Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Vorstellung des finalen BSI-Standards 200-4 BCM

Organisationale Resilienz und IT-Grundschutz:
Von der Informationssicherheit zur Business Continuity

Daniel Gilles | Referat SZ 13 – BSI-Standards und IT-Grundschutz | 14.06.2023 | Limburg

Was woll(t)en **wir** erreichen?

Als **alleinstehender** Standard anwendbar

Ähnlich zu 200-2: **Stufenmodell**

Stärkere **Synergien** mit 200-x & ITSCM

Kompatibel zur **ISO 22301:2019**

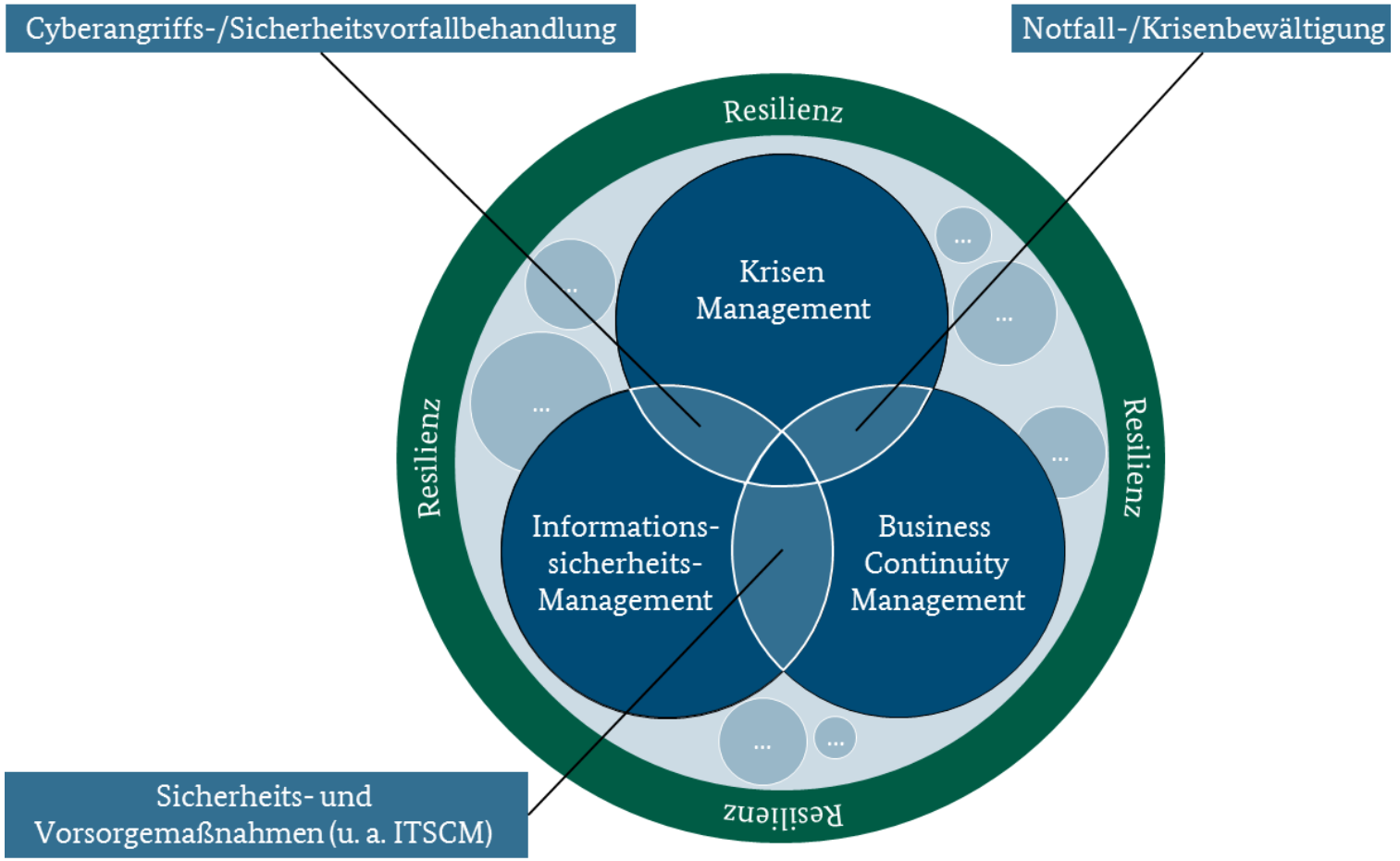
Anleitung mit **Best Practices** zur Etablierung und Aufrechterhaltung sowie **kontinuierlichen Verbesserung** eines institutionsweiten BCMS

Für wen? Institutionen **beliebiger** Art, Branche und Größe

Praxisnah, handhabbar und adaptierbar

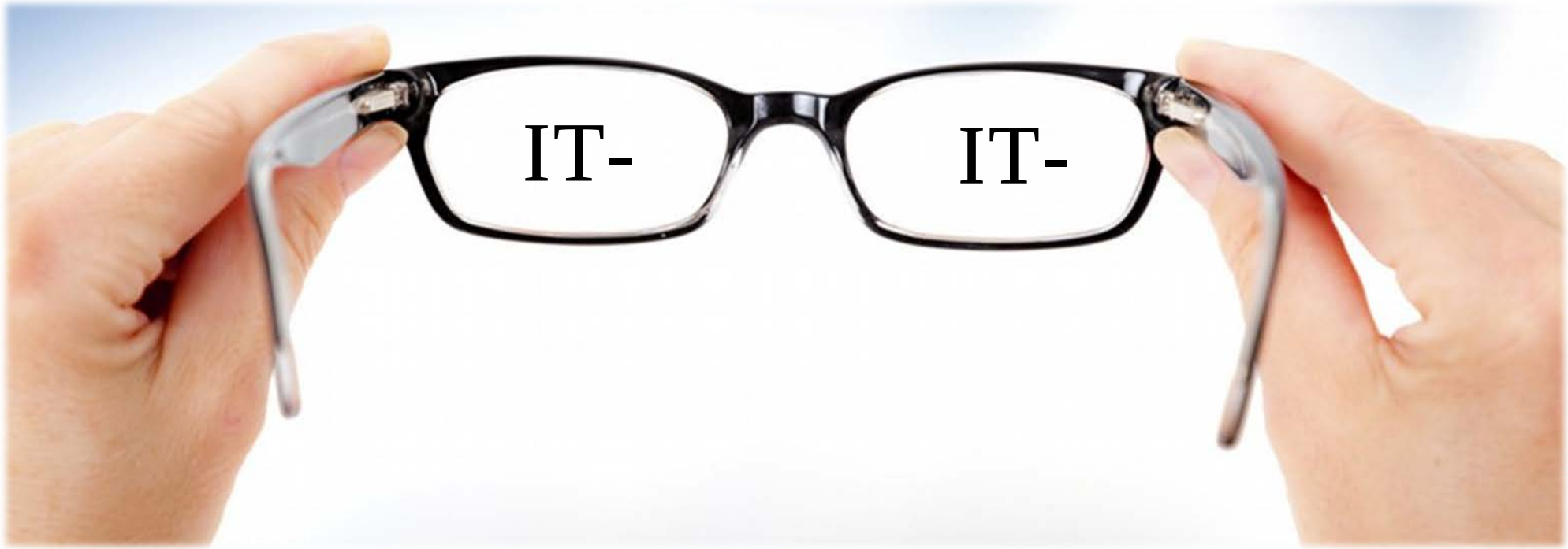
Agenda

1. Basics und grundlegende Begriffe
2. Das Stufenmodell und der BCMS-Prozess
3. Übersicht über wesentliche Neuerungen
4. Veröffentlichung des Standards
5. Zeit für Ihre Fragen



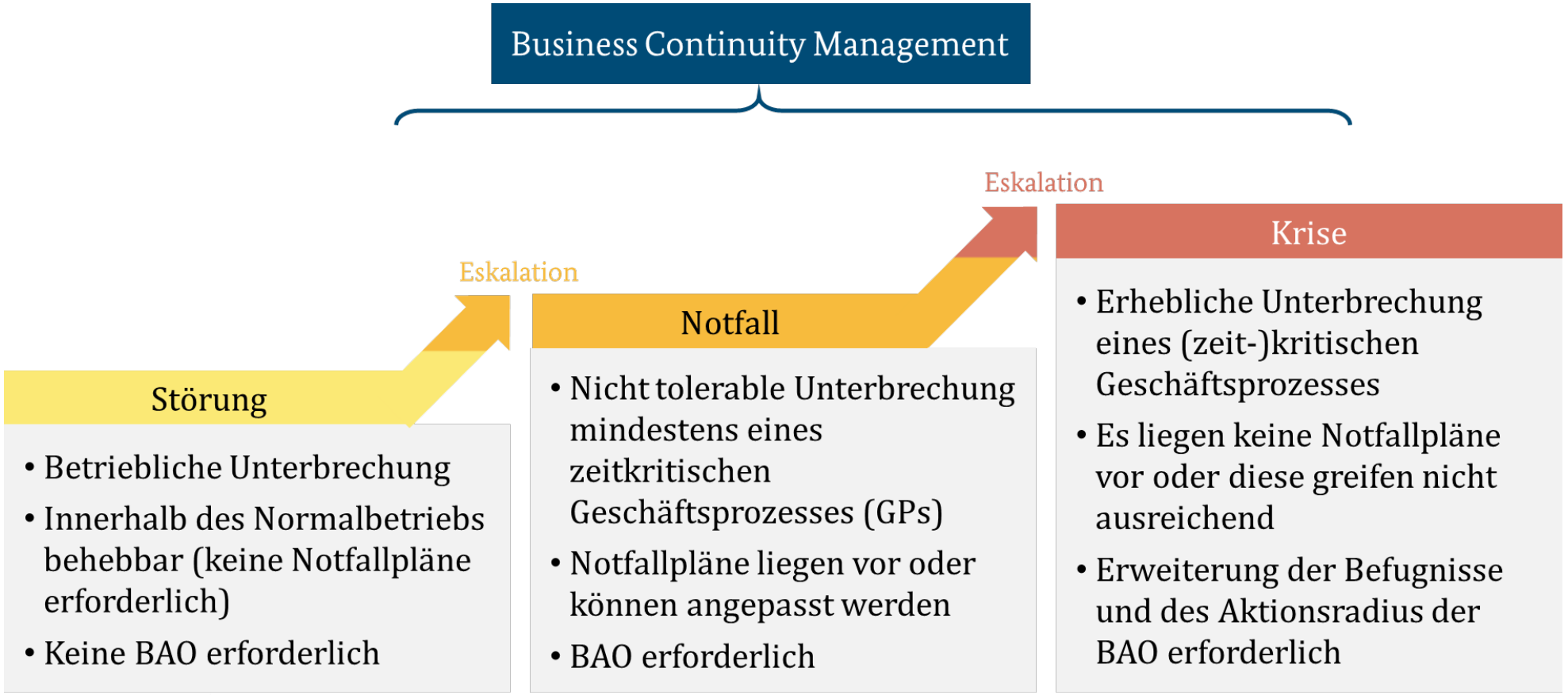
Basics und grundlegende Begriffe

Vorbemerkung

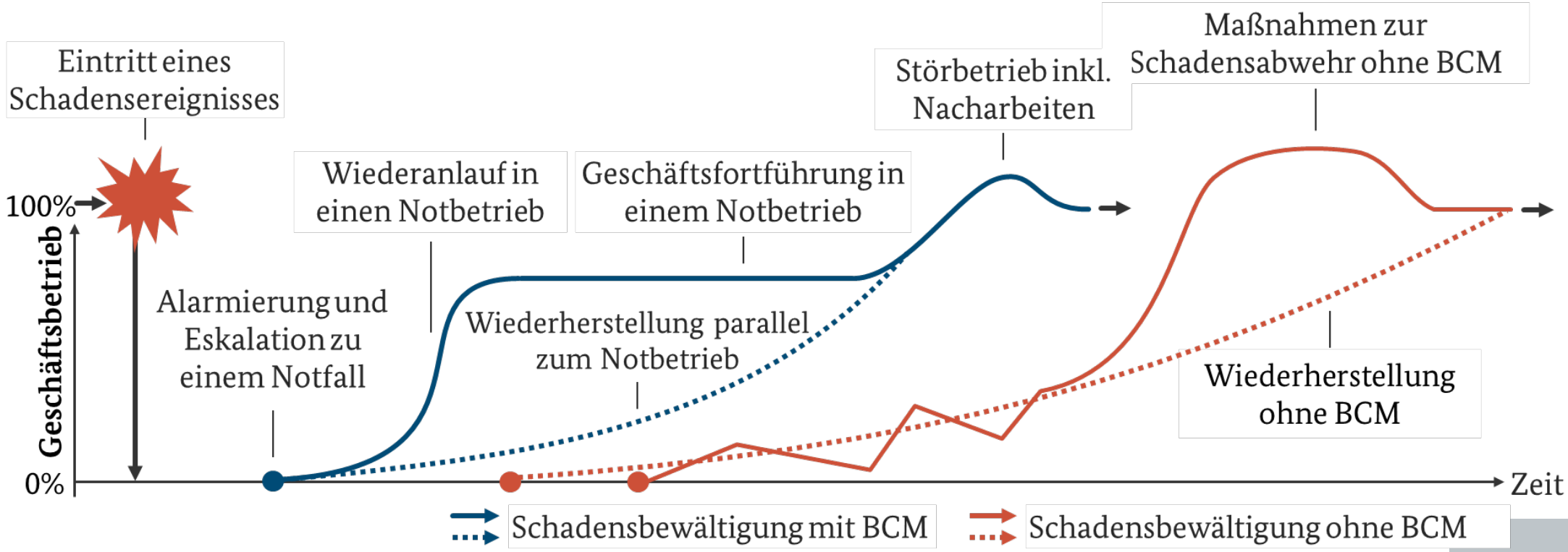


Setzen Sie die IT-Brille ab

Definitionen Störung, Notfall und Krise

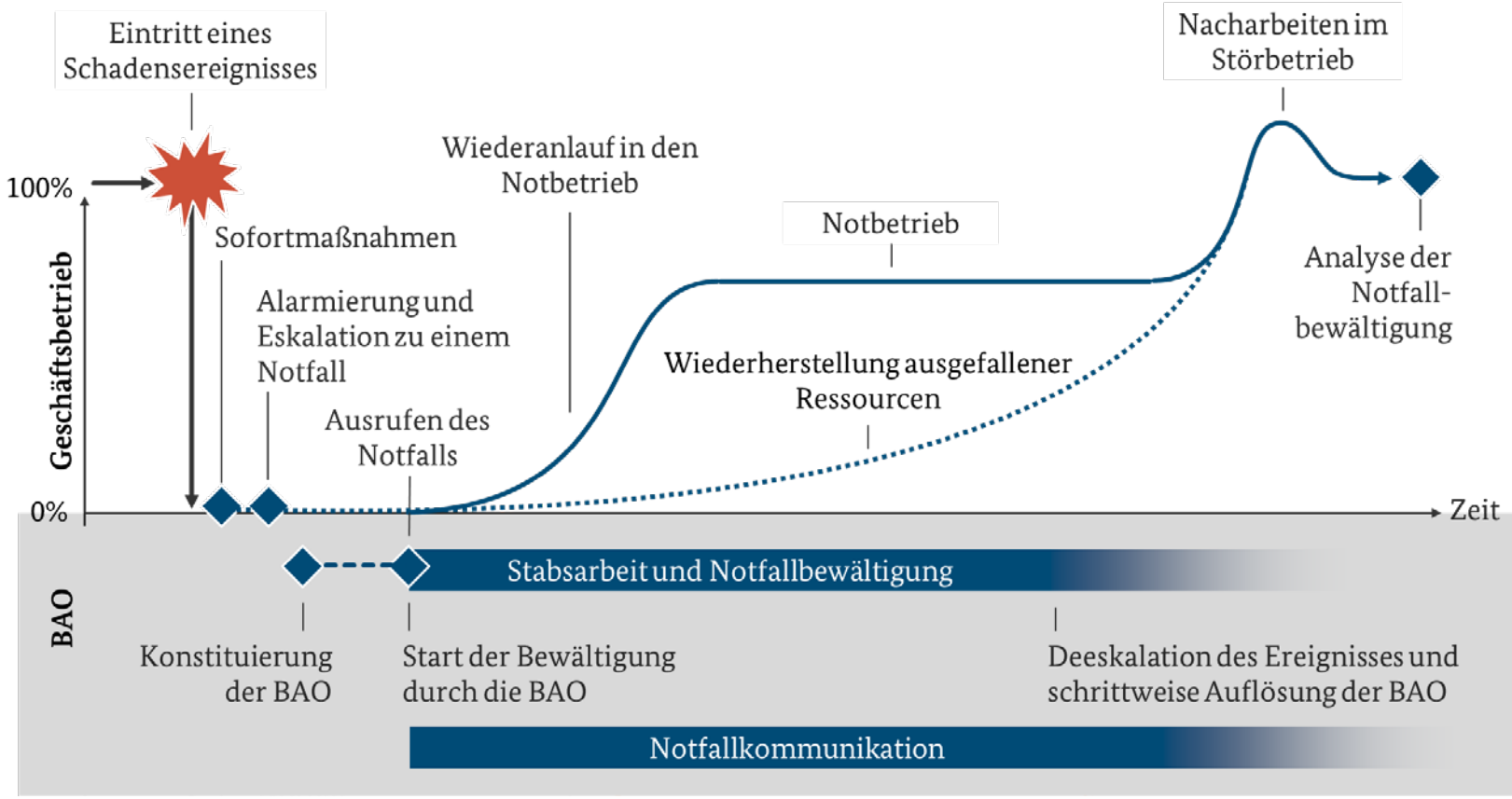


Übersicht über die Notfallbewältigung



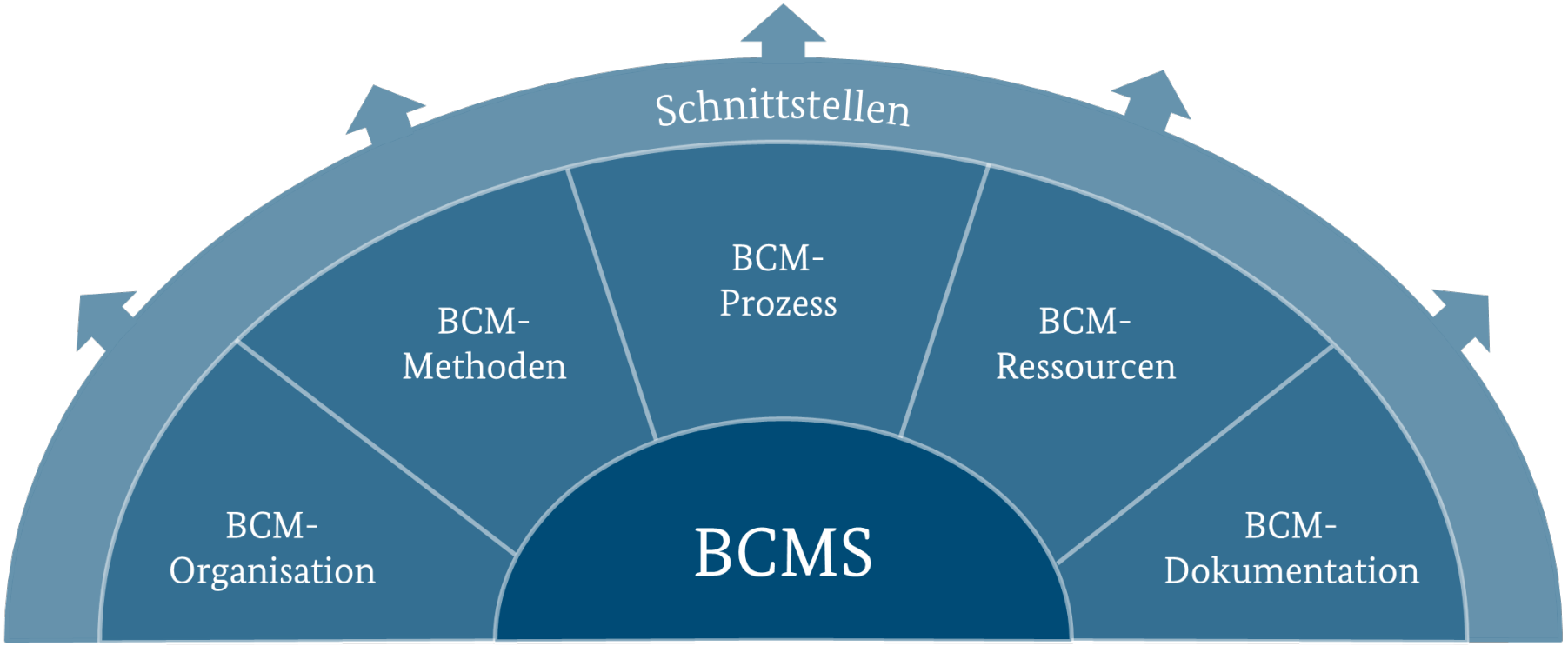
Ohne BCMS

Übersicht über die Notfallbewältigung



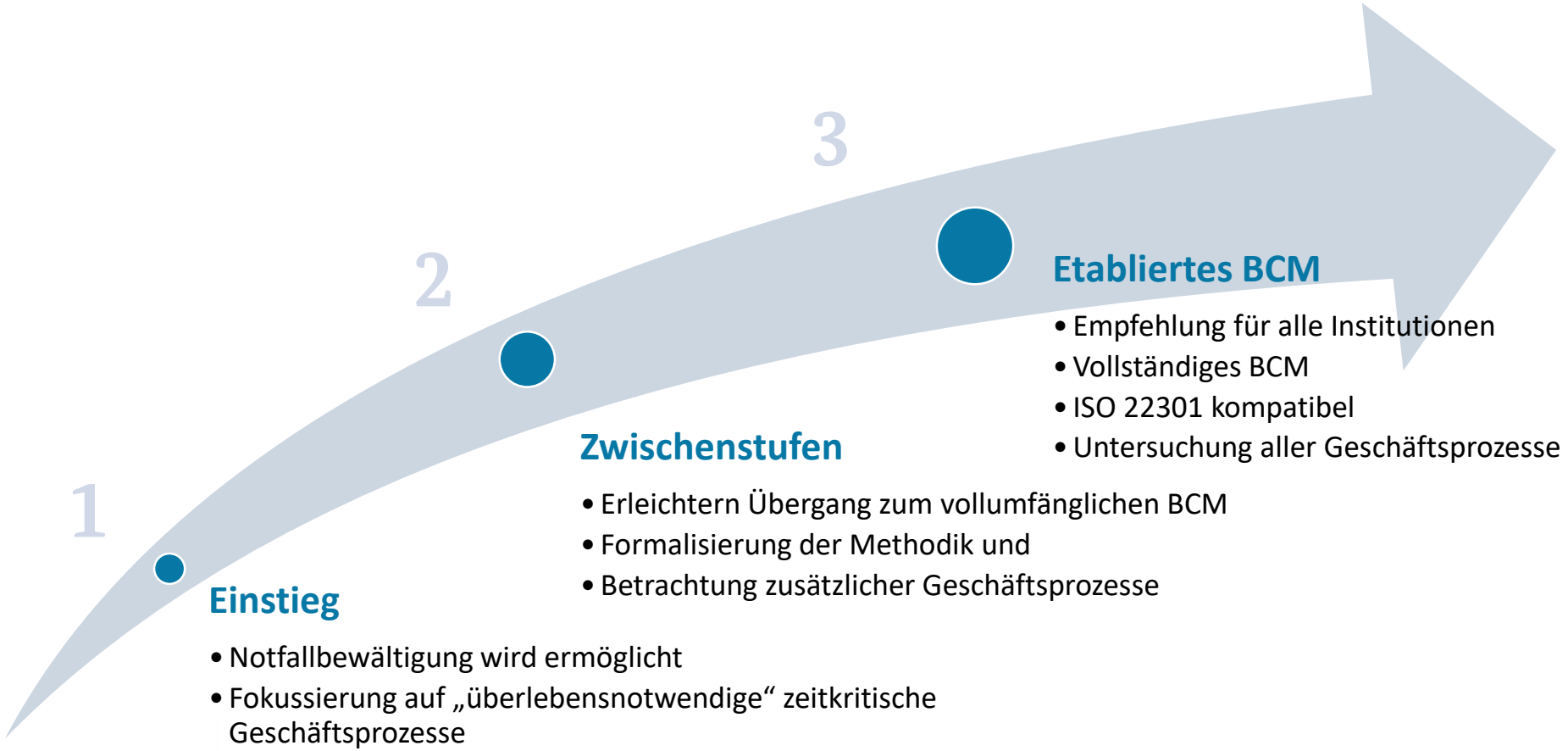
Mit BCMS

Bestandteile eines BCMS



Das Stufenmodell und der BCMS-Prozess

Schrittweiser Einstieg ins BCM



Einstieg

- Notfallbewältigung wird ermöglicht
- Fokussierung auf „überlebensnotwendige“ zeitkritische Geschäftsprozesse

Zwischenstufen

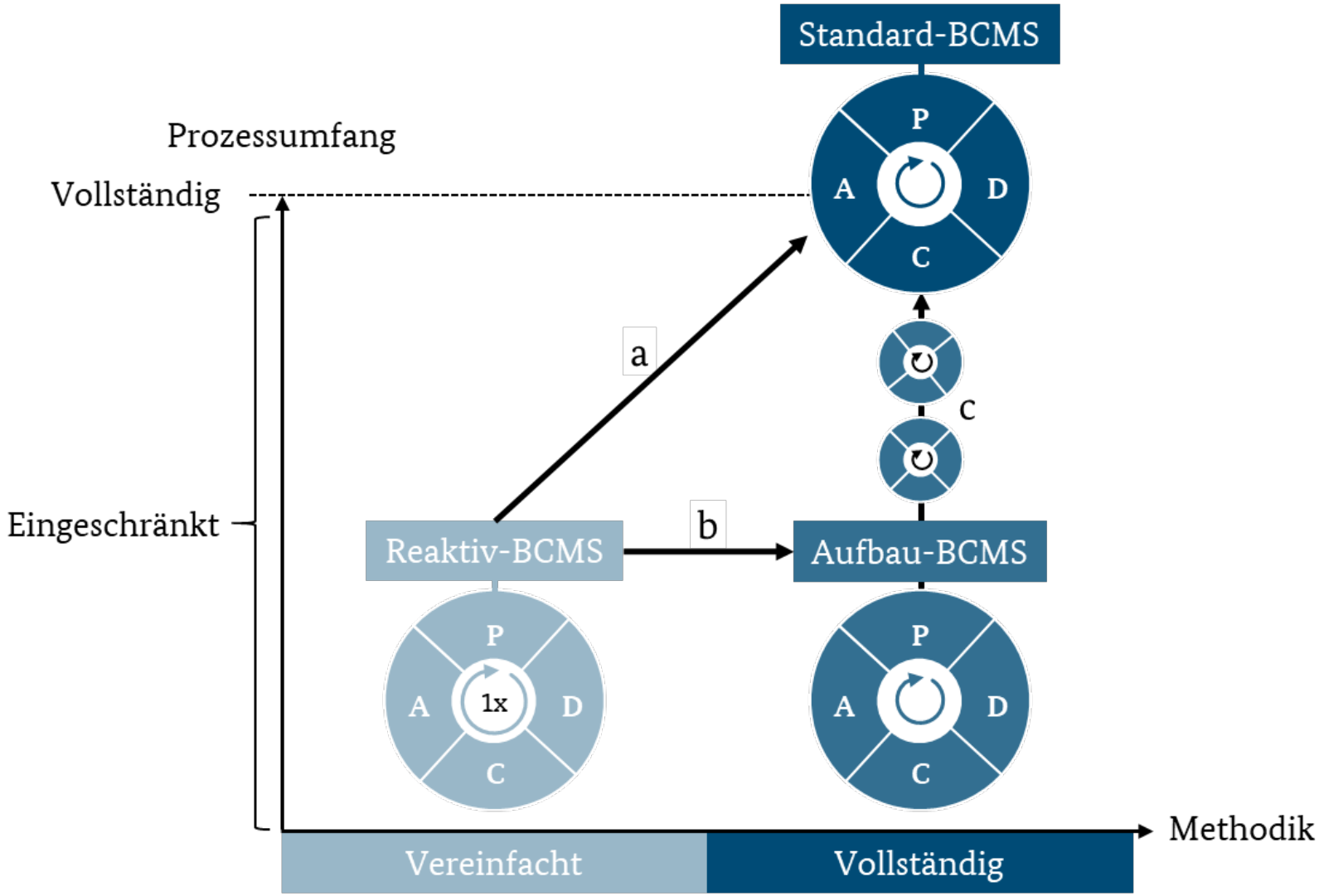
- Erleichtern Übergang zum vollumfänglichen BCM
- Formalisierung der Methodik und
- Betrachtung zusätzlicher Geschäftsprozesse

Etabliertes BCM

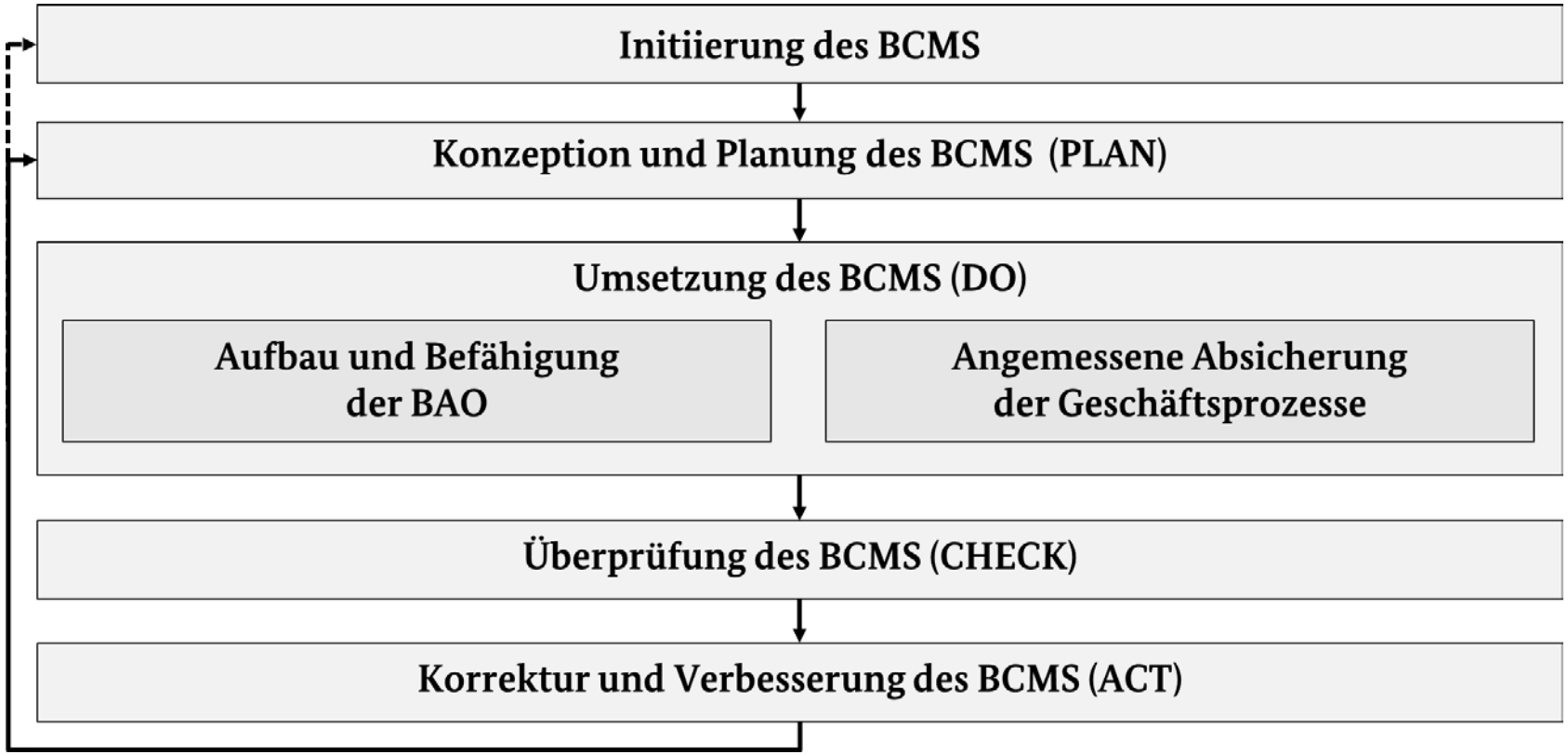
- Empfehlung für alle Institutionen
- Vollständiges BCM
- ISO 22301 kompatibel
- Untersuchung aller Geschäftsprozesse

BCM

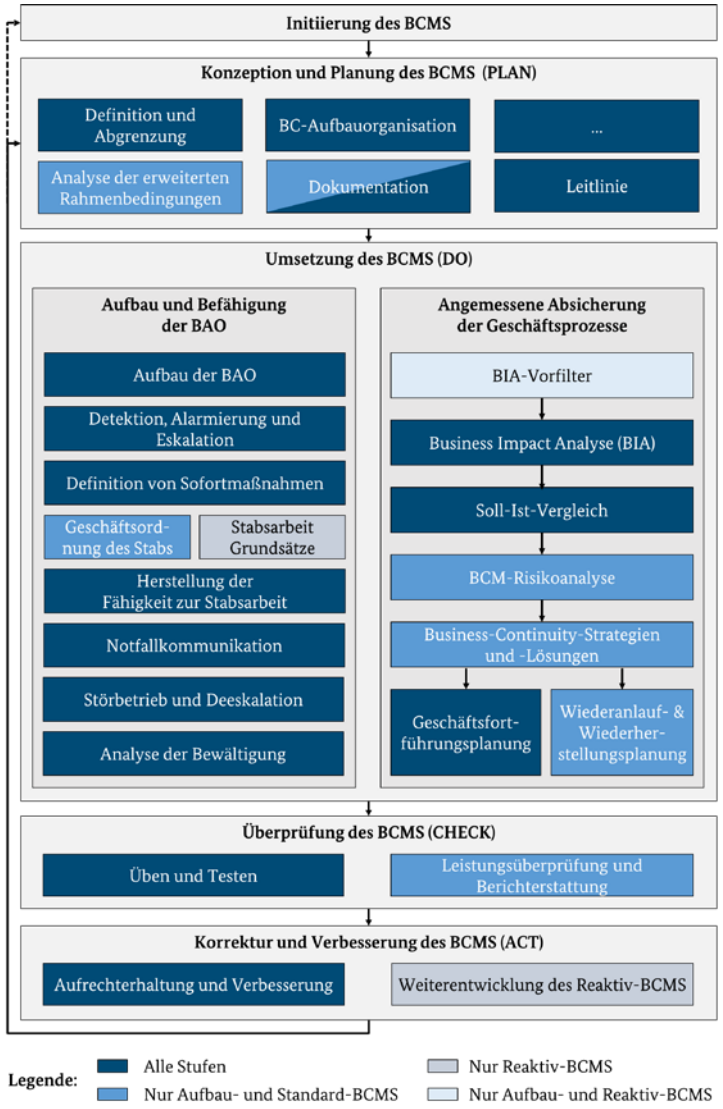
Schrittweiser Einstieg ins BCM



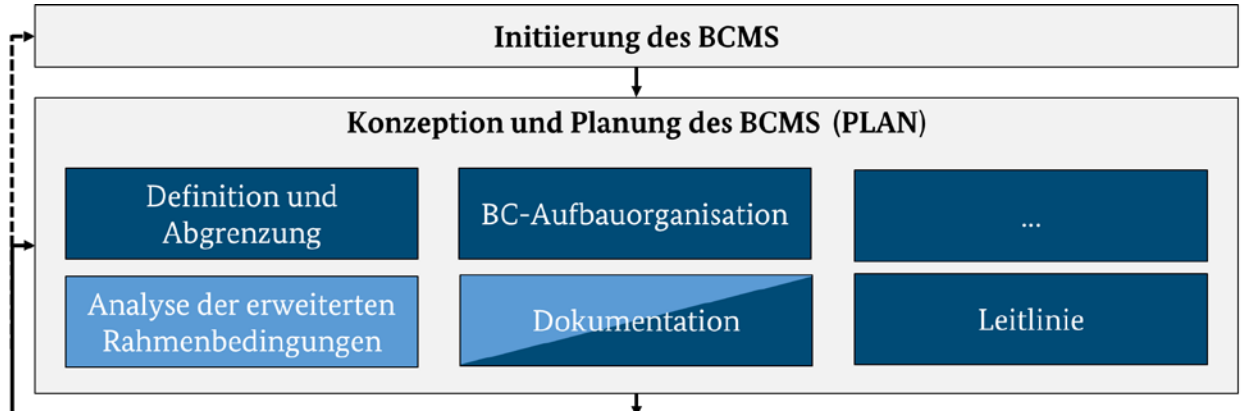
Übersicht über den BCMS-Prozess



Übersicht über den BCMS-Prozess

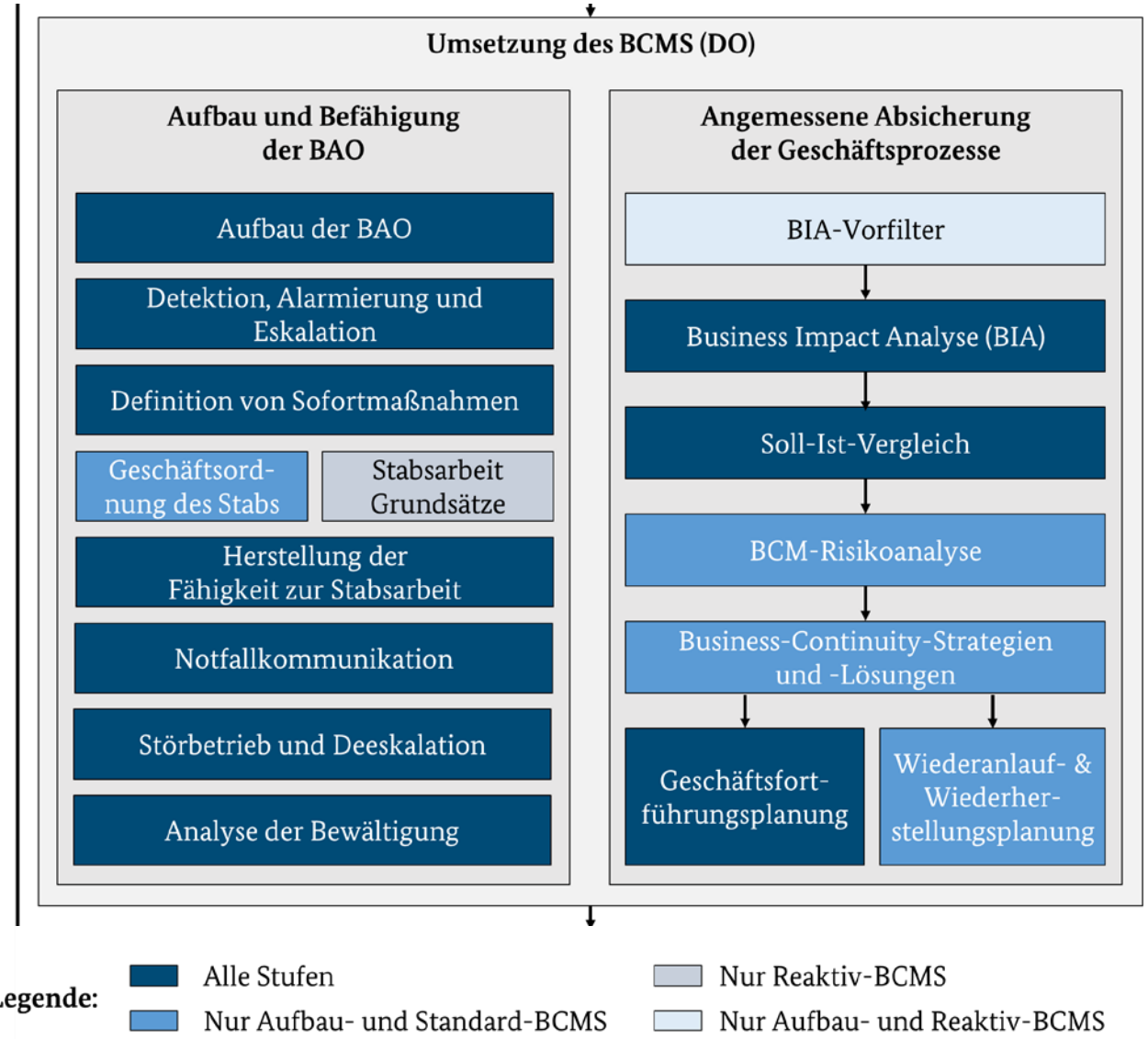


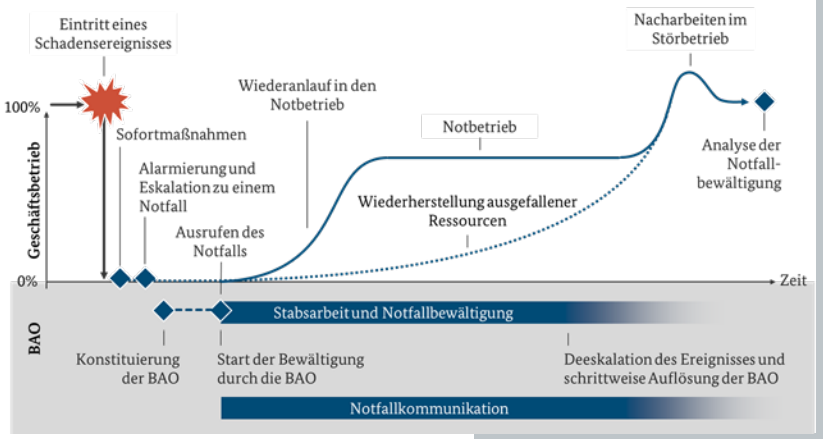
Übersicht über den BCMS-Prozess



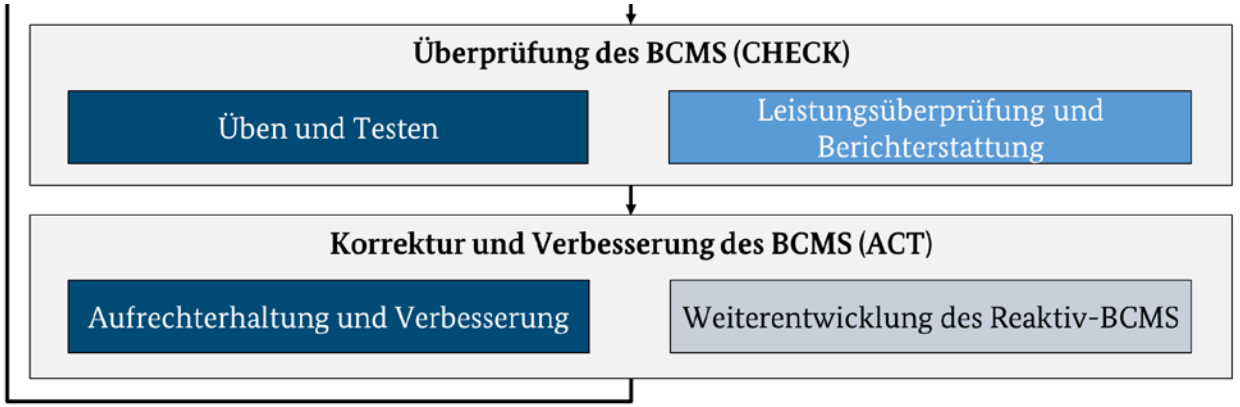
Legende:
- Alle Stufen
- Nur Aufbau- und Standard-BCMS
- Nur Reaktiv-BCMS
- Nur Aufbau- und Reaktiv-BCMS

Übersicht über den BCMS-Prozess





Übersicht über den BCMS-Prozess



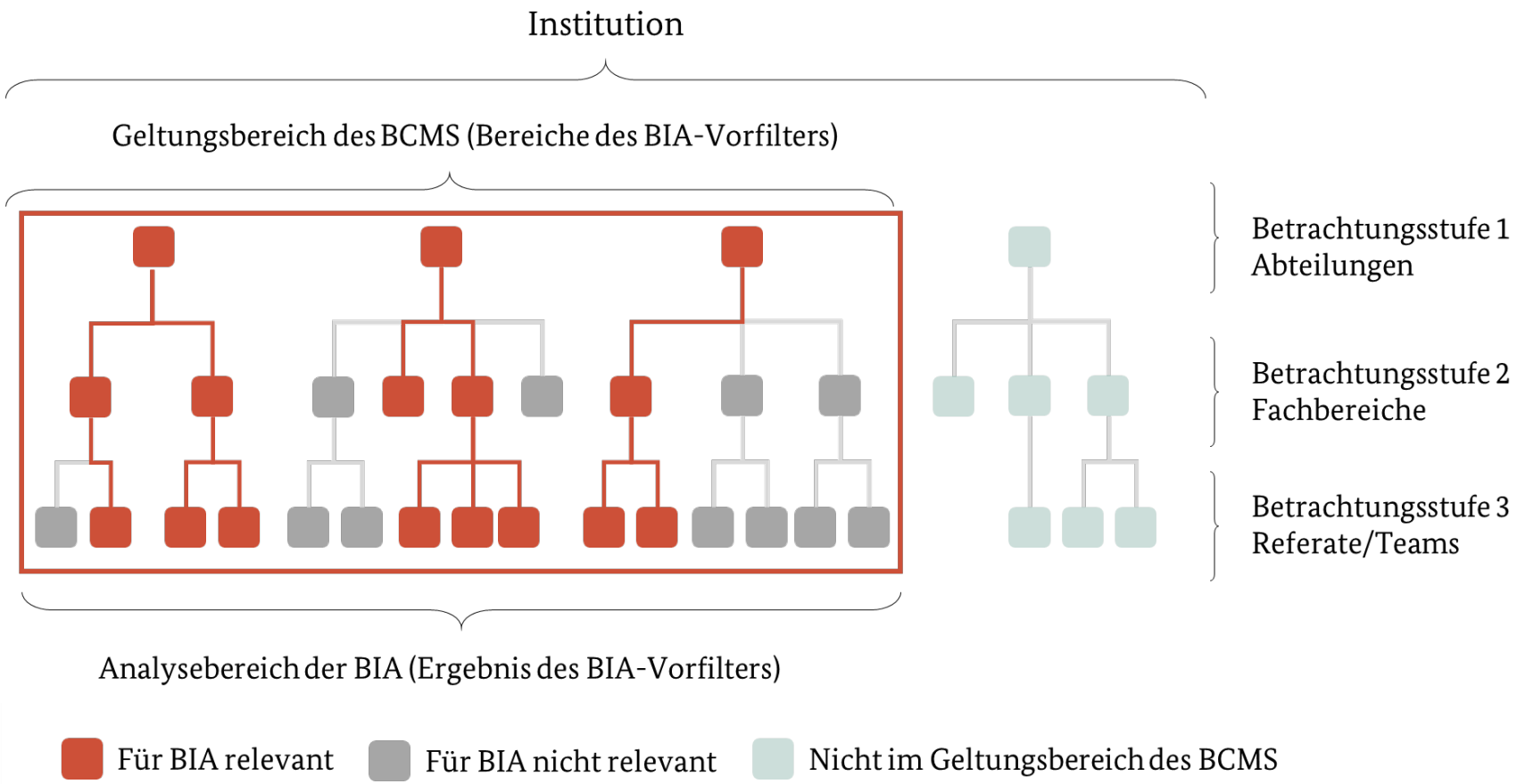
Legende:

- Alle Stufen
- Nur Aufbau- und Standard-BCMS
- Nur Reaktiv-BCMS
- Nur Aufbau- und Reaktiv-BCMS

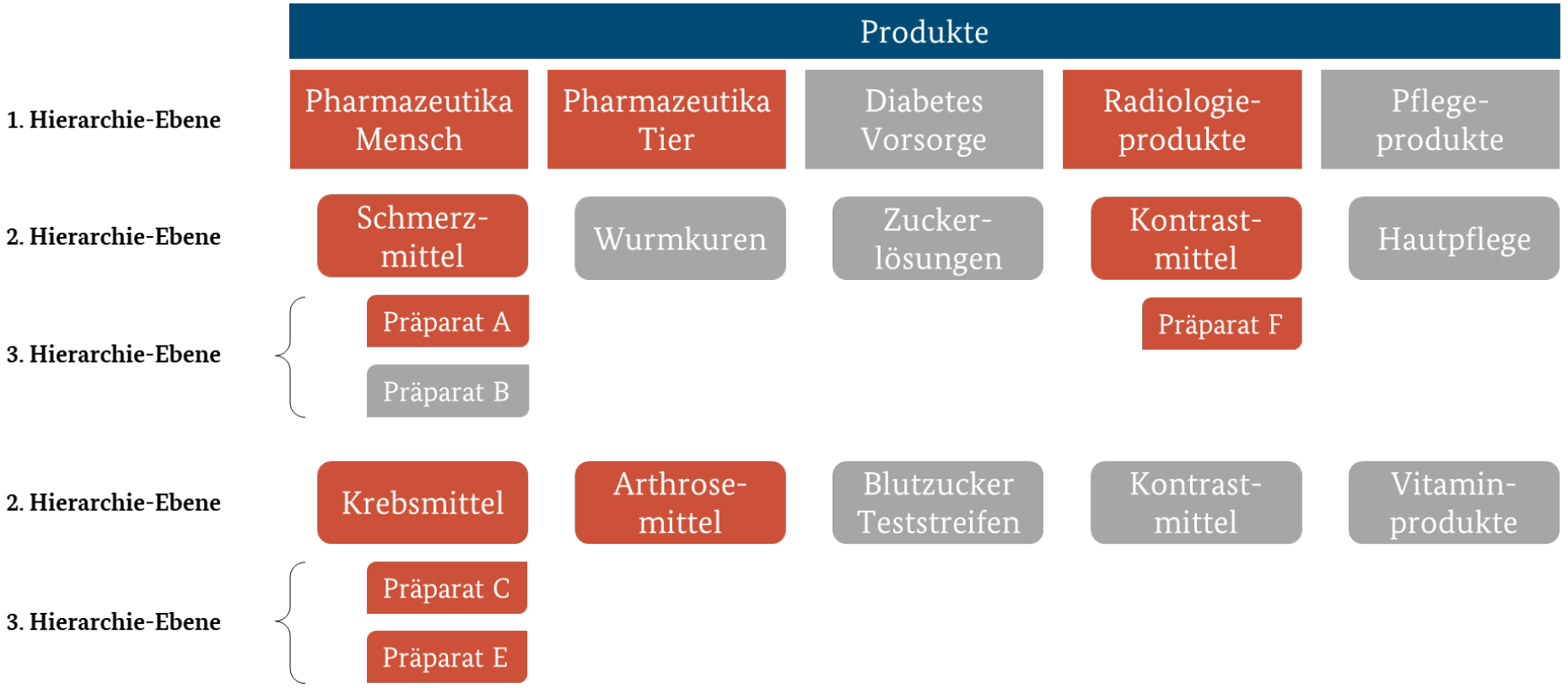
Reduktion des Untersuchungsbereichs der BIA anhand von Geschäftsprozessen

Geeignete Detailebenen für den BIA-Vorfilter		Geeignete Detailebene für die BIA
Prozessebene 1	**Prozessebene 2**	**Prozessebene 3**
Kundschaftsbeziehungsmanagement	Kundschaftsstrategie	...
	Kundschaftsbetreuung und -bindung	Schlüsselkundschaftsbetreuung
		Markenbindung
		Präsente und Aufmerksamkeiten
		Kontaktpflege und Öffentlichkeitsarbeit
		...
	Kundschaftshilfe	Selbsthilfe (FAQ)
		Automatisierte Kundschaftshilfe
		Kundschaftscenter (Telefon und Email)
		Kundschaftsanfragen bearbeiten
		...
	Kundschafts-zufriedenheit	Kundschaftszufriedenheitsumfragen
		Trendanalyse und Reporting
		...
Personal-management	Personalbeschaffung	Personalrekrutierung
		Einstellungsverfahren
		...
	Personalbetreuung	Personalservice
		Personalentwicklung
		Personalaustritt
		...

Reduktion des Untersuchungsbereichs der BIA anhand von Organisationseinheiten

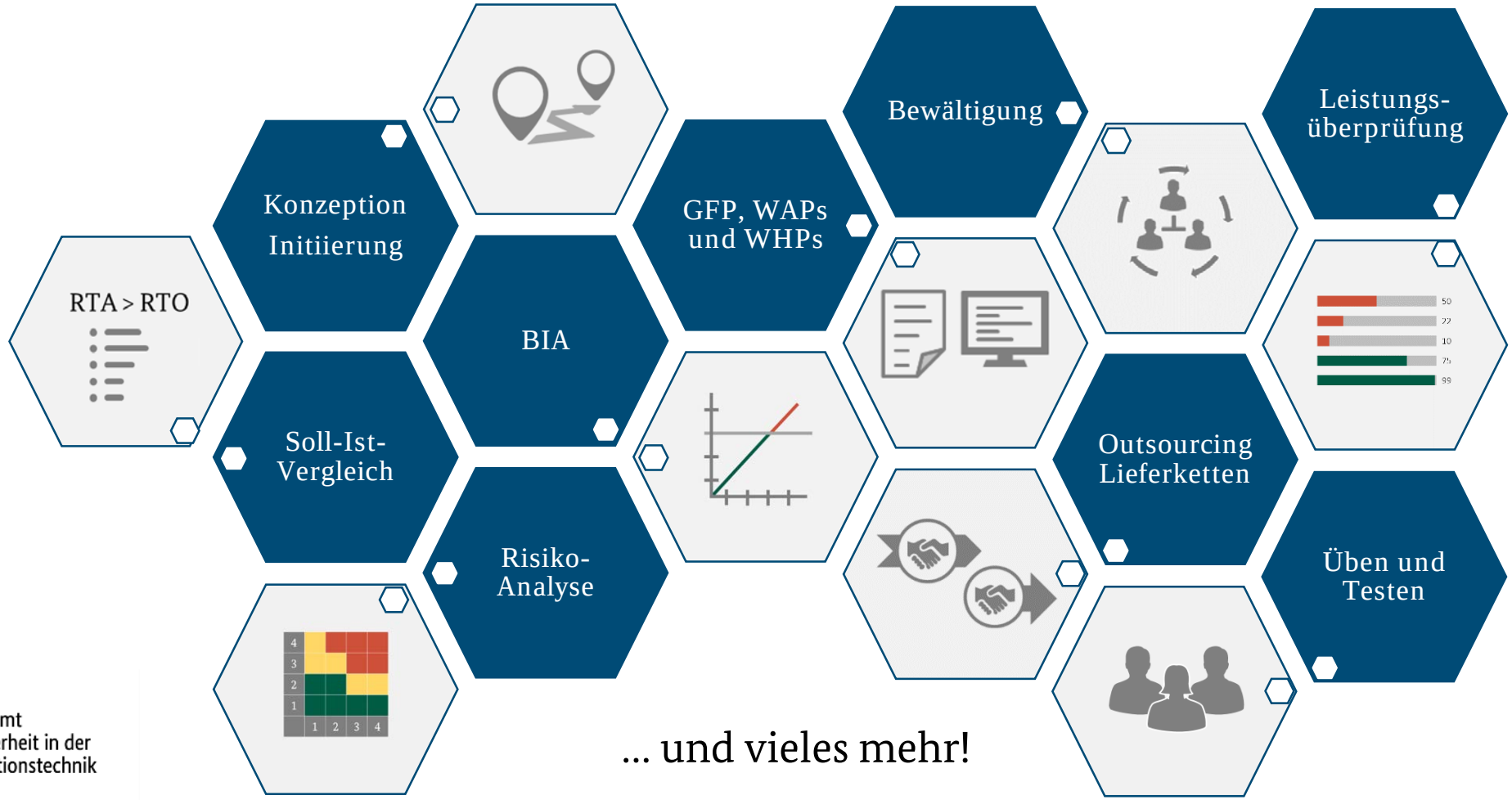


Reduktion des Untersuchungsbereichs der BIA anhand von Produkten und Services



Übersicht über weitere wesentliche Neuerungen

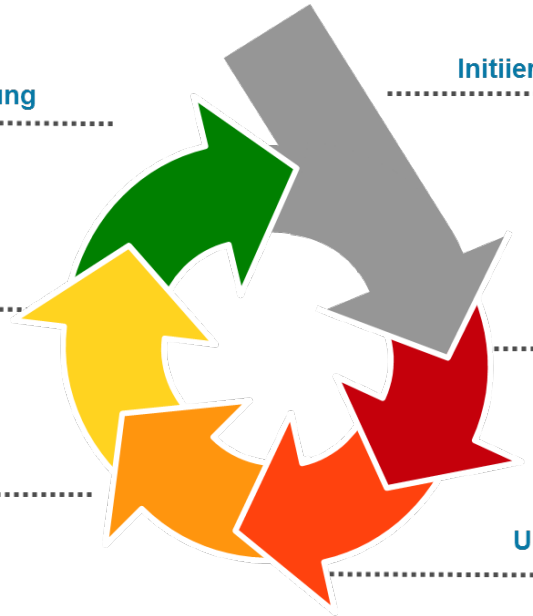
Grundlegende Überarbeitung in nahezu allen Bereichen gegenüber dem BSI-Standard 100-4



Erklärender Schritt für Schritt Charakter des 200-4

Der BSI-Standard führt die BCMS-Prozessschritte des BSI-Standards 100-4 weitestgehend fort, erläutert diese jedoch feingranularer und schließt Lücken des 100-4

BSI-Standard 100-4



Initiierung des Notfallmanagements
Verantwortung
Organisatorische Strukturen
Leitlinie zum Notfallmanagement
Einbindung Mitarbeiter

Konzeption
Business Impact Analyse
Risikoanalyse
Ist-Zustand
Kontinuitätsstrategien

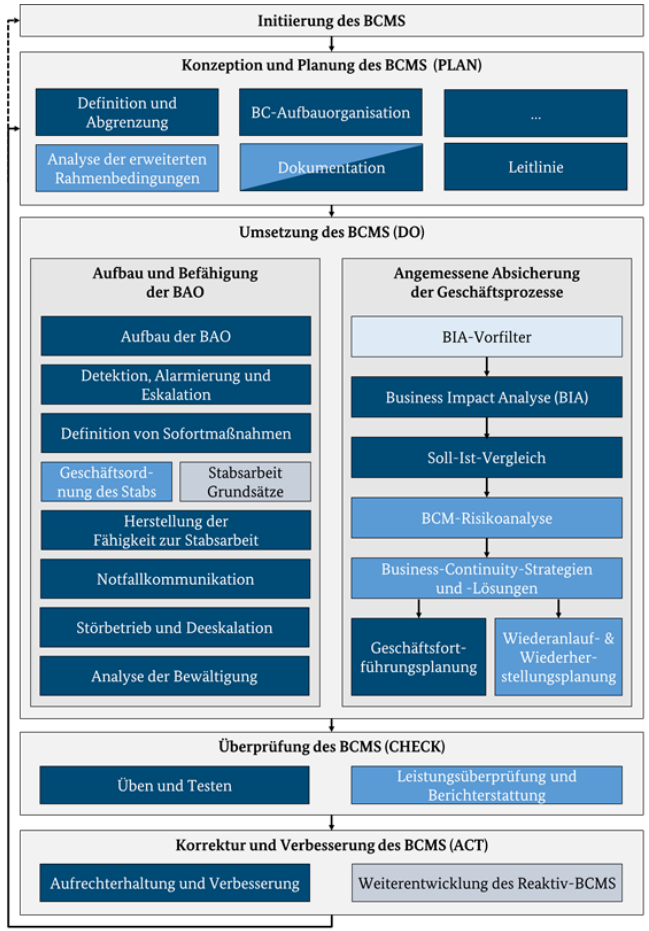
Umsetzung des Notfallkonzepts
Kosten- und Aufwandsabschätzung
Umsetzungsreihenfolge
Aufgaben und Verantwortung
Realisierungsbegleitende Maßnahmen

Notfallbewältigung
Ablauforganisation
Krisenkommunikation
Notfallhandbuch

Tests und Übungen
Übungsarten
Dokumente
Durchführung

Überprüfung und Verbesserung
Self-Assessment, Revision
Verbesserungsprozess

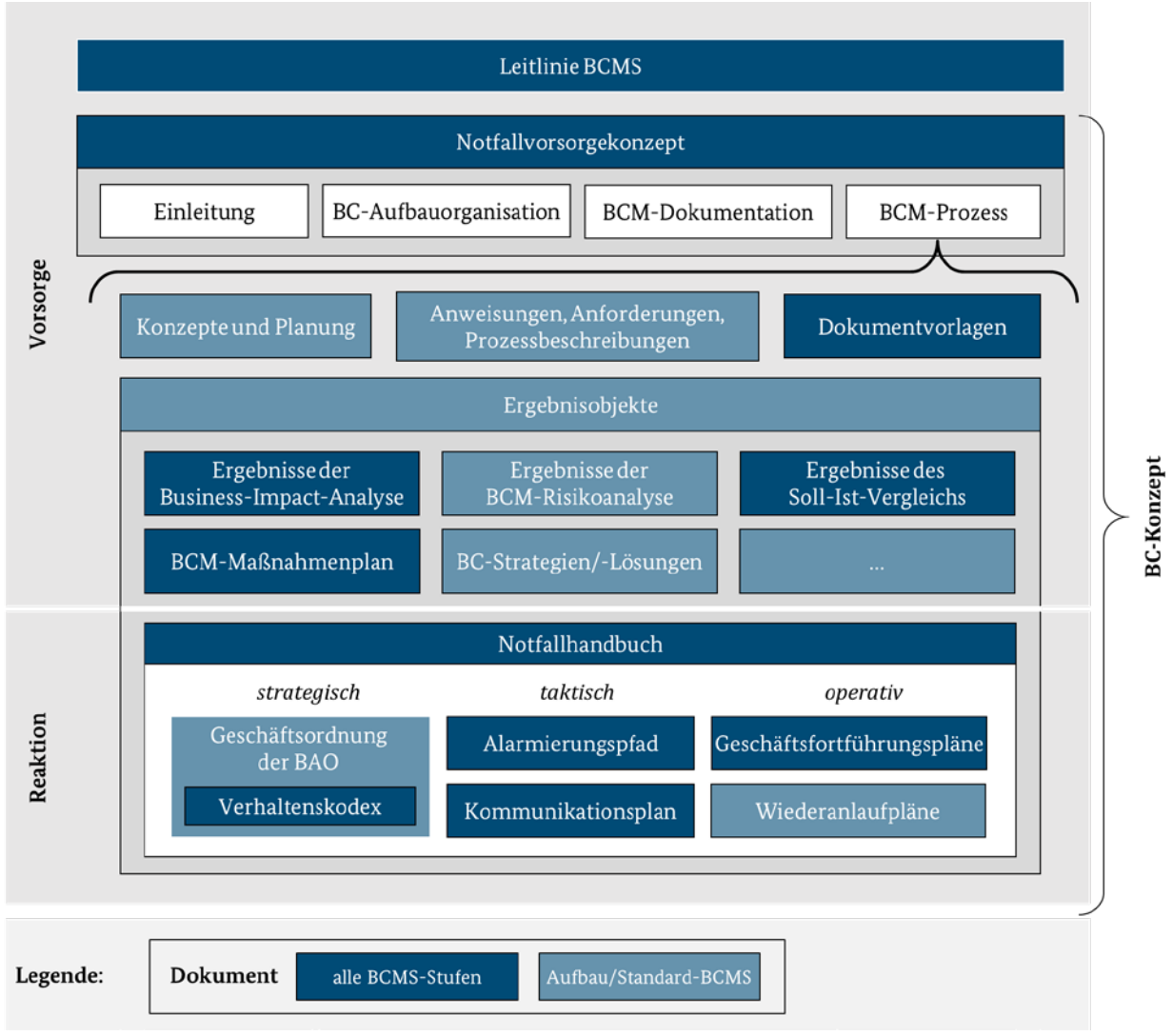
BSI-Standard 200-4



Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Beibehaltung der grundlegenden Dokumententypen und Dokumentenstruktur des BSI-Standards 100-4



Unterstützung durch eine Vielzahl an Hilfsmitteln

Dokumentvorlagen mit Beispieltexten

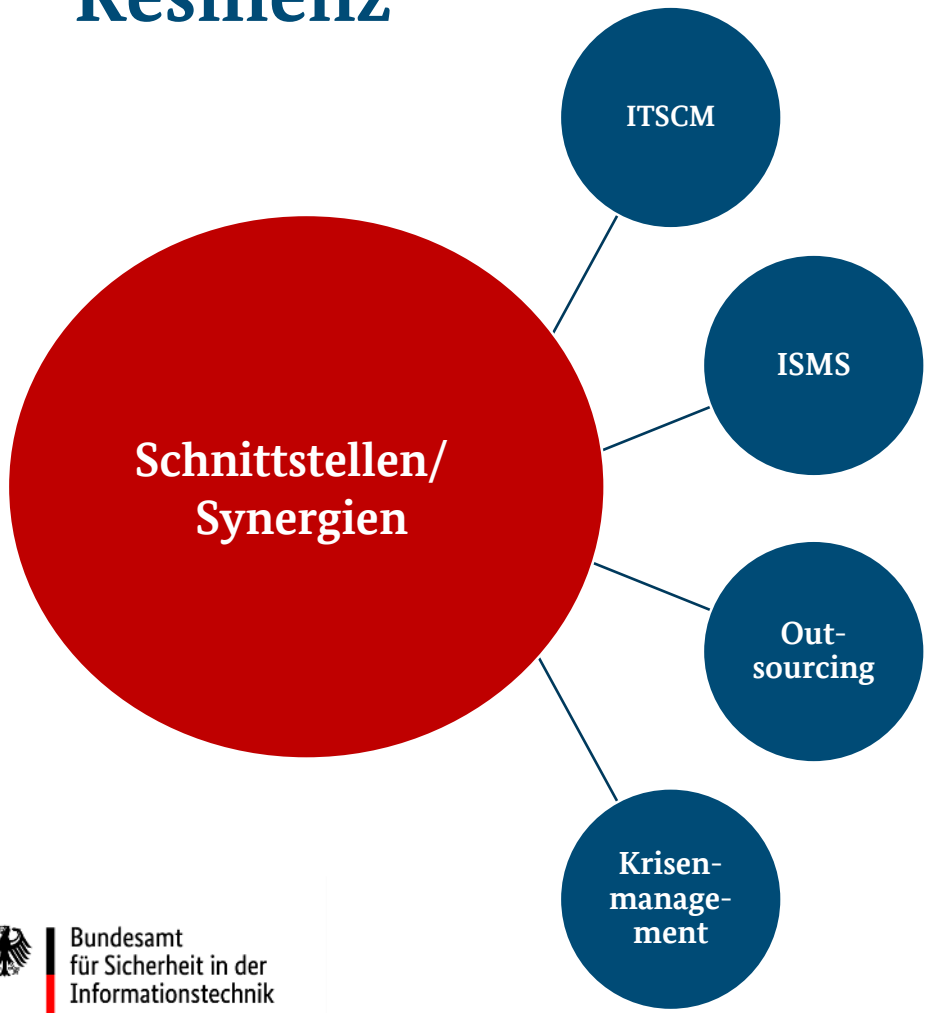
- Leitlinie
- Beispiel für eine BCM-Organisation
- Präsentationsvorlage zur Business-Impact-Analyse
- Übersicht über Schadensszenarien und -kategorien
- Bewertungstabelle BC-Strategien
- Notfallvorsorgekonzept
- Notfallhandbuch
- Beispiel Verhaltenskodex
- Schaubild Eskalations- und Alarmierungspfade
- Geschäftsfortführungsplan (GFP)
- Wiederanlauf- / Wiederherstellungsplan (WAP/WHP)
- Übungskonzept
- BCM-Maßnahmenplan
- Grundanforderungskatalog für Outsourcing und Lieferketten

Weiterführende Informationen

Die folgenden Dokumente liefern Hintergrundinformationen zu ausgewählten Bereichen des BCM und sind nicht normativ:

- Weiterführende Aspekte zur Bewältigung
- Vorschläge zu BC-Strategien
  (in Überarbeitung)
- Kennzahlen im BCM
- Weiterführende Informationen zu BCM-Tools
- Weiterführende Informationen zur Eintrittshäufigkeit von Ausfallrisiken

Fokus auf Synergien zur ganzheitlichen organisatorischen Resilienz



Mögliche Synergien

- **Viele** Möglichkeiten zum Austausch/Abgleich und zur Wiederverwendung von Ergebnissen
- Möglichkeiten zur **gemeinsamen** Erhebung
- Klare Aufteilung der **Verantwortlichkeiten/Zuständigkeiten** – auch im Notfall & in der Krise
- Darstellung in **Synergieboxen**

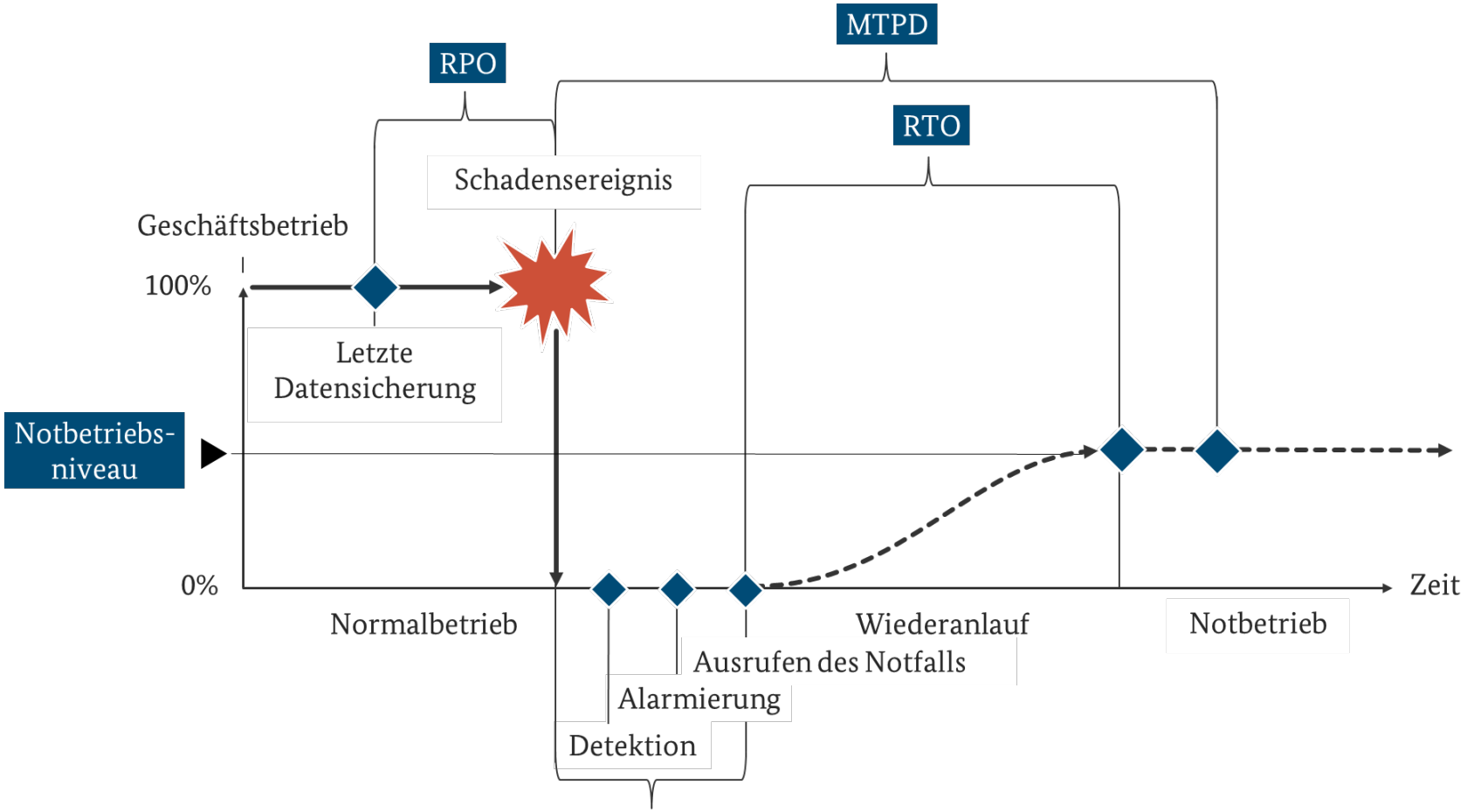
Synergiepotenzial

Synergiepotenzialboxen weisen auf Möglichkeiten zur effektiven, ressourcenschonenden Zusammenarbeit mit angrenzenden Themen hin.

- ...und vieles mehr.

Wesentliche Neuerungen im finalen Standard gegenüber dem CD 2.0

Anpassung der Definition der RTO zur klareren Planung der BIA-Parameter und des Wiederanlaufs



Sprachliche Qualitätssicherung und Anpassung des Satzes

- Umbenennung der Voranalyse in **BIA-Vorfilter**
- Allgemeine Fehlerkorrektur
- Umformulierung des gesamten Standards in geschlechtergerechte Sprache
- Anpassung des Satzes und der Abbildungen für das **neue Format**
- Nochmalige **Homogenisierung** des Wordings

Identische **digitale** und **analoge** Version

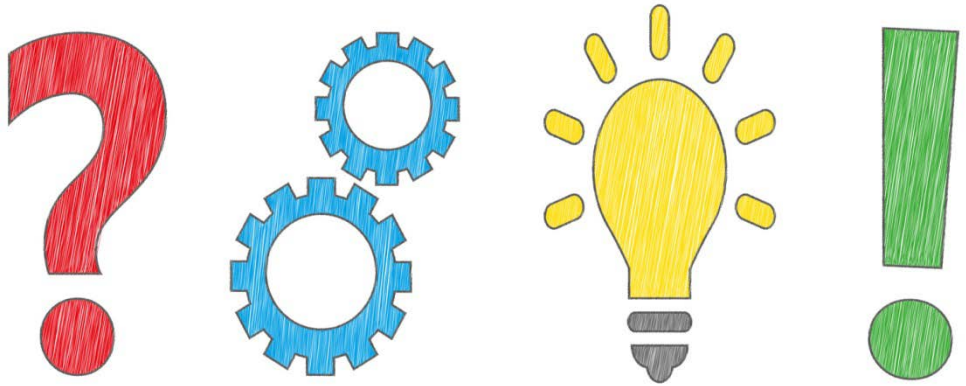
Bereitstellung des aktualisierten Anforderungskatalogs mit ISO 22301:2019 Mapping

	A	B	C	D	E
1	ISO-Chapter	ISO-Clause	BSI-Kapitel	BSI-Anforderung	BSI-Anforderung
2	**4 Context of the organization**				
3	4.1	4.1 Understanding the organization and its context	4.2.1	KONZ-005	Die Institution MUSS die relevanten Interessengruppen und deren Anforderungen an das BCMS sowie deren Einflussfaktoren auf das BCMS ermitteln.
4	*4.1*	4.1 Understanding the organization and its context	15	KVP-001-a	Die Institutionsleitung MUSS Korrekturbedarfe und Verbesserungsmöglichkeiten auf strategischer Ebene identifizieren und durch Neuausrichtung der Ziele und Rahmenbedingungen des BCMS behandeln.
5	*4.1*	4.1 Understanding the organization and its context	**3.2.1**	**INIT-002-a**	**Die Institution SOLLTE ihre individuellen Gründe für ein BCM identifizieren, dokumentieren und das BCMS danach ausrichten.**
6	4.2	**4.2 Understanding the needs and expectations of interested parties**			
7	4.2	4.2.1 General			
8	4.2	4.2.1 a)	4.2.1	KONZ-005	Die Institution MUSS die relevanten Interessengruppen und deren Anforderungen an das BCMS sowie deren Einflussfaktoren auf das BCMS ermitteln.

Veröffentlichung und Bereitstellung

- Bereitstellung des digitalen finalen BSI-Standards 200-4 und des aktualisierten Anforderungskatalogs mit integriertem ISO-Mapping **heute im Laufe des Nachmittags auf unserer Webseite** unter:
  - https://www.bsi.bund.de/gs-standard200-4
- Bezug des **gedruckten** BSI-Standards über den Reguvis-Verlag

Zeit für Ihre Fragen



IT-Grundschutz

Deutschland
Digital•Sicher•BSI•

Vielen Dank für Ihre Aufmerksamkeit!

Daniel Gilles

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

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

Bundesamt
für Sicherheit in der
Informationstechnik