IT-SICHERHEIT UND DATENSCHUTZ

KAPITEL 11 – IT-GRUNDSCHUTZ

buchmann@hft-leipzig.de

LERNZIEL UND AUFBAU DIESES KAPITELS

- Wie kommt man zu einem sinnvollen Sicherheitsniveau?
- IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik
  - BSI-Standard 200-1: Managementsysteme für Informationssicherheit
  - BSI-Standard 200-2: Vorgehensweise nach IT-Grundschutz
  - BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz
- IT-Grundschutz-Kompendium
- IT-Grundschutz-Profile

- Lernziele
  - Sie können erklären, wie man systematisch zu einem definierten Sicherheitsniveau gelangt.
  - Sie sind in der Lage, für ein einfaches Szenario eine Basis-Absicherung nach IT-Grundschutz durchzuführen.

ZIELE DER IT-SICHERHEIT

- „Security triad“
  - **Vertraulichkeit**: Asset ist nur Autorisierten zugänglich
  - **Integrität:** Asset kann nur von Autorisierten modifiziert werden
  - **Verfügbarkeit**: Asset kann von Autorisierten genutzt werden

- ISO 7498-2 fügt hinzu
  - **Authentisierung**: Identität eines Senders wird überwacht
  - **Nichtabstreitbarkeit**: Sender kann nicht abstreiten, das eine Nachricht von ihm kam
- US Department of Defense fügt hinzu
  - **Auditierbarkeit**: Alle Aktionen mit dem Asset sind nachvollziehbar

MOTIVATION EINES GANZHEITLICHEN ANSATZES

SCHUTZ VON INFORMATIONEN

Informationen…

- … sind Werte, die (wie auch die übrigen Geschäftswerte) wertvoll für eine Organisation sind und deshalb in geeigneter Weise geschützt werden müssen.
- … sollten deshalb - unabhängig von ihren Erscheinungsform sowie Art der Nutzung und Speicherung - immer angemessen geschützt werden.

Quelle: ISO/IEC 17799:2005, Einleitung

TYPISCHE PROBLEME IN DER PRAXIS
JEDER TUT, WAS ER WILL

- Konfusion im Notfall
  - Was ist zu tun? Wer hilft?
- lückenhafte Datensicherung
  - Notebooks, Telearbeitsplätze, lokale Datenhaltung
- fehlende Klassifizierung von Informationen
  - Verschlüsselung, Weitergabe und Austausch von Informationen
- gefährliche Internetnutzung
  - Was alle machen, kann doch nicht unsicher sein?
- Disziplinlosigkeit
  - Ignoranz und Arroganz statt geregelter Prozesse
  - Konsequenzen bleiben aus, sind zu hart, sind willkürlich

„SCHIEFE“ RISIKOWAHRNEHMUNG

- Die meisten Datenverluste entstehen durch Irrtum und/oder Nachlässigkeit
- Ergebnisse einer Befragung von 300 Windows Netz- und Systemadministratoren[1)]:
  - 70% der Befragten schätzen die Gefahr durch unbeabsichtigtes Löschen von wichtigen Daten höher ein als durch Virenbefall
  - 90% davon erklären dies durch einfache Anwenderfehler

[1)] Quelle: Broadcasters Res. International Information Security

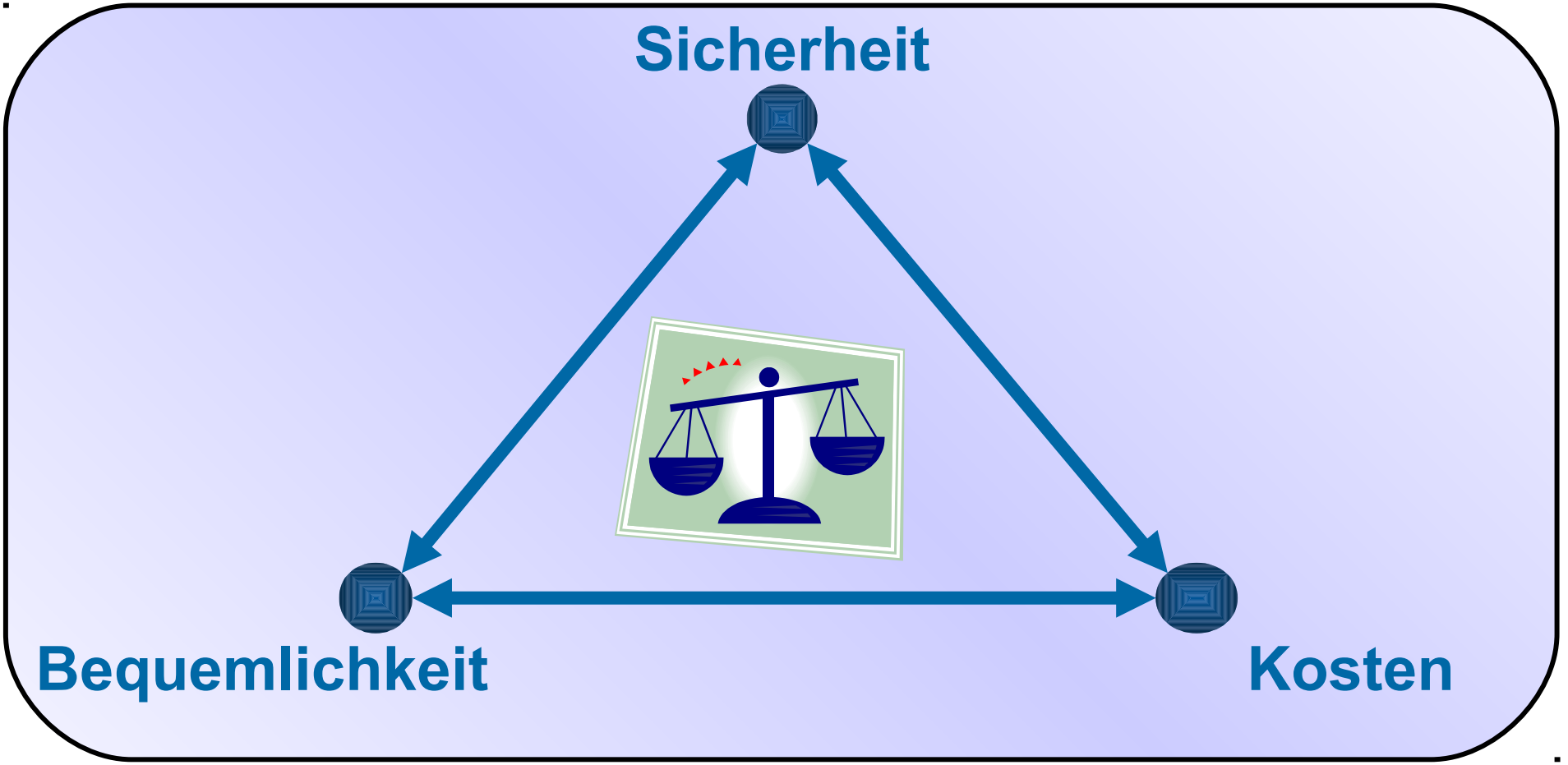
NACHGEWIESENE IT-SICHERHEIT LOHNT SICH …

- Optimierung der internen Prozesse führt zu einem geordneten, effektiven und effizienten IT-Betrieb

  ➔mittelfristige Kosteneinsparungen
- IT-Sicherheitsniveau ist messbar
- Erhöhung der Attraktivität für Kunden und Geschäftspartner mit hohen Sicherheitsanforderungen
- Mitarbeiter und Unternehmensleitung identifizieren sich mit IT-Sicherheitszielen und sind stolz auf das Erreichte
- Versicherungen honorieren zunehmend IT-Sicherheit

SICHER, BEQUEM, BILLIG

„Suchen Sie sich zwei davon aus!“



IT-GRUNDSCHUTZ

ZIEL DES IT-GRUNDSCHUTZES

Durch infrastrukturelle, organisatorische, personelle und technische

Standard-Sicherheitsmaßnahmen

ein

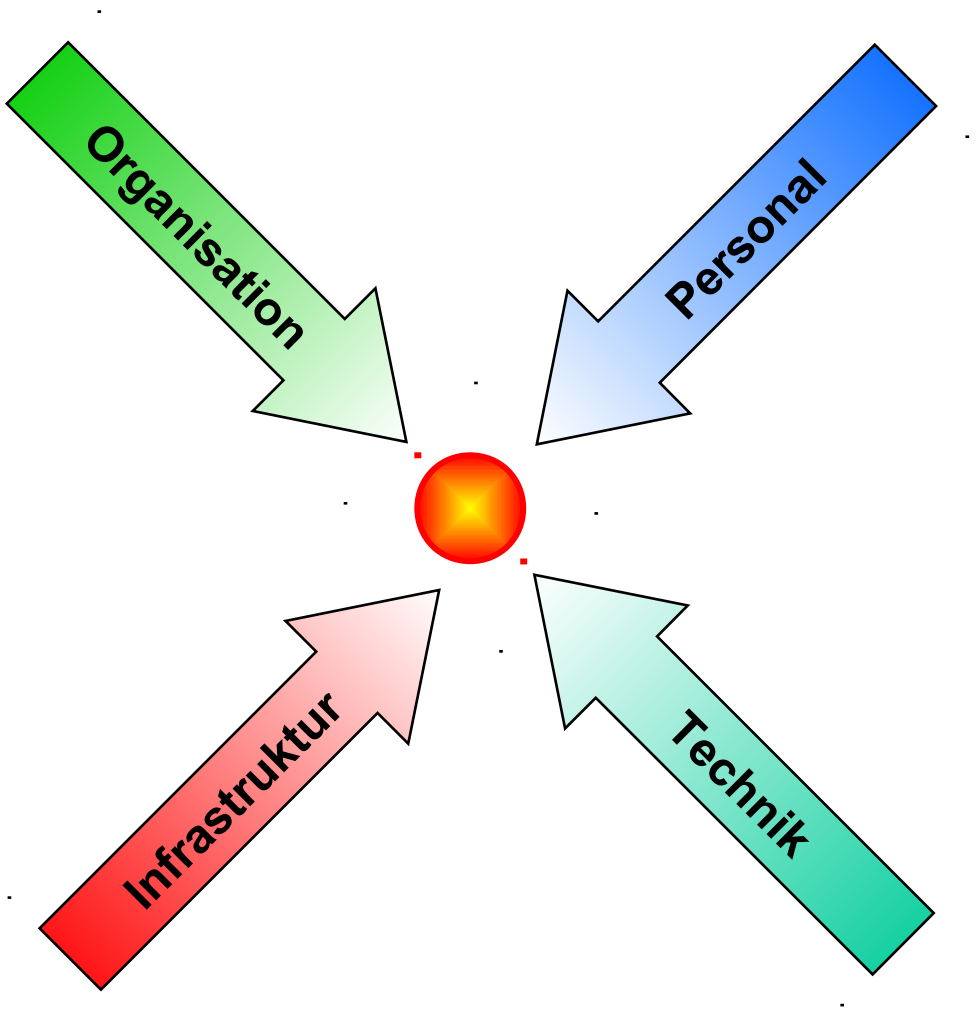
Standard-Sicherheitsniveau

aufbauen, das auch für sensiblere Bereiche

ausbaufähig

ist.

VERSCHIEDENE FACETTEN VON IT-GRUNDSCHUTZ



- Vorgehensweise zur Erstellung von IT-Sicherheitskonzepten (Methode für ein „Information Security Management System“)
- Sammlung von Standard-Sicherheitsmaßnahmen
- ganzheitlicher Ansatz
- Nachschlagewerk
- Referenz und Standard für IT-Sicherheit

IT-GRUNDSCHUTZ - VORTEILE

- arbeitsökonomische Anwendungsweise durch **Soll-Ist-Vergleich**
- kompakte IT-Sicherheitskonzepte durch Verweis auf **Referenzquelle**
- praxiserprobte, meist kostengünstige Maßnahmen mit hoher **Wirksamkeit**
- **Erweiterbarkeit** und **Aktualisierbarkeit**

MODERNISIERUNG IT-GRUNDSCHUTZ (2017)

- Reduktion der Komplexität
  - Module wurden neu aufgestellt, nun nur noch Anforderungen
  - Verweise zur Umsetzung nun separat
- Niedrigere Hürden bei der Umsetzung, insbesondere für kleine/mittlere Unternehmen
  - Drei Schutzlevel (Basis, Standard, Kernabsicherung)
  - Standardisierte Profile für spezifische Branchen/Einsatzgebiete
- Anpassung an neue Technologien/Bedrohungen
  - Industrial Control Systems, Cloud Computing, Virtualisierung, Internet of Things
  - Bausteine für Incident Detection/Response

BSI-Standards

IT-Grundschutz Kompendium

BSI STANDARDS FÜR IT-SECURITY

BSI-Standard 200-1:
Information Security Management Systems

BSI-Standard 200-2:
IT-Grundschutz Methodik

BSI-Standard 200-3:
Risikoanalyse basierend auf dem IT-Grundschutz

zusätzlich:

- BSI-Standard 100-4 (Business Continuity Management)

- Anleitung zur Umsetzung des Schutzlevels „Basis“

1. INFORMATIONSSICHERHEITSMANAGEMENTSYSTEM

BSI-STANDARD 200-1
- BSI-STANDARD ZUR IT SICHERHEIT -

BSI-Standards zur IT-Sicherheit

- Bereich IT-Sicherheitsmanagement -

BSI Standard 200-1:
ISMS: Managementsysteme für Informationssicherheit

BSI Standard 200-2:
IT-Grundschutz-Vorgehensweise

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

IT-Grundschutz-Kompendium

Kapitel 1: Einleitung

Kapitel 2: Schichtenmodell und Modellierung

Elementargefährdungen

Grundschutz-Schichten

Prozessmodule:

- ISMS – Sicherheitsmanagement
- ORP – Organisation und Personal
- CON – Konzepte und Vorgehensweisen
- OPS – IT-Betrieb
- DER – Detektion und Reaktion

IT System-Module:

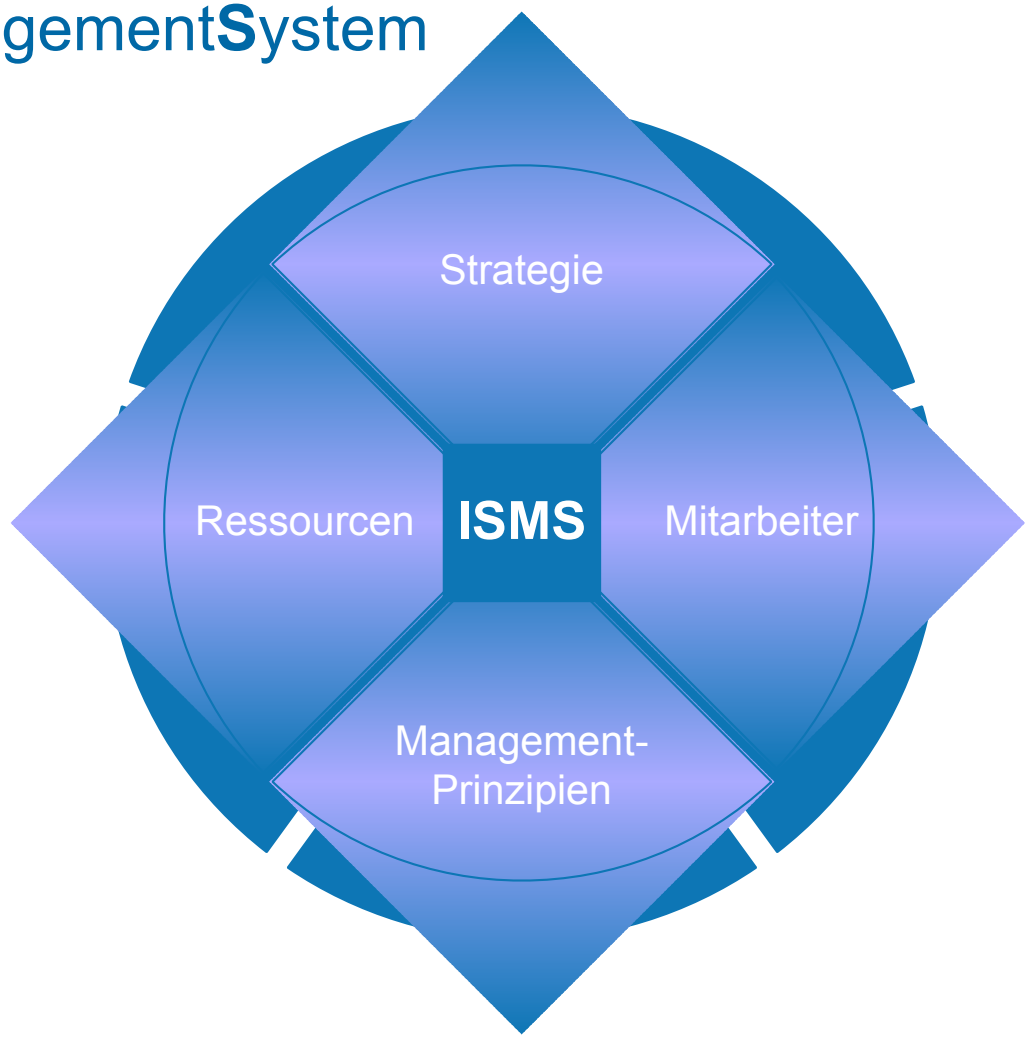
- IND – Industrielle IT
- APP – Anwendungen
- SYS – IT-Systems
- NET – Netze und Kommunikation
- INF – Infrastruktur

BSI-STANDARD 200-1

ISMS

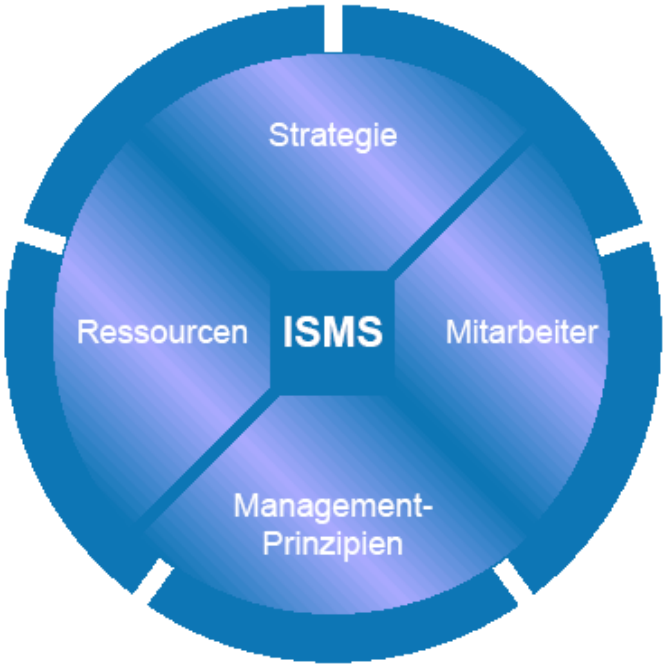
ISMS: **I**nformations**S**icherheits**M**anagement**S**ystem

- Zielgruppe: Management
- Allgemeine Anforderungen an ein ISMS
- Kompatibel mit ISO/EIC 27001
- Didaktische Aufbereitung



BSI-STANDARD 200-1
KOMPONENTEN EINES ISMS

- Komponenten:
  - Management-Prinzipien
  - Ressourcen
  - Mitarbeiter
  - IT-Sicherheitsprozess
    - IT-Sicherheitsleitlinie
      (einschl. IT-Sicherheitsziele und -strategie)
    - IT-Sicherheitskonzept
    - IT-Sicherheitsorganisation



BEISPIEL: SICHERHEITSLEITLINIE ZUR IT-NUTZUNG

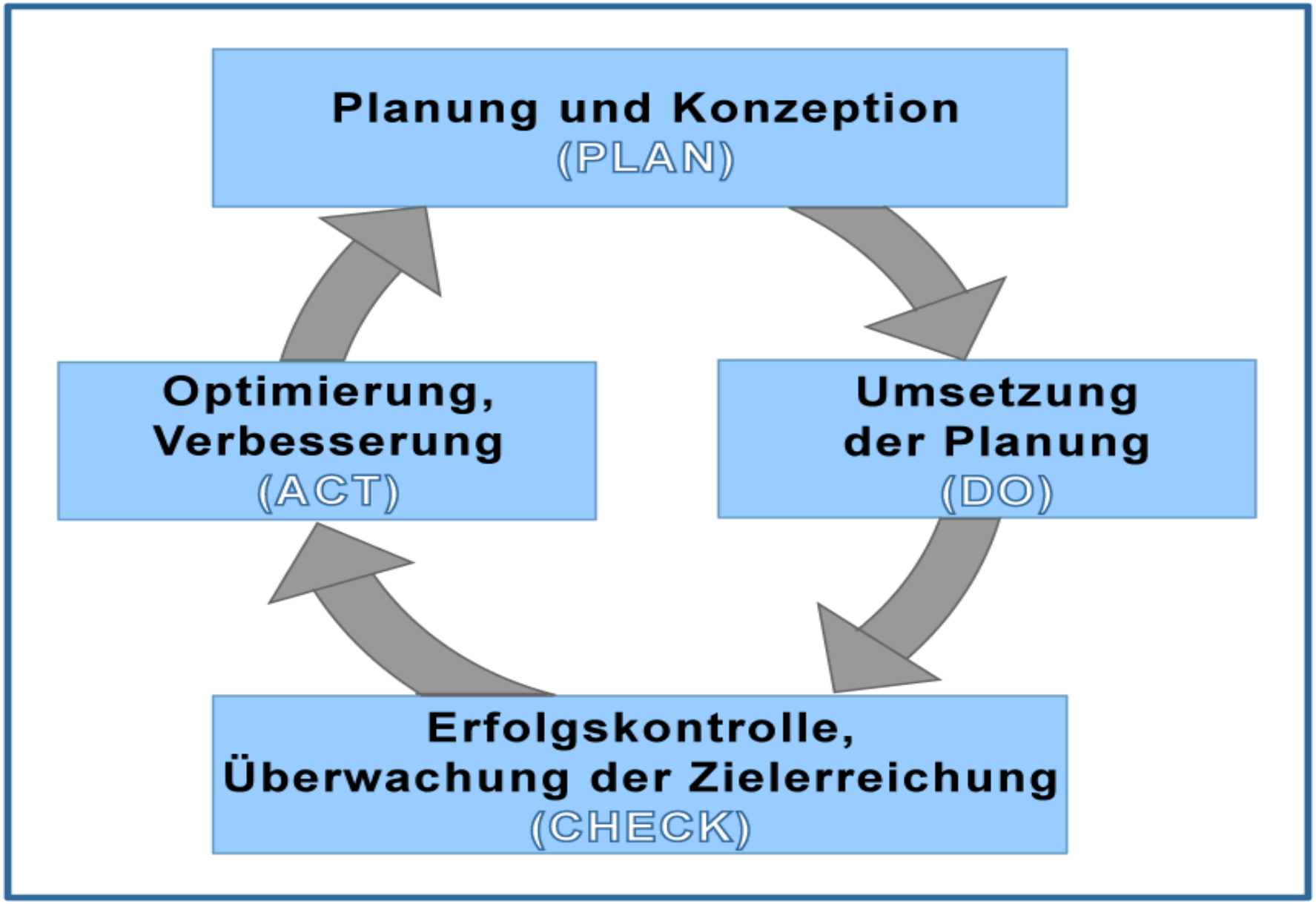
- Umgang mit schützenswerten Informationen (Informationseigentümer, Klassifizierung von Informationen nach Schutzbedürftigkeit)
- Relevante Gesetze und Vorgaben
- Kurzbeschreibung wichtiger Rollen (z. B. IT-Sicherheitsbeauftragter, Administrator, IT-Benutzer)
- Ausbildung des Personals
- Pflicht zur Einrichtung von Vertretungsregelungen
- Anforderungen an die Verwaltung von IT (Beschaffung, Einsatz, Wartung, Revision und Entsorgung)
- Grundlegende Sicherheitsmaßnahmen (Zutritt zu Räumen und Zugang zu IT-Systemen, Verschlüsselung, Virenschutz, Datensicherung, Notfallvorsorge)
- Regelungen für spezifische IT-Dienste (Datenübertragung, Internetnutzung)

BSI-STANDARD 200-1
INHALTE

1. Einleitung
2. Einführung in die Informationssicherheit
3. ISMS-Definition und Prozessbeschreibung
4. Management-Prinzipien
5. Ressourcen für Informationssicherheit
6. Einbindung der Mitarbeiter in den Sicherheitsprozess
7. Der Sicherheitsprozess
8. Sicherheitskonzept
9. Zertifizierung der ISMS
10. Das ISMS auf Basis von BSI IT-Grundschutz

BSI-STANDARD 200-1

LEBENSZYKLUS



BSI-STANDARD 200-1

LEBENSZYKLUS (FORTS.)

P

Planung und Konzeption

- Auswahl einer Methode zur Risikobewertung
- Klassifizierung von Risiken
- Risikobewertung
- Entwicklung einer Strategie zum Umgang mit Risiken
- Auswahl von Schutzmaßnahmen

D

Umsetzung der Planung

- Implementierungsplan für das Sicherheitskonzept
- Umsetzung der Schutzmaßnahmen
- Überwachung und Kontrolle der Umsetzung
- Notfallvorsorge und Behandlung von Sicherheitsvorfällen
- Schulung und Sensibilisierung

C

Erfolgskontrolle und Überwachung der Zielerreichung

- Identifikation von Sicherheitsvorfällen während des Betriebs
- Überwachung der Einhaltung von Vorschriften
- Überwachung der Eignung und Wirksamkeit der Schutzmaßnahmen
- Überwachung der Leistung der Schutzmaßnahmen
- Managementberichte

A

Optimierung und Verbesserung

- Beheben von identifizierten Mängeln
- Verbesserung der Schutzmaßnahmen

2. IT-GRUNDSCHUTZ VORGEHENSWEISE

BSI-STANDARD 200-1
- BSI-STANDARD ZUR IT SICHERHEIT -

BSI-Standards zur IT-Sicherheit

- Bereich IT-Sicherheitsmanagement -

BSI Standard 200-1:
ISMS: Managementsysteme für Informationssicherheit

BSI Standard 200-2:
IT-Grundschutz-Vorgehensweise

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

IT-Grundschutz-Kompendium

Kapitel 1: Einleitung

Kapitel 2: Schichtenmodell und Modellierung

Elementargefährdungen

Grundschutz-Schichten

Prozessmodule:

- ISMS – Sicherheitsmanagement
- ORP – Organisation und Personal
- CON – Konzepte und Vorgehensweisen
- OPS – IT-Betrieb
- DER – Detektion und Reaktion

IT System-Module:

- IND – Industrielle IT
- APP – Anwendungen
- SYS – IT-Systems
- NET – Netze und Kommunikation
- INF – Infrastruktur

BSI-STANDARD 200-2
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 Schutzmaßnahmen
  - IT-Sicherheit aufrecht erhalten und verbessern

BEISPIEL: DATENSICHERUNGSKONZEPT

- Wo werden die Daten gespeichert?
- Welche Daten werden gesichert?
- Wer ist für die Datensicherungen zuständig?
- Wie wird gesichert? (Technik, Sicherungsmedien, Intervalle),
- Wie lange werden Datensicherungen aufbewahrt?
- Wie wird mit Notebooks verfahren, die nicht ständig am Netz angeschlossen sind?
- Wie wird überprüft, ob die Datensicherungen tatsächlich zuverlässig funktioniert haben?
- Wie können die Daten im Schadensfall rekonstruiert werden?

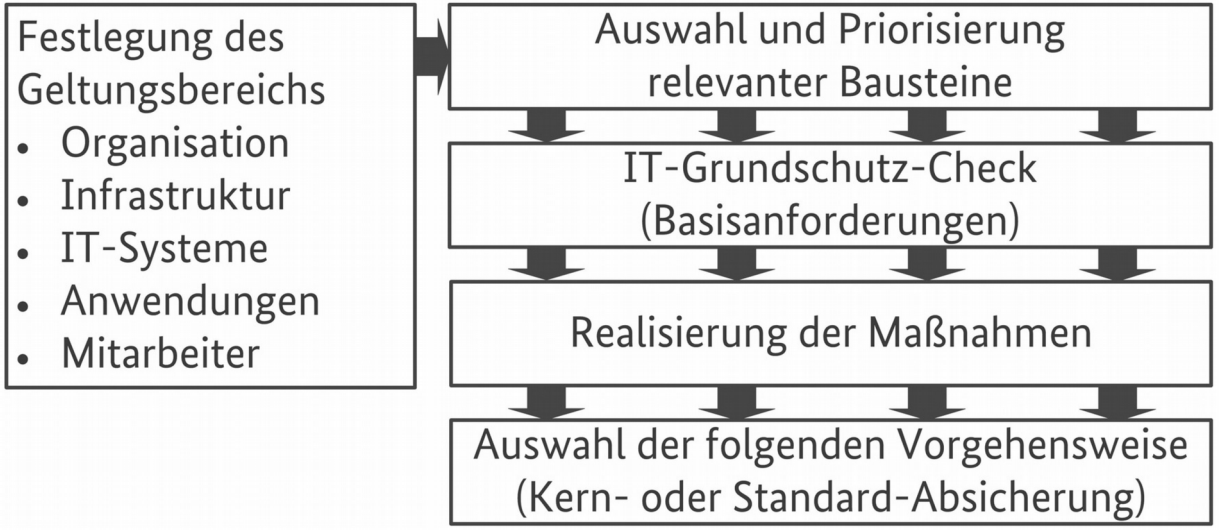
BSI-STANDARD 200-2
WESENTLICHE MERKMALE

- Interpretation der Anforderungen aus ISO 13335, 17799 und 27001
- Hinweise zur Umsetzung mit Hintergrund Know-how und Beispielen
- Verweis auf IT-Grundschutz-Kompendium zur detaillierten (auch technischen) Umsetzung
- Erprobte und effiziente Möglichkeit, die Anforderungen der ISO-Standards zu erfüllen

BSI-STANDARD 200-2
INHALTE

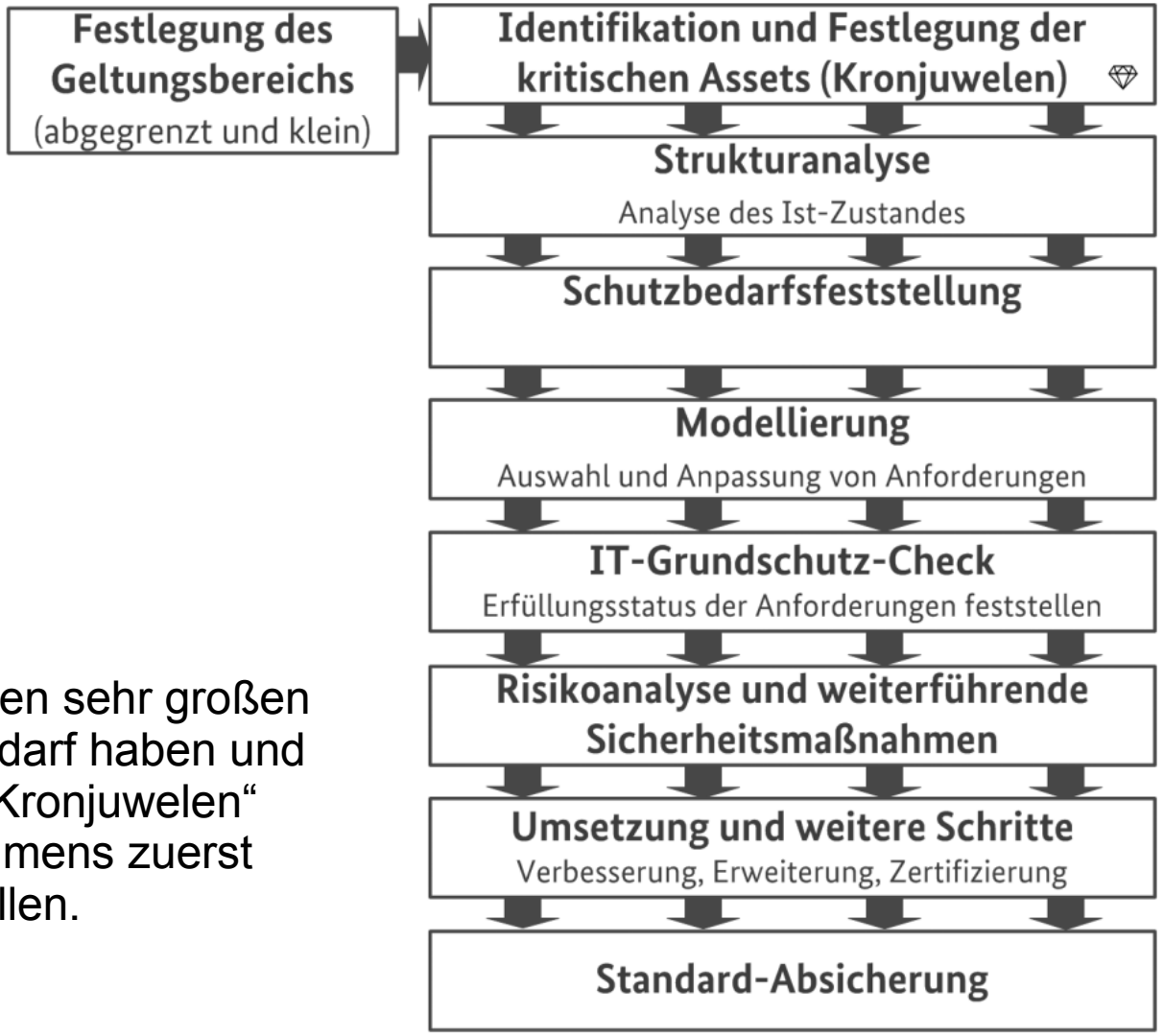
1. Einleitung
2. Informationssicherheitsmanagement mit IT-Grundschutz
3. Initiierung des IT-Sicherheitsprozesses
4. Organisation des IT-Sicherheitsprozesses
5. Dokumentation des IT-Sicherheitsprozesses
6. Erstellung einer Sicherheitskonzeption nach der Vorgehensweise „Basisabsicherung“, „Kernabsicherung“, „Standardabsicherung“
9. Umsetzung des IT-Sicherheitsprozesses
10. Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit
11. Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz

BSI-STANDARD 200-2
BASIS-ABSICHERUNG



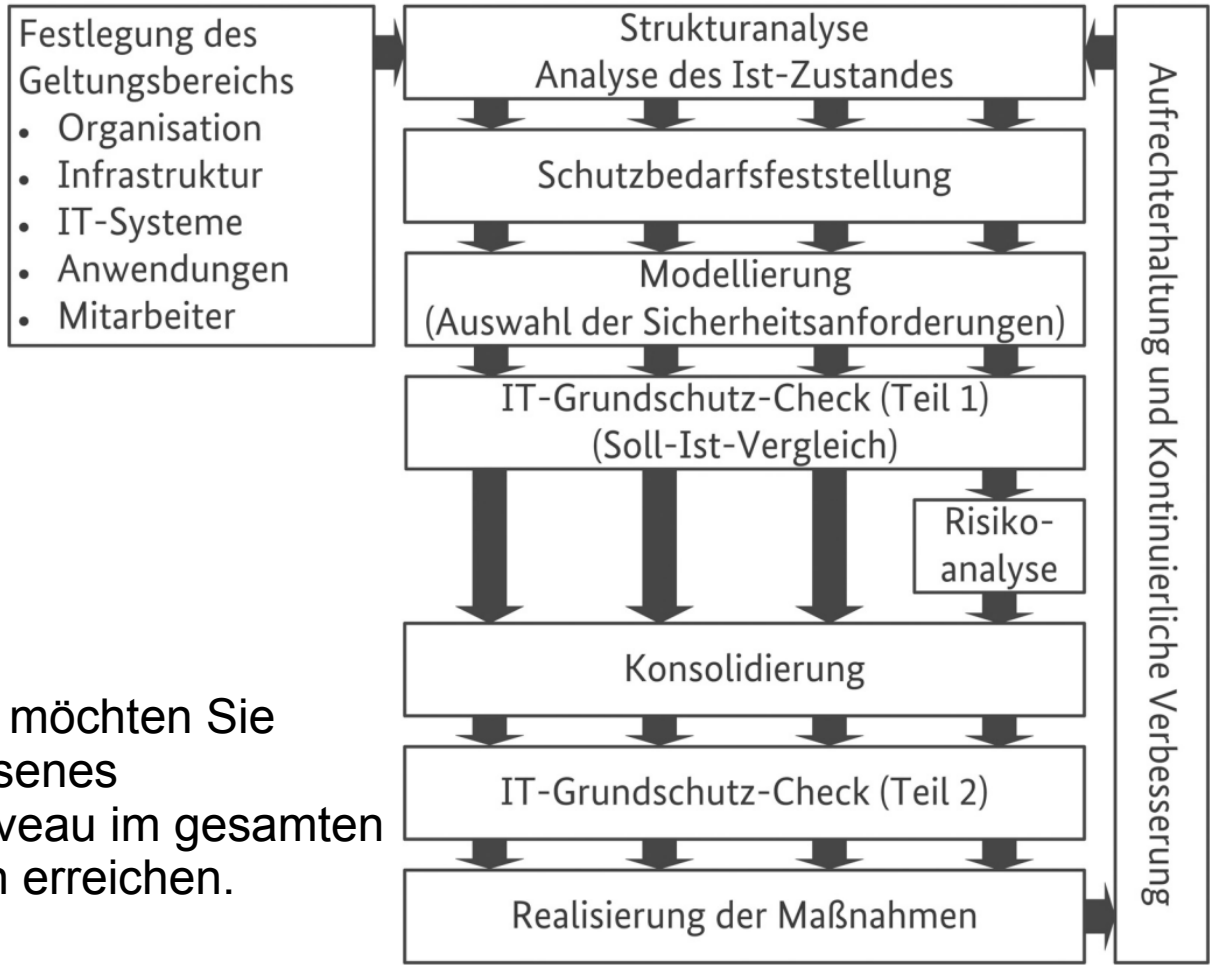
Das müssen Sie auf jeden Fall tun.

BSI-STANDARD 200-2
KERN-ABSICHERUNG



Wenn Sie einen sehr großen Handlungsbedarf haben und deshalb die „Kronjuwelen“ des Unternehmens zuerst absichern wollen.

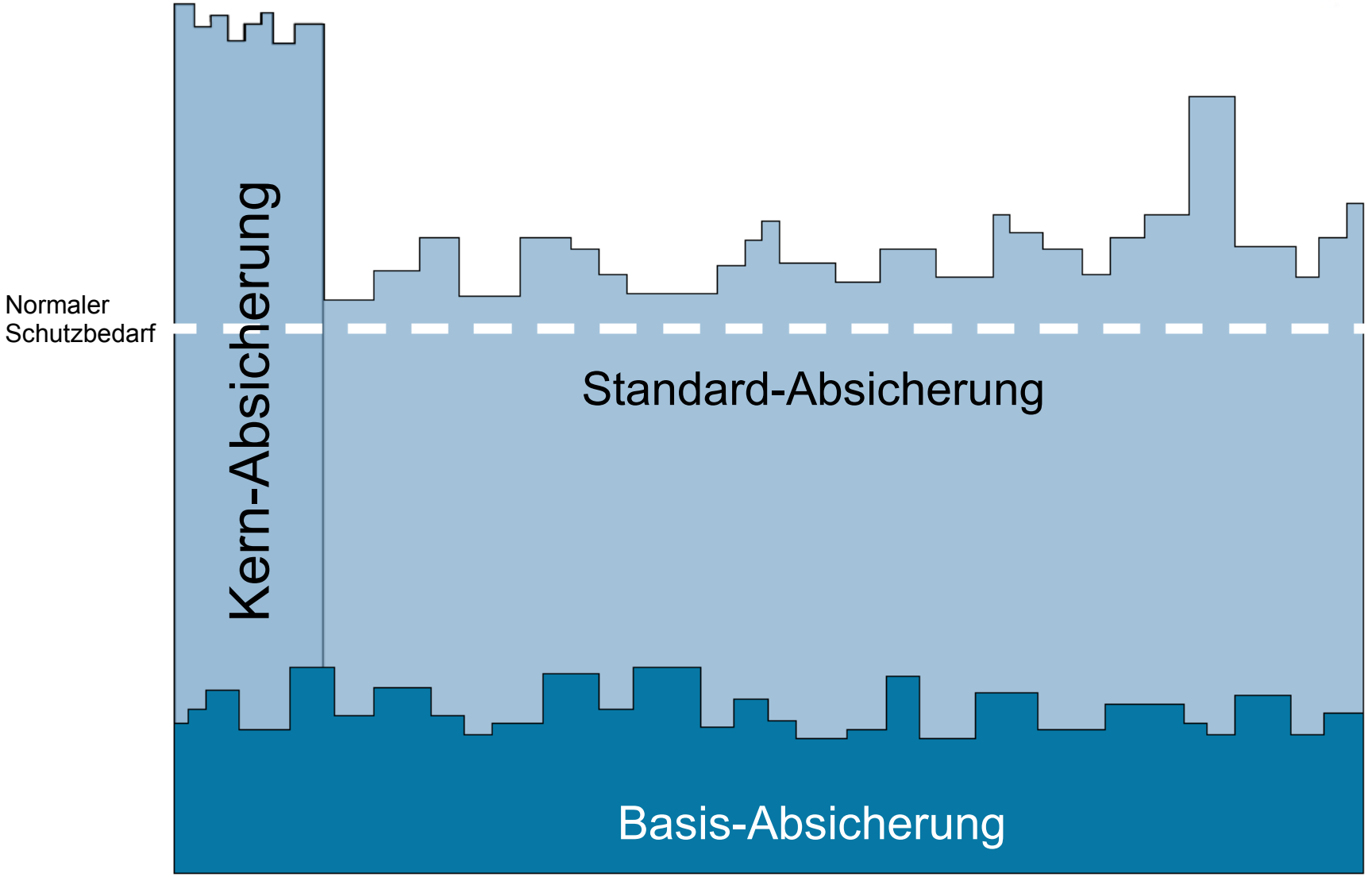
BSI-STANDARD 200-2
STANDARD-ABSICHERUNG



Diesen Level möchten Sie als angemessenes Sicherheitsniveau im gesamten Unternehmen erreichen.

BSI-STANDARD 200-2

SICHERHEITSNIVEAUS



BSI-STANDARD 200-2
STRUKTURANALYSE

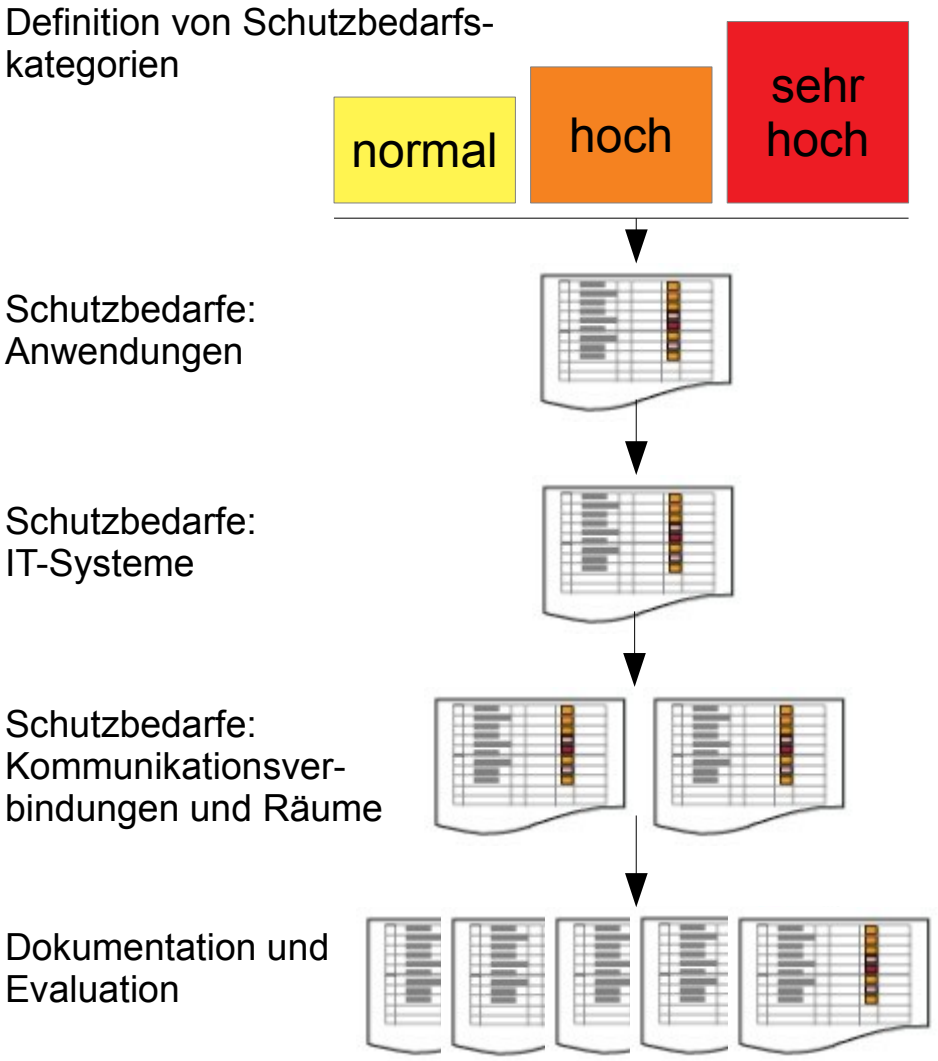
- Der Informationsverbund...

...ist die Menge an Assets aus den Bereichen **Infrastruktur**, **Organisation, Personal** und **Technik**, die nötig sind um eine bestimmte Geschäftsaufgabe zu erfüllen.

...muss eine sinnvolle Größe haben. Für ein angemessenes Sicherheitsniveau ist es angeraten, ein Institution vollständig abzusichern.

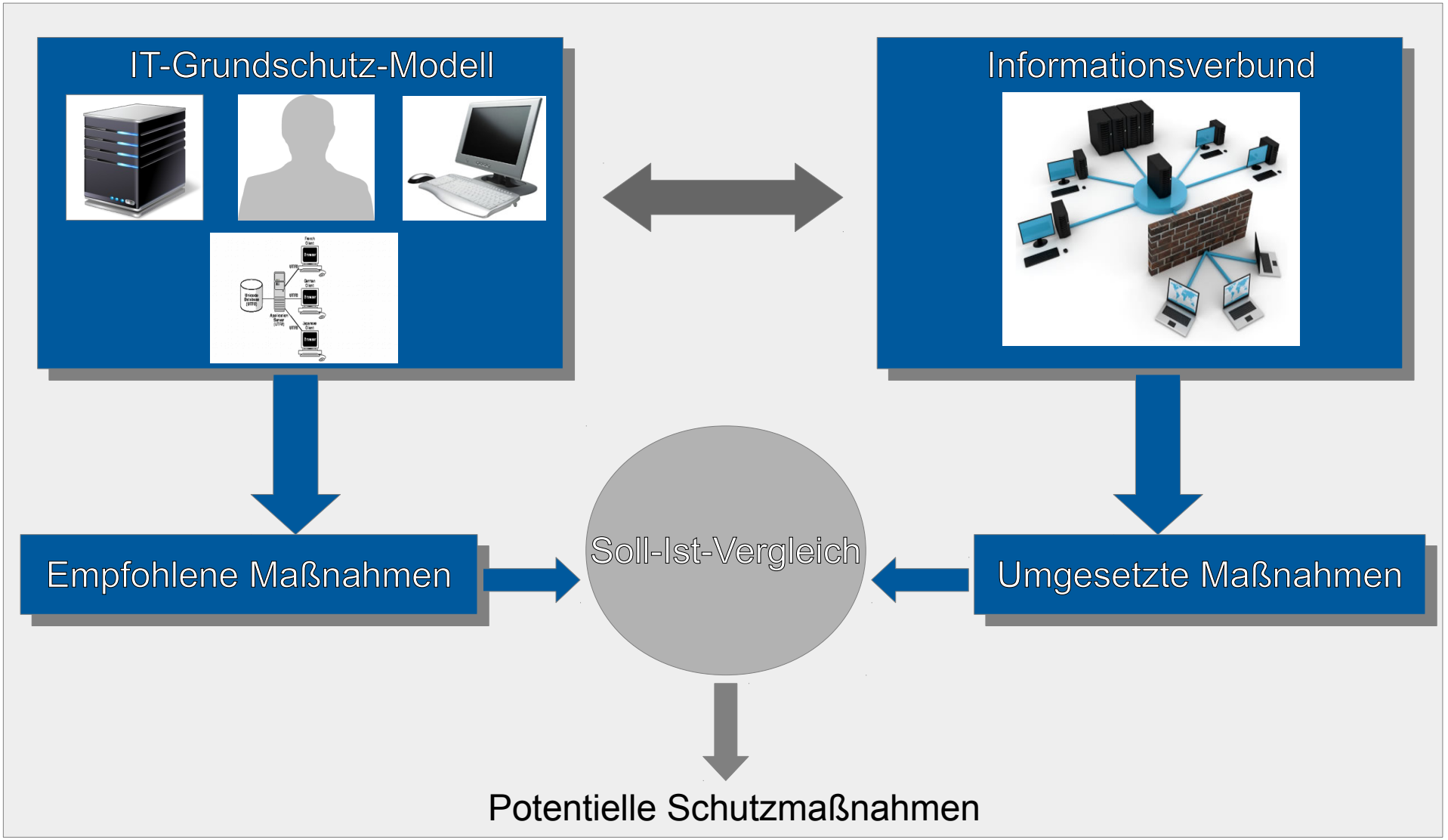
...sollte in sinnvoll handhabbare Abschnitte untergliedert werden, z.B. in Organisationseinheiten oder Geschäftsbereiche

BSI-STANDARD 200-2
SCHUTZBEDARFSFESTSTELLUNG

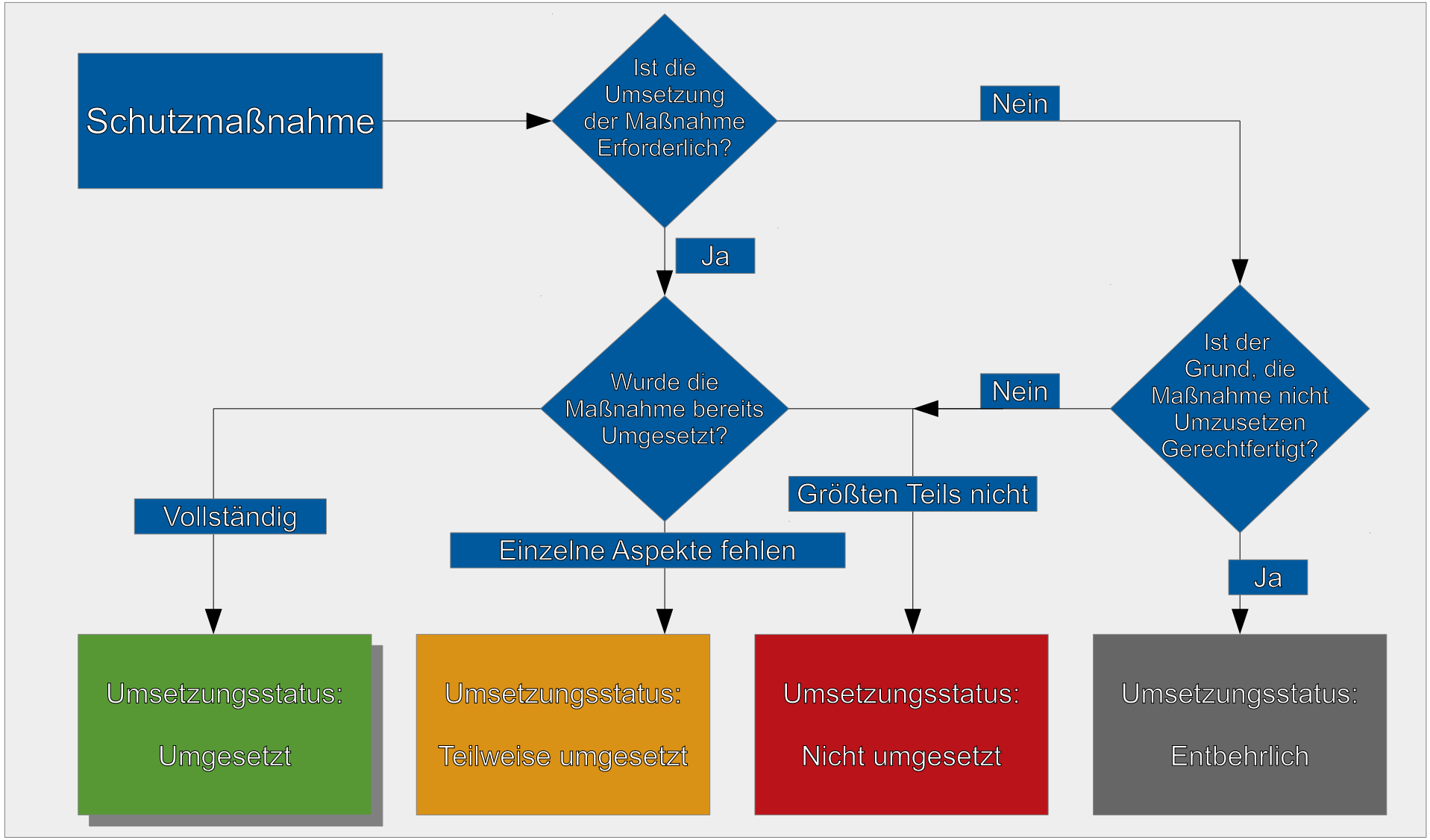


- Definiere Schutzbedarfskategorien "normal", "hoch" and "sehr hoch"
- Bestimme die Schutzbedarfe der Anwendungen mit diesen Kategorien
- Leite die Schutzbedarfe der IT-Systeme von den Schutzbedarfen der Anwendungen ab, die darauf laufen.
- Bestimme daraus die Schutzbedarfe der Kommunikationsverbindungen und der Infrastruktur, die von den IT-Systemen genutzt werden
- Dokumentiere und evaluiere die so erhaltenen Schutzbedarfe

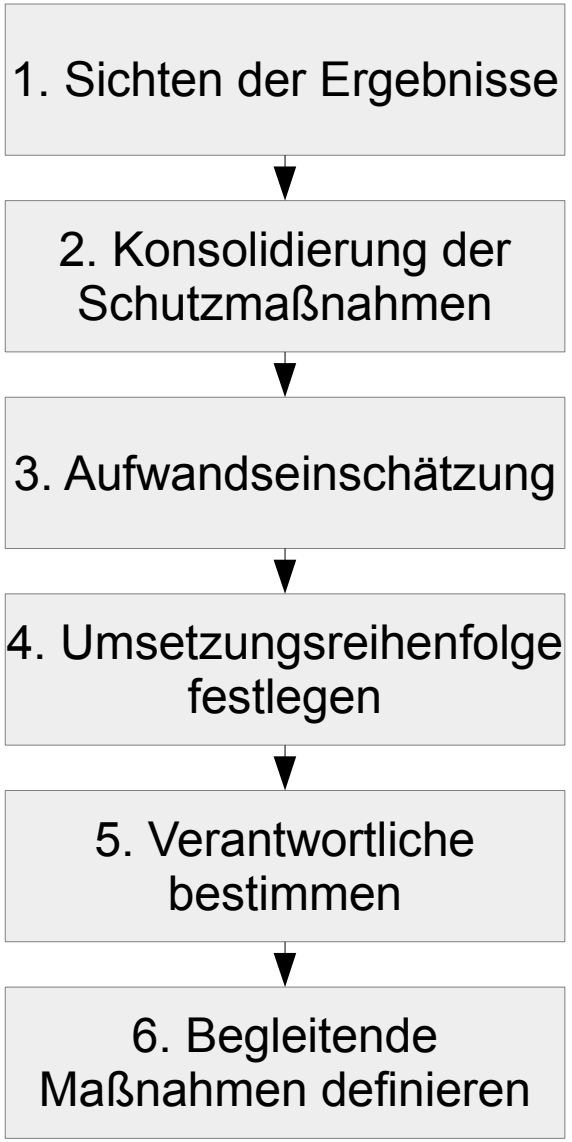
BSI-STANDARD 200-2
IT-GRUNDSCHUTZ-CHECK



BSI-STANDARD 200-2
IT-GRUNDSCHUTZ-CHECK (FORTS.)



BSI-STANDARD 200-2
IMPLEMENTIERUNG DER SCHUTZMAßNAHMEN



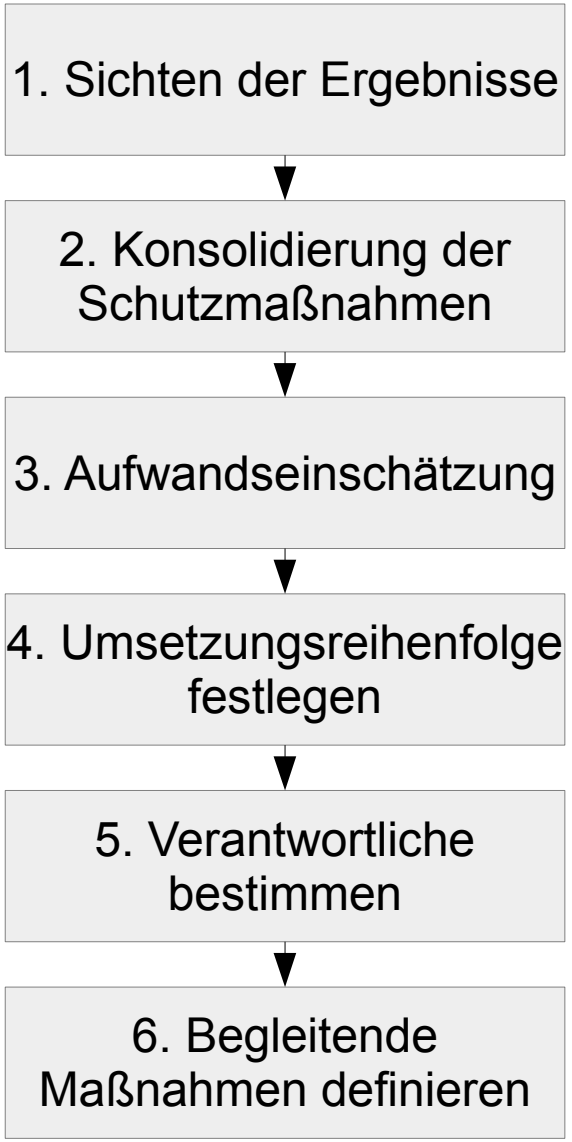
(1) Prüfen der Ergebnisse des IT-Grundschutz-Checks. Zusammenfassung der bisher nicht vollständig umgesetzten Schutzmaßnahmen in tabellarischer Form.

(2) Prüfen, welche der identifizierten Schutzmaßnahmen tatsächlich benötigt werden.
- Identifizierung von Schutzmaßnahmen, deren Ziel durch andere Schutzmaßnahmen bereits erreicht wird.
- Identifizierung von Schutzmaßnahmen, die im Konflikt mit anderen Schutzmaßnahmen stehen.
- Identifizierung von Schutzmaßnahmen, die angepasst werden müssen.

Ziel: Minimierung des Personal- und Ressourcenbedarfs

Ergebnis: präziser und individueller Maßnahmenkatalog

BSI-STANDARD 200-2
IMPLEMENTIERUNG DER SCHUTZMAßNAHMEN (FORTS.)



(3) Abschätzung des finanziellen und personellen Aufwands während der Umsetzung der Schutzmaßnahme. Unterscheidung zwischen einmaligem und wiederkehrendem Aufwand.

(4) Festlegung einer sinnvollen Umsetzungsreihenfolge. Fokussierung auf Assets mit hohem Schutzbedarf und Bereiche, in denen viele Schutzmaßnahmen fehlen.

(5) Festlegung eines Zeitplans zur Umsetzung der Schutzmaßnahmen, sowie Bestimmung des Verantwortlichen für deren Initiierung, Umsetzung und Überwachung.

(6) Die praktische Wirksamkeit der Sicherheitsmaßnahmen hängt von der Akzeptanz und dem Verhalten der Mitarbeiter ab. Daher ist eine Identifizierung von Schulungsbedarfen und Sensibilisierung notwendig.

3. RISIKOANALYSE

BSI-STANDARD 200-1
- BSI-STANDARD ZUR IT SICHERHEIT -

BSI-Standards zur IT-Sicherheit

- Bereich IT-Sicherheitsmanagement -

BSI Standard 200-1:
ISMS: Managementsysteme für Informationssicherheit

BSI Standard 200-2:
IT-Grundschutz-Vorgehensweise

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

IT-Grundschutz-Kompendium

Kapitel 1: Einleitung

Kapitel 2: Schichtenmodell und Modellierung

Elementargefährdungen

Grundschutz-Schichten

Prozessmodule:

- ISMS – Sicherheitsmanagement
- ORP – Organisation und Personal
- CON – Konzepte und Vorgehensweisen
- OPS – IT-Betrieb
- DER – Detektion und Reaktion

IT System-Module:

- IND – Industrielle IT
- APP – Anwendungen
- SYS – IT-Systems
- NET – Netze und Kommunikation
- INF – Infrastruktur

BSI-STANDARD 200-3
RISIKOANALYSE – EIN ZWEISCHICHTIGER ANSATZ

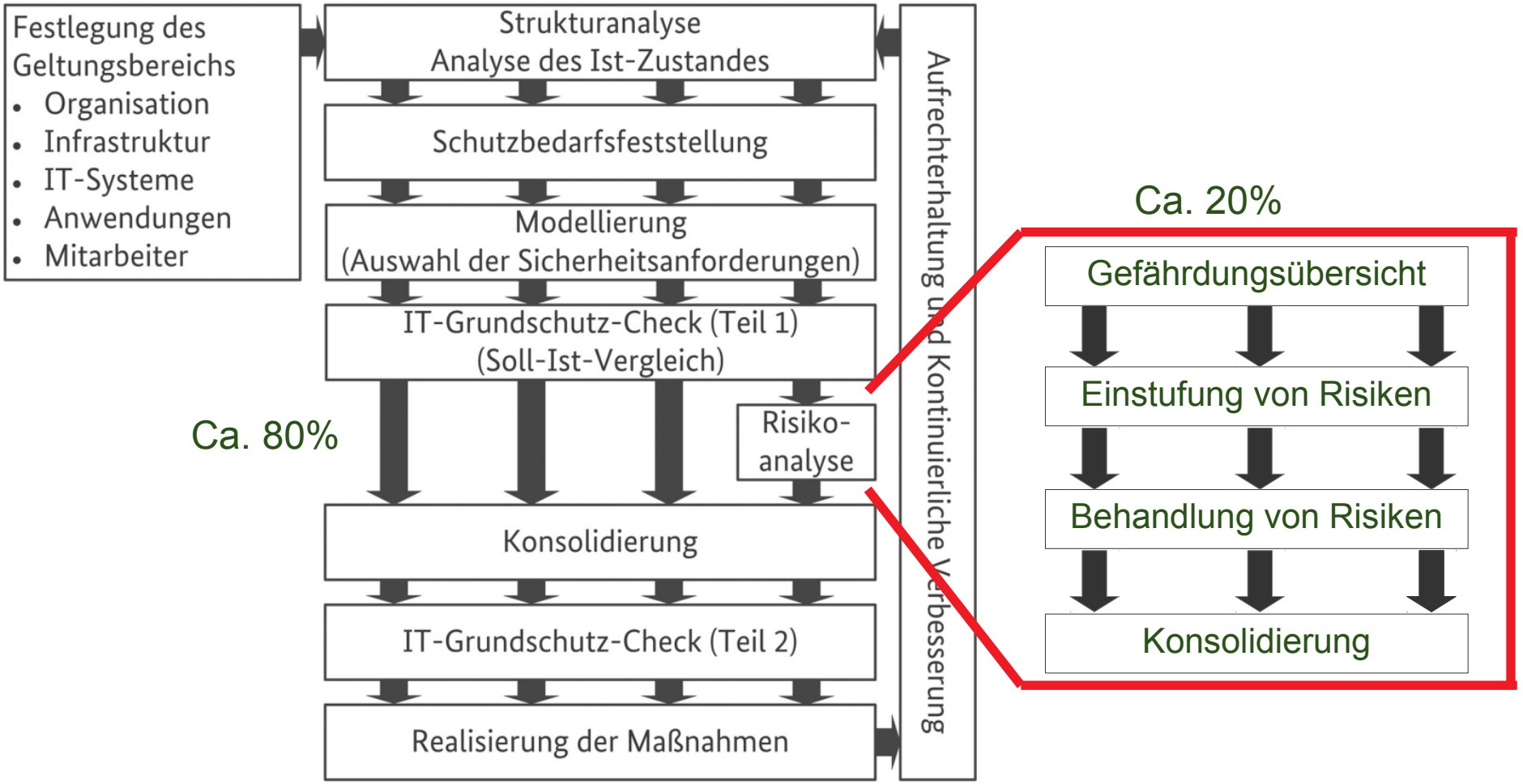
(1) Für normale Schutzbedarfe, typische Anwendungsszenarien und bestehende IT-Grundschutz Kompendium Bausteine:

- Die qualitative Risikoanalyse ist bereits berücksichtigt und in der IT-Grundschutz-Methodik enthalten
- Kann direkt in ähnlichen IT-Architekturen und vergleichbaren Geschäftsumgebungen mit ähnlichen Risikostufen verwendet werden

(2) Für hohe Schutzbedarfe, ungewöhnliche Anwendungsszenarien, wenn keine IT-Grundschutz Kompendium Bausteine existieren oder es das Management verlangt:

- Ergänzende Risikoanalyse nach BSI-Standard 200-3

BSI-STANDARD 200-3
RISIKOANALYSE - VORGEHENSWEISE



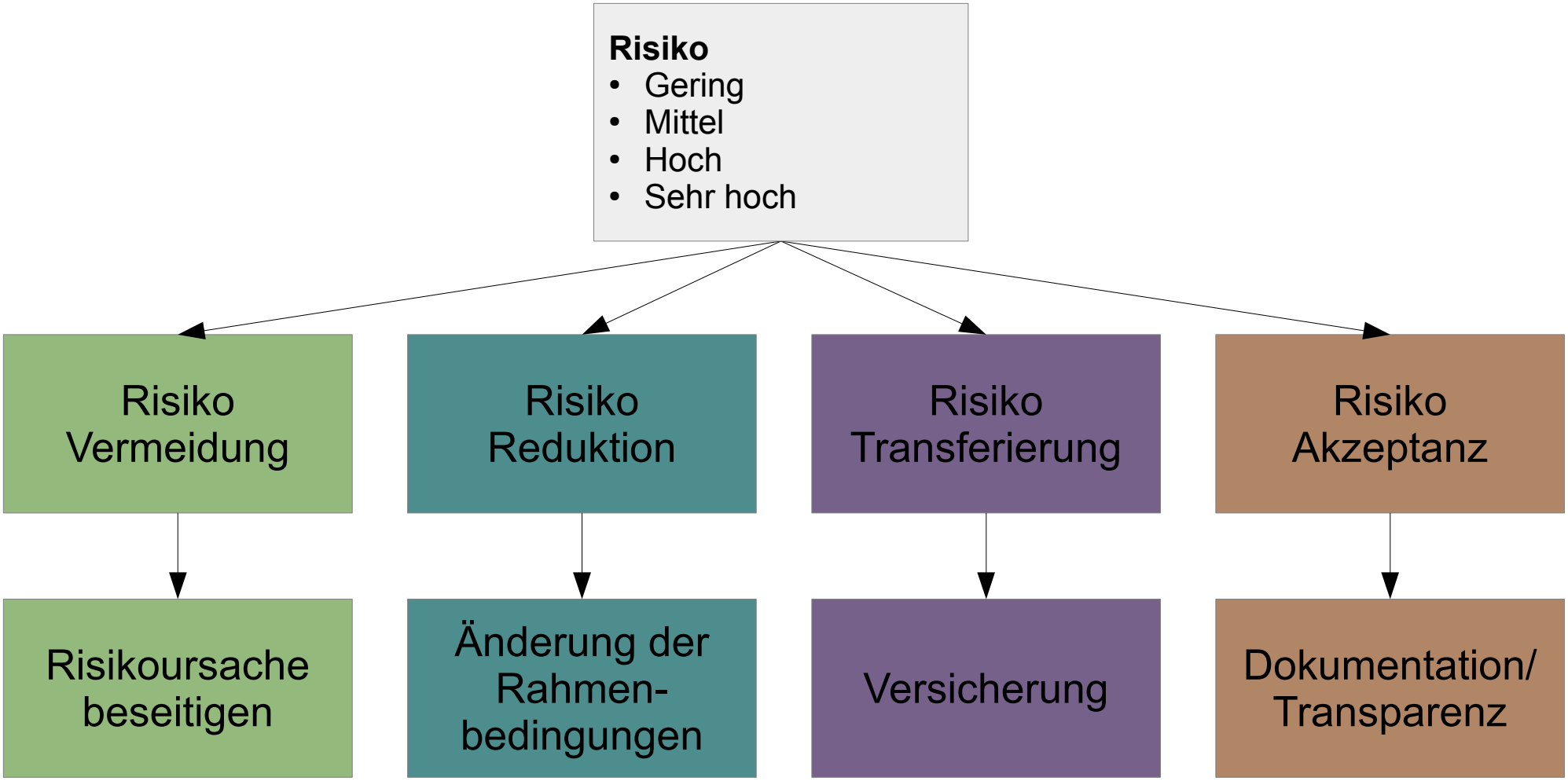
BSI-STANDARD 200-3
RISIKOANALYSE - GEFÄHRDUNGSÜBERSICHT

Vorgehensweise zur Identifikation zusätzlicher Gefährdungen:

- Moderiertes brainstorming mit klarer Agenda und Zeitvorgabe:
  - Bedrohungen, die nicht im IT-Grundschutz Kompendium enthalten sind
  - Realistische Bedrohungen, die erheblichen Schaden anrichten können
  - Bedrohungen durch höhere Gewalt, organisatorische Mängel, menschliches Versagen, technisches Versagen, externe und interne Angreifer
  - Bedrohungen aus externen Quellen

BSI-STANDARD 200-3
RISIKOANALYSE - EINSTUFUNG VON RISIKEN

BSI-STANDARD 200-3
RISIKOANALYSE - BEHANDLUNG VON RISIKEN



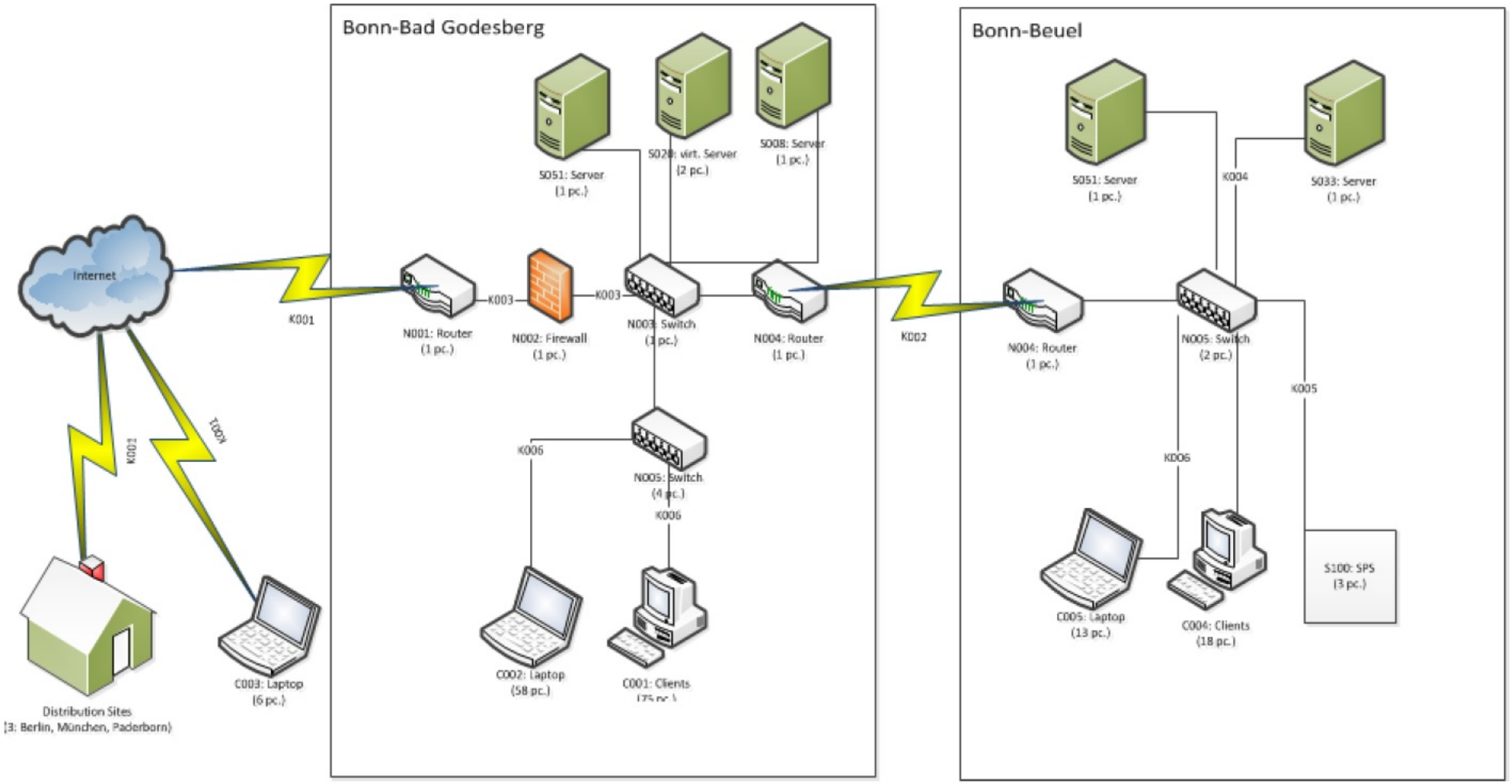
BSI-STANDARD 200-3
KONSOLIDIERUNG

Die Konsolidierung ist nach folgenden Fragen strukturiert:

- Sind die Schutzmaßnahmen sinnvoll?
- Sind die Schutzmaßnahmen angemessen?
- Sind die Schutzmaßnahmen dazu geeignet, die entsprechenden Bedrohungen abzuwehren?
- Welche IT-Grundschutz-Maßnahmen werden durch andere Maßnahmen abgelöst, die ein höheres oder gleichwertiges Sicherheitsniveau bieten?
- Sind die Sicherheitsmaßnahmen benutzerfreundlich und allgemein anwendbar?
- Können neue Bedrohungen und Anforderungen in einem benutzerdefinierten Baustein erfasst werden?
- *Optional*: Können bestehende Bausteine um die neuen Bedrohungen und Anforderungen ergänzt werden?

4. BEISPIEL

RECPLAST GMBH



NETZPLAN

Aktionspunkte zu 8.1.4 Netzplanerhebung
• Existierende grafische Darstellungen des Netzes, beispielsweise Netztopologiepläne, sichten • Netzpläne gegebenenfalls aktualisieren oder neu erstellen • Existierende Zusatzinformationen über die enthaltenen IT-, ICS- und IoT-Systeme sichten und gegebenenfalls aktualisieren und vervollständigen • Existierende Zusatzinformationen über die enthaltenen Kommunikationsverbindungen sichten und gegebenenfalls aktualisieren und vervollständigen

STRUKTURANAYLSE (IT-SYSTEME)

A.1 Strukturanalyse der RECPLAST GmbH									
Bez.	Beschreibung des Zielobjekts	Plattform / Baustein	Ort	Gebäude	Raum	#	Status	Benutzer	Verantwortlich / Administrator
N001	**Router Internetanbindung:** Regelt die Kommunikation zw. dem Internet und internen Prozessen	Router/Switch	Bonn	BG	Server Raum	1	In Betrieb	Administrator	IT-Betrieb
N002	**Firewall Internet:** Dient als Schutz zw. dem internen Netz und dem Internet	Security Gateway	Bonn	BG	Server Raum	1	In Betrieb	Administrator	IT-Betrieb
N003	**Switch - Verteilung:** Verantwortlich für den Datenfluss zw. internem Netz und Internet	Router/Switch	Bonn	BG	Server Raum	1	In Betrieb	Administrator	IT-Betrieb
N004	**Router Bonn BG – Beuel:** Diese beiden Standorte sind über eine Standleitung verbunden	Router/Switch	Bonn	-	Server Raum	2	In Betrieb	Administrator	IT-Betrieb
S008	**Print Server:** Server für zentral verwaltete Druckdienste	Windows Server 2012	Bonn	BG	Server Raum	1	In Betrieb	Alle Mitarbeiter	IT-Betrieb
S008	**File Server:** Server für zentral verwaltete Dateien	Windows Server 2012	Bonn	BG	Server Raum	1	In Betrieb	Administrator	IT-Betrieb
S020	**Virtueller Server (Config. 1):** Dieser Server kann bis zu 20 virtuelle Server hosten. Virtuelle Systeme werden durch dedizierte Software verwaltet	Unix/Linux Server	Bonn	BG	Server Raum	2	In Betrieb	Administrator	IT-Betrieb
S033	**Server Produktion:** Auf diesem Server werden zentrale Daten für die Produktion verarbeitet.	Unix/Linux Server	Bonn	Beuel	Server Raum	1	In Betrieb	Mitarbeiter Produktion	IT-Betrieb

(Anmerkung: Dies ist nur ein Ausschnitt)

STRUKTURANALYSE (RÄUME)

A.1 Strukturanalyse der RECPLAST GmbH									
Bez.	Beschreibung des Zielobjekts	Plattform / Baustein	Ort	Gebäude	Raum	#	Status	Benutzer	Verantwortlich / Administrator
R001	**Büros:** Ein Standard-Büro beinhaltet Schreibtisch, Schränke, Verkabelung usw. Büros können verschlossen werden. Jedes Büro kann von einem bis sechs Mitarbeitern genutzt werden.	Büro	Bonn	BG	-	27	In Betrieb	Alle Mitarbeiter	Haustechnik
R002	**Meeting Räume:** Am Standort Bad-Godesberg stehen mehrere Meeting Räume zur Verfügung. Jeder enthält Schreibtische, Stühle, Schränke und Kabel. Besucher sind in diesen Räumen unter Aufsicht erlaubt .	Meeting Raum	Bonn	BG	-	5	In Betrieb	Alle Mitarbeiter	Haustechnik
R003	**Heimarbeit:** Einige Mitarbeiter dürfen zu Hause arbeiten. Der Arbeitsplatz muss gegen Diebstahl von Firmenmaterial geschützt sein. Die ISO prüft den Arbeitsplatz nach vorheriger Ankündigung.	Telearbeit	Mobiler Arbeits-platz	-	-	27	In Betrieb	Telearbeiter	ISB
R004	**Mobiler Arbeitsplatz:** Alle Mitarbeiter, die für ihre Arbeit Laptop/Notebook verwenden, dürfen ihren Arbeitsplatz auch außerhalb der RECPLAST-Gebäude frei wählen. Es gelten Regeln. Firmendokumente dürfen nur unter strengen Richtlinien mit nach draußen genommen werden.	Mobiler Arbeitsplatz	Mobiler Arbeits-platz	-	-	75	In Betrieb	Führungs-kräfte, Mitarbeiter	IT-Betrieb

(Anmerkung: Dies ist nur ein Ausschnitt)

STRUKTURANALYSE (FORTS.)

- Weiterhin sind zu erfassen
  - Anwendungen, die auf den IT-Systemen betrieben werden
  - Auf den Anwendungen basierende Geschäftsprozesse
  - IoT-Geräte
  - Industrial Control Systems (ICS)
  - …

DEFINITION DER SCHUTZBEDARFSKATEGORIEN

Schutzbedarfskategorien	
„normal“	Die Schadensauswirkungen sind begrenzt und überschaubar.
„hoch“	Die Schadensauswirkungen können beträchtlich sein.
„sehr hoch“	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

SCHUTZBEDARFSFESTSTELLUNG FÜR DIE ELEMENTE DER STRUKTURANALYSE

Aktionspunkte 8.2.4, 8.2.5 und 8.2.6 Definition der Schutzbedarfe der IT-, ICS-Systeme und anderer Geräte

• Ermittlung des Schutzbedarf der IT-, ICS-Systeme und anderer Geräte auf Basis des Schutzes der Geschäftsprozesse und Anwendungen.

• Berücksichtigung der Abhängigkeiten (**Maximalprinzip** und ggf. **Kumulations-** oder **Verteilungseffekte**).

• Dokumentierung des Ergebnisses hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit sowie die Begründung des Schutzbedarfs für jedes System.

SCHUTZBEDARFSFESTSTELLUNG (IT-SYSTEME)

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH								
Bez.	Beschreibung des Zielobjekts	Plattform / Baustein	Vertrau-lichkeit	Begründung Vertraulichkeit	Integrität	Begründung Integrität	Verfüg-barkeit	Begründung Verfügbarkeit
N001	**Router Internetanbindung**	Router/ Switch	hoch	Der Router verbindet das Produktionsnetzwerk mit dem Internet.	normal	Der Zugang ist nur für autorisiertes Personal möglich.	normal	Gerät kann schnell ausgetauscht werden, Ersatzteile sind verfügbar.
N002	**Firewall Internet:**	Security Gateway	hoch	Die Konfiguration muss vertraulich behandelt werden.	normal	Der Zugang ist nur für autorisiertes Personal möglich.	normal	Gerät kann schnell ausgetauscht werden, Ersatzteile sind verfügbar.
N003	**Switch - Verteilung:**	Router/ Switch	normal	Eingehende Daten werden an den richtigen Empfänger gesendet.	normal	Der Zugang ist nur für autorisiertes Personal möglich.	normal	Gerät kann schnell ausgetauscht werden, Ersatzteile sind verfügbar.
N004	**Router Bonn BG – Beuel:**	Router/ Switch	normal	Die Konfiguration muss vertraulich behandelt werden.	normal	Der Zugang ist nur für autorisiertes Personal möglich.	normal	Gerät kann schnell ausgetauscht werden, Ersatzteile sind verfügbar.
S008	**Print Server:**	Windows Server 2012	normal	Der Server stellt alle Druckertreiber bereit.	normal	Serverüberwach-ung kann Fehler schnell erkennen.	normal	Kann schnell als virtuelle Maschine neu installiert werden.
S008	**File Server:**	Windows Server 2012	hoch	Der Server speichert Kundendaten.	hoch	Kundendaten dürfen nicht manipuliert werden	hoch	Kundendaten sollten aus Servicegründen ständig verfügbar sein.
S020	**Virtueller Server (Config. 1):**	Unix/Linux Server	normal	Befindet sich in einem Serverraum mit dedizierter Zugangskontrolle.	normal	Befindet sich in einem Serverraum mit dedizierter Zugangskontrolle.	normal	Dienste sind redundant aufgebaut, sodass ein ausgefallener Server durch einen anderen kompensiert werden kann.
S033	**Server Produktion:**	Unix/Linux Server	sehr hoch	Die verarbeiteten Informationen für Produktion notwendig.	hoch	Es existiert ein Berechtigungskon-zept.	sehr hoch	Der Server muss während der Produktionszeiten verfügbar sein.

(Anmerkung: Dies ist nur ein Ausschnitt)

MAXIMUMPRINZIP

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH

Bez.	Beschreibung des Zielobjekts	Plattform / Baustein	Vertrau-lichkeit	Begründung Vertraulichkeit	Integrität	Begründung Integrität	Verfüg-barkeit	Begründung Verfügbarkeit
N001	**Router Internetanbindung**	Router/ Switch	hoch	Der Router verbindet	normal	Der Zugang ist nur	normal	Gerät kann schnell ausgetauscht werden, Ersatzteile sind verfügbar.
N002	**Firewall Internet:**	Security Gateway	hoch				normal	Gerät kann schnell ausgetauscht werden, Ersatzteile sind verfügbar.
N003	**Switch - Verteilung:**	Router/ Switch	normal				normal	Gerät kann schnell ausgetauscht werden, Ersatzteile sind verfügbar.
N004	**Router Bonn BG – Beuel:**	Router/ Switch	normal	Die muss beha den.		nur für autorisiertes Personal möglich.	normal	Gerät kann schnell ausgetauscht werden, Ersatzteile sind verfügbar.
S008	**Print Server:**	Windows Server 2012	normal	Der Server stellt alle Druckertreiber bereit.	normal	Serverüberwach-ung kann Fehler schnell erkennen.	normal	Kann schnell als virtuelle Maschine neu installiert werden.
S008	**File Server:**	Windows Server 2012	hoch	Der Server speichert Kundendaten.	hoch	Kundendaten dürfen nicht manipuliert werden	hoch	Kundendaten sollten aus Servicegründen ständig verfügbar sein.
S020	**Virtueller Server (Config. 1):**	Unix/Linux Server	normal	Befindet sich in einem Serverraum mit dedizierter Zugangskontrolle.	normal	Befindet sich in einem Serverraum mit dedizierter Zugangskontrolle.	normal	Dienste sind redundant aufgebaut, sodass ein ausgefallener Server durch einen anderen kompensiert werden kann.
S033	**Server Produktion:**	Unix/Linux Server	sehr hoch	Die verarbeiteten Informationen für Produktion notwendig.	hoch	Es existiert ein Berechtigungskon-zept.	sehr hoch	Der Server muss während der Produktionszeiten verfügbar sein.

Anwendung des Maximumprinzips

- Server führt 2 verschiedene Dienste aus
- Diese haben unterschiedliche Schutzbedarfe (normal und hoch)
- Der höchste Schutzbedarf ist “hoch“
- Somit gilt für den gesamten Server ein hoher Schutzbedarf

(Anmerkung: Dies ist nur ein Ausschnitt)

SCHUTZBEDARFSFESTSTELLUNG (RÄUME)

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH								
Bez.	Beschreibung des Zielobjekts	Plattform / Baustein	Vertrau-lichkeit	Begründung Vertraulichkeit	Integrität	Begründung Integrität	Verfüg-barkeit	Begründung Verfügbarkeit
R001	Büros	Büro	normal	Alle Büros verfügen über abschließbare Schränke. Mitarbeiter müssen vertrauliches Material beim Verlassen des Büros abschließen.	normal	Büros können verschlossen werden, es gibt keinen Zutritt für Unbefugte.	normal	Es gibt viele Büros, Räume können leicht gewechselt werden.
R002	Meeting Räume	Meeting Räume	normal	In Meeting Räumen werden keine Dokumente aufbewahrt.	normal	In Meeting Räumen werden keine Dokumente aufbewahrt.	normal	Meeting Räume werden nicht dauerhaft genutzt.
R003	Heimarbeit	Telearbeit	normal	Zu Hause sind keine vertraulichen Informationen erlaubt.	normal	Zu Hause sind keine vertraulichen Informationen erlaubt.	normal	Nur selten verwendet. Der reguläre Arbeitsplatz ist in den RECPLAST-Büros.
R004	Mobiler Arbeitsplatz	Mobiler Arbeitsplatz	normal	Außerhalb des Büros sind keine vertraulichen Informationen erlaubt.	normal	Außerhalb des Büros sind keine vertraulichen Informationen erlaubt.	normal	Nur selten verwendet. Der reguläre Arbeitsplatz ist in den RECPLAST-Büros.

(Anmerkung: Dies ist nur ein Ausschnitt)

SCHUTZBEDARFSFESTSTELLUNG (FORTS.)

- Weiterhin sind zu erfassen
  - Anwendungen, die auf den IT-Systemen betrieben werden
  - Auf den Anwendungen basierende Geschäftsprozesse
  - IoT-Geräte
  - Industrial Control Systems (ICS)
  - …

IT GRUNDSCHUTZ KOMPENDIUM

IT-GRUNDSCHUTZ KOMPENDIUM

BSI-Standards zur IT-Sicherheit

- Bereich IT-Sicherheitsmanagement -

BSI Standard 200-1:
ISMS: Managementsysteme für Informationssicherheit

BSI Standard 200-2:
IT-Grundschutz-Vorgehensweise

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

IT-Grundschutz-Kompendium

Kapitel 1: Einleitung

Kapitel 2: Schichtenmodell und Modellierung

Elementargefährdungen

Grundschutz-Schichten

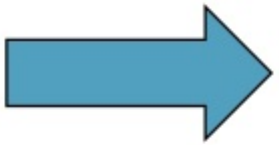
Prozessmodule:

- ISMS – Sicherheitsmanagement
- ORP – Organisation und Personal
- CON – Konzepte und Vorgehensweisen
- OPS – IT-Betrieb
- DER – Detektion und Reaktion

IT System-Module:

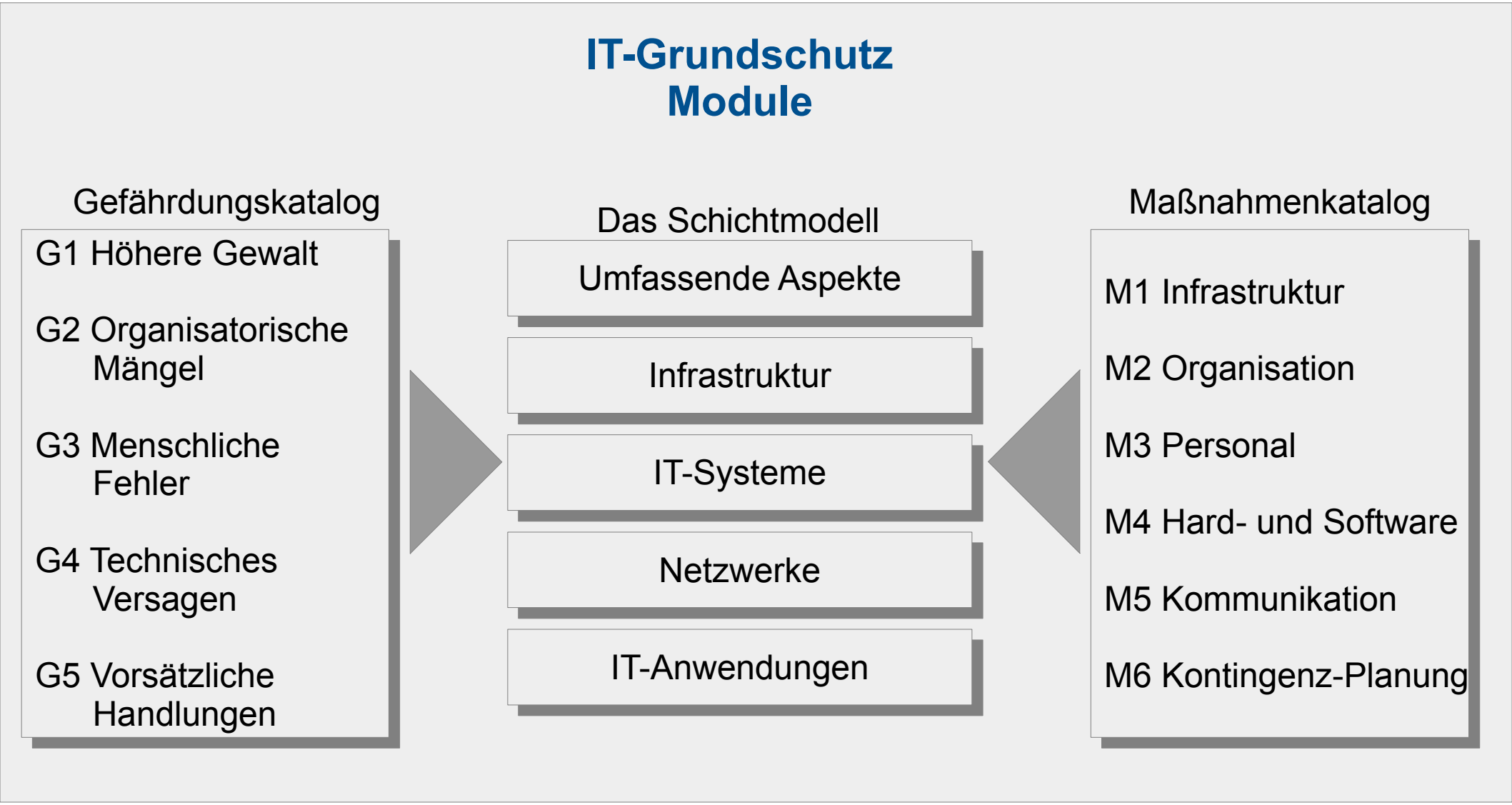
- IND – Industrielle IT
- APP – Anwendungen
- SYS – IT-Systems
- NET – Netze und Kommunikation
- INF – Infrastruktur

IT-GRUNDSCHUTZ KATALOGE VS. KOMPENDIUM



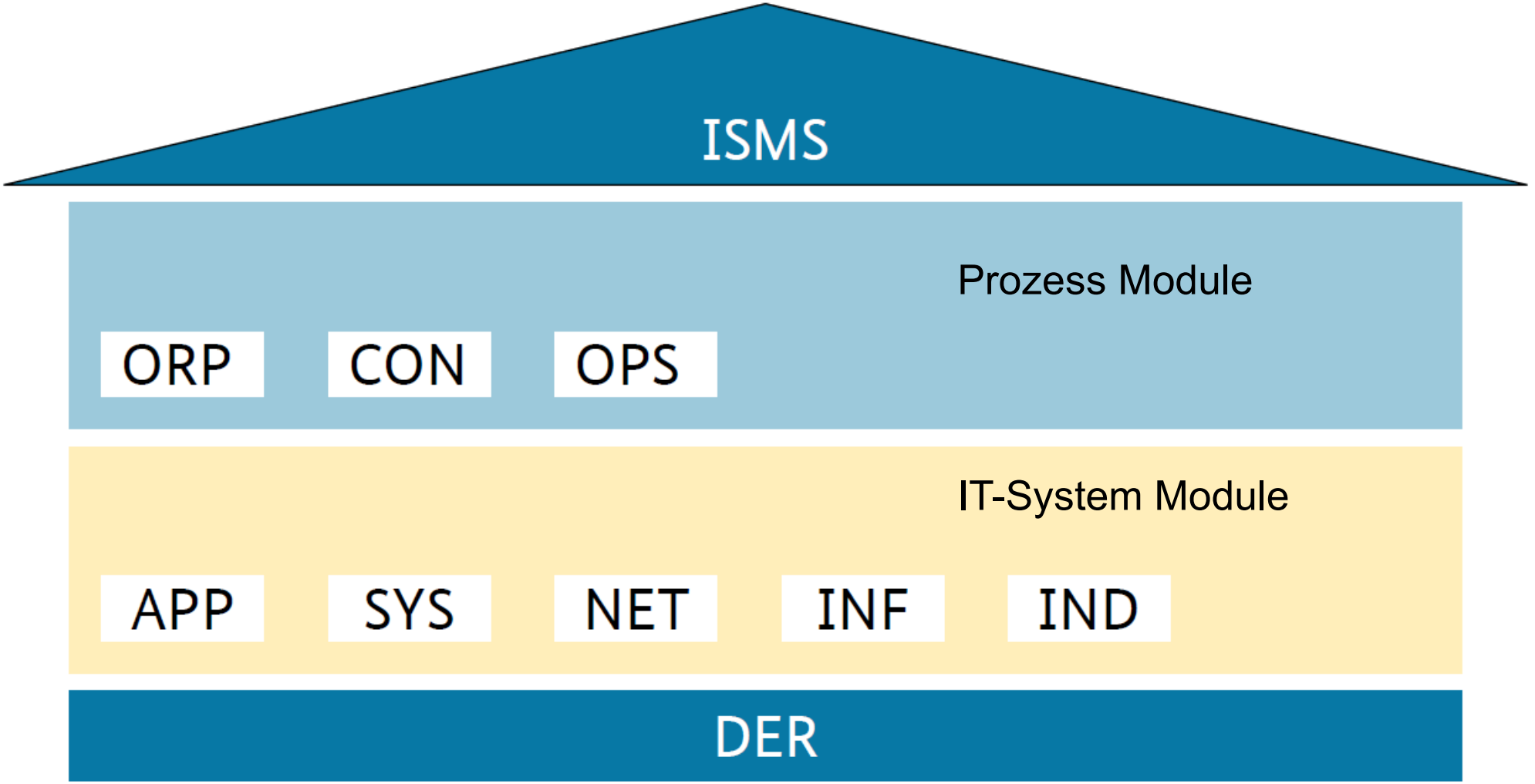
Offizielles Erscheinungsdatum: 01.02.2018

IT-GRUNDSCHUTZ KATALOGE
ALTES SCHICHTEN-MODELL



IT-GRUNDSCHUTZ KOMPENDIUM

NEUES MODELL



- Voraussetzung: Alle Prozesse, Anwendungen und IT-Systeme sind dokumentiert, die Strukturanalyse und Schutzbedarfsfeststellung wurde bereits durchgeführt

OBERE- UND UNTERE SCHICHT

- Von oben: **ISMS** *(Information Security Management System)* Schicht
  - Ein Sicherheitsmanagementsystem ist die Basis für alle Aktivitäten rund um den Sicherheitsprozess.

- Von unten: **DER** *(Detection and Reaction)*
  - Beinhaltet alle relevanten Bausteine für
    - Überprüfung der Umsetzung Schutzmaßnahmen
    - Erkennen von Sicherheitsvorfällen
    - Reaktion auf Sicherheitsvorfälle
  - Typische Bausteine: Behandlung von Sicherheitsvorfällen, Notfallmanagement

PROZESS BAUSTEINE

- **ORP** *(Organisation and Personnel)*
  - organisatorische und personalbezogene Sicherheitsaspekte
  - Typische Bausteine: Sensibilisierung und Schulung zur Informationssicherheit

- **CON** *(Concepts and Procedures)*
  - Bausteine zu Konzepten und Vorgehensweisen
  - Typische Bausteine: Löschen und Vernichten, Datenschutz

- **OPS** *(Operational Security Aspects)*
  - Aspekte der Betriebssicherheit, einschließlich an Dritte ausgelagerte Dienstleistungen
  - Typische Bausteine: Archivierung, Software-Tests- und -Freigaben

IT-SYSTEM BAUSTEINE

- **APP** *(Applications)*
  - Sichern von Anwendungen und Diensten, einschließlich Kommunikation, Verzeichnisdienste, Netzwerkdienste und Geschäfts-/Client-Apps
  - Typische Bausteine: Office-Produkte, Webserver, Relationale Datenbanken

- **SYS** *(Systems)*
  - Sicherheitsaspekte einzelner IT-Systeme
  - Typische Bausteine: Mobile Devices, Virtualisierung, IoT-Geräte

- **IND** *(Industrial IT)*
  - Sicherheitsaspekte industrieller Prozessleitsysteme
  - Typische Bausteine: ICS-Komponenten

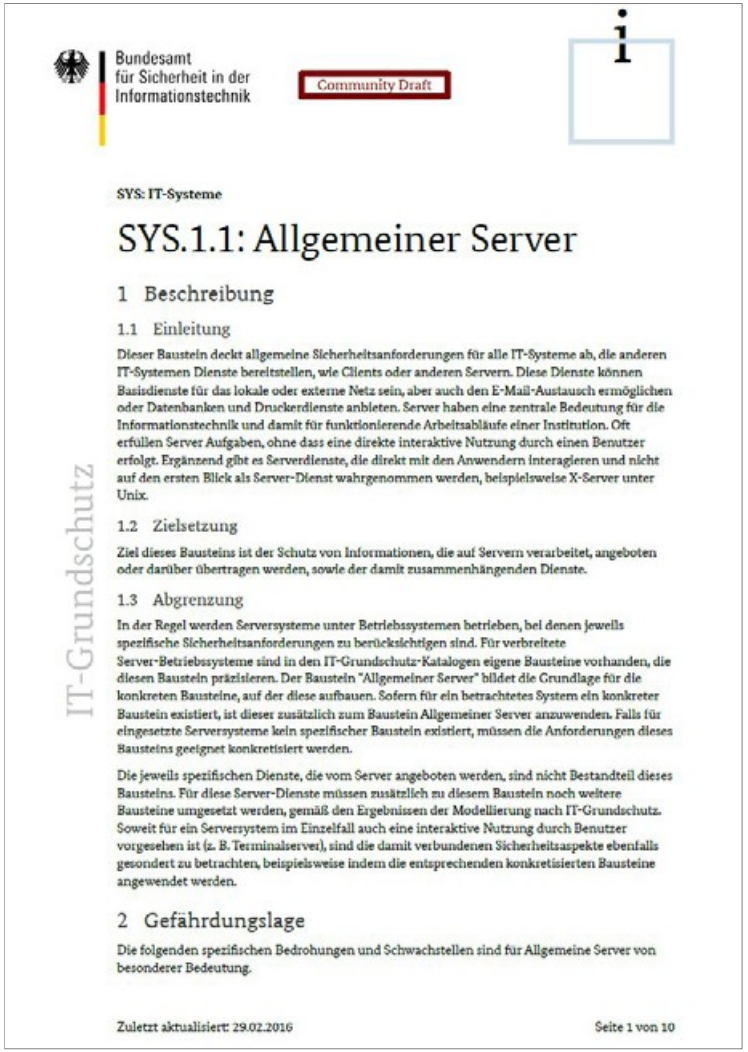
IT-SYSTEM BAUSTEINE (FORTS.)

- **NET** *(Network)*
  - Sicherheitsaspekte in Bezug auf Netzwerkverbindungen und Kommunikationsleitungen
  - Typische Bausteine: VPN, Firewalls

- **INF** *(Infrastructure)*
  - Sicherheitsaspekte von Bürogebäuden, Rechenzentrumseinrichtungen usw.
  - Typische Bausteine: Büroarbeitsplatz, Häuslicher Arbeitsplatz, Verkabelung

AUFBAU EINES BAUSTEINS

- Umfang: Etwa 10 Seiten
- 1. Beschreibung
  - Einleitung
  - Zielsetzung
  - Abgrenzung und Modellierung
- 2. Gefährdungslage
- 3. Anforderungen
  - Basis-Anforderungen
  - Standard-Anforderungen
  - Anforderungen bei erhöhtem Schutzbedarf
- 4. Weiterführende Informationen



Bundesamt für Sicherheit in der Informationstechnik

Community Draft

SYS: IT-Systeme

SYS.1.1: Allgemeiner Server

1 Beschreibung

1.1 Einleitung

Dieser Baustein deckt allgemeine Sicherheitsanforderungen für alle IT-Systeme ab, die anderen IT-Systemen Dienste bereitstellen, wie Clients oder anderen Servern. Diese Dienste können Basisdienste für das lokale oder externe Netz sein, aber auch den E-Mail-Austausch ermöglichen oder Datenbanken und Druckerdienste anbieten. Server haben eine zentrale Bedeutung für die Informationstechnik und damit für funktionierende Arbeitsabläufe einer Institution. Oft erfüllen Server Aufgaben, ohne dass eine direkte interaktive Nutzung durch einen Benutzer erfolgt. Ergänzend gibt es Serverdienste, die direkt mit den Anwendern interagieren und nicht auf den ersten Blick als Server-Dienst wahrgenommen werden, beispielsweise X-Server unter Unix.

1.2 Zielsetzung

Ziel dieses Bausteins ist der Schutz von Informationen, die auf Servern verarbeitet, angeboten oder darüber übertragen werden, sowie der damit zusammenhängenden Dienste.

1.3 Abgrenzung

In der Regel werden Serversysteme unter Betriebssystemen betrieben, bei denen jeweils spezifische Sicherheitsanforderungen zu berücksichtigen sind. Für verbreitete Server-Betriebssysteme sind in den IT-Grundschutz-Katalogen eigene Bausteine vorhanden, die diesen Baustein präzisieren. Der Baustein "Allgemeiner Server" bildet die Grundlage für die konkreten Bausteine, auf der diese aufbauen. Sofern für ein betrachtetes System ein konkreter Baustein existiert, ist dieser zusätzlich zum Baustein Allgemeiner Server anzuwenden. Falls für eingesetzte Serversysteme kein spezifischer Baustein existiert, müssen die Anforderungen dieses Bausteins geeignet konkretisiert werden.

Die jeweils spezifischen Dienste, die vom Server angeboten werden, sind nicht Bestandteil dieses Bausteins. Für diese Server-Dienste müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz. Soweit für ein Serversystem im Einzelfall auch eine interaktive Nutzung durch Benutzer vorgesehen ist (z. B. Terminalserver), sind die damit verbundenen Sicherheitsaspekte ebenfalls gesondert zu betrachten, beispielsweise indem die entsprechenden konkretisierten Bausteine angewendet werden.

2 Gefährdungslage

Die folgenden spezifischen Bedrohungen und Schwachstellen sind für Allgemeine Server von besonderer Bedeutung.

Zuletzt aktualisiert: 29.02.2016

Seite 1 von 10

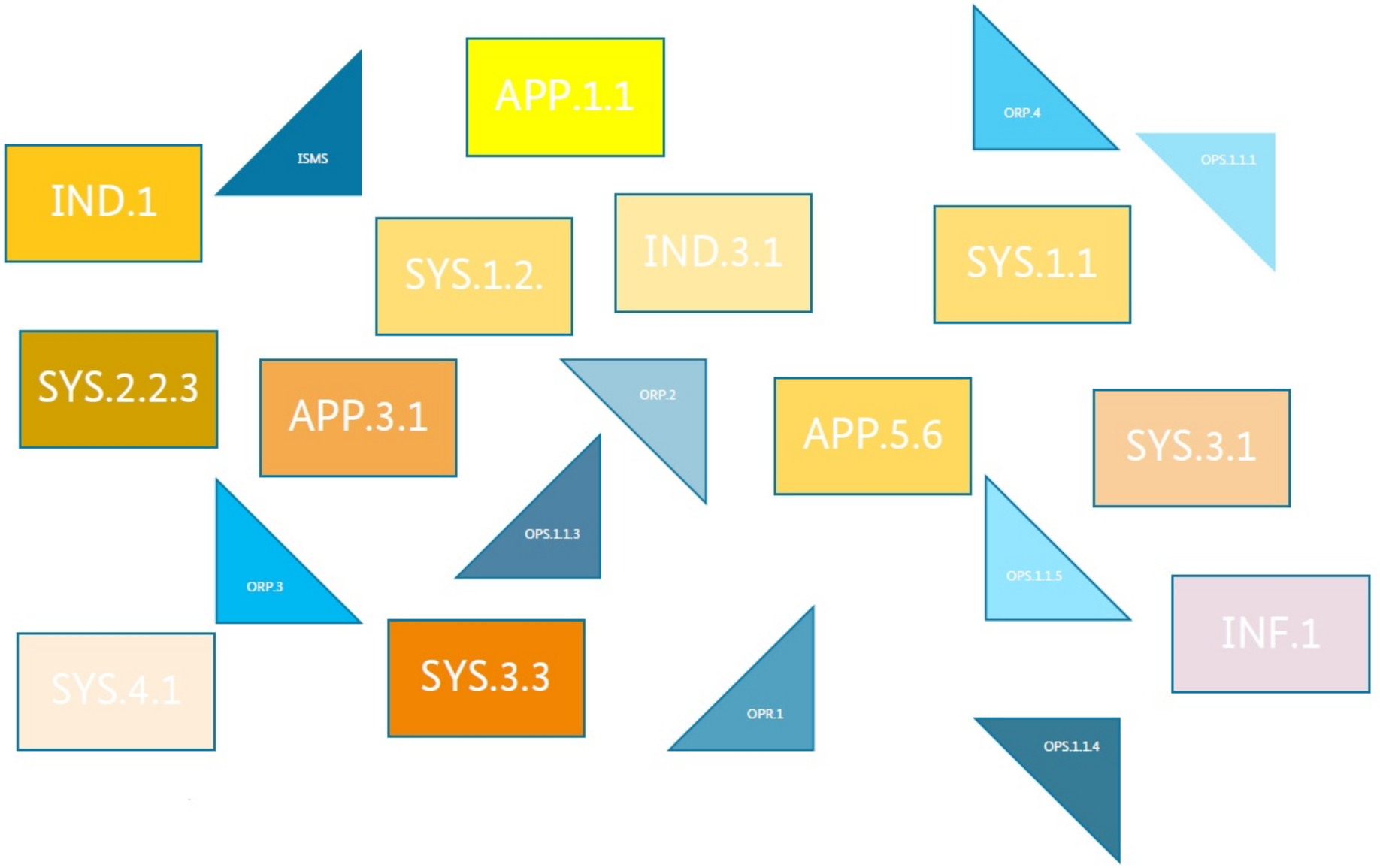
IT-Grundschutz

IT-GRUNDSCHUTZ PROFILE

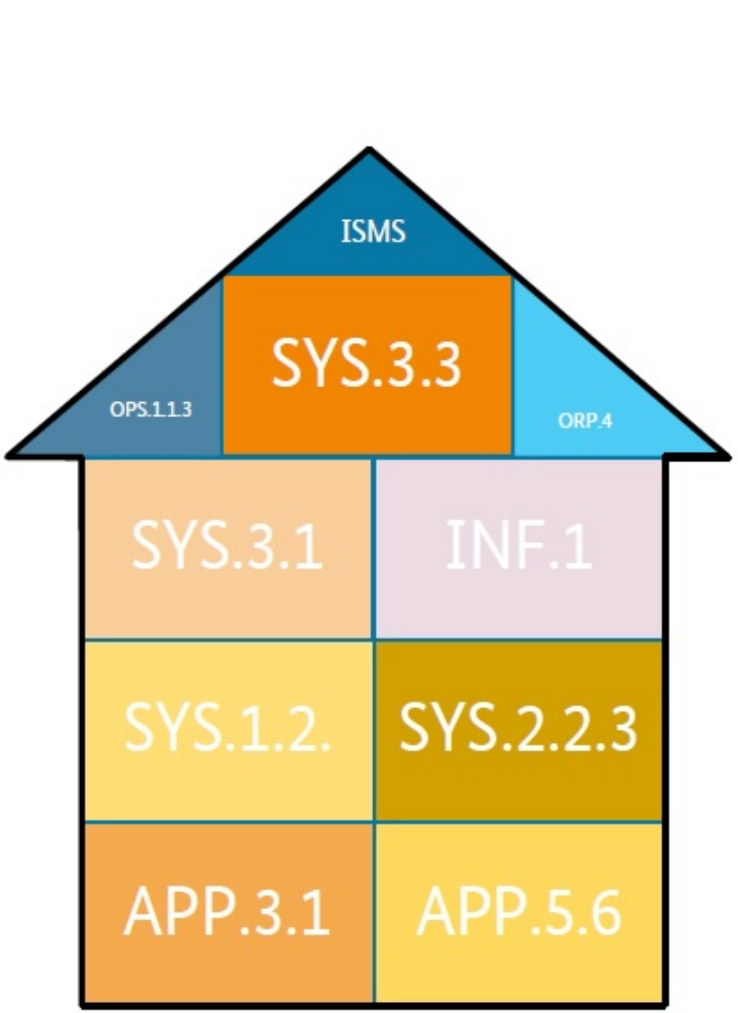
EIN IT-GRUNDSCHUTZ PROFIL IST...

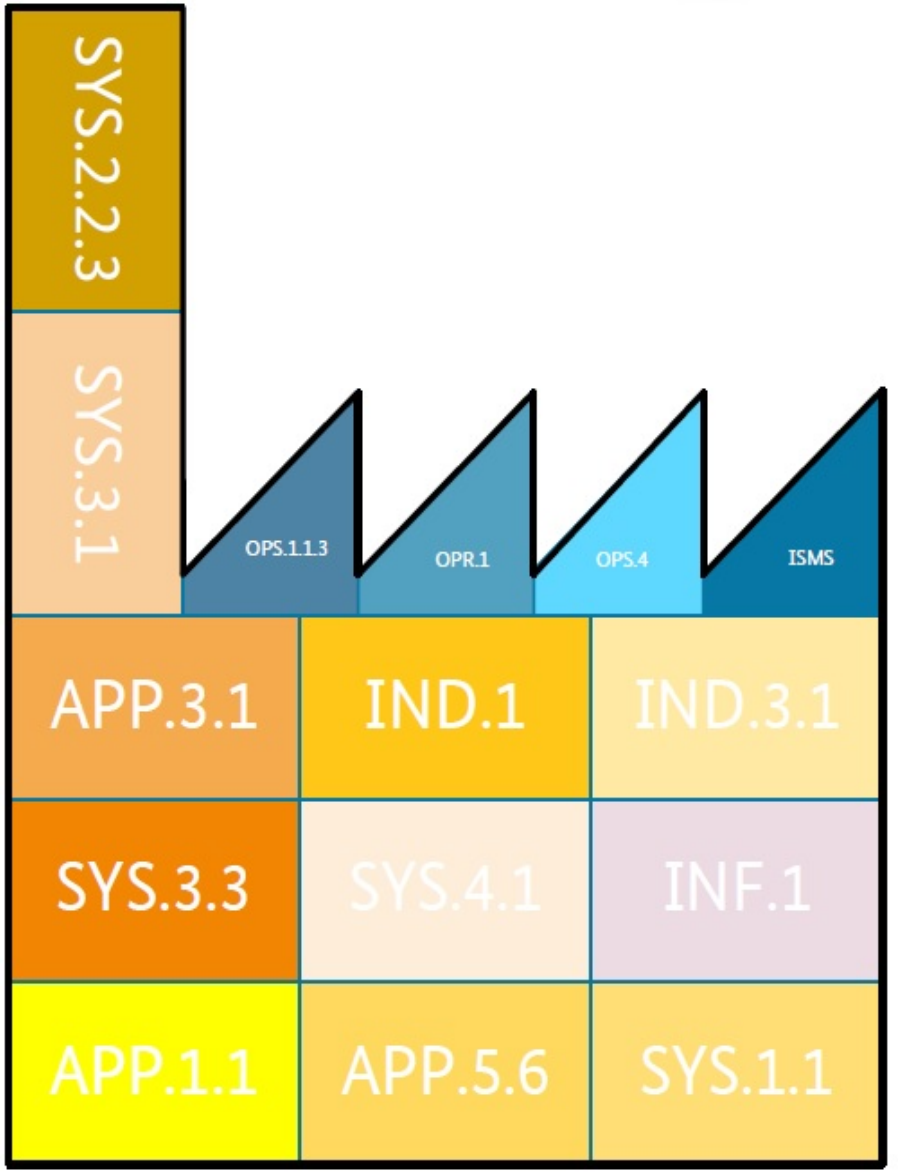
- eine Vorlage eines Sicherheitskonzepts für ein ausgewähltes Szenario (Verbund oder Prozess). Es beinhaltet...
  - ...das Ergebnis mehrerer Prozessschritte der IT-Grundschutz-Methodik (z. B. Strukturanalyse, Schutzbedarfsfeststellung, Modellierung)
  - ...eine Auswahl mehrerer Anforderungen von IT-Grundschutz-Bausteinen, damit diese leicht an ähnliche Szenarien angepasst werden können

VERWENDUNG EINER VORLAGE

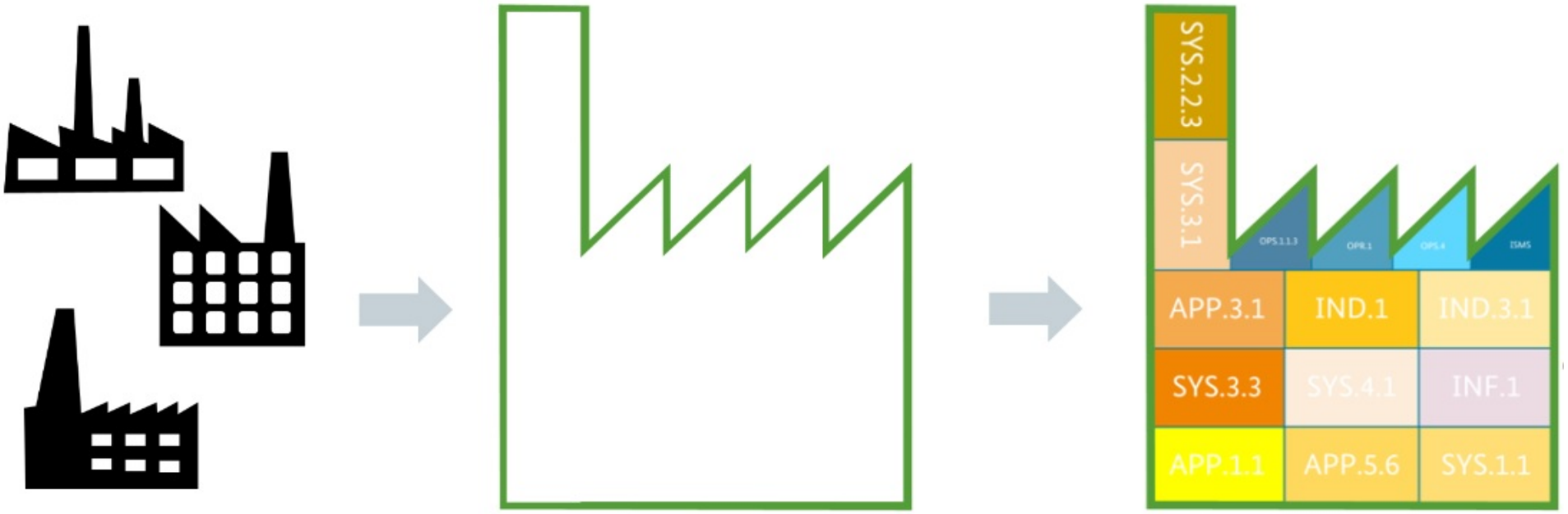


VERWENDUNG EINER VORLAGE (FORTS.)





DIE IDEE DER IT-GRUNDSCHUTZ PROFILE



1. Gruppe ähnlicher Unternehmen

2. Referenz-Unternehmen

3. **Profile** = IT-Grundschutz angewendet auf das Referenz-Unternehmen

VORTEILE DER IT-GRUNDSCHUTZ PROFILE

1. Ein grundlegendes Sicherheitsverständnis ist ausreichend

- IT-Grundschutz beinhaltet Expertenwissen
- Risikoanalyse ist nur in Ausnahmefällen notwendig

2. Zeitersparnis durch strukturiertes Vorgehen

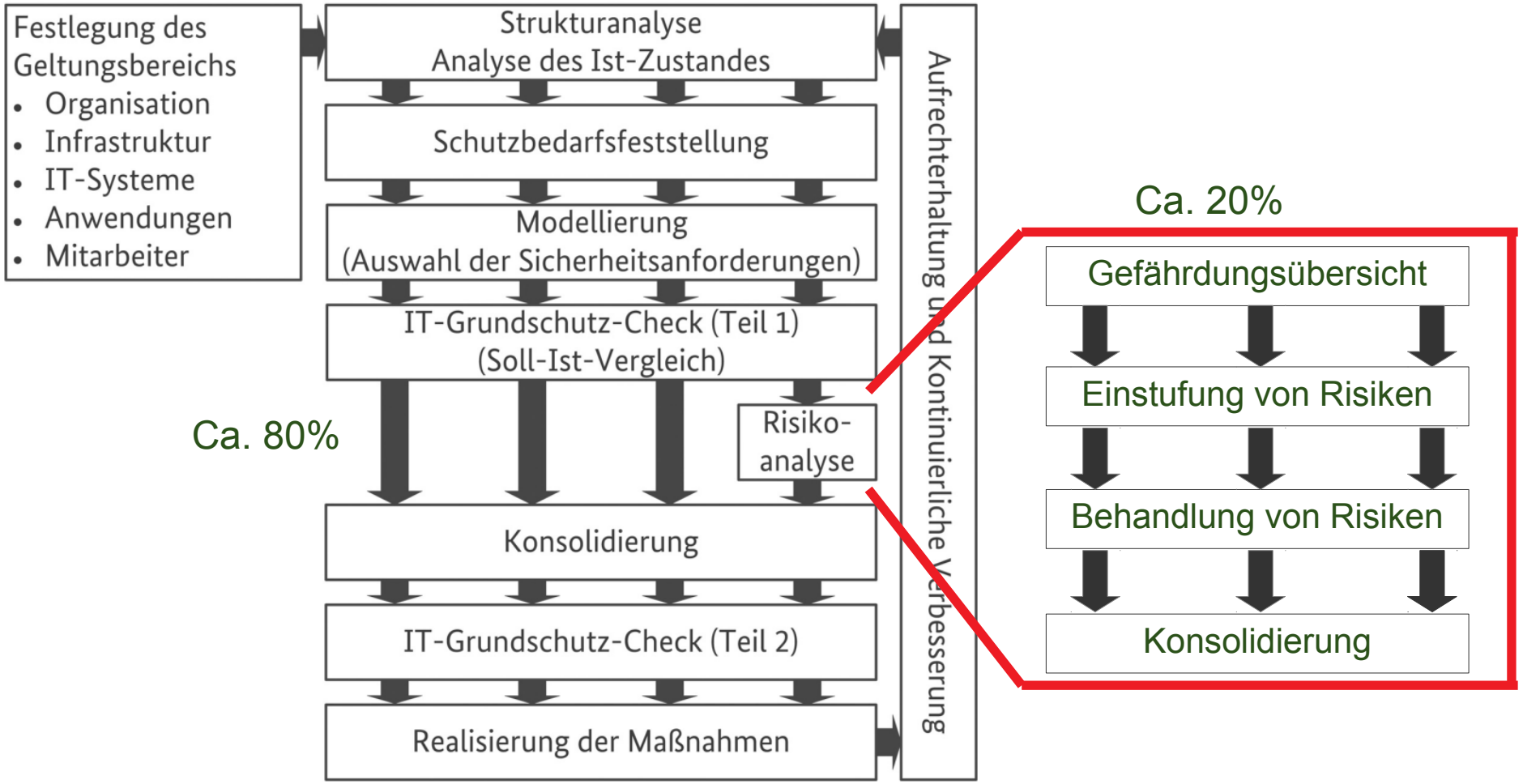
- Grundidee der Profile: Benutzer von der Modellierung entlasten
- Die Homogenität des IT-Grundschutz-Kompendiums gewährleistet eine gute Passform der Bausteine

3. Geringer Dokumentationsaufwand

- Ein Großteil der Dokumentation liegt dem Profil bei und kann vom Benutzer einfach angepasst werden

ABSCHLUSS

ZUSAMMENFASSUNG
IT-GRUNDSCHUTZ METHODIK



MÖGLICHE PRÜFUNGSFRAGEN

- Warum ist der IT-Grundschutz vor allem für Unternehmen geeignet, die bisher wenig Erfahrung mit IT-Sicherheit haben?
- Worin unterscheidet sich die Standard-Absicherung von der Kern-Absicherung?
- Erklären Sie den Ablauf einer Risikoanalyse.
- Unter welchen Umständen eignet sich eine Anwendung der IT-Grundschutz Profile nicht?

LITERATUR

IT-Grundschutz Kompendium Edition 2021

BSI Standard 200-1

BSI Standard 200-2

BSI Standard 200-3