheit
- Risikomanagement und IT-Sicherheitsmanagement
- Internationale Standards zum Management der Informationssicherheit
- BSI-Standards zum IT-Sicherheitsmanagement
- Vorgehensweise IT-Grundschutz

Kurzportrait

Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Das BSI auf einen Blick
- Arbeitsschwerpunkte
- Zielgruppen

Das BSI

... ist eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft.

- Gründung 1991 per Gesetz als nationale Behörde für IT-Sicherheit.
- Jahresbudget: € 52 Mio. (2005)
- Mitarbeiter: 458 (Stand: Dez. 2005)
- Standort: Bonn

Arbeitsschwerpunkte des BSI

- Internetsicherheit
- sicheres E-Government
- IT-Grundschutz
- nationale / internationale Sicherheits-kooperationen
- Kryptoinnovation
- Biometrie
- Abhörsicherheit
- Sensibilisierungskampagne IT-Sicherheit
- Zertifizierung und Zulassung
- Schutz kritischer Infrastrukturen

Zielgruppen des BSI

Regierung und Verwaltung

- IT-Sicherheitsberatung
- Entwicklung von Kryptosystemen
- Lauschabwehr
- Betrieb des Regierungsnetzes SINA VPN
- Unterstützung der E-Government Initiative

Bürger

- Sensibilisierungskampagnen
- Info - CD´s
- BSI - Internetangebot
  - www.bsi.bund.de
  - www.bsi-fuer-buerger.de
  - www.buerger-cert.de
- Fachbeiträge in Zeitschriften

Wissenschaft

- Kooperation mit Universitäten
- Trendanalysen
- Vergabe von Forschungsaufträgen

Wirtschaft

- Nationales CERT
- IT-Grundschutz
- Zertifizierung
- Sicherheitspartnerschaften

IT-Sicherheit

Trends:

- Abhängigkeit von der IT wird weiter zunehmen
- Die eigene IT (und damit Geschäftsprozesse) wird von innen und außen bedroht
- Bewusstsein für IT-Bedrohungen muss stärker werden
- Prävention stellt eine zentrale Aufgabe dar
- IT-Sicherheit wird Teil des Risikomanagements
- Vorgaben werden schärfer
- Ein ganzheitlicher, nicht nur auf die Technik gerichteter Ansatz ist notwendig

Gesetzliche Rahmenbedingungen

Vorgaben:

- Basel II
- Solvency II
- Sarbanes Oxley Act (SOX)
- KonTraG sowie GmbHG, AktG, HGB, GoBS, BDSG, ...
  - ➔ BSI-Projekt zu Rechtsentwicklung in der IT-Sicherheit
- Compliance zu Kontrollforderungen - Risiken müssen transparent werden
- ausreichende Kontrollmöglichkeiten vorhanden?

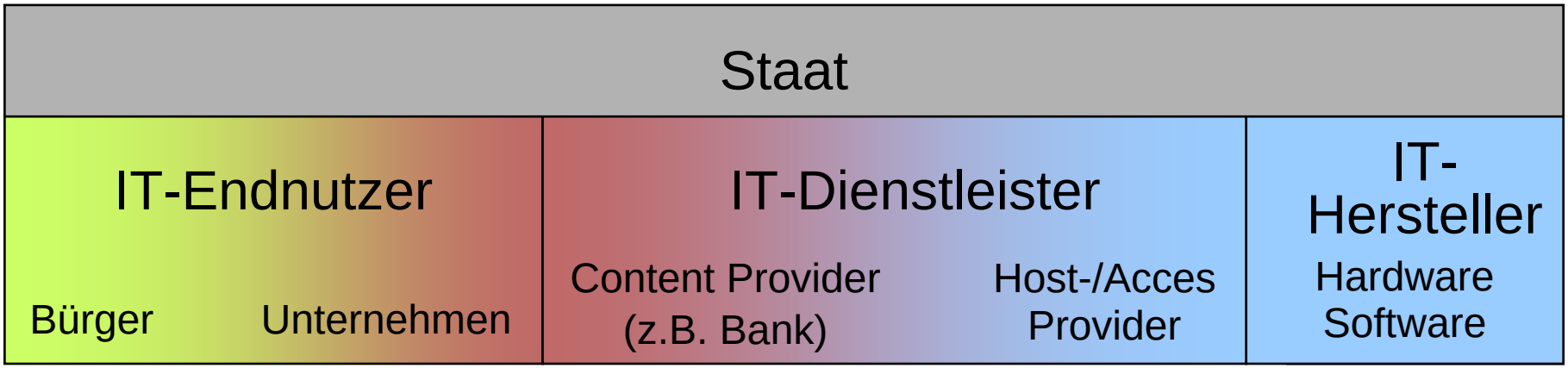
Gesetzliche Rahmenbedingungen

- Angemessenes Risikomanagement ist Grundlage zur Erfüllung dieser Richtlinien
- Risikomanagement umfasst IT-Sicherheitsmanagement
- Tendenz: Weg von technischen Einzelmaßnahmen, hin zu umfassendem Information Security Management System (ISMS)

➔ IT-Grundschutz als Basis für Compliance und Risikomanagement

- keine Garantie, aber gute Ausgangslage
- Reduzierter Aufwand bei Prüfungen (Anerkennung von Zertifikaten und Dokumentationen)

Zuordnung von Verantwortungsbereichen



Zuordnung von Verantwortungsbereichen

Verantwortlichkeit für DDoS-Attacke aus Bot-Netz?

(Schurke S)

Dienstleister D

Unsichere Verbindung

Nutzer N

Schwacher Schutz

Unternehmen U

Schwacher Schutz

Produzenten P

Programmschwachstelle

Umsetzung von Sicherheits-Standards

IT-Sicherheit und Sicherheitsmanagement

- **IT-Sicherheitsmanagement** (=Systematisches Vorgehen zum Erreichen eines angemessenen IT-Sicherheitsniveaus in Bezug auf Verfügbarkeit, Integrität, Vertraulichkeit)

Optimaler Einsatz der Ressourcen für IT-Sicherheit

- Optimierung der internen Prozesse führt zu einem geordneten, effektiven und effizienten IT-Betrieb --> mittelfristige Kosteneinsparungen
- Attraktivität für Kunden und Geschäftspartner durch Vertrauen
- Nutzung von Referenzwerken und Standards erhöht die Effizienz und Nachweisbarkeit

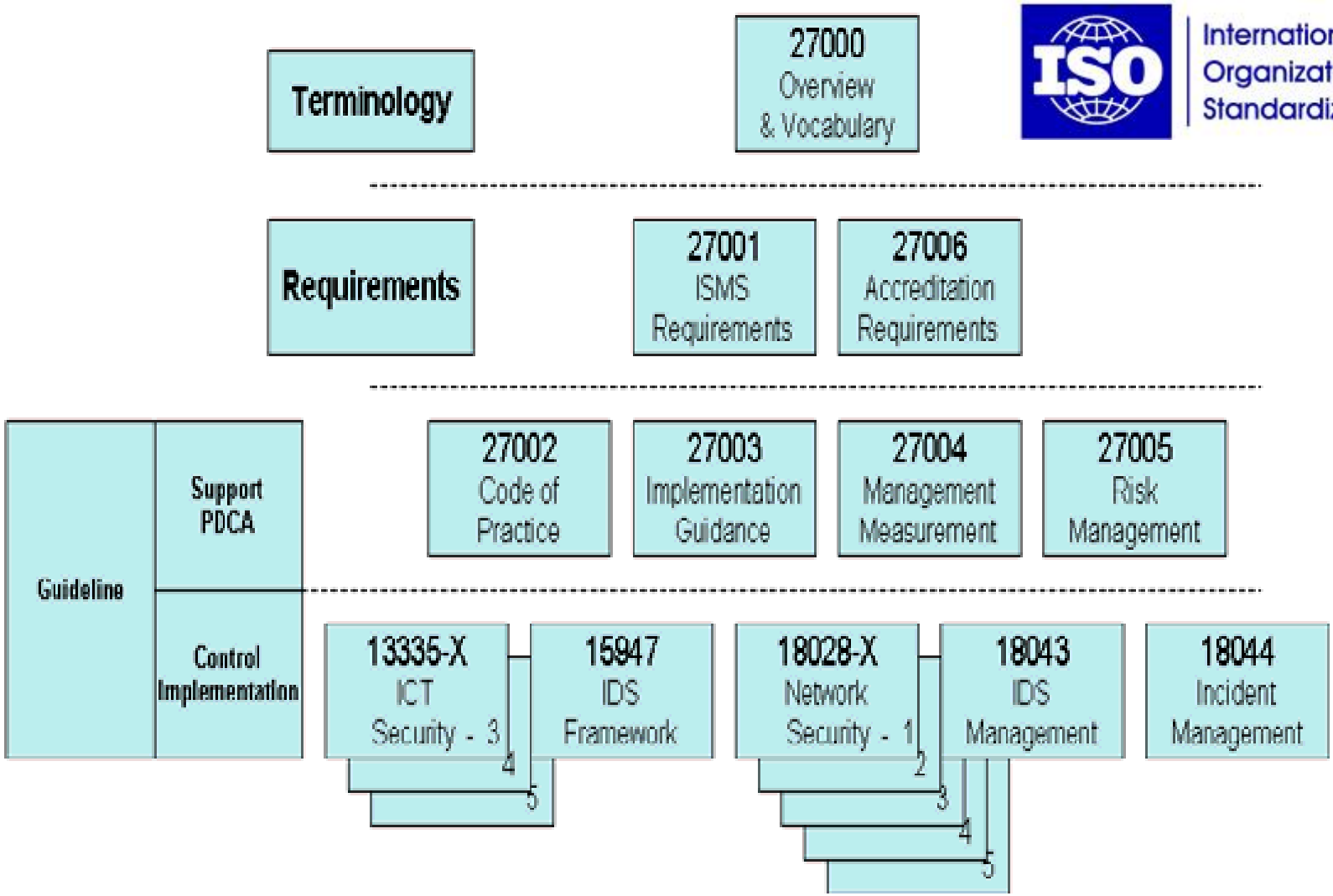
Internationale Standards zum Management der Informationssicherheit

International Organization for Standardization

ISO 27000 ff.:

- ISO 27000 (geplant, basierend auf ISO 13335-1): Informationssicherheits-Managementsysteme – Begriffe und Definitionen
- ISO 27001 (veröffentlicht, basierend auf BS 7799-2): Informationssicherheits-Managementsysteme – Anforderungen (ISMS-Zertifizierungsstandard)
- ISO 27002 (Umbenennung ISO 17799): Leitfaden für Informationssicherheits-Management (Detaillierung des Maßnahmenkatalogs der ISO 27001)
- ...

Internationale Standards zum Management der Informationssicherheit



IT-Grundschutz

BSI-Standards zur IT-Sicherheit

- Bereich IT-Sicherheitsmanagement -

BSI Standard 100-1:
ISMS: Managementsysteme für Informationssicherheit

BSI Standard 100-2:
IT-Grundschutz-Vorgehensweise

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

IT-Grundschutz-Kataloge

Kapitel 1: Einleitung

Kapitel 2: Schichtenmodell und Modellierung

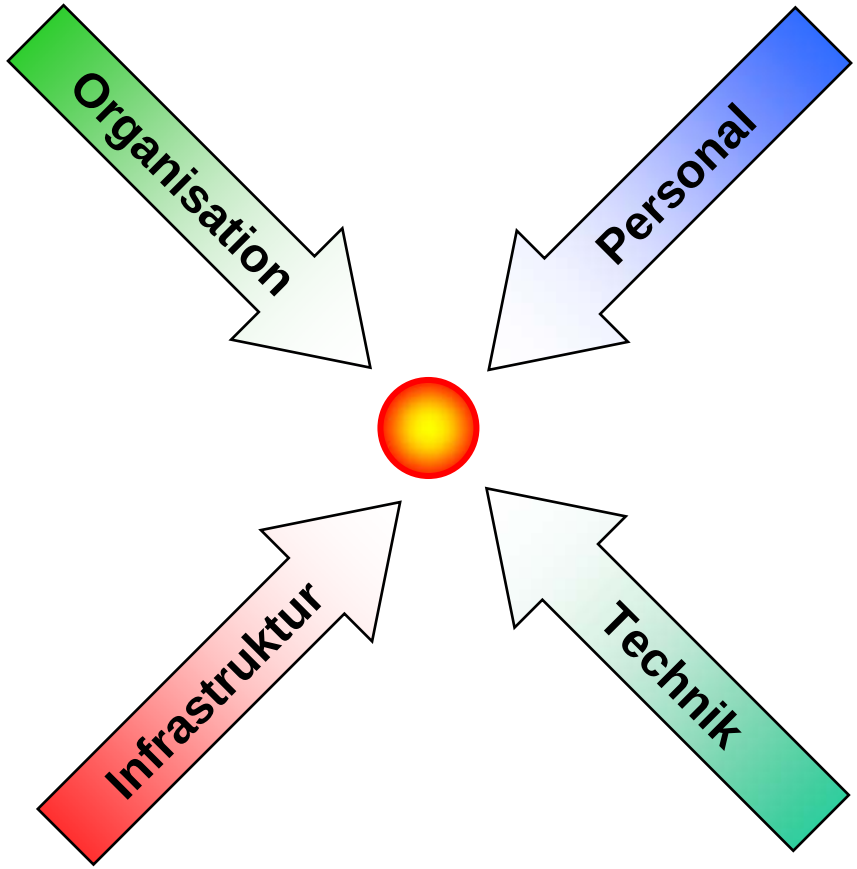
Kapitel 3: Glossar

Kapitel 4: Rollen

- **Bausteinkataloge**
  - Kapitel B1 "Übergreifende Aspekte"
  - Kapitel B2 "Infrastruktur"
  - Kapitel B3 "IT-Systeme"
  - Kapitel B4 "Netze"
  - Kapitel B5 "IT-Anwendungen"
- **Gefährdungskataloge**
- **Maßnahmenkataloge**

IT-Grundschutz

Ein System mit verschiedenen Gesichtern



- Information Security Management System
- Vorgehensweise zur Erstellung von IT-Sicherheitskonzepten
- Sammlung von Standard-Sicherheitsmaßnahmen für typische IT-Systeme
- Nachschlagewerk
- Referenz und Standard für IT-Sicherheit
- Basis für Zertifizierung

Ausgangspunkt für diverse Produkte und Dienstleistungen

Ziel des IT-Grundschutzes

Durch infrastrukturelle, organisatorische, personelle und technische

Standard-Sicherheitsmaßnahmen

ein

Standard-Sicherheitsniveau

für typische Geschäftsprozesse und Informations-systeme aufbauen, das auch für sensiblere Bereiche

ausbaufähig

ist.

BSI-Standards

BSI-Standard 100-1
Managementsysteme für Informationssicherheit

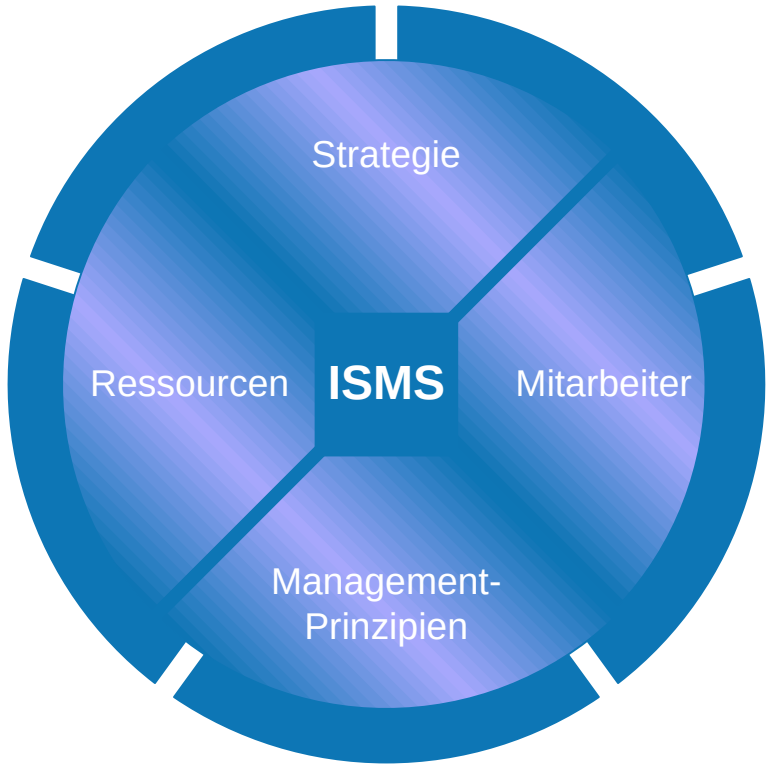
BSI-Standard 100-2
Vorgehensweise nach IT-Grundschutz

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

BSI-Standard 100-1
ISMS

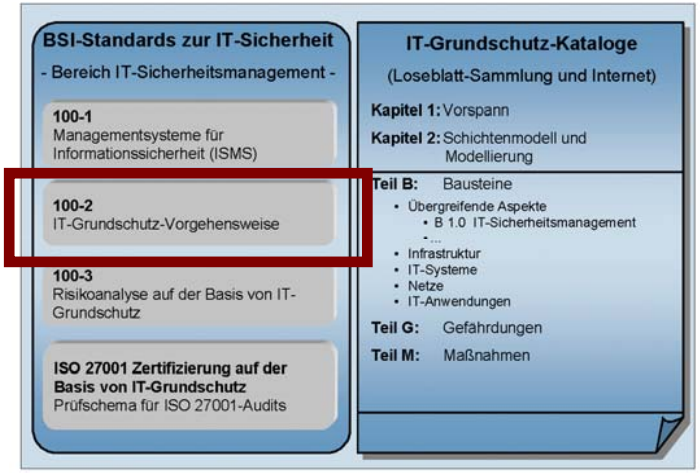
ISMS: Managementsysteme für Informationssicherheit

- Zielgruppe: Management
- Allgemeine Anforderungen an ein ISMS
- Kompatibel mit ISO 27001
- Empfehlungen aus ISO 13335 und ISO 17799



BSI-Standard 100-2
Wesentliche Merkmale

- Aufbau und Betrieb eines IT-Sicherheitsmanagements (ISMS) in der Praxis



- Anleitungen zu:
  - Aufgaben des IT-Sicherheitsmanagements
  - Etablierung einer IT-Sicherheitsorganisation
  - Erstellung eines IT-Sicherheitskonzepts
  - Auswahl angemessener IT-Sicherheitsmaßnahmen
  - IT-Sicherheit aufrecht erhalten und verbessern

Übersicht über den IT-Sicherheitsprozess

1 Initiative der Geschäftsführung

- Analyse: Geschäftsprozesse, Unternehmensziele
- IT-Sicherheitsleitlinie
- IT-Sicherheitsorganisation

2 Analyse der Rahmen-bedingungen

- Informationen, IT-Systeme, Anwendungen
- Schutzbedarf (Szenarien)

3 Sicherheitscheck

- Sicherheitsmaßnahmen
- Identifikation von Sicherheits-lücken

Übersicht über den IT-Sicherheitsprozess

4 Planung von Maßnahmen

- Liste geeigneter Maßnahmen
- Kosten- und Nutzenanalyse
- Auswahl umzusetzender Maßnahmen
- Dokumentation des Restrisikos

5 Umsetzung von Maßnahmen

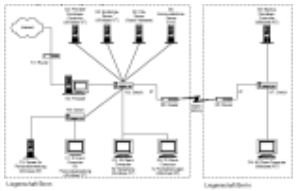
- Implementierung
- Test
- Notfallvorsorge

6 Sicherheit im laufenden Betrieb

- Sensibilisierung
- Schulung
- Audit, Kontrollen, Monitoring, Revision
- Notfallvorsorge

IT-Sicherheitskonzeption

IT-Verbund



- Infrastruktur
- Organisation
- Personal
- Technik

IT-Strukturanalyse
Analyse des Ist-Zustands
Welche Systeme und Anwendungen?

Feststellung des Schutzbedarfs

IT-Grundschutzanalyse:
Modellierung des IT-Verbundes (Auswahl der Maßnahmen)
Basis-Sicherheitscheck (Soll-Ist-Vergleich)

ca. 80%

ergänz. Sicherheitsanalyse
bei hohem Schutzbedarf

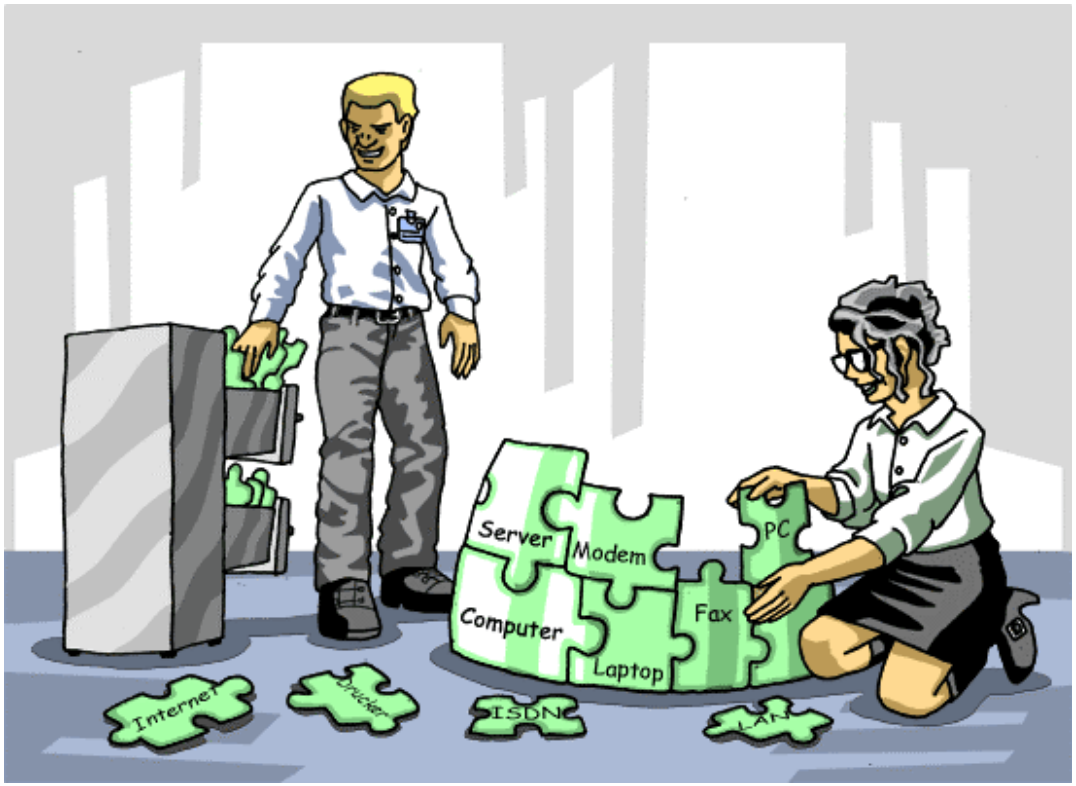
ca. 20%

Konsolidierung der Maßnahmen

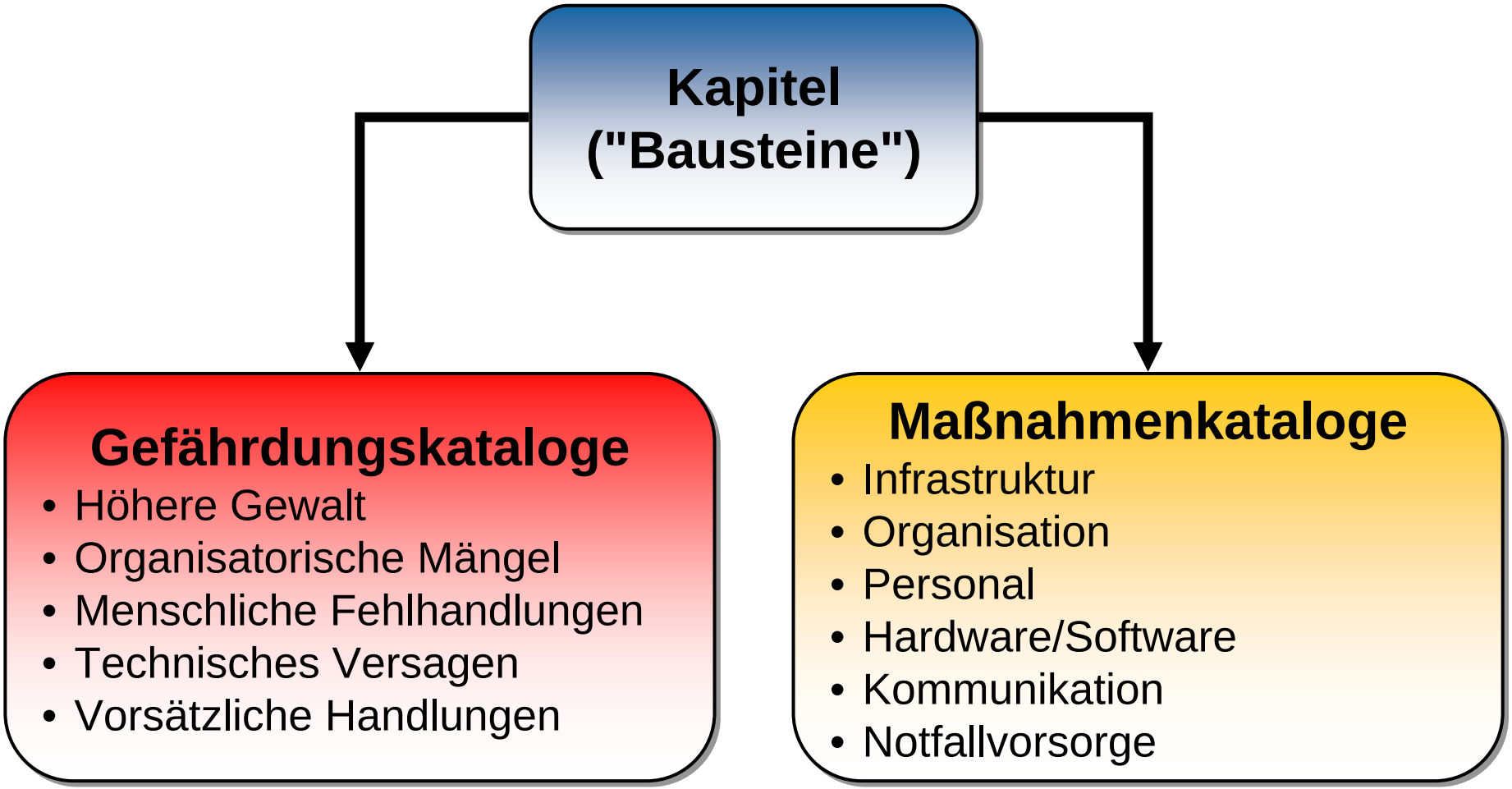
Realisierung der Maßnahmen

Modellierung nach IT-Grundschutz

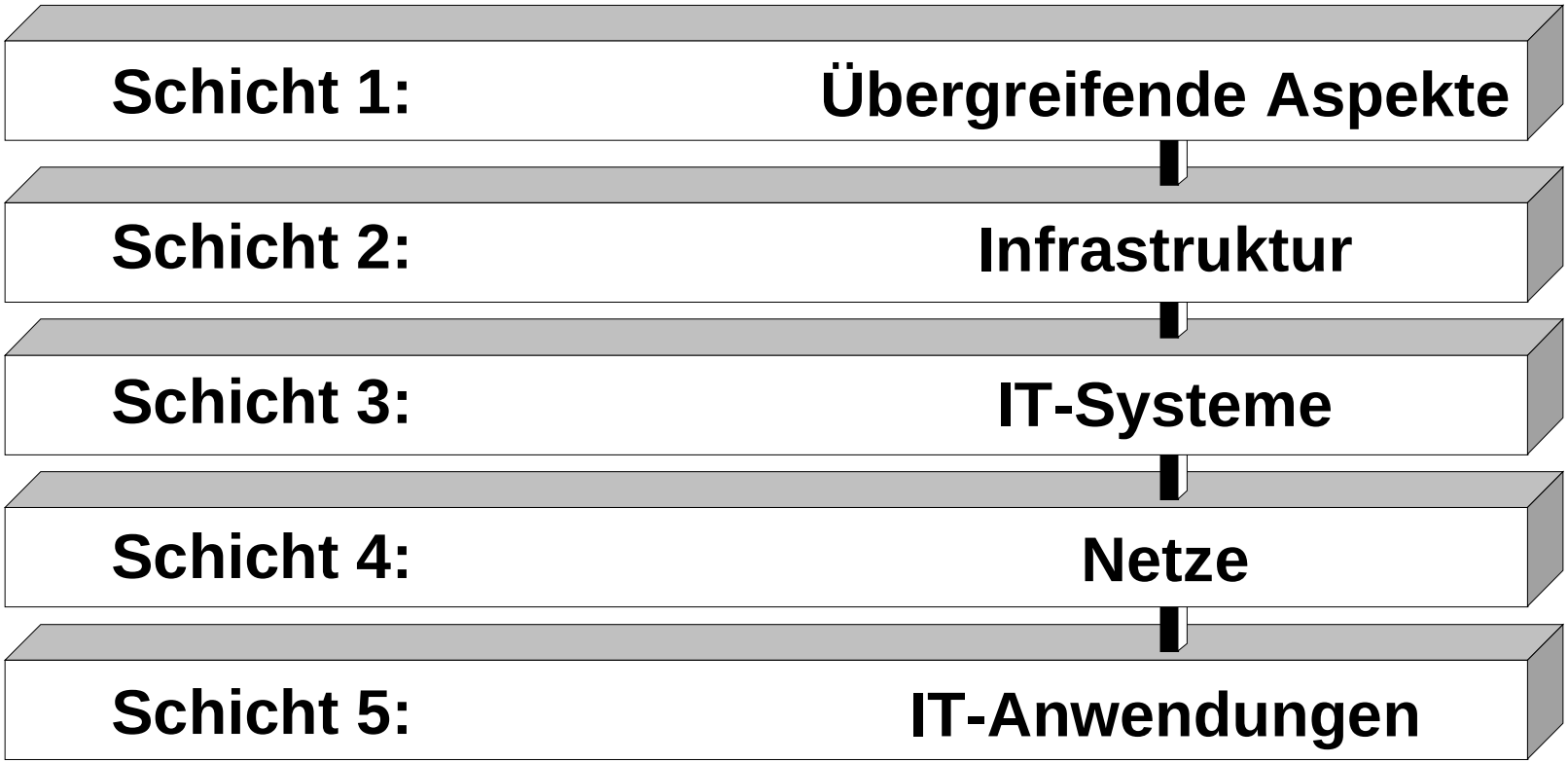
Nachbildung des IT-Verbunds durch Bausteine der IT-Grundschutz-Kataloge



IT-Grundschutz-Bausteine
Struktur

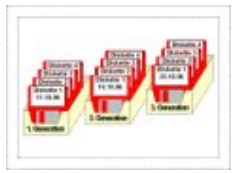


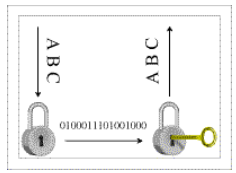
Schichtenmodell



Schicht 1: Übergreifende Aspekte

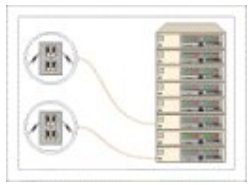
- Modellierung der Aspekte, die dem betrachteten IT-Verbund insgesamt übergeordnet sind
- **Bausteine:**
  - IT-Sicherheitsmanagement
  - Organisation
  - Personal
  - Notfall-Vorsorgekonzept
  - Datensicherungskonzept
  - Computer-Virenschutzkonzept
  - Kryptokonzept
  - Behandlung von Sicherheitsvorfällen
  - Hard- und Software-Management
  - Standardsoftware
  - Outsourcing
  - Archivierung
  - IT-Sicherheitssensibilisierung und -schulung





Schicht 2: Infrastruktur

- Modellierung der für den IT-Verbund relevanten baulichen Gegebenheiten
- **Bausteine:**
  - Gebäude
  - Verkabelung
  - Büroraum
  - Serverraum
  - Datenträgerarchiv
  - Raum für technische Infrastruktur
  - Schutzschrank
  - häuslicher Arbeitsplatz
  - Rechenzentrum
  - Mobiler Arbeitsplatz
  - Besprechungs-, Veranstaltungs- und Schulungsräume

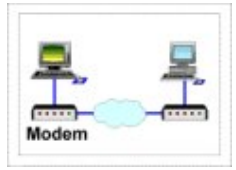


Schicht 3: IT-Systeme

- Modellierung der im IT-Verbund eingesetzten IT-Systeme:
- **Bausteine:**
  - Allgemeiner Server
    - Server unter Unix
    - Server unter Windows NT
    - Server unter Novell Netware 3.x
    - Server unter Novell Netware Version 4.x
    - Server unter Windows 2000
    - S/390- und zSeries-Mainframe
  - TK-Anlage
  - Faxgerät
  - Anrufbeantworter
  - Mobiltelefon
  - Allgemeiner Client
  - Allgemeines nicht vernetztes IT-System
  - Laptop
    - Client unter Unix
    - Client unter Windows NT
    - Client unter Windows 95
    - Client unter Windows 2000
    - Internet-PC
    - Client unter Windows XP
  - Sicherheitsgateway (Firewall)
  - Router und Switches
  - PDA

Schicht 4: Netze

- Modellierung der im IT-Verbund zutreffenden Netz-Aspekte



- **Bausteine:**
- Heterogene Netze
- Netz- und Systemmanagement
- Modem
- Remote Access
- LAN-Anbindung eines IT-Systems über ISDN

Schicht 5: Anwendungen

- Modellierung der im IT-Verbund eingesetzten Anwendungen

- **Bausteine:**
  - Peer-to-Peer-Dienste
  - Datenträgeraustausch
  - E-Mail
  - Webserver
  - Lotus Notes
  - Faxserver
  - Datenbanken
  - Telearbeit
  - Internet Information Server
  - Apache Webserver
  - Exchange/ Outlook 2000
  - Novell eDirectory

Maßnahmenkataloge
Typische Maßnahmen

M1: Infrastruktur
- Schutz vor Einbrechern
- Brandschutzmaßnahmen
- Energieversorgung

M2: Organisation
- Zuständigkeiten
- Dokumentationen
- Arbeitsanweisungen

M3: Personal
- Vertretungsregelungen
- Schulung
- Maßnahmen beim Weggang von Mitarbeitern

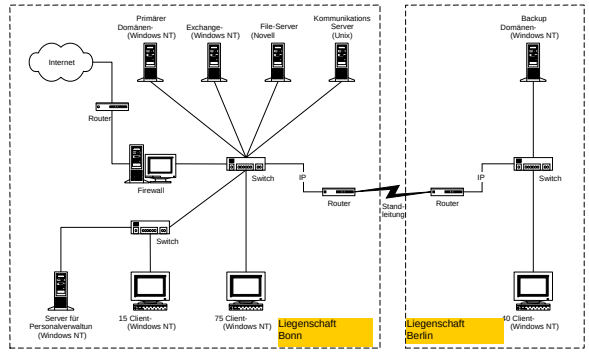
M4: Hardware/Software
- Passwortgebrauch
- Protokollierung
- Vergabe von Berechtigungen

M5: Kommunikation
- Konfiguration
- Datenübertragung
- E-Mail, SSL, Firewall

M6: Notfallvorsorge
- Notfallpläne
- Datensicherung
- Vorsorgemaßnahmen (z. B. redundante Systemauslegung)

Basis-Sicherheitscheck

IT-Grundschutz-Modell



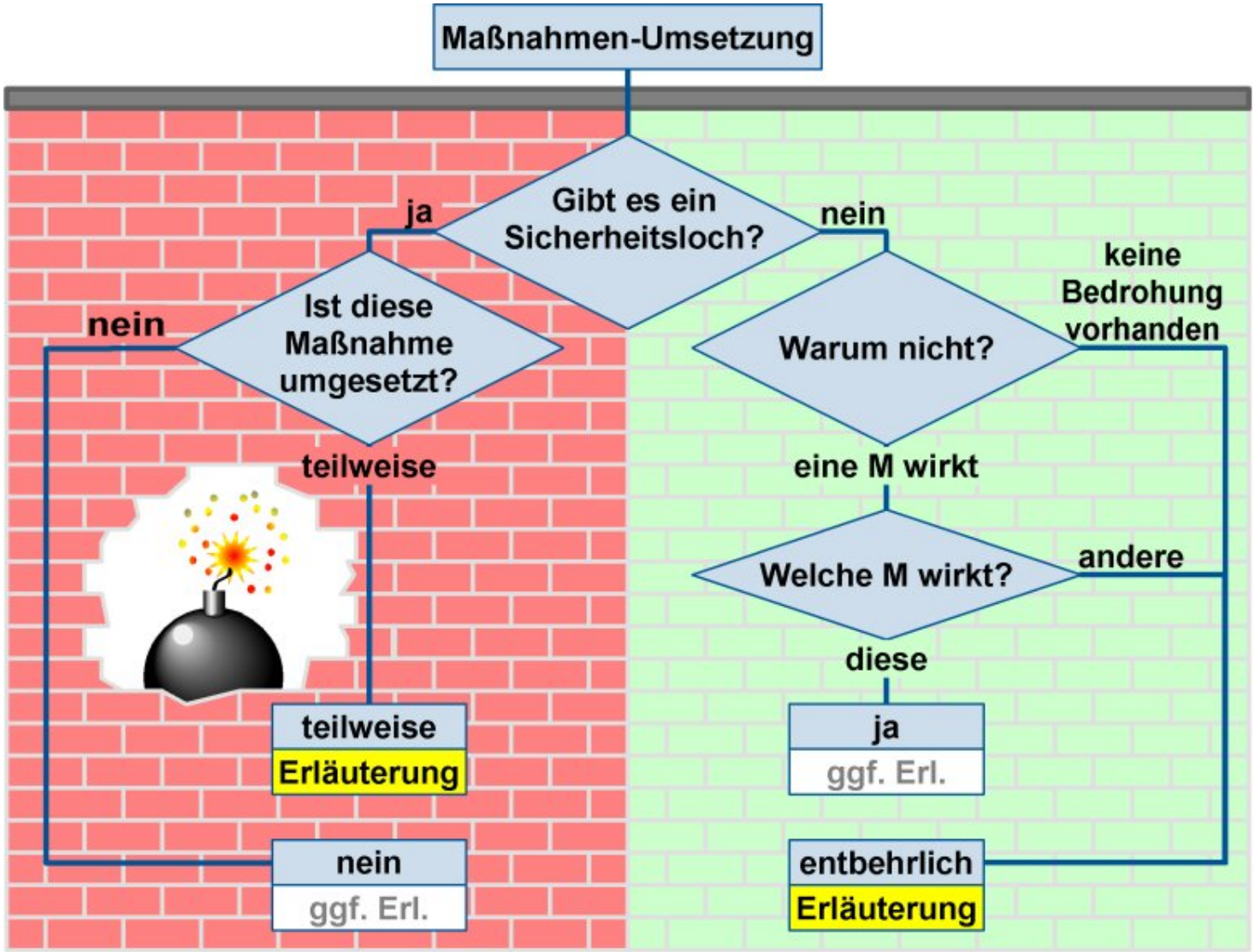
Maßnahmen-empfehlungen

Soll-/Ist-Vergleich

Realisierte Maßnahmen

umzusetzende Maßnahmen

Maßnahmenumsetzung



IT-Grundschutz

BSI-Standards zur IT-Sicherheit

- Bereich IT-Sicherheitsmanagement -

BSI Standard 100-1:
ISMS: Managementsysteme für Informationssicherheit

BSI Standard 100-2:
IT-Grundschutz-Vorgehensweise

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

IT-Grundschutz-Kataloge

Kapitel 1: Einleitung

Kapitel 2: Schichtenmodell und Modellierung

Kapitel 3: Glossar

Kapitel 4: Rollen

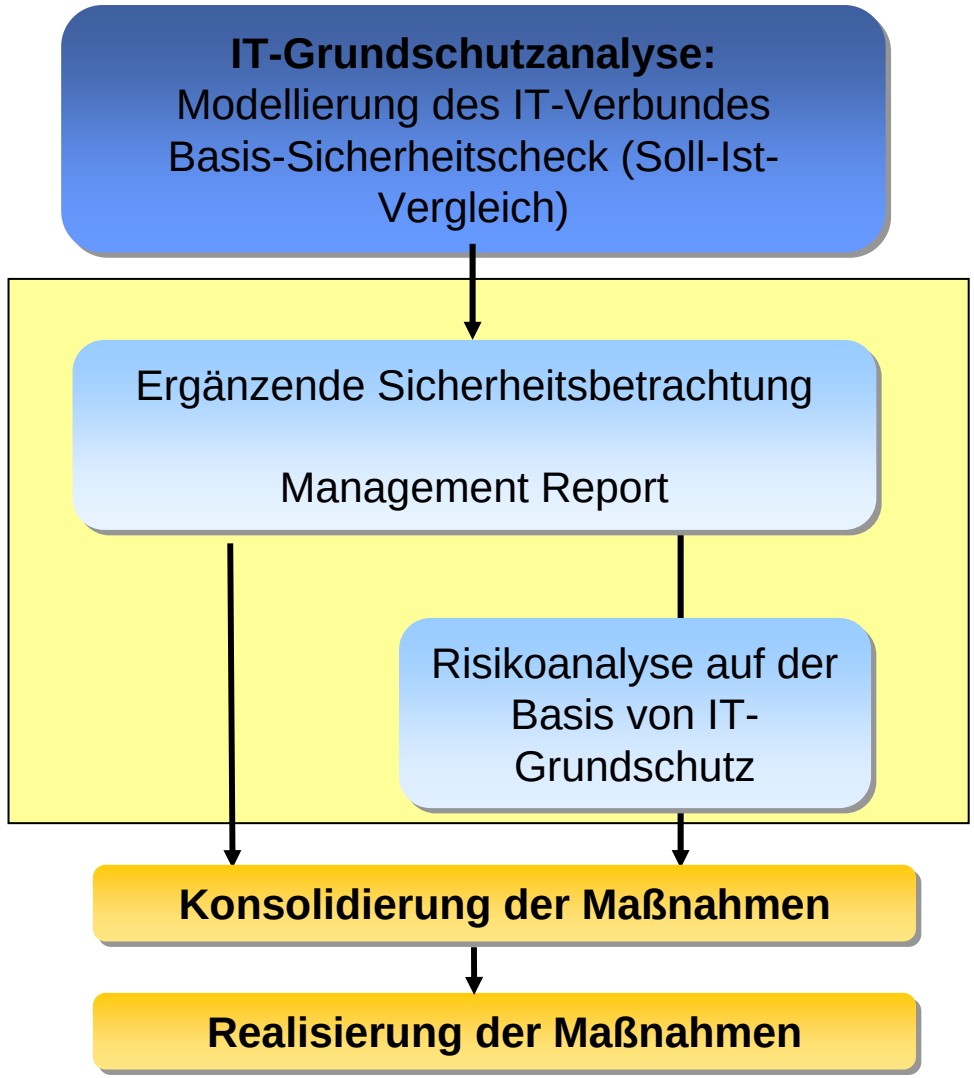
- **Bausteinkataloge**
  - Kapitel B1 "Übergreifende Aspekte"
  - Kapitel B2 "Infrastruktur"
  - Kapitel B3 "IT-Systeme"
  - Kapitel B4 "Netze"
  - Kapitel B5 "IT-Anwendungen"
- **Gefährdungskataloge**
- **Maßnahmenkataloge**

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

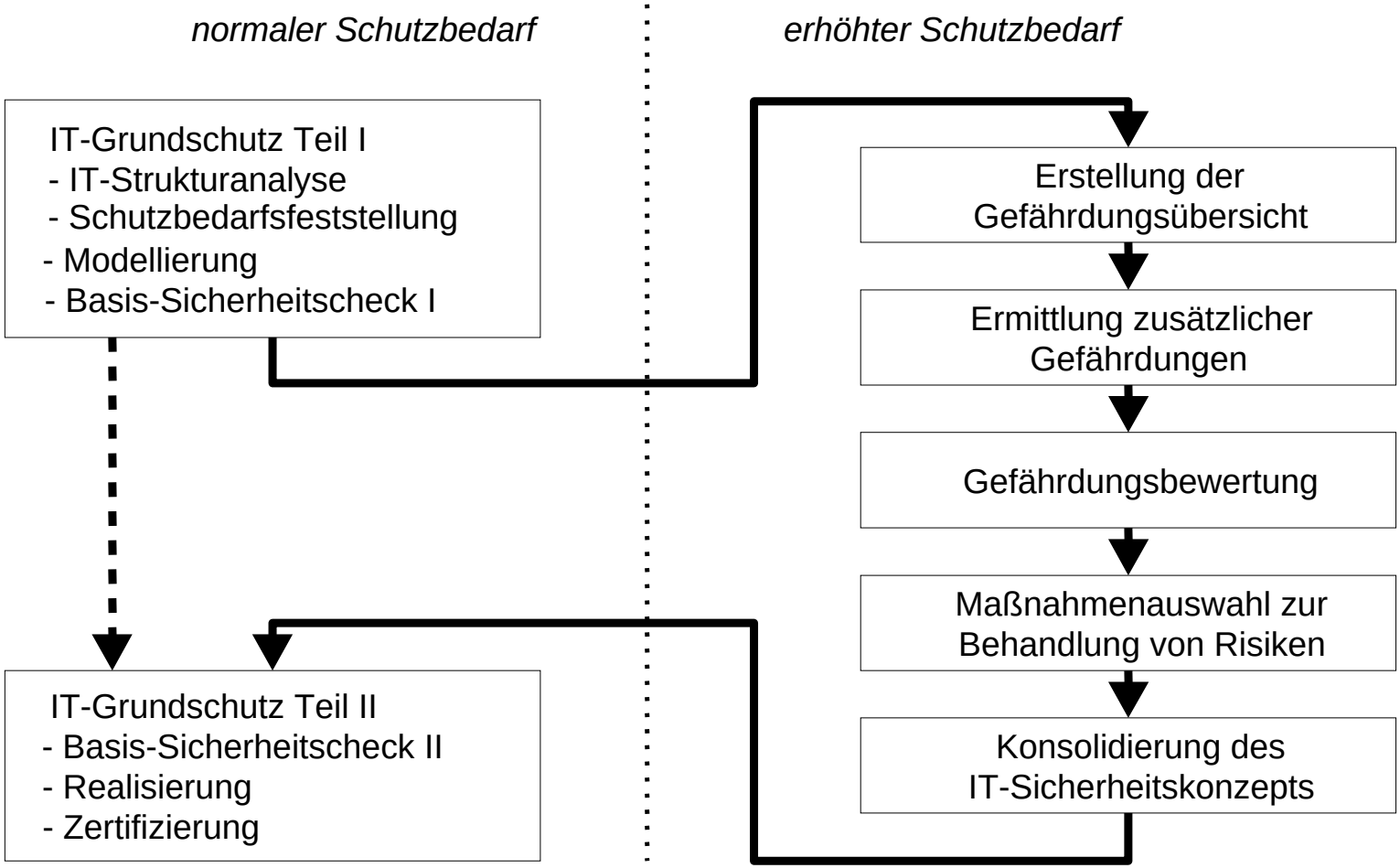
Risikoanalyse auf der Basis von IT-Grundschutz

Eine „Ergänzende Sicherheits-analyse“ ist durchzuführen, wenn:

- hoher oder sehr hoher Schutzbedarf vorliegt,
- zusätzlicher Analysebedarf besteht oder
- für bestimmte Aspekte kein geeigneter Baustein in den IT-Grundschutz-Katalogen existiert.



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



IT-Grundschutz

BSI-Standards zur IT-Sicherheit

- Bereich IT-Sicherheitsmanagement -

BSI Standard 100-1:
ISMS: Managementsysteme für Informationssicherheit

BSI Standard 100-2:
IT-Grundschutz-Vorgehensweise

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

IT-Grundschutz-Kataloge

Kapitel 1: Einleitung

Kapitel 2: Schichtenmodell und Modellierung

Kapitel 3: Glossar

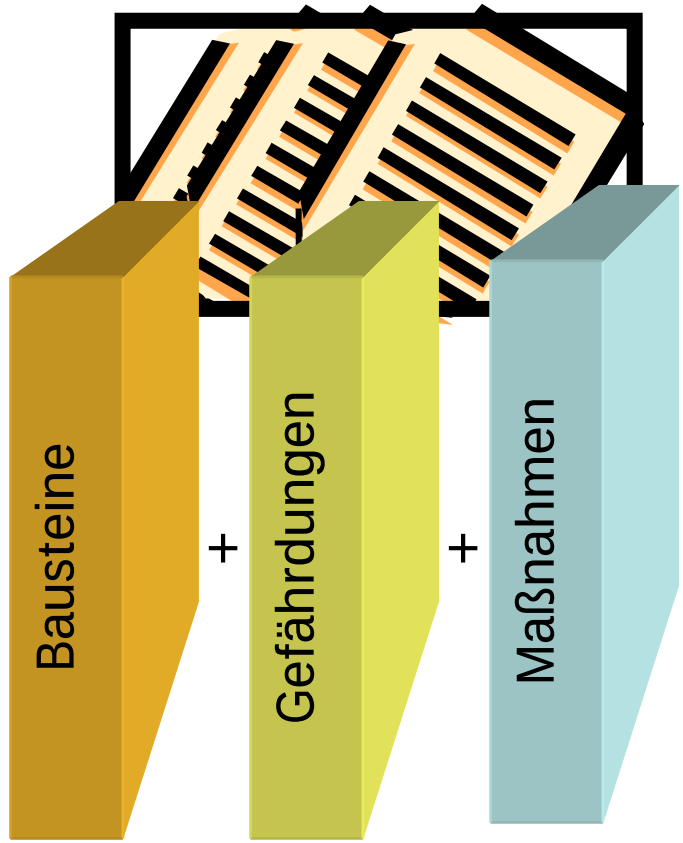
Kapitel 4: Rollen

- **Bausteinkataloge**
  - Kapitel B1 "Übergreifende Aspekte"
  - Kapitel B2 "Infrastruktur"
  - Kapitel B3 "IT-Systeme"
  - Kapitel B4 "Netze"
  - Kapitel B5 "IT-Anwendungen"
- **Gefährdungskataloge**
- **Maßnahmenkataloge**

IT-Grundschutz-Kataloge ab 2005

Kataloge

- Einführung
- Modellierungshinweise
- Baustein-Katalog
- Gefährdungskatalog
- Maßnahmenkatalog



Loseblattsammlung

IT-Grundschutz-Kataloge 2005

7. Ergänzungslieferung

- Schulung und Sensibilisierung zu IT-Sicherheit (Schicht 1)
- Besprechungs- und Schulungsräume (Schicht 2)
- Mobiler Arbeitsplatz
- Windows XP (Schicht 3)

Plus:

Überarbeitungen von

- IT-Sicherheitsmanagement
- Organisation
- Personal
- Allgemeiner Client
- Allgemeiner Server
- Laptop

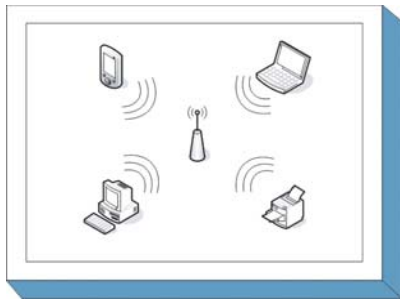
IT-Grundschutz-Kataloge 2006

8. Ergänzungslieferung

- SAP (Schicht 5)
- Speichersysteme (Schicht 3)
- Windows 2003 (Schicht 3)
- WLAN (Schicht 4)
- Voice over IP (Schicht 4)
- zusätzliche Gefährdungen und Maßnahmen

Überarbeitung:

- Datenbanken



Ausblick 2007

folgende Ergänzungslieferungen

- Energieversorgung
- Kommunikationsverbindungen
- System-Entwicklung
- Bluetooth
- Netz-Drucker (Multifunktionsgeräte)
- Löschen und Vernichten von Informationen

Überarbeitung:

- Virenschutz

Dienstleistungen und Produkte rund um den IT-Grundschutz

Sicherheitsbedarf, Anspruch

\- o +

Leitfaden IT-Sicherheit

Webkurs zum Selbststudium

Hilfsmittel & Musterrichtlinien

Software: „GSTOOL“

Beispiele: „GS-Profile“

ISO 27001-Zertifikat

CERT | Viren | Internet | Zerti-fizierung | kritische Infrastruk-turen | Krypto-graphie | Mobilfunk | E-Govern-ment | Biometrie | ...

Wo gibt es das alles?

- auf der BSI-CD-ROM
- als Buch
- auf der BSI-Webseite www.bsi.de

Ihre Mithilfe ist gefragt!

Änderungsvorschläge zum IT-Grundschutz sind uns immer willkommen!

!

!

Welche Bausteine werden Ihrer Meinung nach benötigt?

!

Welche Maßnahmen oder Gefährdungen fehlen?

!

Welche Maßnahmen sind zu verbessern, ergänzen oder reduzieren?

!

IT-Grundschutz-Informationen

IT-Grundschutz-Hotline

Telefon: 0228-9582-5369

E-Mail: gshb@bsi.bund.de

IT-Grundschutz-Tool

Telefon: 0228-9582-5299

E-Mail: gstool@bsi.bund.de

http://www.bsi.bund.de/gshb

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Godesberger Allee 195-198
53175 Bonn

Tel: +49 (0)1888-9582-5369
Fax: +49 (0)1888-9582-5405

gshb@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de