IT-Grundschutz heute und morgen

Alex Didier Essoh

Bundesamt für Sicherheit in der Informationstechnik

Agenda

- Klassischer IT-Grundschutz
  - Einführung
  - BSI-Standard 100-1: Sicherheitsmanagement
  - BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
  - IT-Grundschutz-Kataloge
- IT-Grundschutz-Modernisierung
  - Kernaspekte der Modernisierung des IT-Grundschutzes
  - Vorgehensweisen
  - Bausteine des IT-Grundschutz-Kompendiums
  - IT-Grundschutz-Profile
- Ausblick und Diskussion

Klassischer IT-Grundschutz

Typische Probleme in der Praxis

- Sicherheit wird als technisches Problem mit technischen Lösungen gesehen
- Zielkonflikte: Sicherheit, Bequemlichkeit, Kosten
- unsystematisches Vorgehen bzw. falsche Methodik
- Management: fehlendes Interesse, schlechtes Vorbild
- Sicherheitskonzepte richten sich an Experten, der IT-Benutzer wird vergessen
- …..

Einführung
Informationssicherheit ist...

- … kein Produkt
  - Sicherheit kann man nicht kaufen, Sicherheit muss man schaffen!
  - Natürlich muss man zum Schaffen von Sicherheit auch auf vorhandene Produkte zurückgreifen.
- … kein Projekt
  - Es genügt nicht, Sicherheit einmal zu schaffen, sondern Sicherheit muss aufrecht erhalten werden!
  - Natürlich kann man Aufbau und Aufrechterhaltung von Sicherheit auch teilweise in Projekten abwickeln.
- … ein Prozess

Informationssicherheit in einer Organisation

Viele Wege führen zur Informationssicherheit...

Welcher Weg ist der effektivste?

ISO-Standards für ISMS

- ISO 27001:2013

  “Information technology - Security techniques - Information security management systems - Requirements“

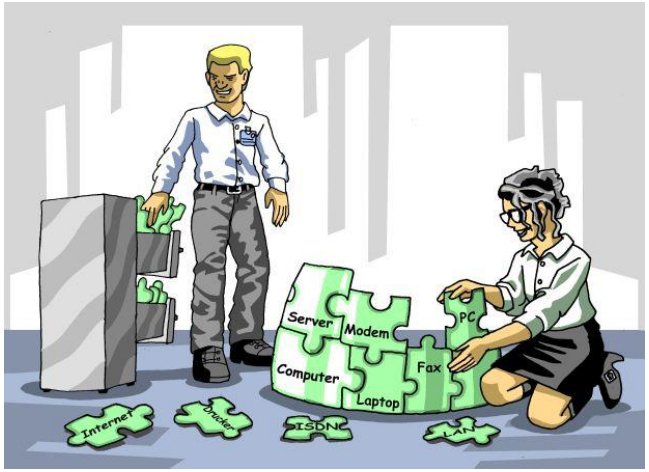
  - erlaubt die Implementierung und den Betrieb von integrierten Managementsystemen für Informationssicherheit (ISO 27001), Qualität (ISO 9001) und Umwelt (ISO 14001)
  - dient als Grundlage einer Zertifizierung

- ISO 27002:2013

  “Information technology - Security techniques - Code of practice for information security management“

  - keine Spezifikation und kein Zertifizierungsstandard
  - dient zum besseren Verständnis der in der ISO 27001 definierten Anforderungen (insbesondere aus Anhang A)

IT-Grundschutz
Die Idee ...



- Typische Komponenten
- Typische Gefährdungen, Schwachstellen und Risiken
- Konkrete Umsetzungshinweise für das Sicherheitsmanagement
- Empfehlung geeigneter Bündel von Standard-Sicherheitsmaßnahmen
- Vorbildliche Lösungen aus der Praxis, „Best Practice“-Ansätze

Quelle: BSI

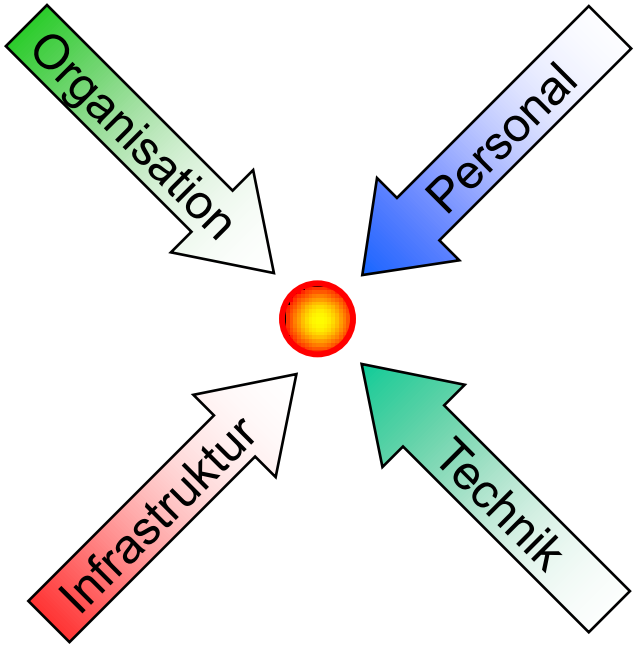
IT-Grundschutz
das Ziel

IT-Grundschutz

- verfolgt einen ganzheitlichen Ansatz
- besteht aus Standard-Sicherheitsmaßnahmen
- bietet ein Standard-Sicherheitsniveau und
- stellt die Basis für einen höheren Schutzbedarf

IT-Grundschutz
die Facetten

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



Quelle: BSI

IT-Grundschutz implementiert ISO 27001

BSI-Standards
- Bereich 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

BSI-Standard 100-4:
Notfallmanagement

Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz

IT-Grundschutz-Kataloge

Kapitel 1: Einleitung

Kapitel 2: Schichtenmodell und Modellierung

Kapitel 3: Glossar

Kapitel 4: Rollen

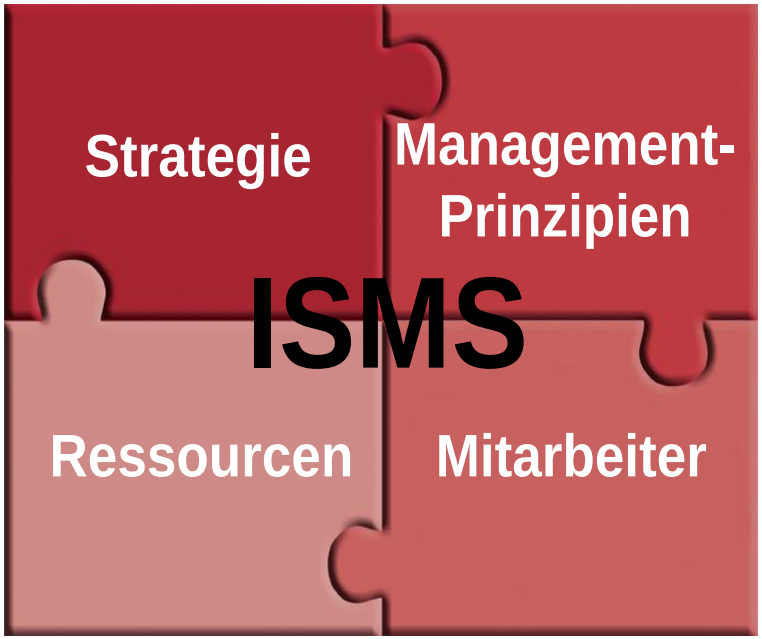
- Bausteinkataloge
  - Kapitel B1 Übergreifende Aspekte
  - Kapitel B2 Infrastruktur
  - Kapitel B3 IT-Systeme
  - Kapitel B4 Netze
  - Kapitel B5 IT-Anwendungen
- Gefährdungskataloge
- Maßnahmenkataloge

Quelle: BSI

BSI-Standard 100-1
ISMS

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

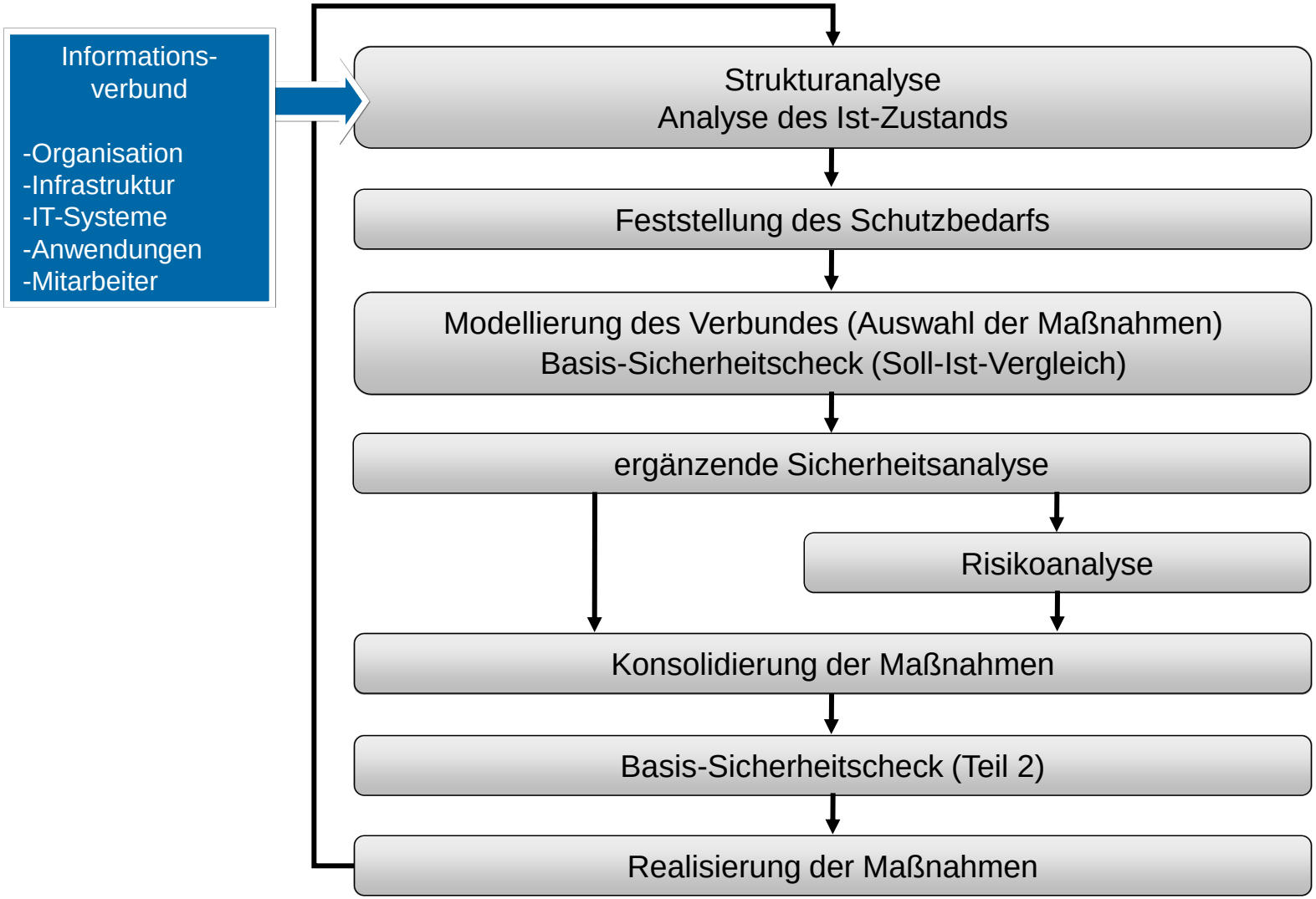
- Zielgruppe: Management
- Kompatibel mit ISO/IEC 27001
- Interpretation der Norm
- allgemeine Anforderungen an ein ISMS



Quelle: BSI

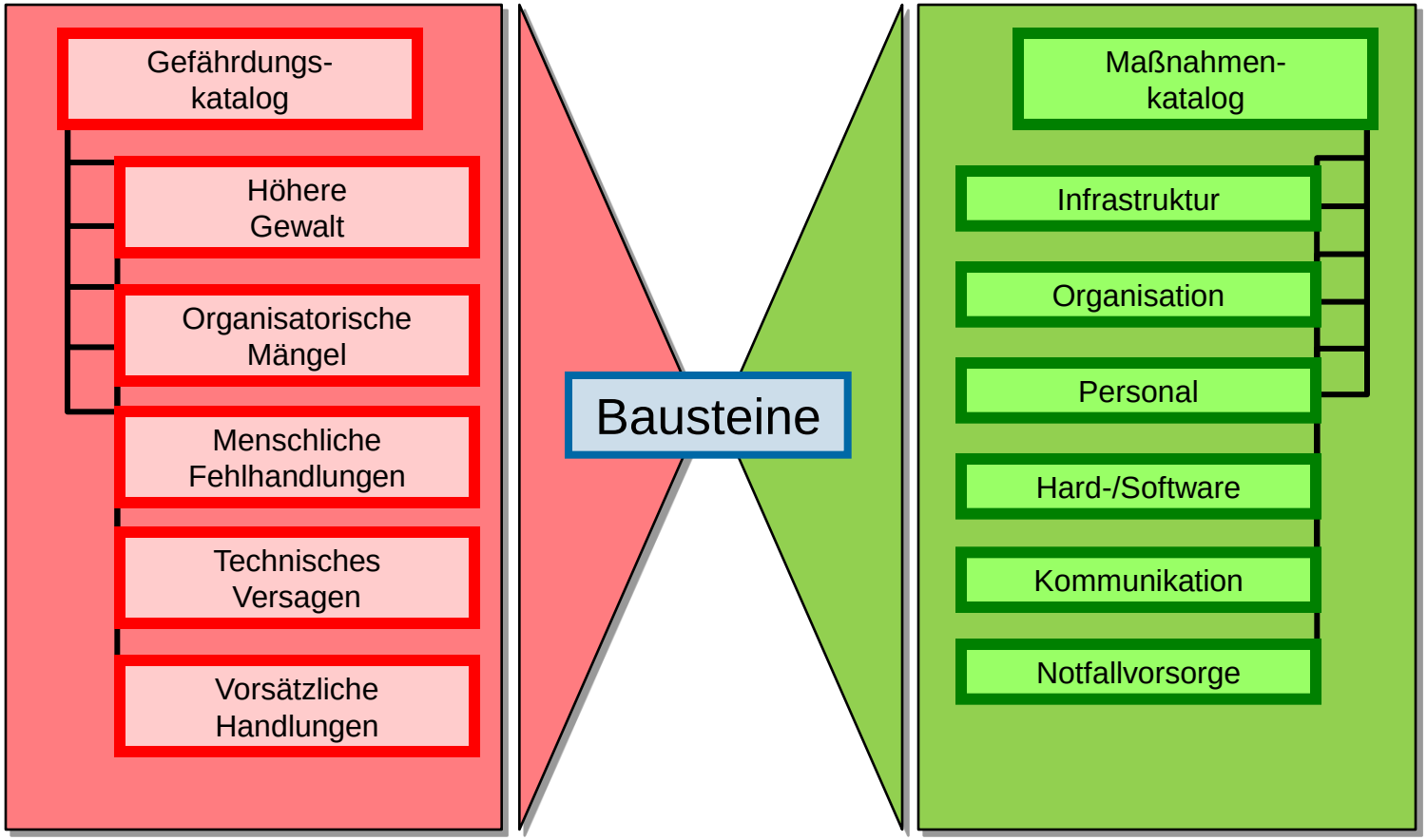
Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Standard 100-2
IT-Grundschutz-Vorgehensweise



Quelle: BSI

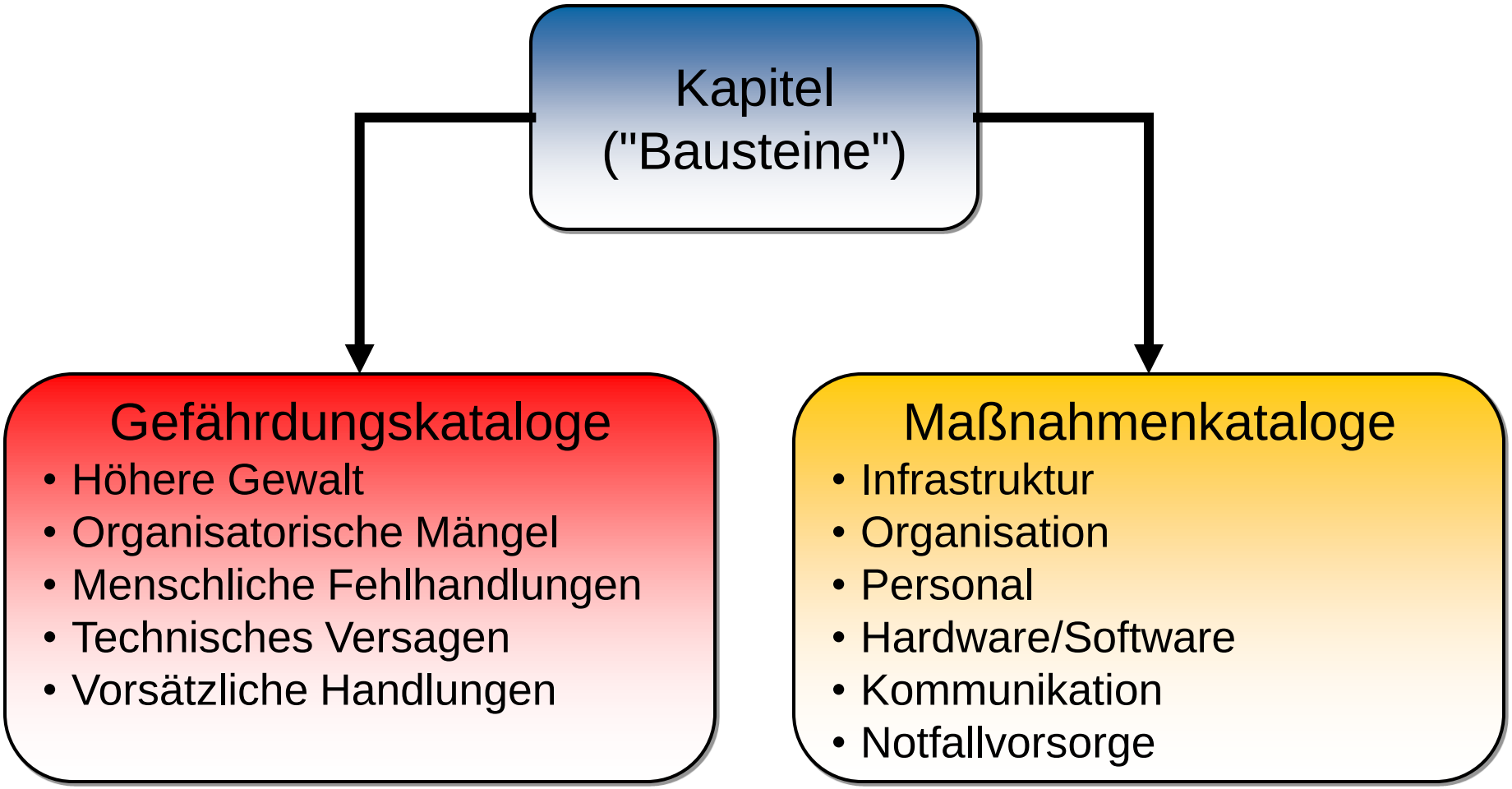
IT-Grundschutz-Kataloge



Stark vereinfachter Risikoansatz

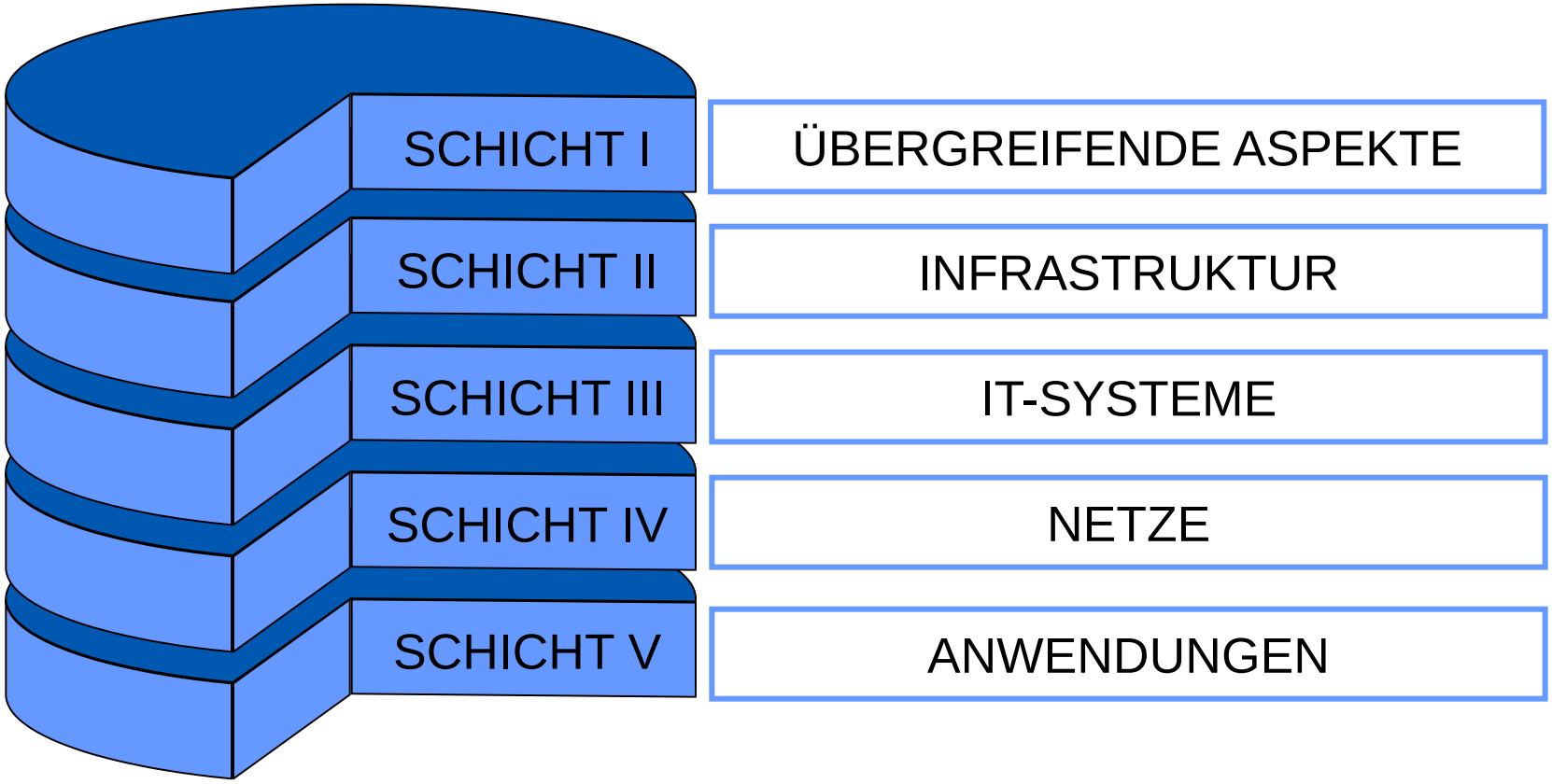
Quelle: BSI

IT-Grundschutz-Kataloge
Bausteine



Quelle: BSI

IT-Grundschutz-Kataloge
Schichtenmodell



Quelle: BSI

Beispiel
B 1.0 Sicherheitsmanagement

B 1.0 IT-Sicherheitsmanagement

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Im Rahmen des IT-Sicherheitsmanagements sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über den Aufbau geeigneter Organisationsstrukturen bis hin zur regelmäßigen Revision. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Einer der Grundpfeiler zur Erreichung eines angemessenen Sicherheitsniveaus ist, dass die Leitungsebene hinter den Sicherheitszielen steht und sich ihrer Verantwortung für IT-Sicherheit bewusst ist. Die Leitungsebene muss den IT-Sicherheitsprozess initiieren, steuern und kontrollieren, damit dieser in der Institution auch in allen Bereichen umgesetzt wird (siehe M 2.336 *Übernahme der Gesamtverantwortung für IT-Sicherheit durch die Leitungsebene*).

Weiterhin muss ein kontinuierlicher IT-Sicherheitsprozess etabliert und eine für die jeweilige Institution passende IT-Sicherheitsstrategie festgelegt werden (siehe M 2.335 *Festlegung der IT-Sicherheitsziele und -strategie*). Die Leitungsebene muss hierfür wie für alle weiteren Sicherheitsfragen eine Person als Hauptverantwortlichen benennen. Diese ist dafür zuständig, eine geeignete Organisationsstruktur für IT-Sicherheit aufzubauen und aufrechtzuerhalten (siehe M 2.193 *Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit*). Als eine der ersten Aktionen sollte eine IT-Sicherheitsleitlinie erstellt werden (siehe M 2.192 *Erstellung einer IT-Sicherheitsleitlinie*).

IT-Sicherheit muss in allen Bereichen der Institution gelebt werden (siehe M 2.337 *Integration der IT-Sicherheit in organisationsweite Abläufe und Prozesse*). Dazu gehört neben der Erarbeitung eines IT-Sicherheitskonzepts (siehe M 2.195 *Erstellung eines IT-Sicherheitskonzepts*) auch die Integration der Mitarbeiter in den Sicherheitsprozess (siehe M 2.197 *Integration der Mitarbeiter in den Sicherheitsprozess*) sowie die Erstellung von zielgruppengerechten IT-Sicherheitsrichtlinien (siehe M 2.338 *Erstellung von zielgruppengerechten IT-Sicherheitsrichtlinien*).

Nachfolgend wird das Maßnahmenbündel für den Bereich "IT-Sicherheitsmanagement" vorgestellt.

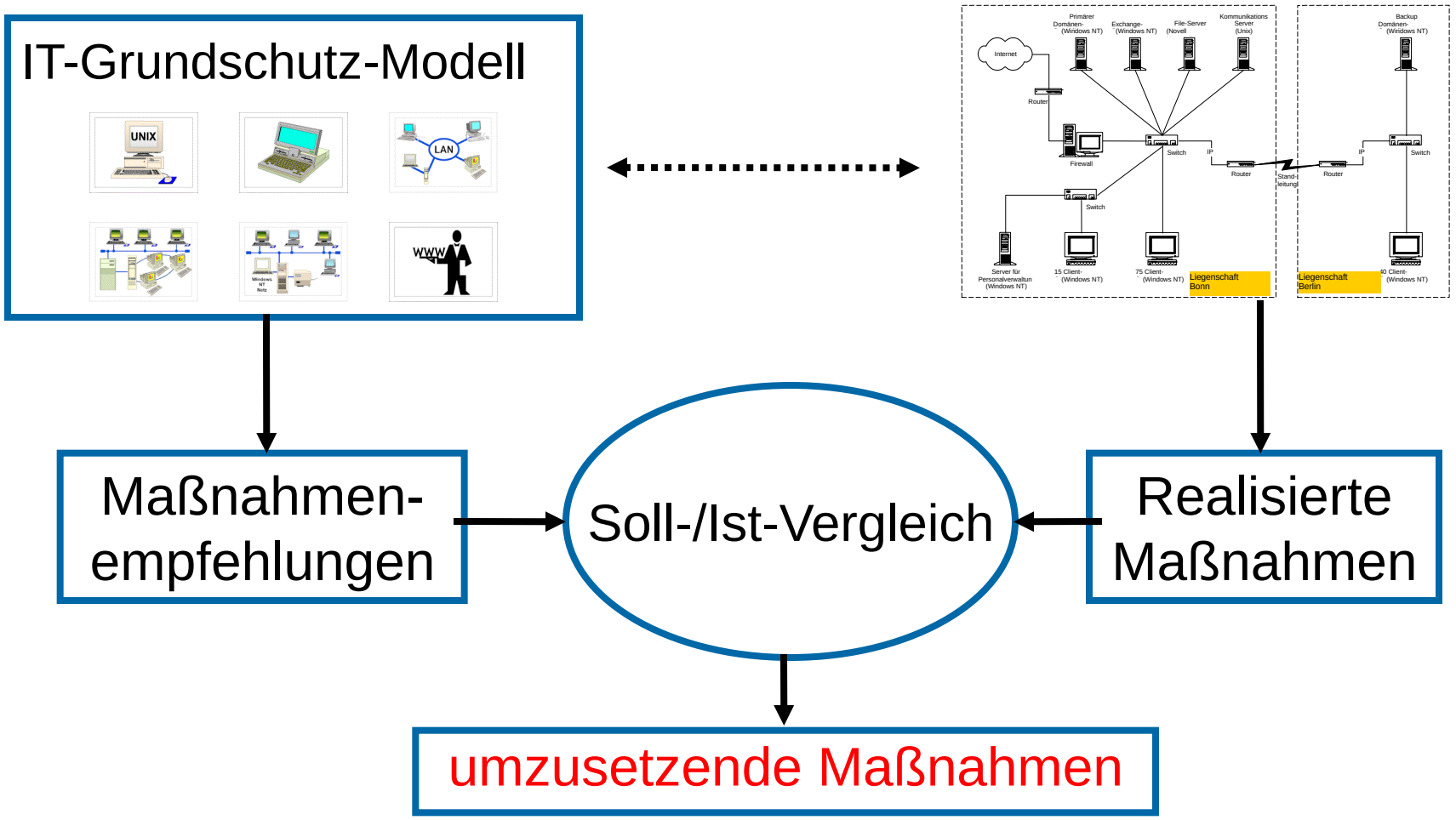
Planung und Konzeption

-	M 2.192	(A)	Erstellung einer IT-Sicherheitsleitlinie
-	M 2.335	(A)	Festlegung der IT-Sicherheitsziele und -strategie
-	M 2.336	(A)	Übernahme der Gesamtverantwortung für IT-Sicherheit durch die Leitungsebene

Umsetzung

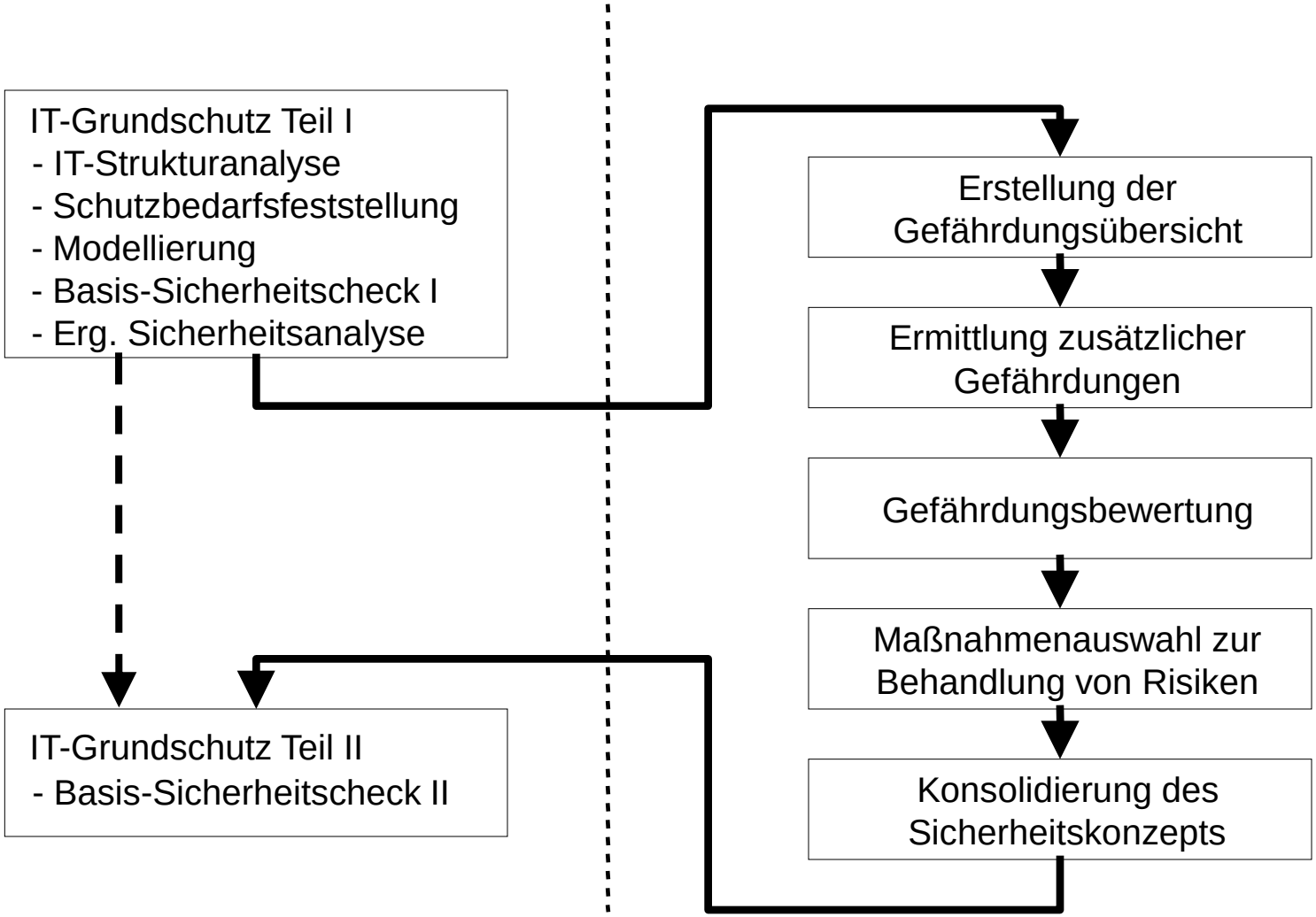
-	M 2.193	(A)	Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit
-	M 2.195	(A)	Erstellung eines IT-Sicherheitskonzepts
-	M 2.197	(A)	Integration der Mitarbeiter in den Sicherheitsprozess
-	M 2.337	(A)	Integration der IT-Sicherheit in organisationsweite Abläufe und Prozesse

Basis-Sicherheitscheck

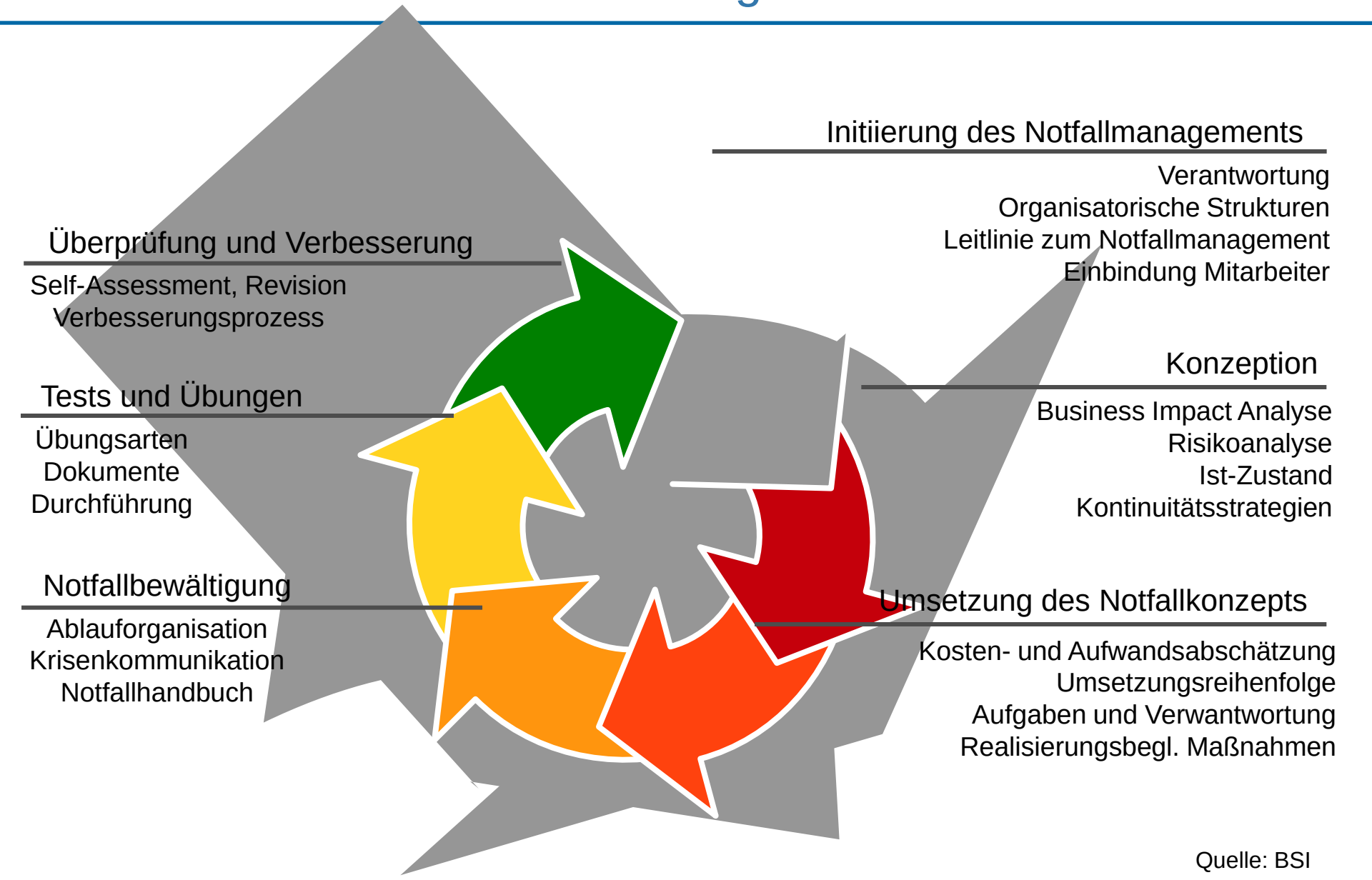


Quelle: BSI

BSI-Standard 100-3
Risikoanalyse



BSI-Standard 100-4
Notfallmanagement



Quelle: BSI

IT-Grundschutz-Kataloge
15. Ergänzungslieferung

- Beinhaltet
  - Bausteine,
  - Gefährdungen und
  - Maßnahmen
- Verfügbare Versionen:
  - Kostenfreie HTML-Version
  - Kostenfreies Metadatenupdate für GSTOOL
  - Kostenpflichtige gedruckte Version über
  - Bundesanzeiger Verlag
  - Preis 15. EL: 152,00 Euro

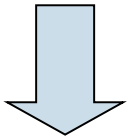
Quelle: BSI

IT-Grundschutz-Modernisierung

Modernisierung IT-Grundschutz
Anlass der GS-Modernisierung

- Vielfältige und schnelllebige Entwicklungen im IT-Bereich
- Umfang der IT-Grundschutz-Kataloge stark gewachsen
- Fundamentale Neuerungen in der IT
- Virtualisierung, Cloud Computing, Mobile Endgeräte, Bring Your Own Device (ByoD)
- Zunehmende Vernetzung von ICS-Systemen mit klassischer IT
- Kritische und dynamische Bedrohungslage
- Hohe Professionalität und Komplexität der Angriffe

Verfügbare Ressourcen in Institutionen wachsen nicht im gleichen Rahmen



Grundlegende Anpassung des Informationssicherheitsmanagement erforderlich

Ziele der IT-Grundschutz-Modernisierung

- Schnellere Bereitstellung von Inhalten/Empfehlungen (Aktualität)
- Bessere Strukturierung und Verschlankung der IT-Grundschutz-Kataloge
- Skalierbarkeit an Größe und Schutzbedarf der Institution
- Integration von industrieller IT und von Detektionsprozessen

Bausteine

- weniger umfangreich
- Anforderungen klarer herausgearbeitet
- Gegliedert in Basis-, Standard- und Hochsicherheits-Anforderungen

20 Jahre IT-Grundschutz – und nun?

- Neue Anforderungen nach 20 Jahren
- Optimierung und Aktualisierung der Vorgehensweise und IT-Grundschutz-Kataloge
- Bedarf der Anwender an aktuellen und praxisnahen Verfahren
- Gewährleistung der Kontinuität:

  Weiterentwicklung der „alten“ IT-Grundschutz-Welt

  Neuausrichtung durch (größtenteils) separate Ressourcen

- Übergeordnetes Ziel: Erhöhung der Attraktivität und Wegbereitung für die nächsten 20 Jahre

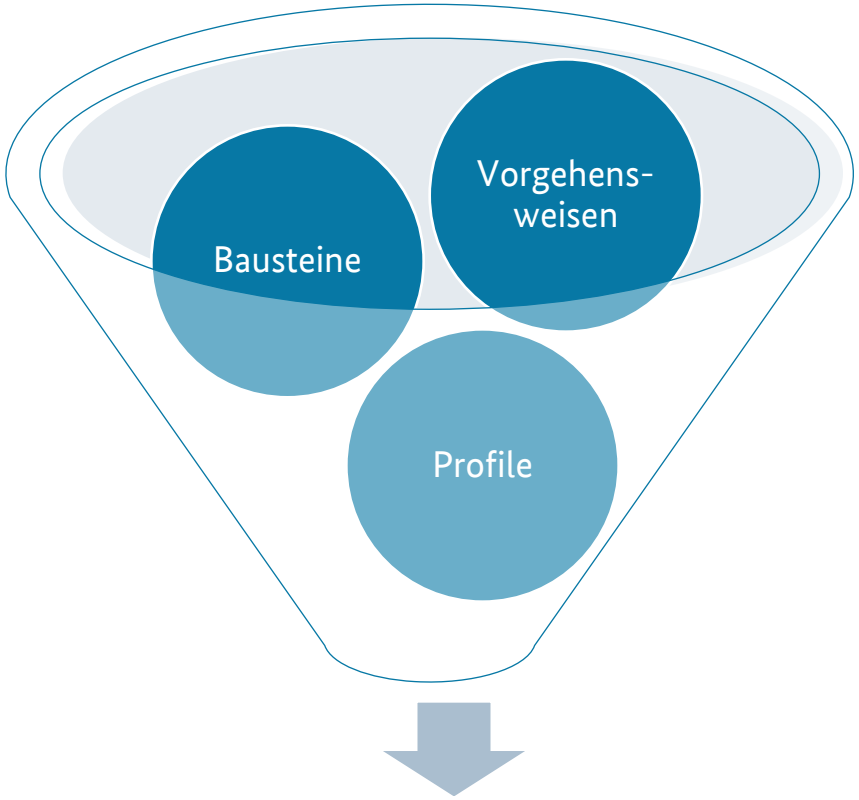
Abstimmung in Findungsphase

Analyse und Diskussion in mehreren Workshops

- 10.09.2013: IT-SiBe-Treffen
- 12.02.2014: BSI-interner Workshop
- 25.02.2014: GS-Auditorentag
- 11.03.2014: CeBIT-Diskussion
- 30.04.2014: mit Auditoren
- 07.05.2014: mit Auditoren
- 13.05.2014: mit Tool-Herstellern
- 22.05.2014: mit Ressort-IT-SiBes des Bundes
- 27.05.2014: mit Power-Usern
- 06.10.2014: IT-SiBe-Tagung der Länder
- 11.11.2014: mit Kommunen
- 28.01.2015: mit Tool-Herstellern
- 18.03.2015: CeBIT-Diskussion
- 29.04.2015: BSI-interner Workshop
- 30.04.2015: mit Anwendern (II)
- 05.05.2015: mit Anwendern (II)
- 24.06.2015: mit Länder-Vertretern
- 24.07.2015: BSI-interner Workshop
- 12.11.2015: mit Tool-Herstellern
- 26./27.11.2015: mit Länder-Vertretern
- 04.12.2015: mit DACHL
- 25.01.2016: mit Kommunen

… und in unzähligen weiteren Terminen

Modernisierung
Kernpunkte



„Modernisierter“
IT-Grundschutz

Quelle: BSI

Vorgehensweisen

Vorgehensweisen
Einstieg

Entscheidung der Leitungsebene, die Informationssicherheit zu verbessern

Benennung des Verantwortlichen für Informationssicherheit

Konzeption und Planung des Einstiegs in Informationssicherheit

- Ermittlung Rahmenbedingungen
- Formulierung allgemeiner Sicherheitsziele
- Bestimmung des angestrebten Sicherheitsniveaus

Ersterfassung

- Von Geschäftsprozessen/Fachaufgaben, Anwendungen und IT-Systemen

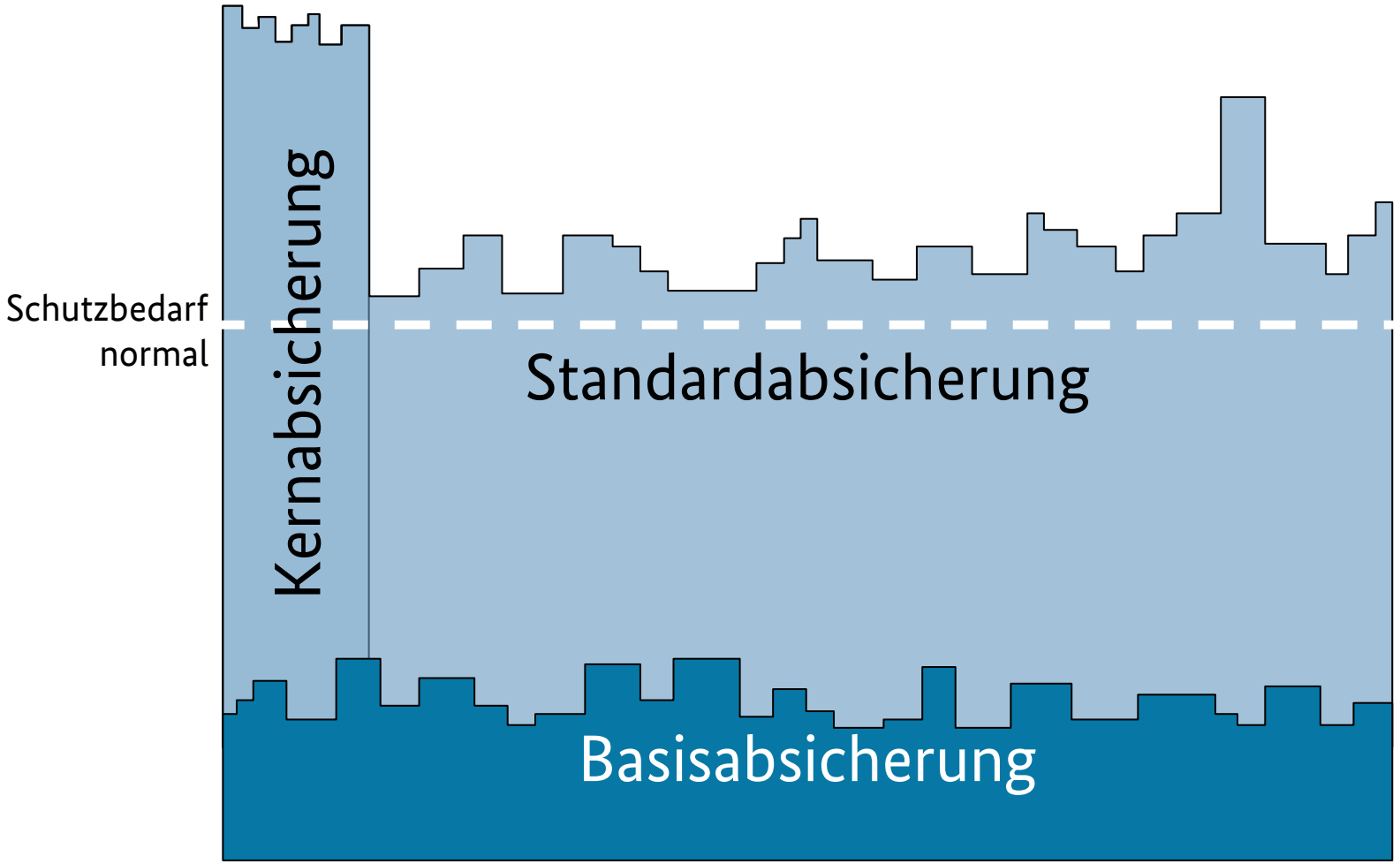
Entscheidung über weitere Vorgehensweise

- Legt Geltungsbereich fest

Quelle: BSI

Vorgehensweisen

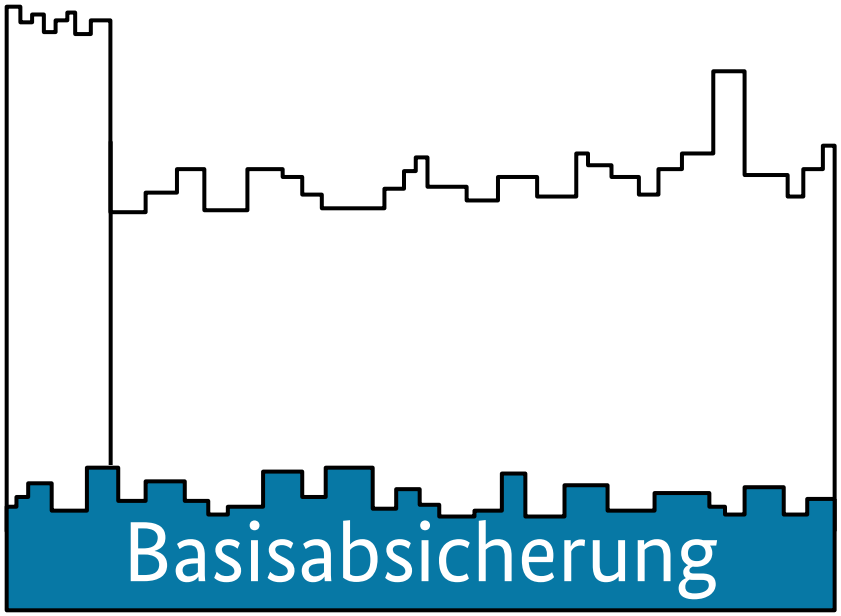
Überblick



Quelle: BSI

Vorgehensweisen
Basisabsicherung

- Vereinfachter Einstieg in das Sicherheitsmanagement
- Grundlegende Erstabsicherung der Geschäftsprozesse und Ressourcen
  - Erstabsicherung in der Breite
  - Umsetzung essentieller Anforderungen
- Auf die Bedürfnisse von KMUs zugeschnitten
- Auch für kleine Institutionen geeignet

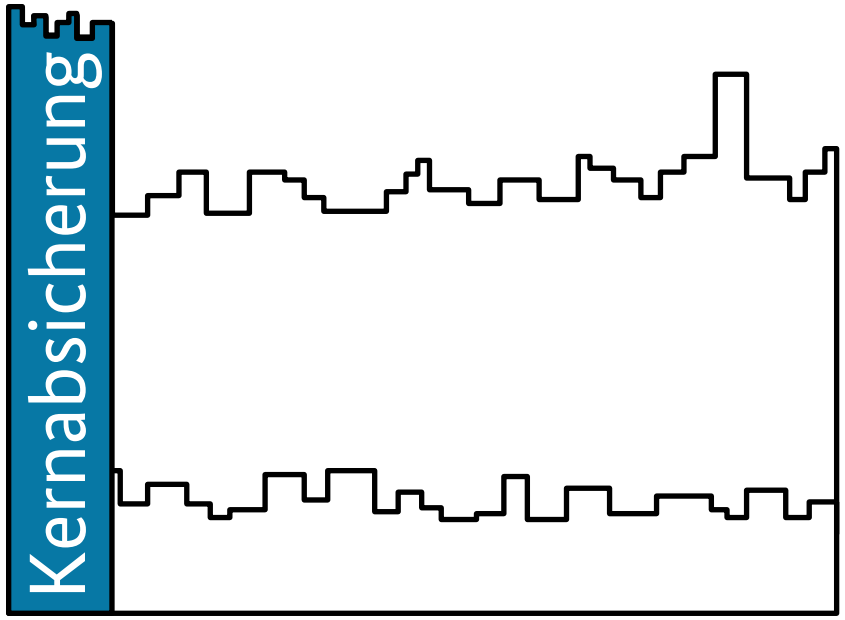


Quelle: BSI

Vorgehensweisen
Kernabsicherung

- Schutz herausragender, besonders gefährdeter Geschäftsprozesse und Ressourcen (Kronjuwelen)
- Unterschied zu IT-Grundschutz Classic: Fokussierung auf einen kleinen, aber sehr wichtigen Informationsverbund

- Zeitersparnis im Vorgehen
- beschleunigte Absicherung dieser Ressourcen in der Tiefe



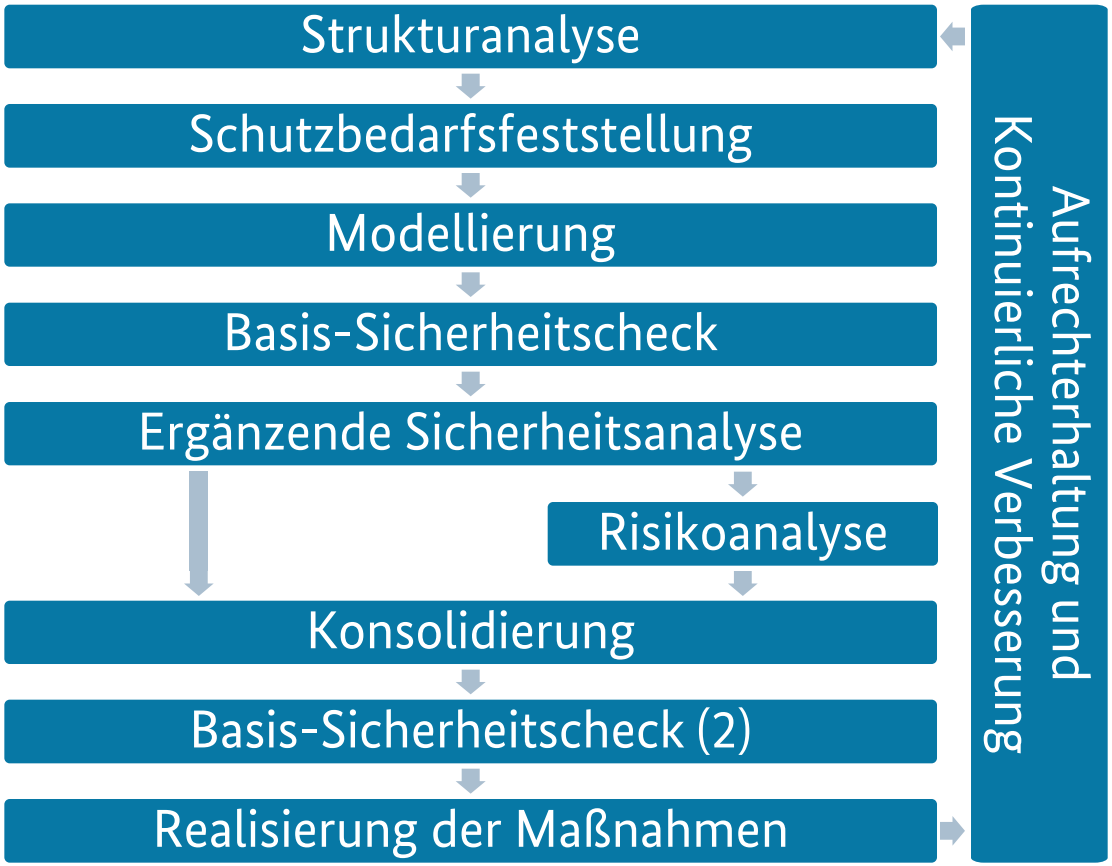
Quelle: BSI

Vorgehensweisen
Standardabsicherung

- Die Methode bleibt in den Grundzügen unverändert
- Implementierung eines vollumfänglichen Sicherheitsprozesses nach (jetzigem) BSI-Standard 100-2
- Weiterhin ISO 27001 Zertifizierung auf der Basis von IT-Grundschutz vorgesehen

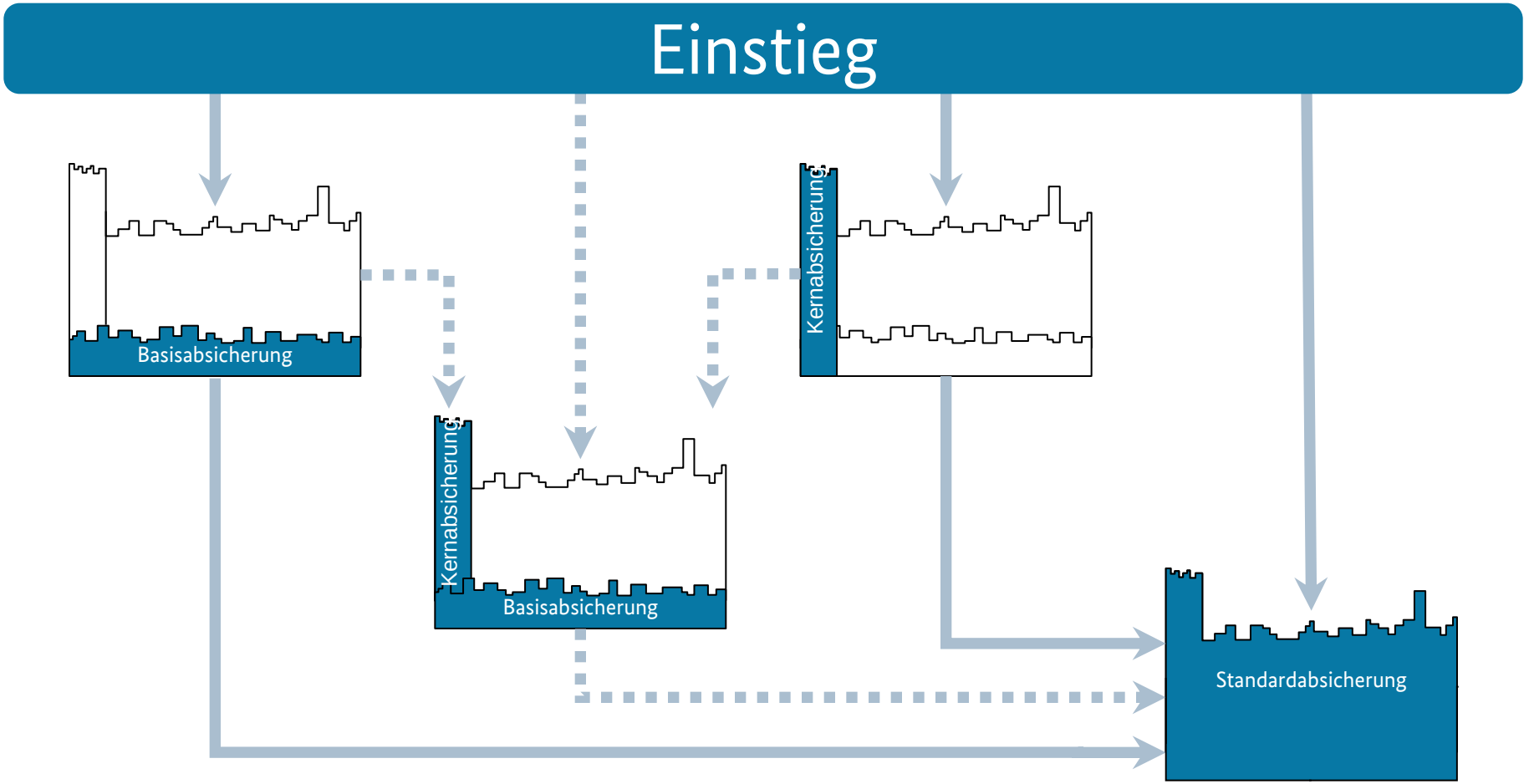
Quelle: BSI

Vorgehensweisen
Standardabsicherung



Quelle: BSI

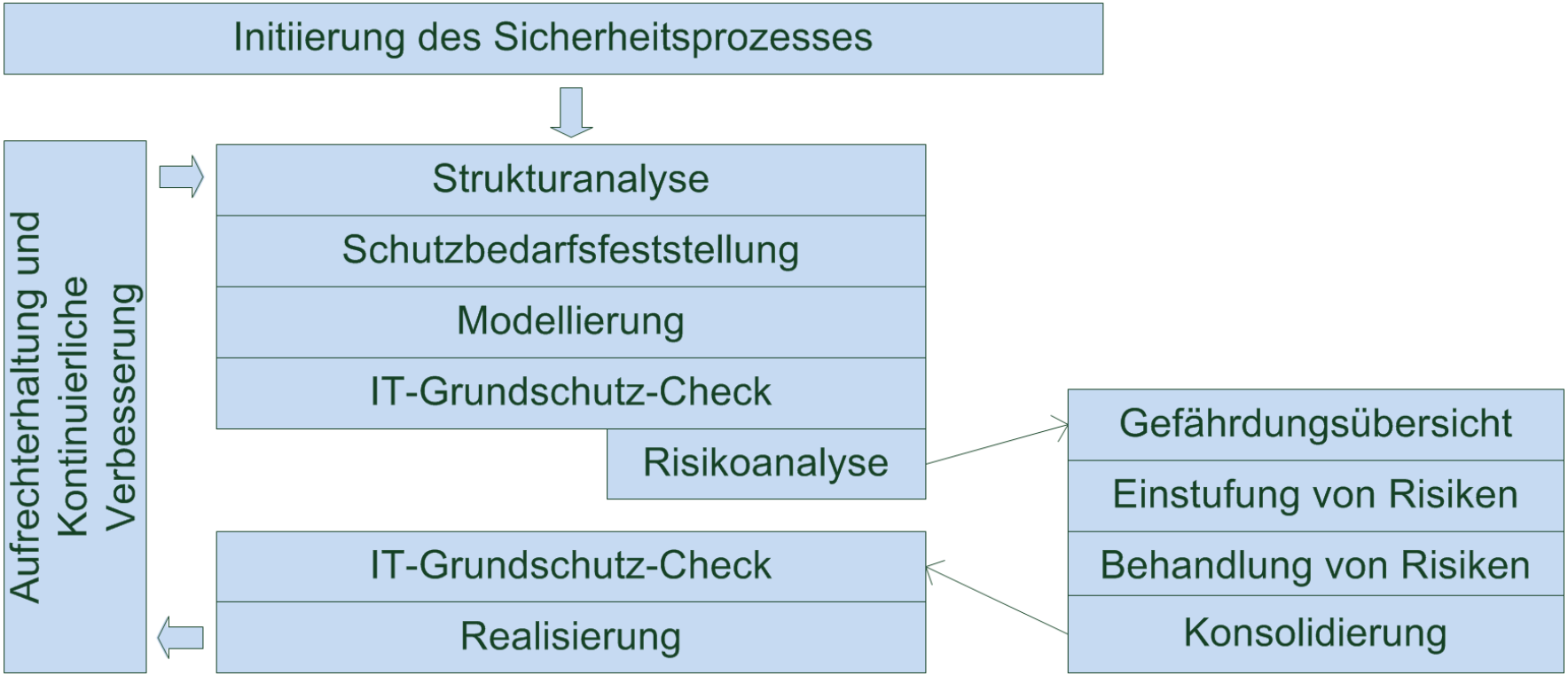
Vorgehensweisen
Wege zur Standardabsicherung



Quelle: BSI

Risikoanalyse nach IT-Grundschutz

BSI-Standard 200-3
Überblick



Quelle: BSI

BSI-Standard 200-3
Risikoanalyse

Bislang:
IT-Grundschutz-spezifisches Verfahren auf der Basis der Gefährdungskataloge

Nun: Bündelung aller risikobezogenen Arbeitsschritte in einem neuen BSI-Standard 200-3

- Implementation eines Risikoentscheidungsprozesses
- Keine Risikoakzeptanz bei den Basis-Anforderungen
- Explizite Möglichkeit der Risikoakzeptanz für Standard-Anforderungen und Anforderungen bei erhöhtem Schutzbedarf

Quelle: BSI

BSI-Standard 200-3
Vorarbeiten

- Strukturanalyse
- Schutzbedarfsfeststellung
- Modellierung
- IT-Grundschutz-Check
- Ergänzende Sicherheitsanalyse

- Geeignete Priorisierung
  - Standard-Absicherung (vorrangig die übergeordneten Zielobjekte bearbeiten)
  - Kern-Absicherung (vorrangig Zielobjekte mit dem höchsten Schutzbedarf bearbeiten)
- Richtlinie zum Umgang mit Risiken

Quelle: BSI

BSI-Standard 200-3
Elementare Gefährdungen

G0-Gefährdungen		
	Gefährdung	Grundwert
G 0.1	Feuer	A
G 0.15	Abhören	C
G 0.16	Diebstahl von Geräten, Datenträgern und Dokumenten	C, A
G 0.18	Fehlplanung oder fehlende Anpassung	C, I, A
G 0.28	Software-Schwachstellen oder –Fehler	C, I, A
G 0.32	Missbrauch von Berechtigungen	C, I, A
G 0.47	Schädliche Seiteneffekte IT-gestützter Angriffe	C, I, A

Quelle: BSI

BSI-Standard 200-3

Erstellung der Gefährdungsübersicht

1. Elementare Gefährdungen

Auszug RECPLAST GmbH

Virtualisierungsserver S1

Vertraulichkeit: hoch
Integrität: hoch
Verfügbarkeit: hoch

G 0.14 Ausspähen von Informationen Spionage
G 0.15 Abhören
G 0.18 Fehlplanung oder fehlende Anpassung
G 0.19 Offenlegung schützenswerter Informationen
G 0.21 Manipulation von Hard- oder Software
G 0.22 Manipulation von Informationen
G 0.23 Unbefugtes Eindringen in IT-Systeme
G 0.25 Ausfall von Geräten oder
Usw.

Smart Meter Gateway Administrator

Vertraulichkeit: hoch
Integrität: hoch
Verfügbarkeit: hoch

G 0.18 Fehlplanung oder fehlende Anpassungen
G 0.21 Manipulation von Hard- oder Software
G 0.22 Manipulation von Informationen
G 0.23 Unbefugtes Eindringen in IT-Systeme
G 0.25 Ausfall von Geräten oder Systemen
G 0.28 Software-Schwachstellen oder –Fehler
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
G 0.43 Einspielen von Nachrichten
Usw.

Quelle: BSI

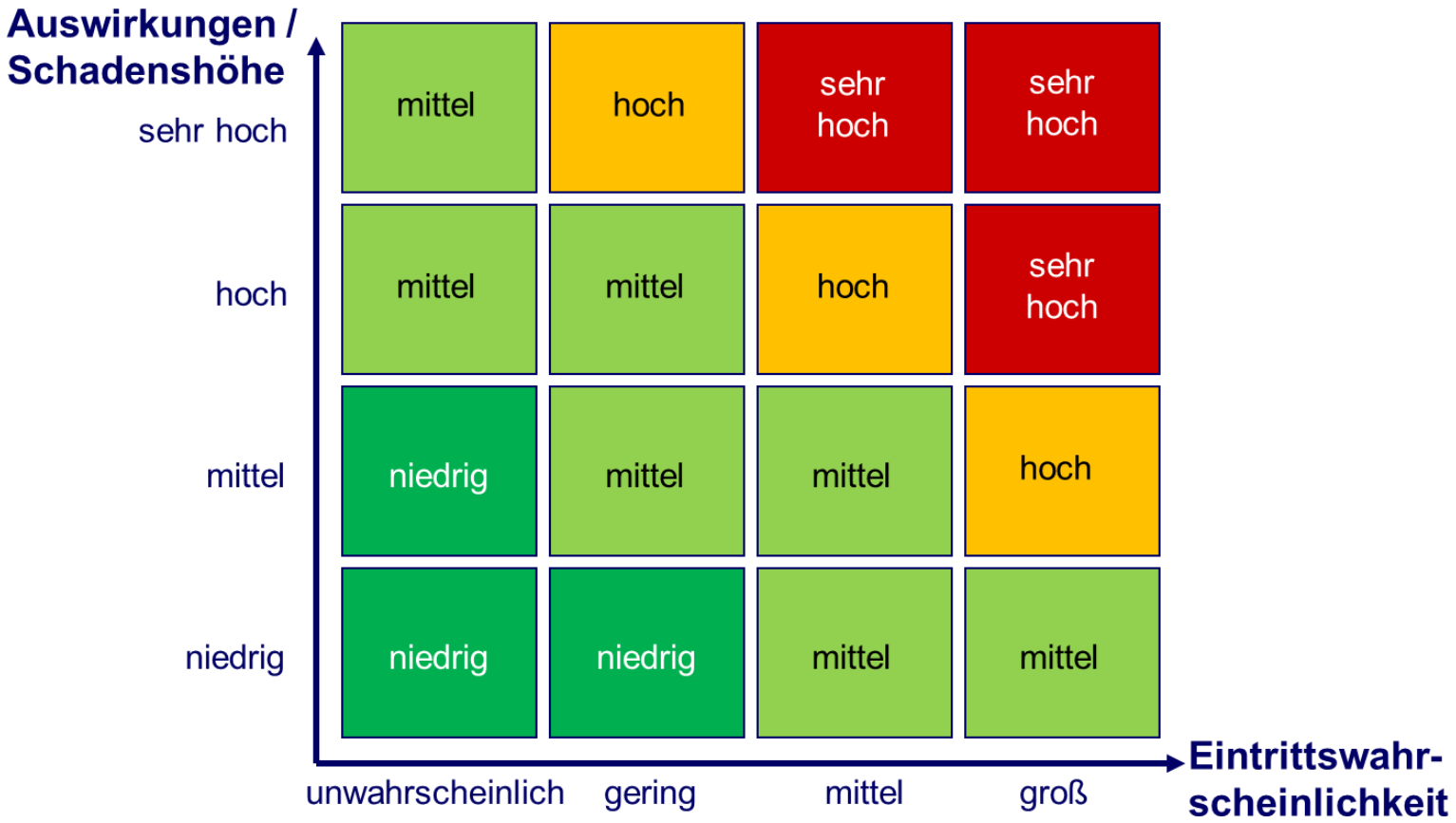
BSI-Standard 200-3
Erstellung der Gefährdungsübersicht

Zusätzliche Gefährdungen

- Moderiertes Brainstorming mit klarem Auftrag und Zeitbegrenzung
- Gefährdungen, die nicht in den IT-Grundschutz-Katalogen aufgeführt sind
- Realistische Gefährdungen mit nennenswerten Schäden
- 3 Grundwerte berücksichtigen
- Höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen, Außen-/Innentäter
- Externe Quellen einbeziehen

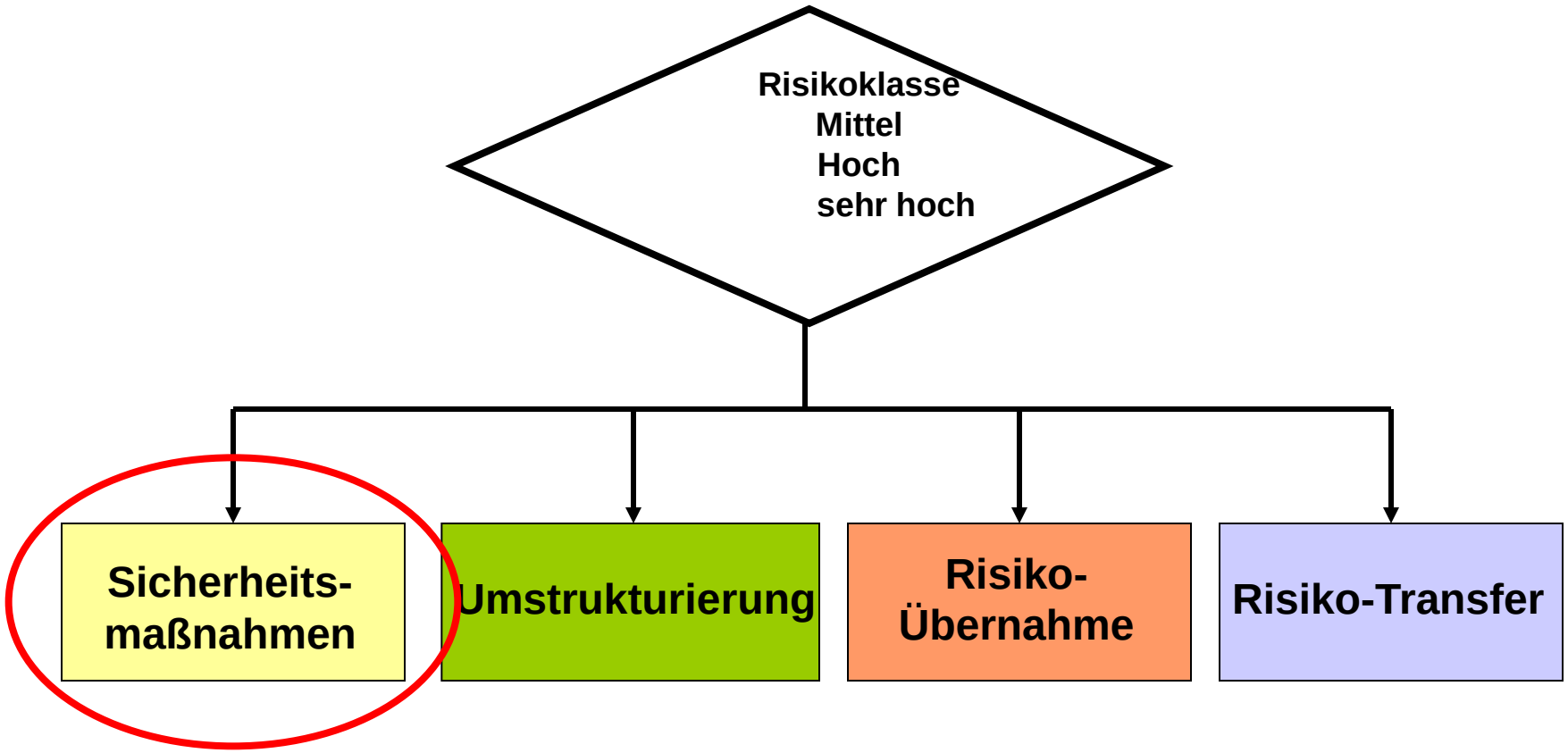
Quelle: BSI

BSI-Standard 200-3
Bewertungsverfahren



Quelle: BSI

BSI-Standard 200-3
Risikobehandlung



BSI-Standard 200-3
Konsolidierung

- Sind die Sicherheitsmaßnahmen zur Abwehr der jeweiligen Gefährdungen geeignet?
- Wirken die Sicherheitsmaßnahmen sinnvoll zusammen?
- Welche IT-Grundschutzmaßnahmen werden durch höher- oder gleichwertige Maßnahmen ersetzt?
- Sind die Sicherheitsmaßnahmen benutzerfreundlich?
- Sind die Sicherheitsmaßnahmen angemessen?

- Verpacken der neu gefundenen Gefährdungen und Anforderungen in einem benutzerdefinierten Baustein
- Ggf. Ergänzung bestehender Bausteine um aus der Risikobewertung ermittelten Anforderungen

Quelle: BSI

IT-Grundschutz-Kompendium

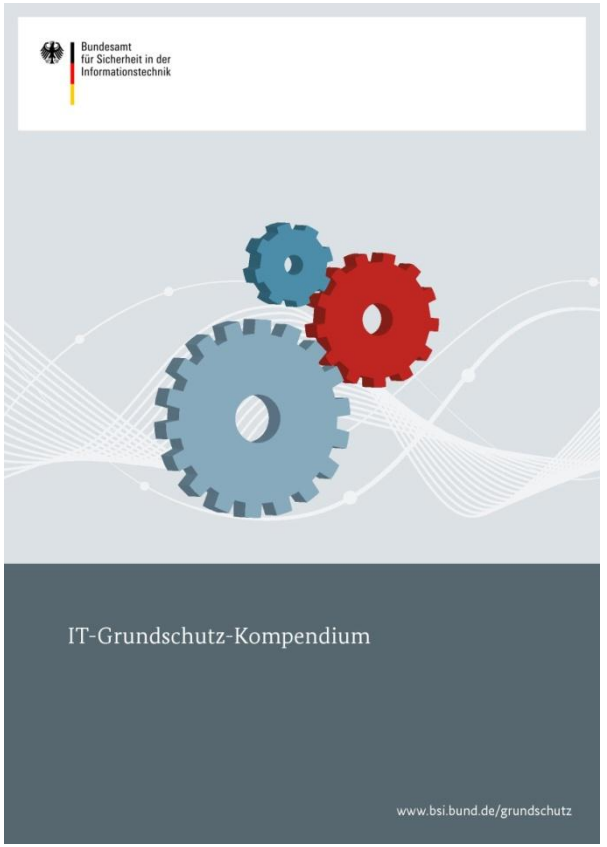
IT-Grundschutz-Kompendium
Überblick

- IT-Grundschutz-Kataloge bisher:
  - Baustein-Kataloge
  - Gefährdungs-Kataloge
  - Maßnahmen-Kataloge
- Neu: IT-Grundschutz-Kompendium
  - Einführung in die IT-Grundschutz-Methodik
  - Modellierung
  - Bausteine
  - Elementare Gefährdungen

- Neue Strukturen
- Andere Inhalte
- Neuer Name

Quelle: BSI

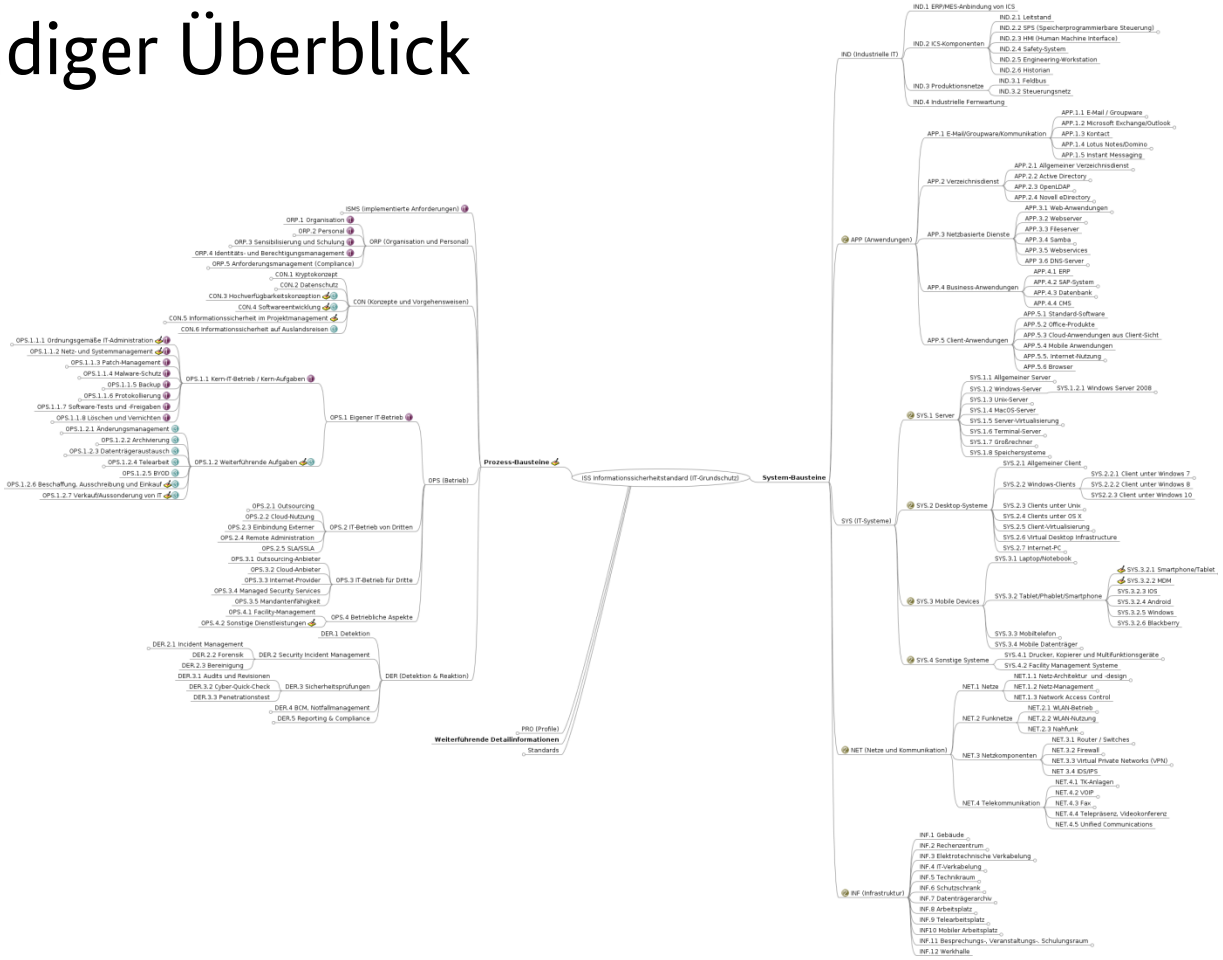
IT-Grundschutz-Kompendium
Überblick



Quelle: BSI

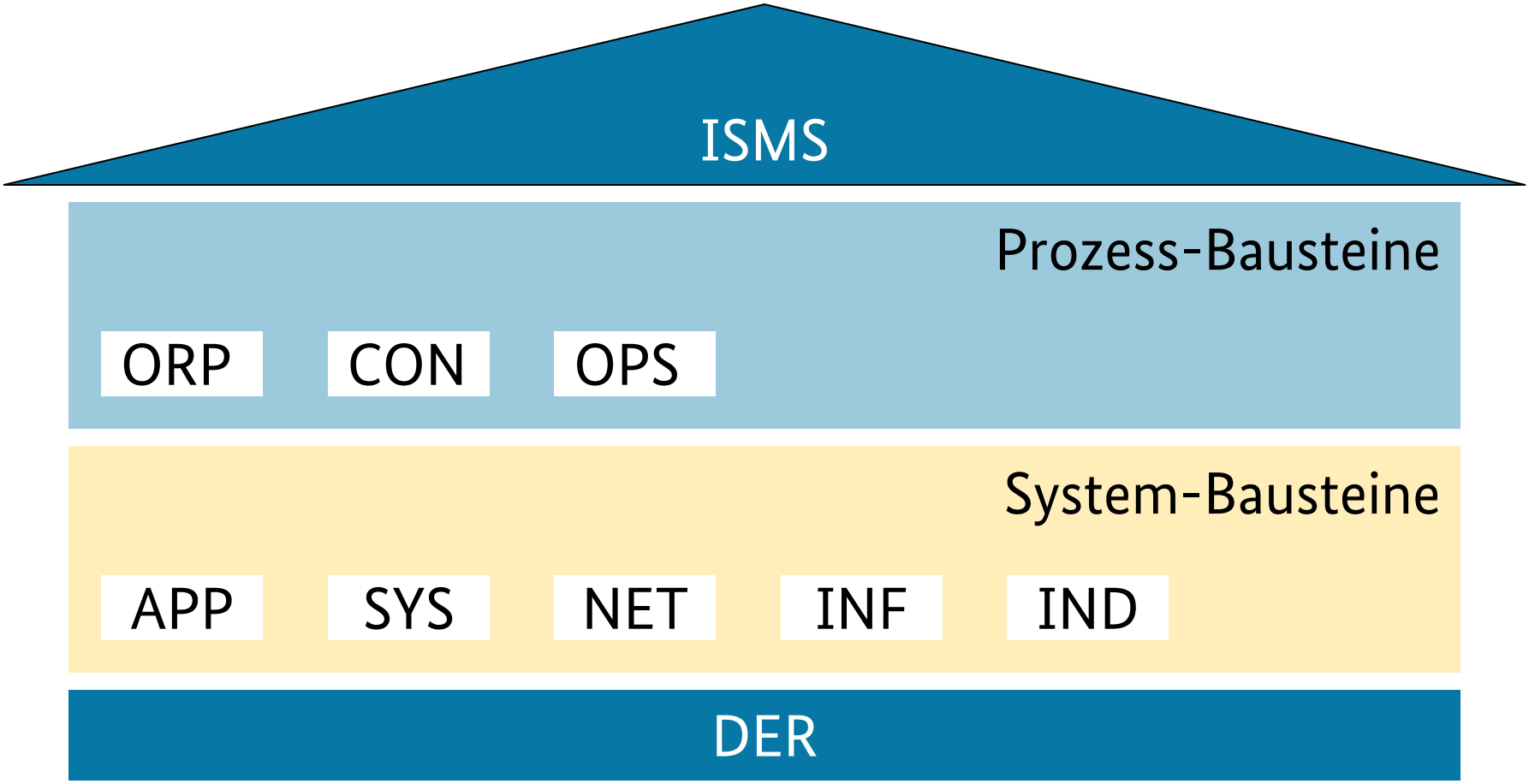
Struktur des IT-Grundschutz-Kompendiums

Vollständiger Überblick



Quelle: BSI

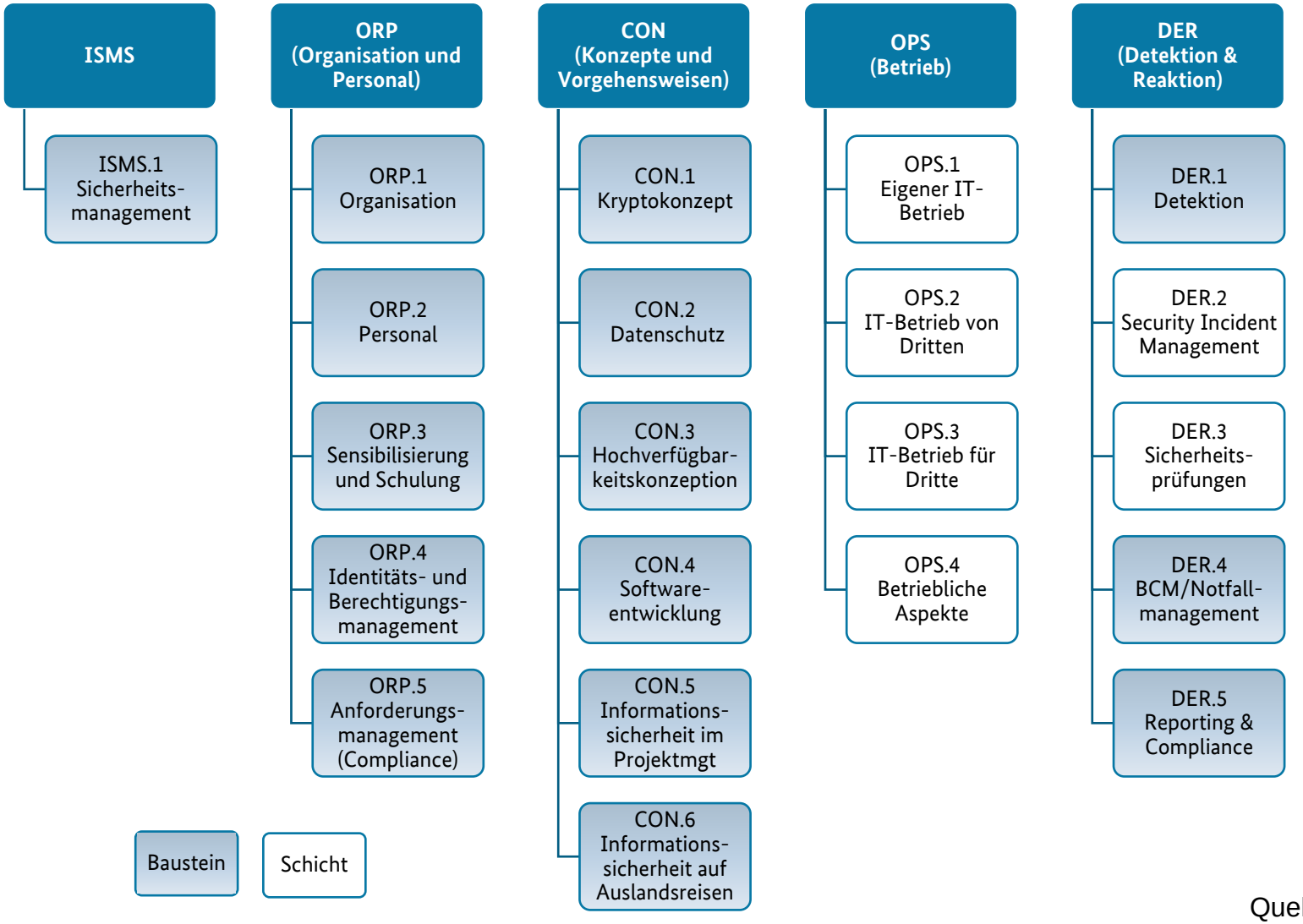
Struktur GS-Kompendium
Nachfolger des Schichtenmodells



Quelle: BSI

Struktur GS-Kompendium

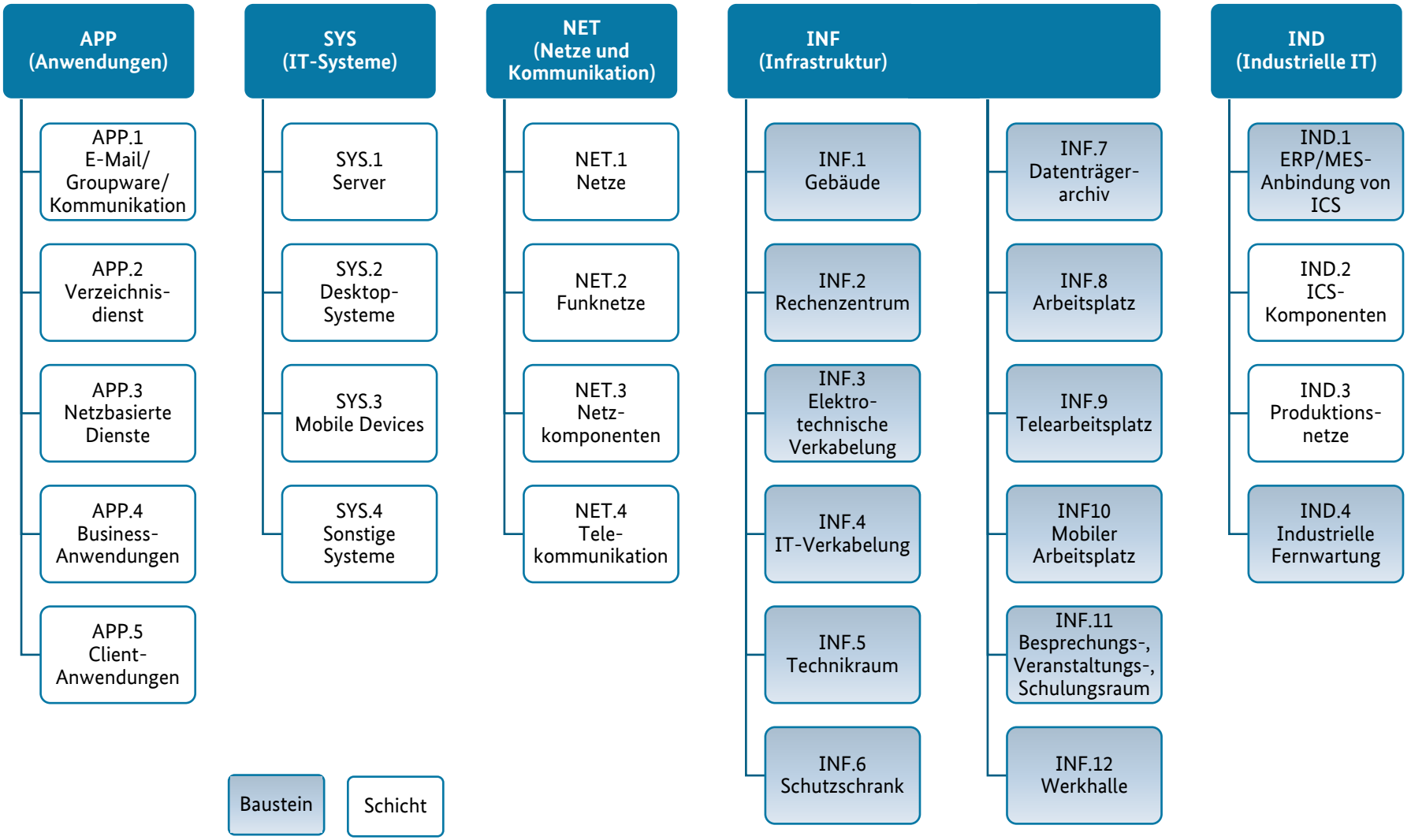
Prozess-Bausteine



Quelle: BSI

Struktur GS-Kompendium

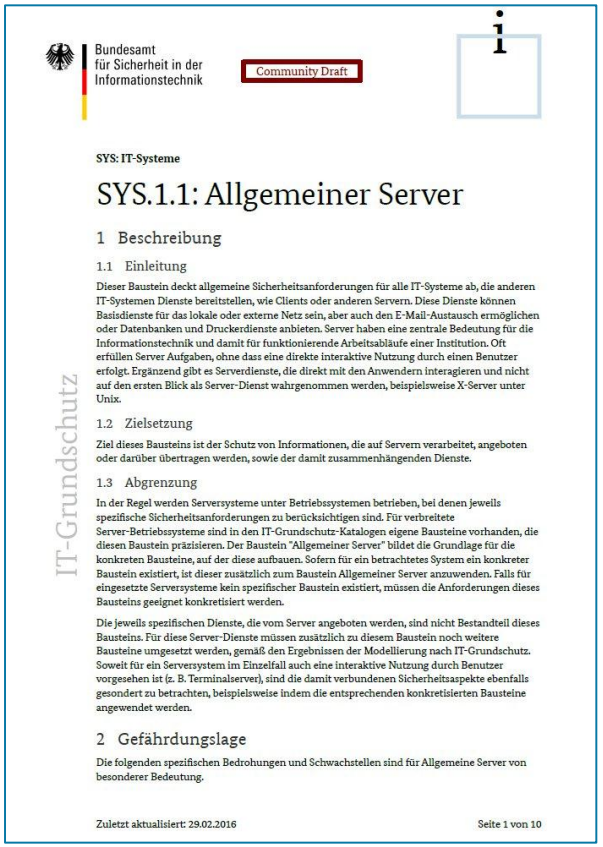
System-Bausteine



Bausteine GS-Kompendium
Dokumentenstruktur

- Umfang: ca. 10 Seiten!
- Beschreibung
  - Einleitung
  - Zielsetzung
  - Abgrenzung
  - Verantwortliche
- Spezifische Gefährdungslage
- Anforderungen (keine Maßnahmen)
  - Basis-Anforderungen
  - Standard-Anforderungen
  - Anforderungen bei erhöhtem Schutzbedarf
- Referenzen auf weiterführende Informationen

Anlage: Kreuzreferenztabelle



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

Quelle: BSI

Bausteine GS-Kompendium
Dokumentenstruktur

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

SYS.1.1.A1 Geeignete Aufstellung [Haustechnik]

Server MÜSSEN an Orten betrieben werden, zu denen nur berechtigte Personen Zutritt haben. Server sollten daher grundsätzlich in Rechenzentren, Rechnerräumen oder abschließbaren Serverschränken aufgestellt beziehungsweise eingebaut werden, siehe hierzu die entsprechenden Bausteine. Es MUSS geregelt werden, wer Zutritt zu den Räumen beziehungsweise Zugriff auf die Server selbst erhält. Server DÜRFEN NICHT als Arbeitsplatzrechner genutzt werden.

Es MUSS auf eine geeignete räumliche Trennung der Systeme, die gesichert werden sollen, von den sichernden Systemen, etwa Backup-Servern, geachtet werden, um die Auswirkungen bei einem physischen Schaden zu begrenzen.

Quelle: BSI

Bausteine GS-Kompendium
Dokumentenstruktur

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für Allgemeine Server. Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.1.1.A8 Festlegung einer Sicherheitsrichtlinie für einen Allgemeinen Server

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die Anforderungen an allgemeine Server konkretisiert werden. Die Richtlinie SOLLTE allen Administratoren und anderen Personen, die an der Beschaffung und dem Betrieb der Servers beteiligt sind, bekannt sein und Grundlage für deren Arbeit sein. Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft und die Ergebnisse SOLLTEN sinnvoll dokumentiert werden.

Quelle: BSI

Bausteine GS-Kompendium
Dokumentenstruktur

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

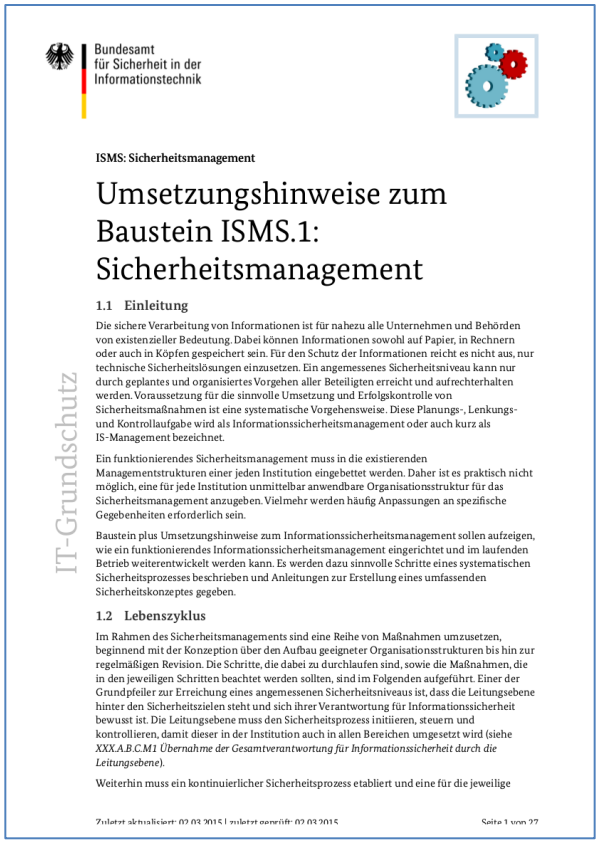
SYS.1.1.A22 Mehr-Faktor-Authentisierung (CIA)

Beim Einsatz von Passwörtern für die Authentisierung besteht grundsätzlich die Gefahr, dass Passwörter weitergegeben, ausgespäht oder von Dritten erraten werden. Bei höherem Schutzbedarf SOLLTE daher eine sichere Zwei- oder Mehr-Faktor-Authentisierung für den Zugang zum Server eingerichtet werden, z. B. mit kryptographischen Zertifikaten, Chipkarten oder Token. Vordringlich SOLLTEN alle administrativen Zugänge zum Server mit Mehr-Faktor-Authentisierung abgesichert werden.

Quelle: BSI

Umsetzungshinweise
Dokumentenstruktur

- Umfang: beliebig
- Gliederung lehnt sich an Bausteine an
- Beschreibung
  - Einleitung
  - Lebenszyklus
- Maßnahmen als Umsetzungshilfen
  - Basis-Maßnahmen
  - Standard-Maßnahmen
  - Maßnahmen bei erhöhtem Schutzbedarf
- Referenzen auf weiterführende Informationen
  - Alte IT-GS-Bausteine, Studien, Herstellerdokumentation etc.



Bundesamt für Sicherheit in der Informationstechnik

ISMS: Sicherheitsmanagement

Umsetzungshinweise zum Baustein ISMS.1: Sicherheitsmanagement

1.1 Einleitung

Die sichere Verarbeitung von Informationen ist für nahezu alle Unternehmen und Behörden von existenzieller Bedeutung. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Für den Schutz der Informationen reicht es nicht aus, nur technische Sicherheitslösungen einzusetzen. Ein angemessenes Sicherheitsniveau kann nur durch geplantes und organisiertes Vorgehen aller Beteiligten erreicht und aufrechterhalten werden. Voraussetzung für die sinnvolle Umsetzung und Erfolgskontrolle von Sicherheitsmaßnahmen ist eine systematische Vorgehensweise. Diese Planungs-, Lenkungs- und Kontrollaufgabe wird als Informationssicherheitsmanagement oder auch kurz als IS-Management bezeichnet.

Ein funktionierendes Sicherheitsmanagement muss in die existierenden Managementstrukturen einer jeden Institution eingebettet werden. Daher ist es praktisch nicht möglich, eine für jede Institution unmittelbar anwendbare Organisationsstruktur für das Sicherheitsmanagement anzugeben. Vielmehr werden häufig Anpassungen an spezifische Gegebenheiten erforderlich sein.

Baustein plus Umsetzungshinweise zum Informationssicherheitsmanagement sollen aufzeigen, wie ein funktionierendes Informationssicherheitsmanagement eingerichtet und im laufenden Betrieb weiterentwickelt werden kann. Es werden dazu sinnvolle Schritte eines systematischen Sicherheitsprozesses beschrieben und Anleitungen zur Erstellung eines umfassenden Sicherheitskonzeptes gegeben.

1.2 Lebenszyklus

Im Rahmen des Sicherheitsmanagements sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über den Aufbau geeigneter Organisationsstrukturen bis hin zur regelmäßigen Revision. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt. Einer der Grundpfeiler zur Erreichung eines angemessenen Sicherheitsniveaus ist, dass die Leitungsebene hinter den Sicherheitszielen steht und sich ihrer Verantwortung für Informationssicherheit bewusst ist. Die Leitungsebene muss den Sicherheitsprozess initiieren, steuern und kontrollieren, damit dieser in der Institution auch in allen Bereichen umgesetzt wird (siehe *XXX.A.B.C.M1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene*).

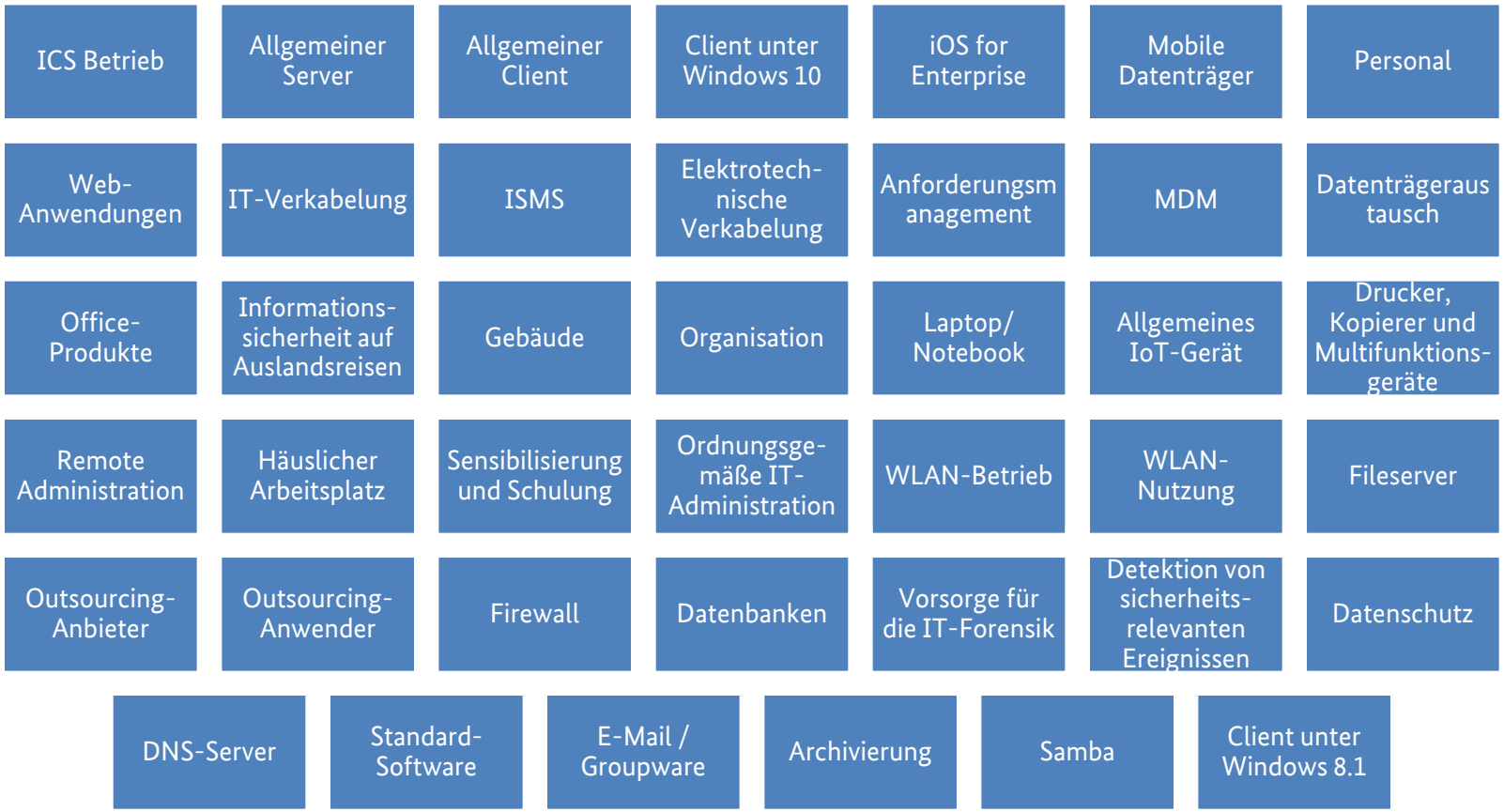
Weiterhin muss ein kontinuierlicher Sicherheitsprozess etabliert und eine für die jeweilige

IT-Grundschutz

Zuletzt aktualisiert: 02.03.2015 | zuletzt geprüft: 02.03.2015 Seite 1 von 27

Quelle: BSI

Veröffentlichungen
Bausteine als Community Draft

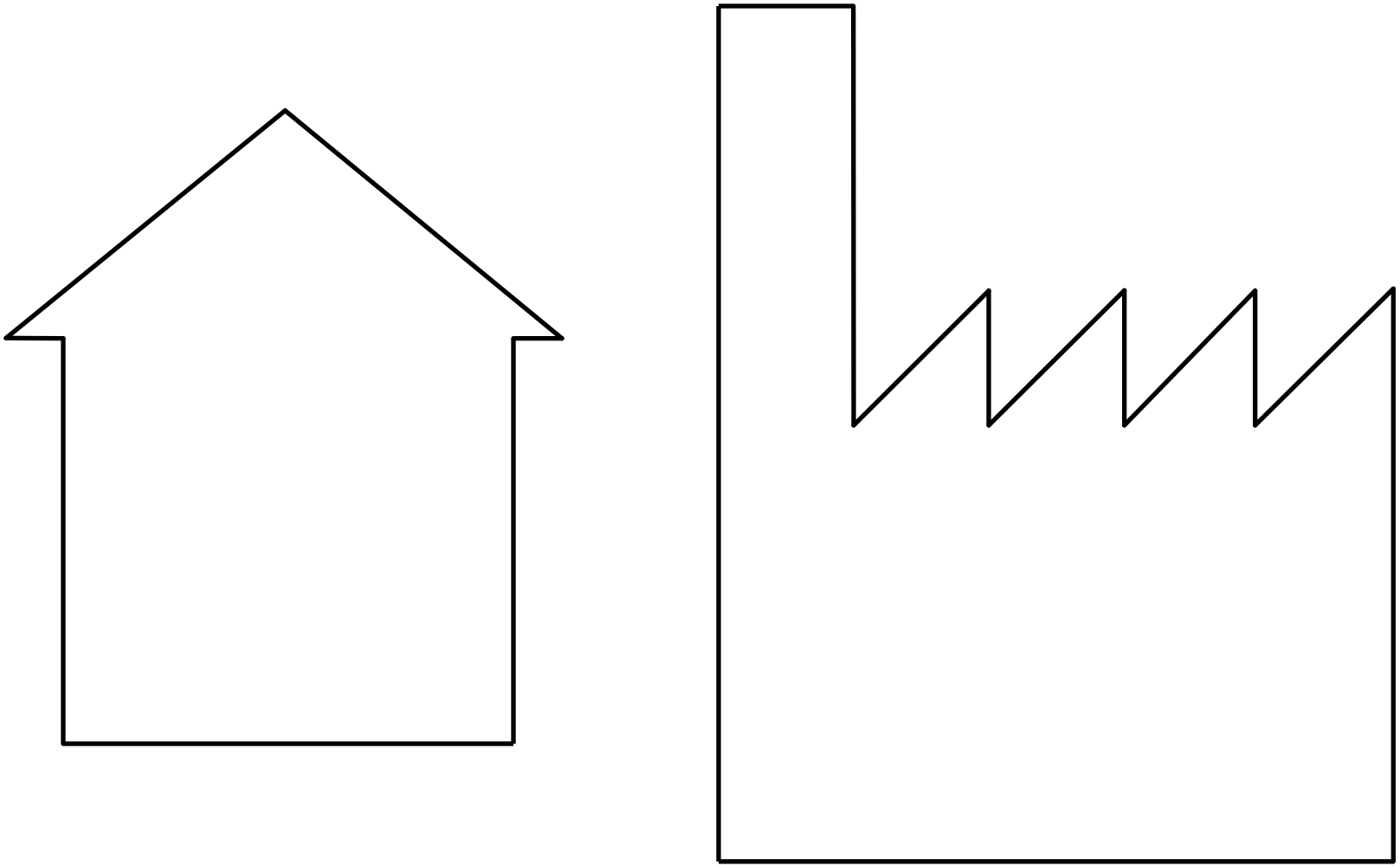


Stand: 21.06.2017

Quelle: BSI

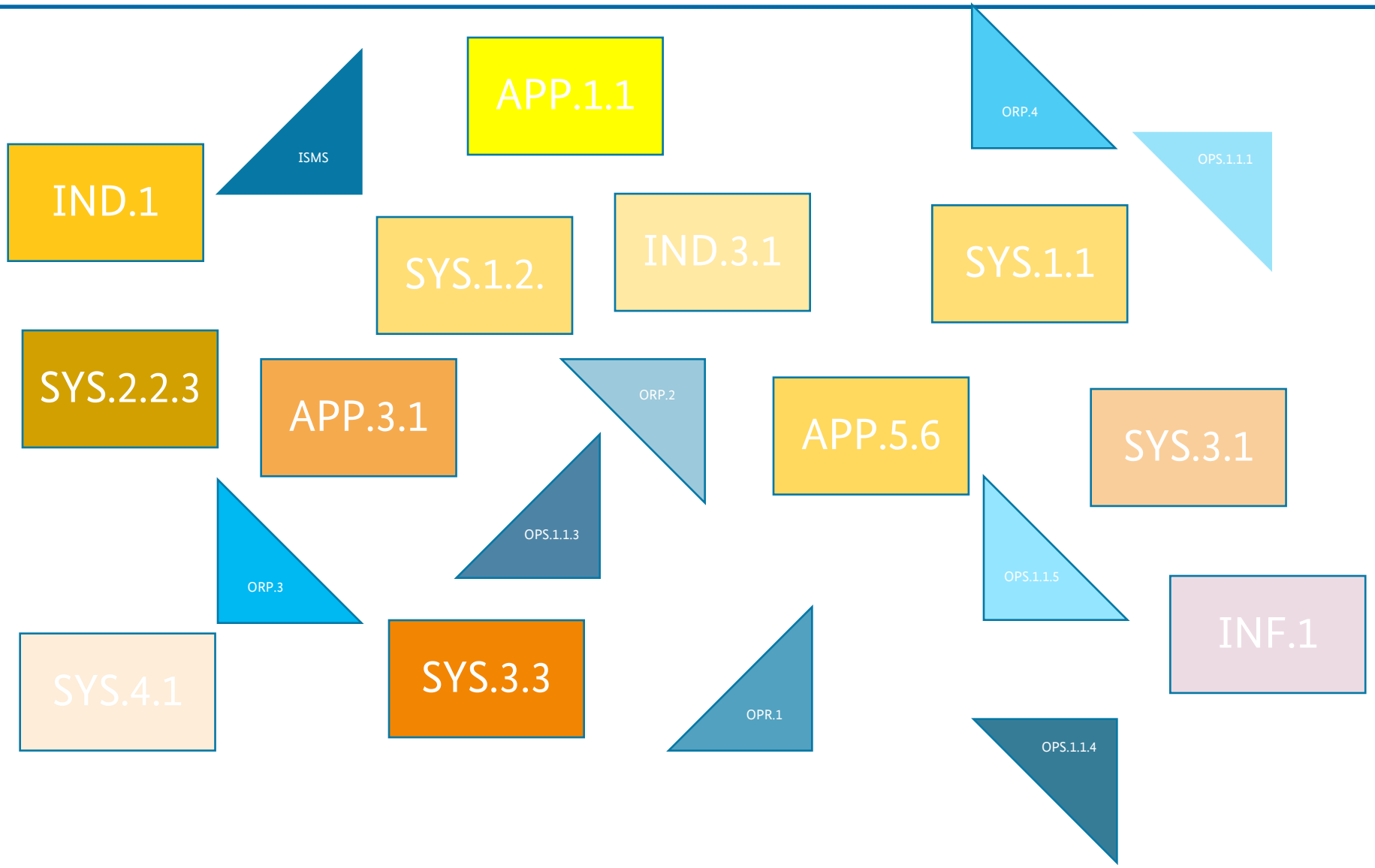
IT-Grundschutz-Profile

IT-Grundschutz-Profile
ein Blick in Institutionen



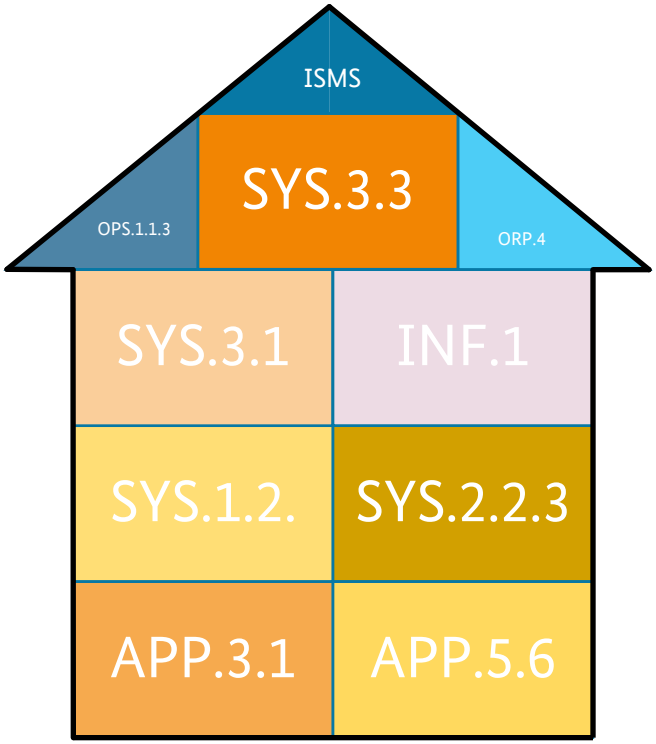
Quelle: BSI

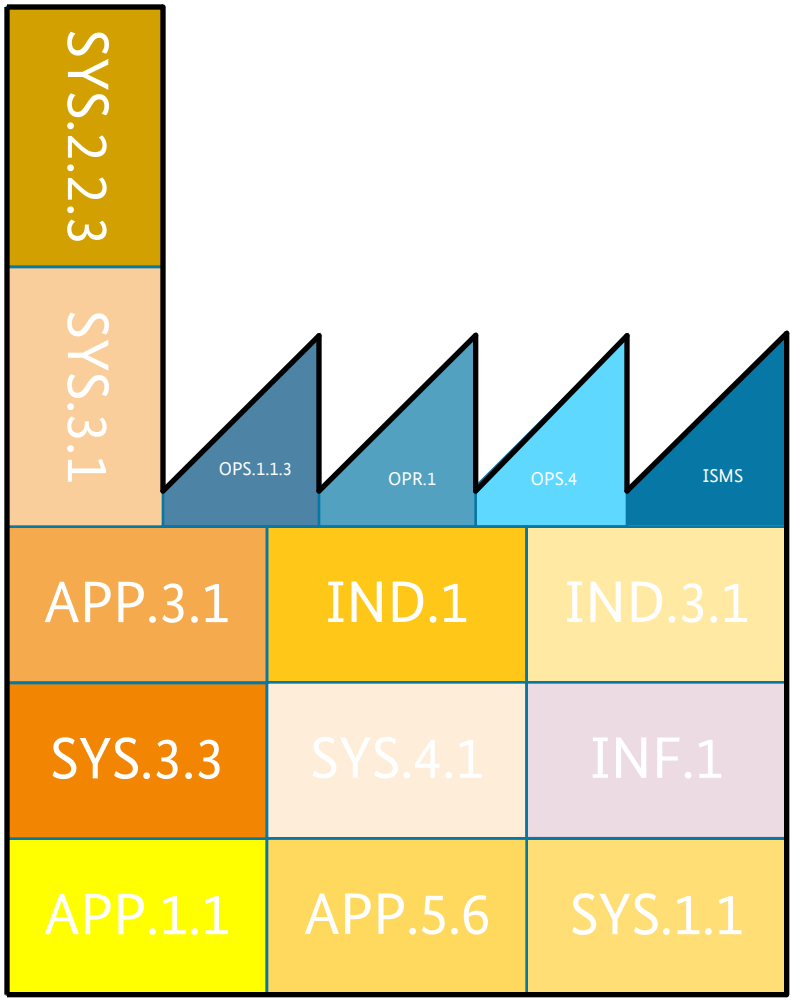
IT-Grundschutz-Profile
ein Blick auf Beispielbausteine



Quelle: BSI

IT-Grundschutz-Profile
Adaption als Schablone





Quelle: BSI

IT-Grundschutz-Profile
Definition

Ein IT-Grundschutz-Profil ist ein Muster-Sicherheitskonzept für ein ausgewähltes Szenario (Verbund oder Prozess), es bereitet

- das Ergebnis mehrerer Prozessschritte der IT-Grundschutz-Vorgehensweise (z.B. Strukturanalyse, Schutzbedarfsfeststellung, Modellierung) und
- einer Auswahl mehrerer Anforderungen der IT-Grundschutz-Bausteine

so auf, dass es als Schablone von ähnlichen Institutionen adaptiert werden kann!

IT-Grundschutz-Profile
Überblick

- Werkzeug für anwenderspezifische Empfehlungen
- Individuelle Anpassungen des IT-Grundschutzes an die jeweiligen Bedürfnisse möglich
- Berücksichtigt Möglichkeiten und Risiken der Institution
- Profile beziehen sich auf typische IT-Szenarien, z.B. Prozesse in Institutionen wie
  - Kommunalverwaltung in Bundesland XY,
  - Krankenhaus
  - Wasserwerk als Kritische Infrastruktur
- Profile werden in der Regel durch Dritte (Verbände, Branchen, ...) und nicht durch das BSI erstellt
- Nicht als BSI-Vorgabe zu verstehen!
- Nachweis für Umsetzung (z. B. Testat) und Anerkennung ausgewählter Profile durch BSI wird diskutiert

Angebote des IT-Grundschutzes

Ergänzung zum BSI-Standard 200-2
Leitfaden zur Basis-Absicherung

Quelle: BSI

BSI-Standards zum IT-Grundschutz

Community Drafts

Quelle: BSI

Vielen Dank für Ihre Aufmerksamkeit!

grundschutz@bsi.bund.de
Tel. +49 (0)22899-9582-5369
Fax +49 (0)22899-10-9582-5369

Bundesamt für Sicherheit in der Informationstechnik
Referat „IT-Grundschutz“
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de