Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Vom BSI-Standard 100-4 „Notfallmanagement“ zu 200-4 „Business Continuity Management (BCM)“

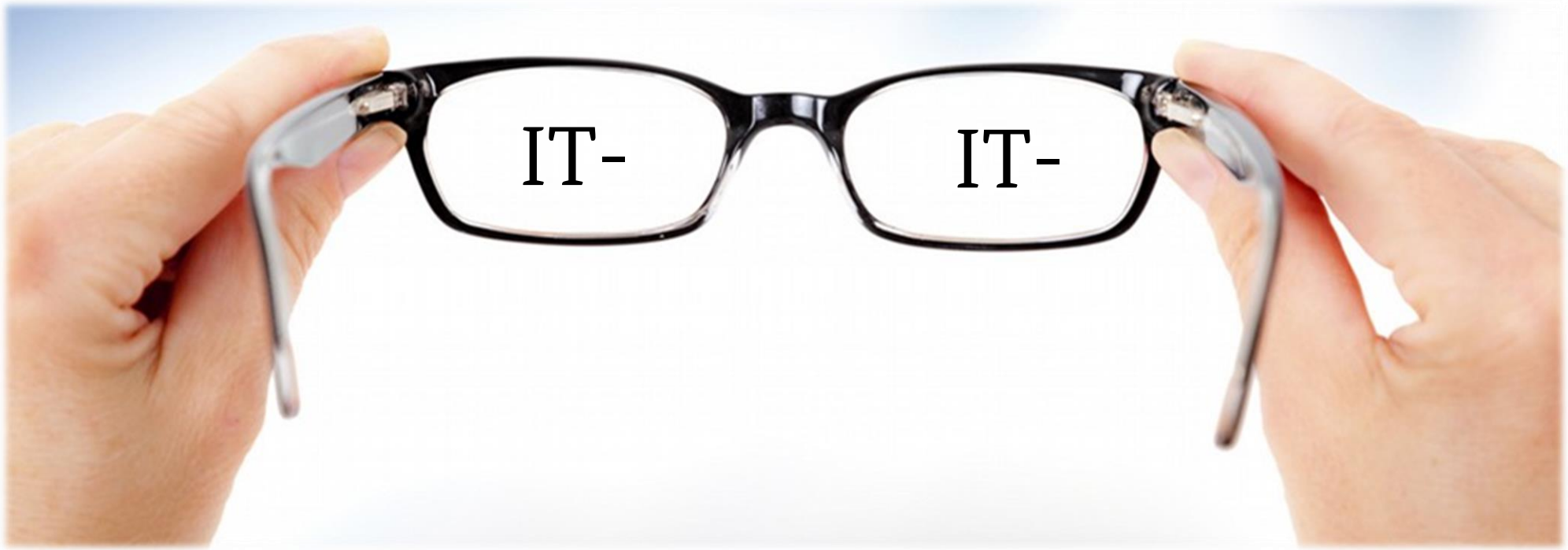
Daniel Gilles
Referat „BSI-Standards und IT-Grundschutz“

DPMA Expertennetz Prozessmanagement zum Thema „Antizipation und Bewältigung von Krisen im modernen Prozessmanagement“

Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft

Bundesamt
für Sicherheit in der
Informationstechnik

Vorbemerkung

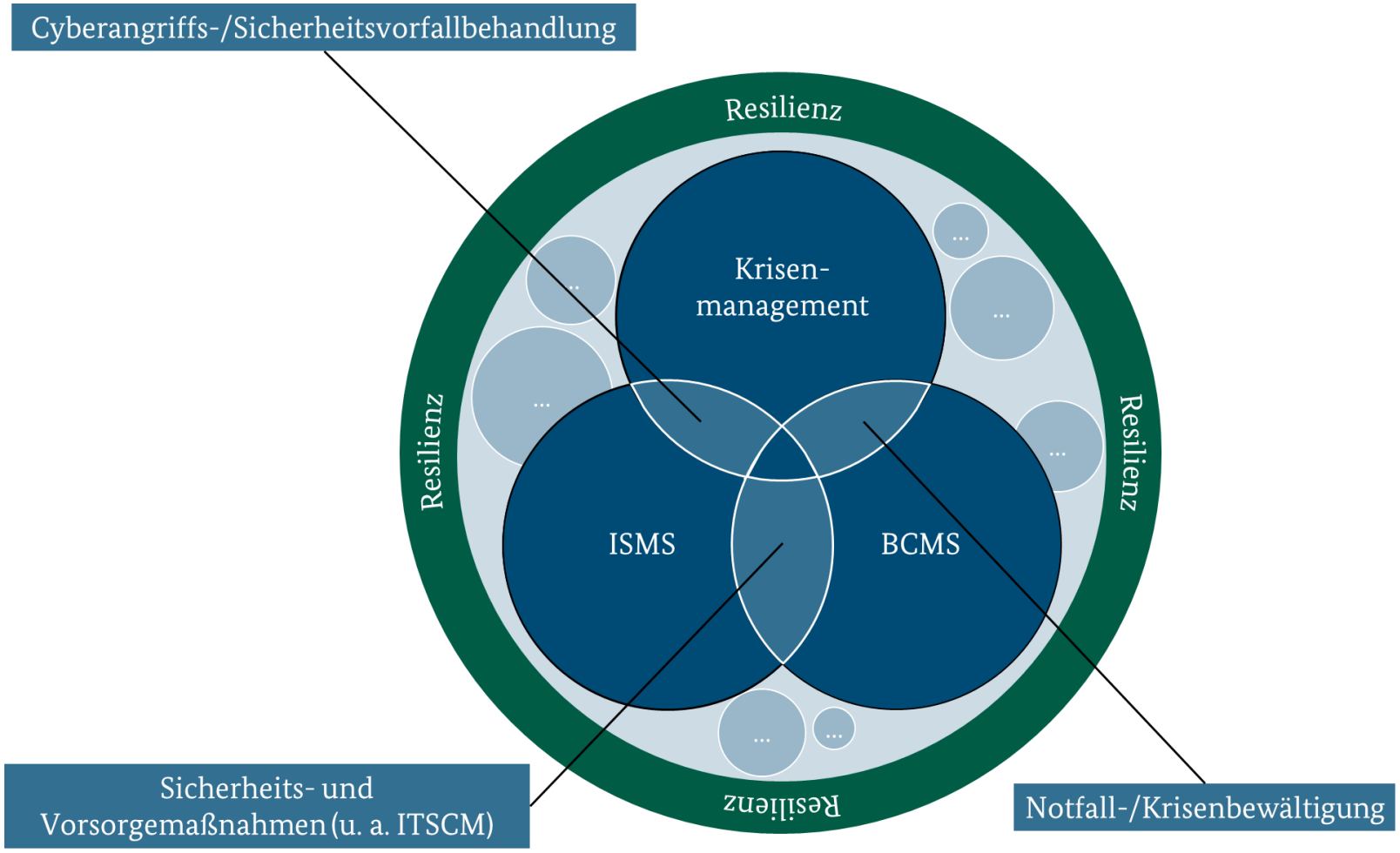


Setzen Sie die IT-Brille ab

Bundesamt
für Sicherheit in der
Informationstechnik

Vom IT-Grundschutz zum BCMS

Bestandteile zur organisatorischen Resilienz

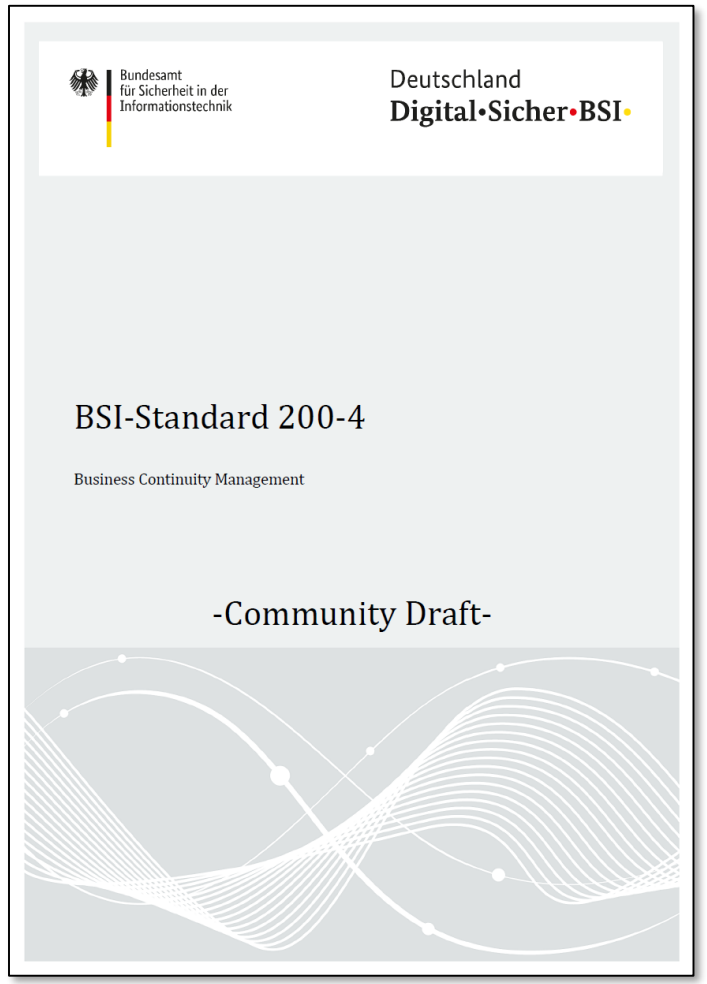


Bundesamt
für Sicherheit in der
Informationstechnik

Weiterentwicklung des BSI-Standards 200-4

Agenda

1. Ziele und Grundlagen
2. Stufenmodell
3. Übersicht über wesentliche Neuerungen
4. Informations- und Beteiligungsmöglichkeiten
5. Ausblick



Bundesamt
für Sicherheit in der
Informationstechnik

Was wollen **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

Grundlagen

Aus Notfallmanagement wird BCM

Eskalation

Störung

- Prozesse oder Ressourcen stehen nicht wie vorgesehen zur Verfügung
- Innerhalb des Normalbetriebs behebbar (keine Notfallpläne erforderlich)
- Keine Besondere Aufbau-Organisation (BAO) erforderlich

Notfall

- Erhebliche Unterbrechung eines zeitkritischen Geschäftsprozesses /Fachaufgabe
- BAO erforderlich
- Notfallpläne liegen vor oder können angepasst werden

Krise

- Massive Unterbrechung eines/r (zeit-)kritischen Geschäftsprozesses/Fach-aufgabe
- Es liegen keine Notfallpläne vor oder die Notfallpläne greifen nicht ausreichend
- Erweiterung der Befugnisse der BAO erforderlich

Eskalation

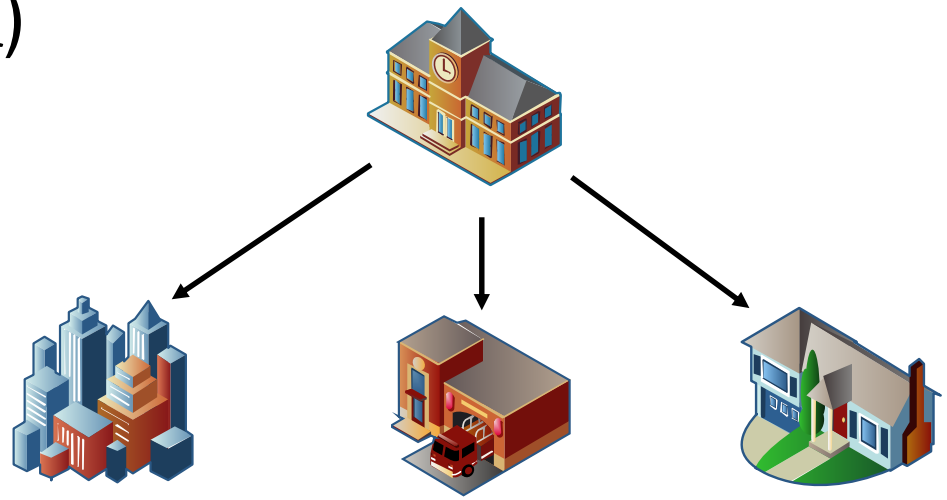
BCM

Grundlegende Definitionen

Abgrenzung BCM (BSI) vom Krisenmanagement zur öffentlichen Gefahrenabwehr (BBK)

„Eigene“ Notfälle und Krisen innerhalb einer Institution (Behörde, Gewerbe etc.)

BCM nach BSI 200-4 zur Aufrecht-erhaltung der zeitkritischen Geschäftstätigkeiten



Öffentliche Krisen und Katastrophen (z.B. Großschadensereignisse, Brände, Terrorismus etc.)

Krisenmanagement nach BBK-Vorgaben bzw. landesrechtlichen Katastrophenschutzgesetzen im Sinne der öffentlichen Gefahrenabwehr

Bundesamt für Sicherheit in der Informationstechnik

Abgrenzung der Begriffe und Zuständigkeiten mit BBK auf Arbeitsebene abgestimmt.

Grundlegende Definitionen

Abgrenzung BCM (BSI) vom Krisenmanagement zur öffentlichen Gefahrenabwehr (BBK)

„Eigene“ Notfälle und Krisen innerh
einer Institution (Behörde, Gewerbe

Beschreibung möglicher Schnittstellen im BSI-Hilfsmittel „Weitergehende Informationen zur Bewältigung“

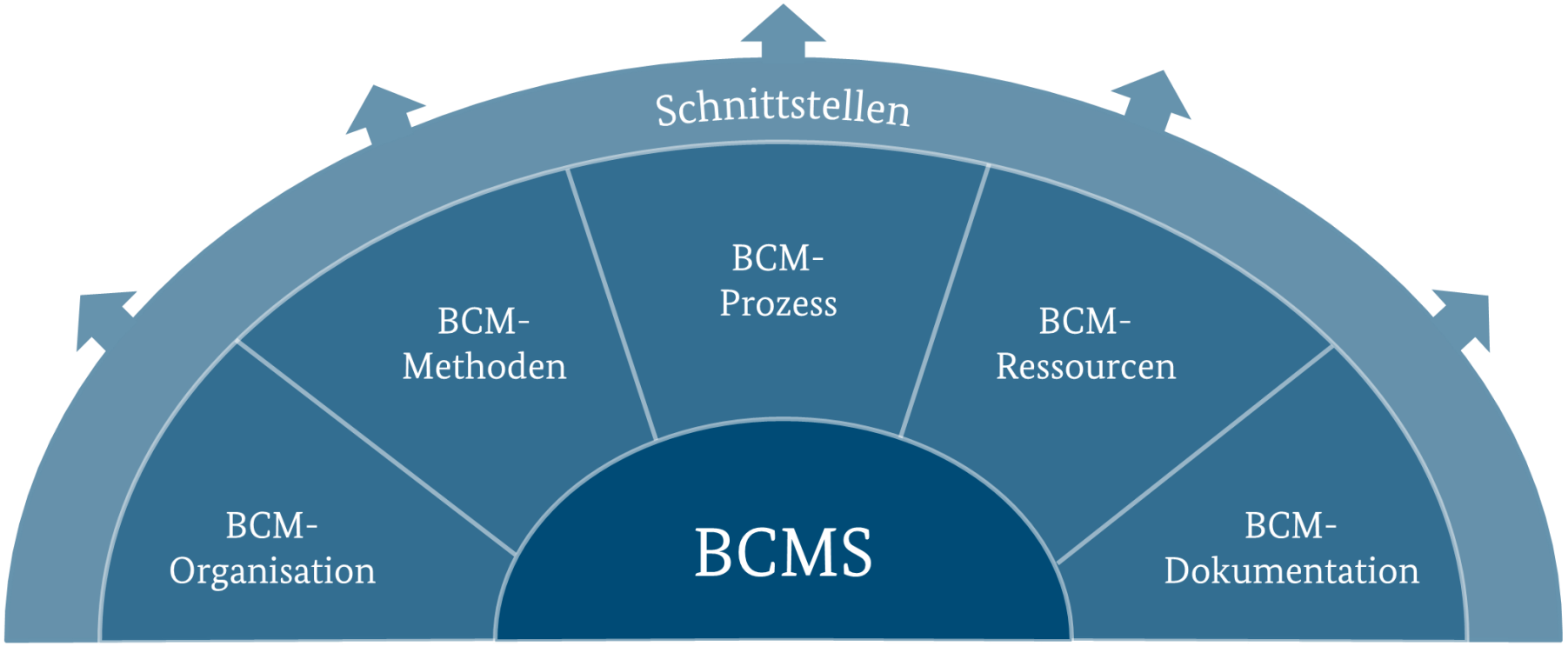
Katastrophen (z.B. Großschadensereignisse, Brände, Terrorismus etc.

BCM nach BSI 200-4 zur Aufrecht-erhaltung der zeitkritischen Geschäftstätigkeiten

Krisenmanagement nach BBK-Vorgaben bzw. landesrechtlichen Katastrophenschutzgesetzen im Sinne der öffentlichen Gefahrenabwehr

Grundlagen

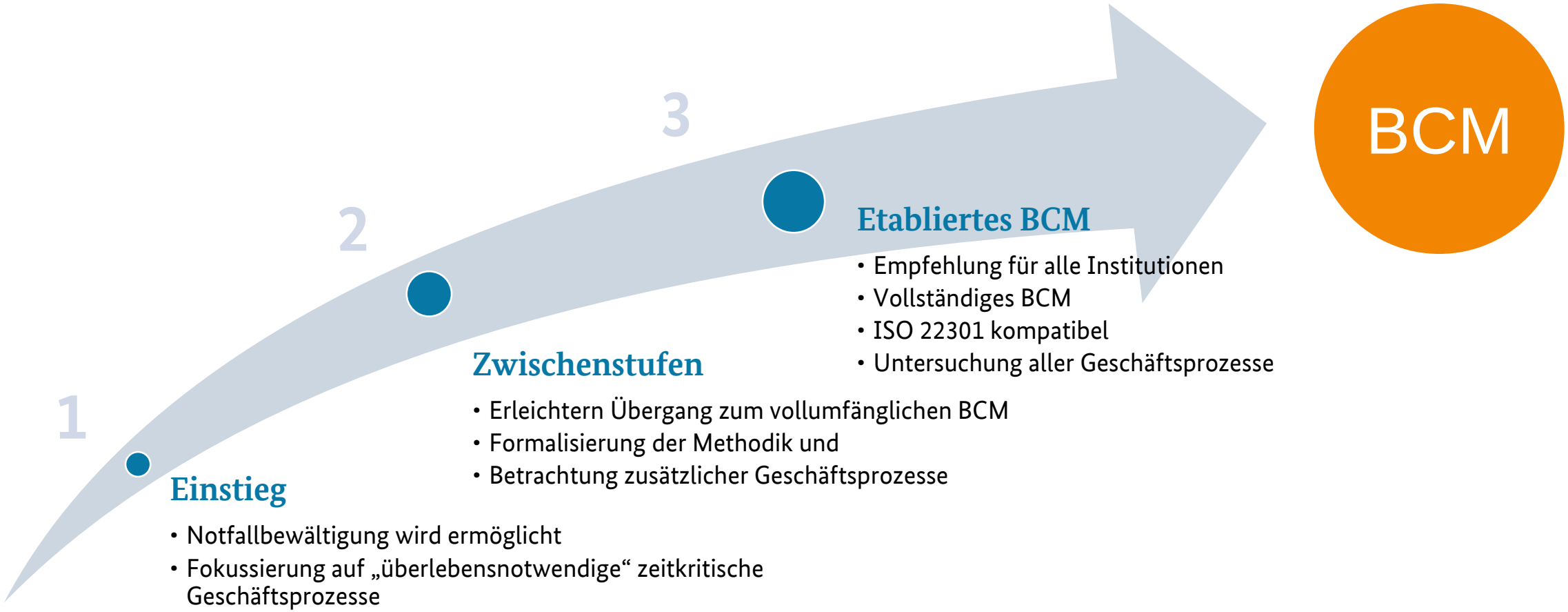
Bestandteile eines BCMS



Stufenmodell

Stufenmodell - Ziele

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

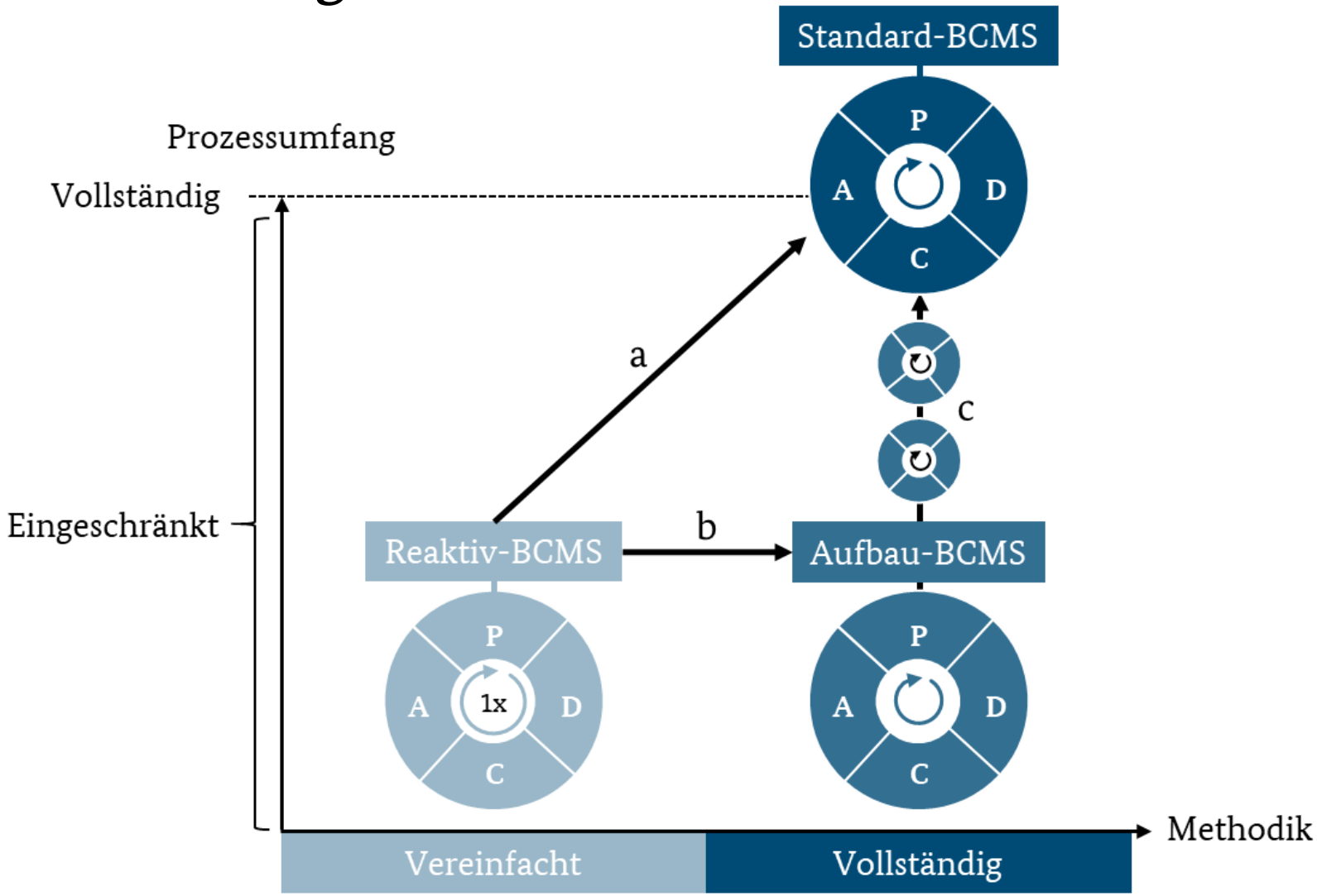
Etabliertes BCM

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

Bundesamt
für Sicherheit in der
Informationstechnik

Stufenmodell - Übersicht

Schrittweiser Einstieg ins BCM



Bundesamt
für Sicherheit in der
Informationstechnik

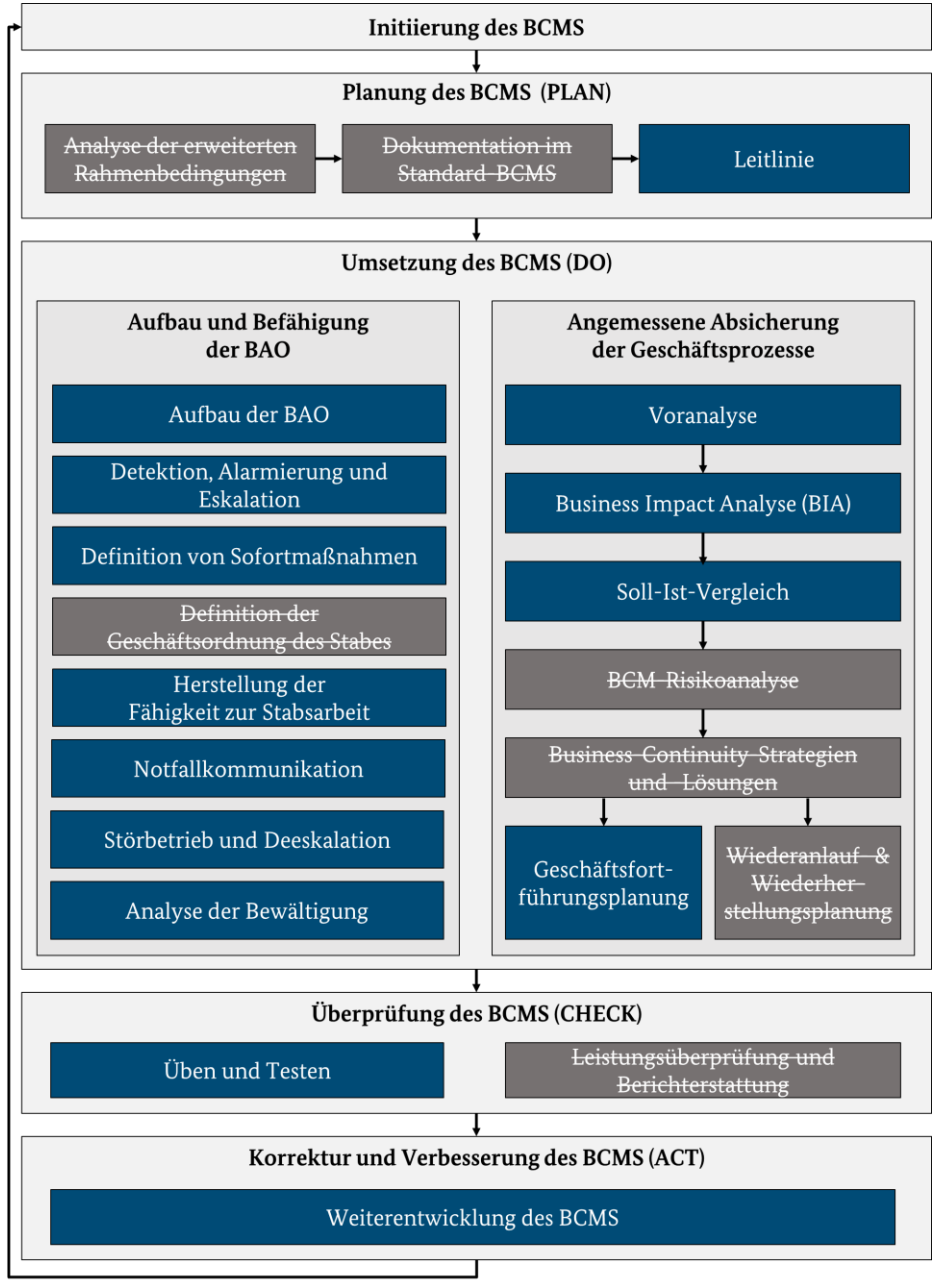
Stufenmodell - Methodik

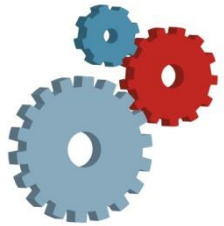
Reaktiv-BCMS

Legende

Prozessschritt des Reaktiv-BCMS

~~Entfallener Prozessschritt des Standard-BCMS~~



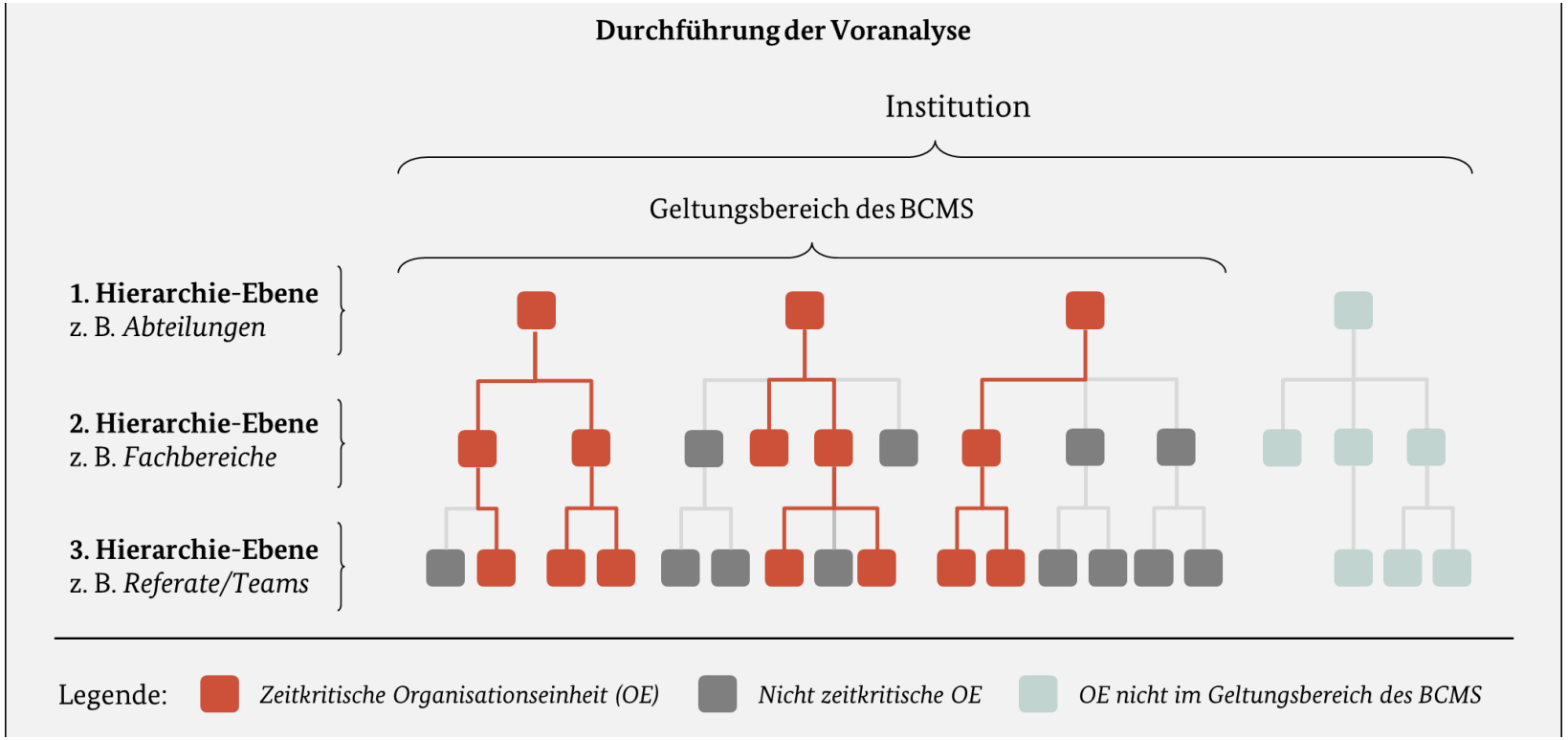


Bundesamt für Sicherheit in der Informationstechnik

Stufenmodell - Eingrenzung des Prozess-Umfangs

Voranalyse im Reaktiv- und Aufbau-BCMS

Anhand der Leitfrage: *„Sind bei einem Ausfall der (Geschäftsprozesse dieser) Organisationseinheit innerhalb von x (z.B. 7) Tagen hohe Schäden für die Institution zu erwarten?“*



Bundesamt für Sicherheit in der Informationstechnik

Übersicht über wesentliche Neuerungen

Neu im BSI-Standard 200-4

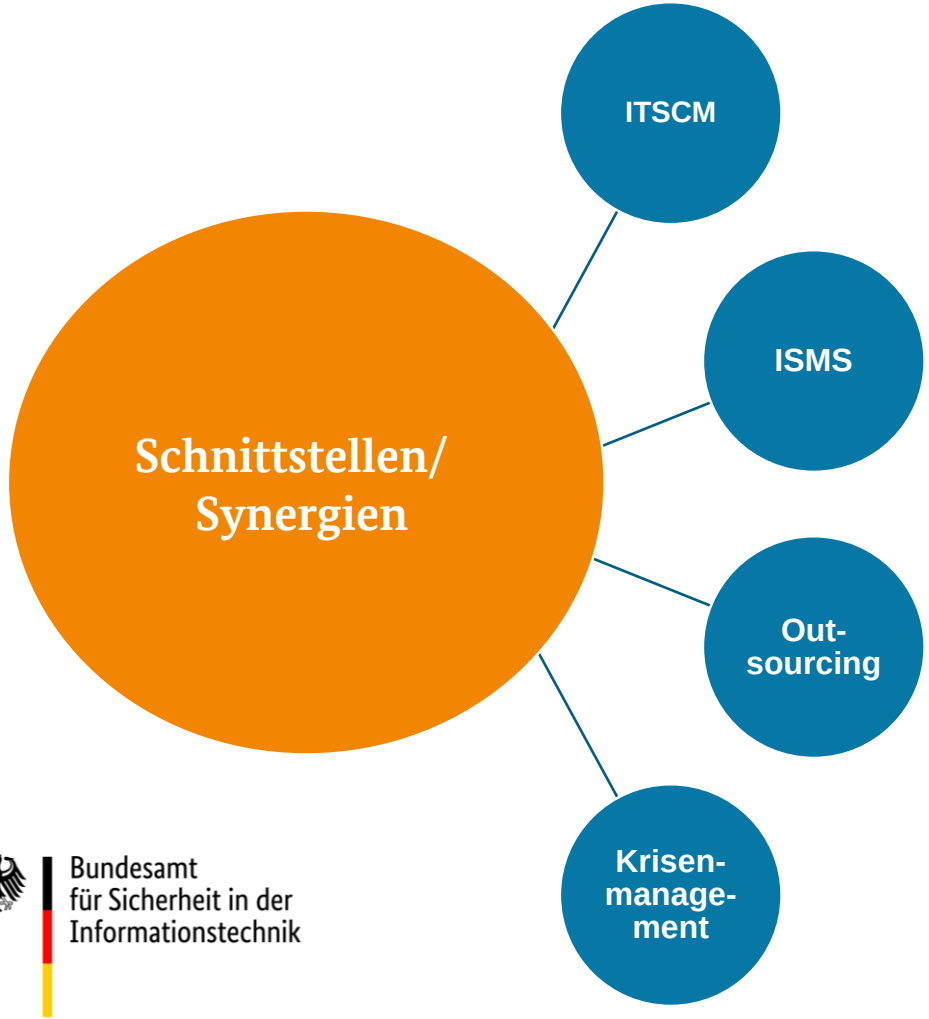
Übersicht über wesentliche Modernisierungen

... und vieles mehr!

Bundesamt für Sicherheit in der Informationstechnik

Neu im BSI-Standard 200-4

Abgrenzung zu weiteren Managementsystemen und Synergien in der Initiierung und darüber hinaus



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**

sichtigen. Unter anderem erfüllen die Risikomanagement-Standards BSI-Standard 200-3 *Risiko-management* sowie die Norm DIN ISO 31000:2018 *Risikomanagement –Leitlinien* diese Voraussetzung.

Synergiepotenzial:

Auf Grund der methodischen Kompatibilität zu anderen Arten von Risikoanalysen ist es nicht zwingend erforderlich, eine eigenständige Methodik für die BCM-Risikoanalyse festzulegen. Es ist empfehlenswert, in einem ersten Schritt zu prüfen, inwieweit vorhandene Risikoanalyse-Methoden der Institution angewendet werden können. Hierzu können die Anforderungen an eine BCM-Risikoanalyse mit den jeweiligen Zuständigen der bestehenden Risikoanalyse-Methoden abgestimmt werden, z. B. dem Risikomanager oder Informationssicherheitsbeauftragten.

- ...und vieles mehr.

Bundesamt
für Sicherheit in der
Informationstechnik

Änderungen gegenüber dem BSI-Standard 100-4

Etablierung und Befähigung der BAO

Prozessuale Beschreibung zur Etablierung der BAO

4.2 Aufbau und Befähigung der BAO

In Kapitel 2.3 *Ablauf der Bewältigung* wurden bereits alle Phasen und Aktivitäten einer Bewältigung schematisch erläutert. Zahlreiche dieser Aktivitäten setzen jedoch voraus, dass die Institution vorbereitend die in diesem Kapitel beschriebenen Maßnahmen plant und umsetzt.

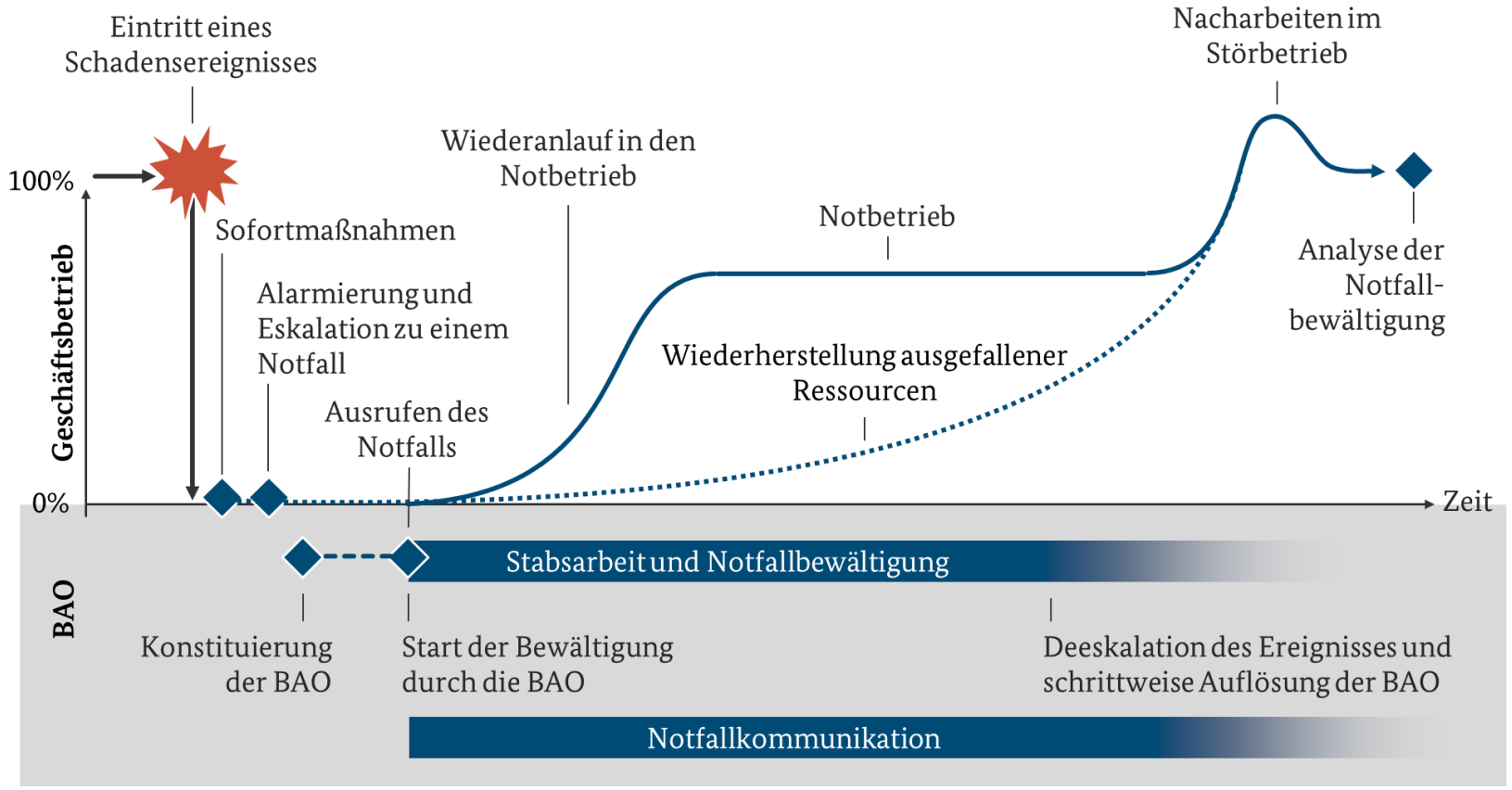
Hinweis:

Grundsätzlich werden Institutionen in die Lage versetzt, innerhalb der Institution alle Arten von Notfällen oder Krisen zumindest rudimentär zu bewältigen, wenn sie die Inhalte dieses Kapitels umsetzen. Wenn die Bewältigungsorganisation steht, jedoch noch keine Notfallpläne vorliegen, unterstützen dennoch die Ergebnisse der Analysen im Not- und Krisenfall die Bewältigungsorganisation. Vor allem die Ergebnisse der BIA sind zur Priorisierung extrem hilfreich.

Da die Bewältigungsorganisation zuerst aufgebaut wird und die Geschäftsprozesse noch nicht angemessen abgesichert wurden, sind bei einem Schadensereignis Ad-hoc-Lösungen erforderlich. Entsprechend der Definition dieses Standards befindet sich die Institution dabei in einer Krise. Da die organisatorischen Voraussetzungen zur Bewältigung für Notfälle und Krisen nahezu identisch sind, wird in diesem Kapitel nicht näher zwischen Notfällen und Krisen unterschieden.

Grundlagen

Übersicht über die Notfallbewältigung



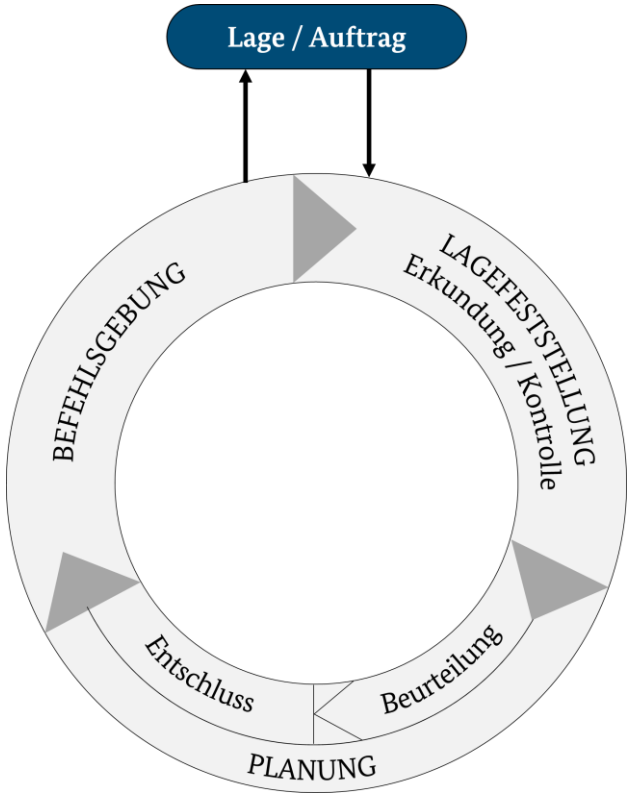
Mit BCMS

Änderungen gegenüber dem BSI-Standard 100-4

Etablierung und Befähigung der BAO

Zusätzliche Hintergrundinformationen in Hilfsmitteln

- Krisen- und Notfallstab
  - Gemeinsamkeiten und Unterschiede
- Führungszyklus
  - Beispielhaft: FOR-DEC und FwDV 100
- Notfall- und Krisenkommunikation
- Zusätzliche Informationen zum IT-Krisenmanagement



Änderungen gegenüber dem BSI-Standard 100-4

Vereinfachungen in der BIA

Vereinfachung in der Dokumentation:

Ausschließliche Dokumentation des kritischsten Schadensszenarios in der Schadensbewertung

Schadensszenario	24 Stunden	3 Tage	7 Tage	14 Tage	30 Tage
Beeinträchtigung der Aufgabenerfüllung	2 - mittel	3 - hoch	3 - hoch	3 - hoch	4 - sehr hoch
Verstoß gegen Gesetze, Vorschriften und Verträge	1 - gering	2 - mittel	2 - mittel	2 - mittel	2 - mittel
Negative Innen- und Außenwirkung	1 - gering	2 - mittel	4 – sehr hoch	4 – sehr hoch	4 – sehr hoch
Finanzielle Auswirkungen	1 - gering	2 - mittel	2 - mittel	2 - mittel	2 - mittel
Beeinträchtigung der persönlichen Unversehrtheit	1 - gering	1 - gering	1 - gering	1 - gering	1 - gering

Geschäftsprozess	24 Stunden	3 Tage	7 Tage	14 Tage	30 Tage
Sicherstellung IT-Betrieb	2-mittel	3 - hoch	4 - sehr hoch	4 - sehr hoch	4 - sehr hoch

+ Dokumentation der Begründung (relevantes Schadensszenario)

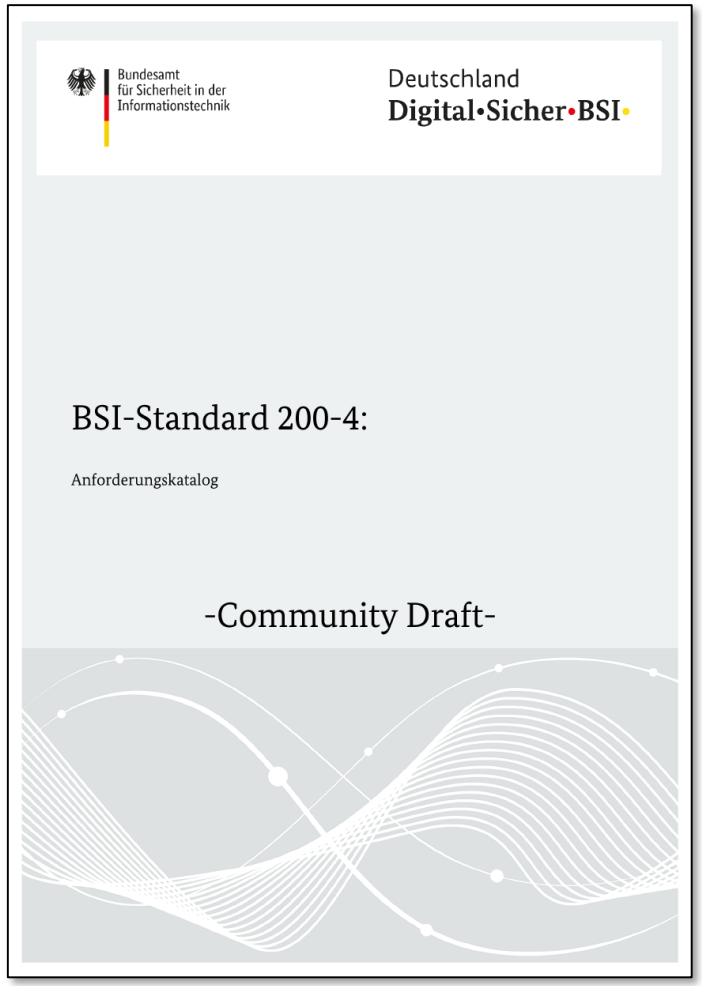
Neu im BSI-Standard 200-4

Anforderungskatalog* im normativen Anhang

Anforderungen auf einen Blick zur schnellen Übersicht

- Verwendung der IT-GS-Modalverben:
  - MUSS und
  - SOLLTE
- Arbeitserleichterung für erfahrene Anwender, welche die grundlegenden Anleitungen des Standards nicht benötigen
- Zusätzliches Mapping innerhalb des Katalogs (oder eines weiteren Hilfsmittels) auf die korrespondierenden Anforderungen der ISO 22301:2019

* Dieser wird in der CD-Phase als Hilfsmittel nachgereicht.



Bundesamt
für Sicherheit in der
Informationstechnik

Neu im BSI-Standard 200-4

Hilfsmittel - Übersicht

- Dokumentenvorlagen mit Beispieltexten (Leitlinie, Notfallvorsorgekonzept, Notfallhandbuch inkl. GFP und WAP)
- BIA-Auswertungsbogen
- BIA-Workshop-Präsentation
- BC-Strategien
- Dokumentenvergleich zur ISO 22301:2019
- Beispiellösungen

Sukzessive Veröffentlichung während der CD-Phase des BSI-Standards 200-4

Bundesamt für Sicherheit in der Informationstechnik

Informations- und Beteiligungsmöglichkeiten

Informations- und Beteiligungsmöglichkeiten

BCM-Info-Gruppe für IT-Grundschutz BCM-Aktivitäten

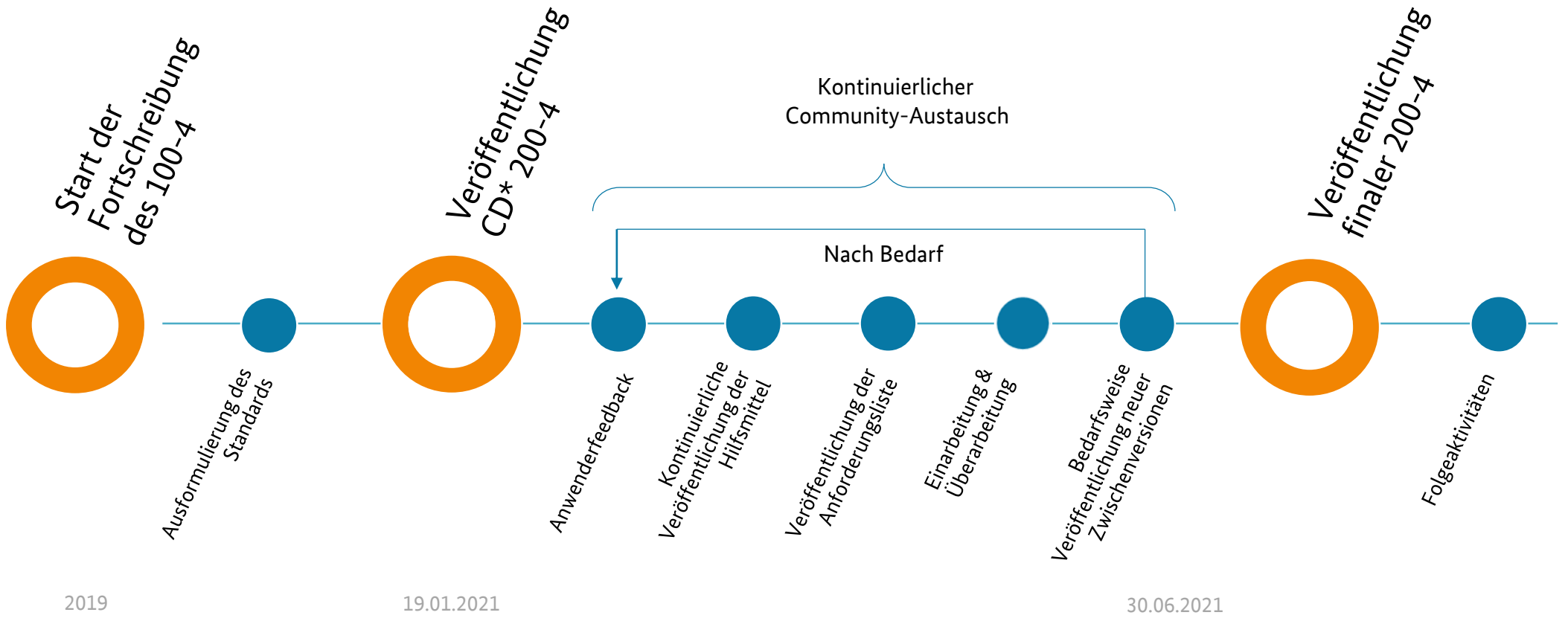
Info-Gruppe

- Information zur Veröffentlichung weiterer Hilfsmittel und weiterer Abfragen
- Kontinuierliche Information über BCM-Aktivitäten und Themen des IT-Grundschutzes
- Langfristiges Ziel: Transformation in ein BCM-Forum zum kontinuierlichen Community-Austausch
- Kein Konkurrenz-Forum zu bestehenden Gremien

Ausblick

Ausblick

Auf die Community-Draft-Phase



Bundesamt für Sicherheit in der Informationstechnik

Community **Draft: Nichtfinale Version des Standards, die zum Austausch mit und zur Kommentierung durch die Anwendercommunity frei veröffentlicht wird.*

Vielen Dank für Ihre Aufmerksamkeit

Kontakt

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

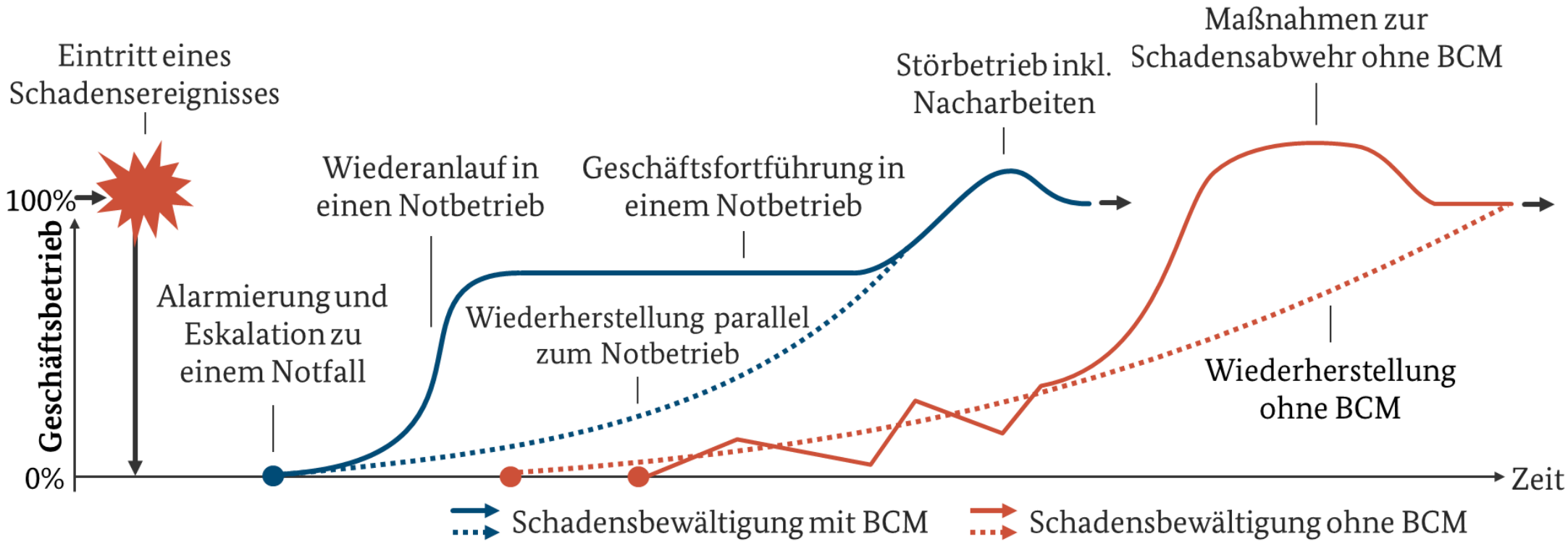
Bundesamt für Sicherheit in der Informationstechnik
Referat „BSI-Standards und IT-Grundschutz“
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Backup

Grundlagen

Übersicht über die Notfallbewältigung



Ohne BCMS

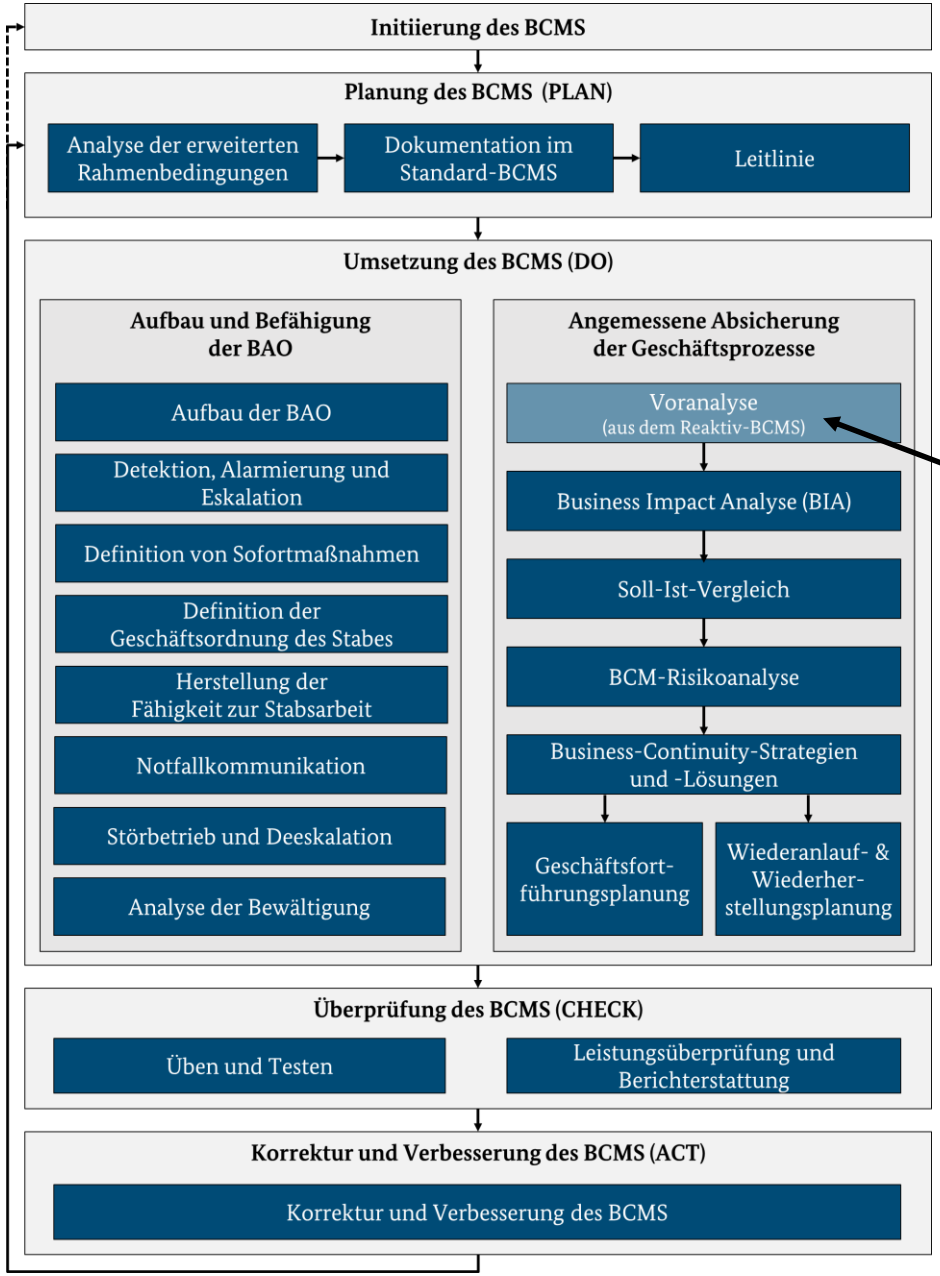
Stufenmodell - Methodik

Aufbau-BCMS
Standard-BCMS

Legende

Prozessschritt des Standard-BCMS

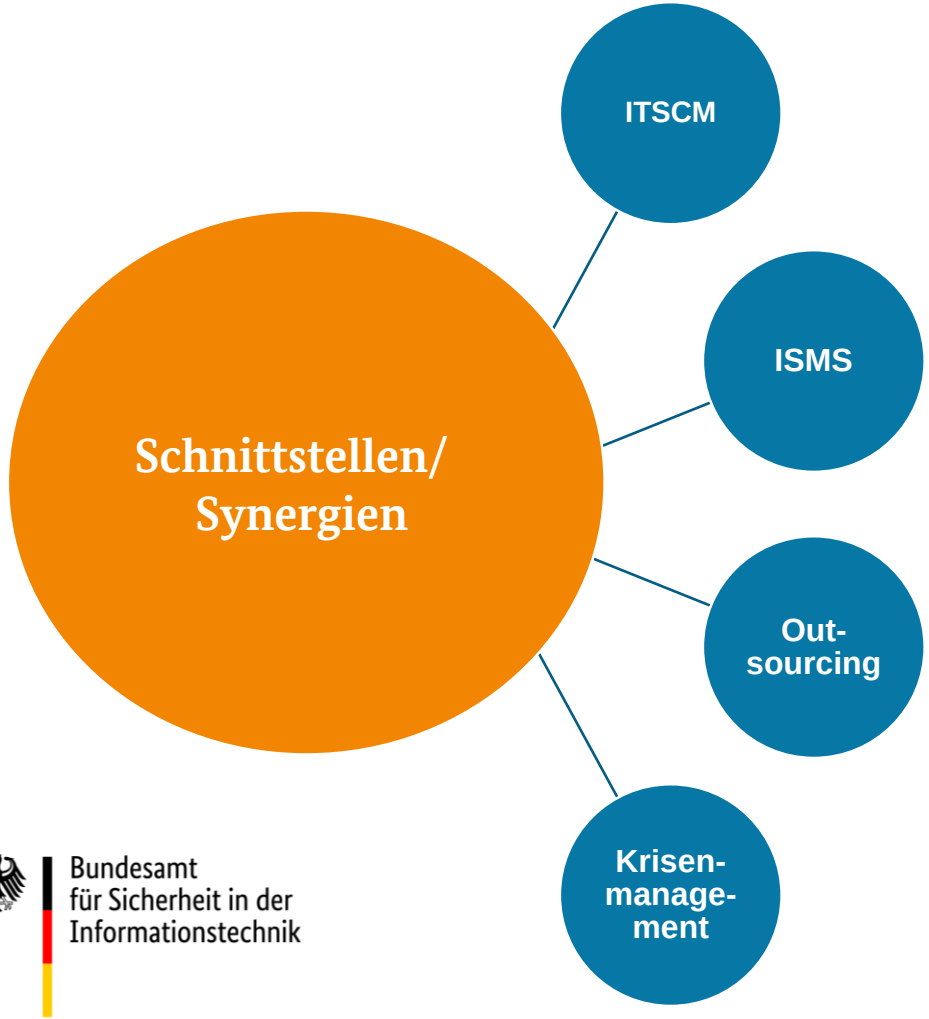
Prozessschritt des Reaktiv-BCMS



Nur für das Aufbau-BCMS relevant

Neu im BSI-Standard 200-4

Abgrenzung zu weiteren Managementsystemen und Synergien in der Initiierung und darüber hinaus



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**

sichtigen. Unter anderem erfüllen die Risikomanagement-Standards BSI-Standard 200-3 *Risiko-management* sowie die Norm DIN ISO 31000:2018 *Risikomanagement –Leitlinien* diese Voraussetzung.

Synergiepotenzial:

Auf Grund der methodischen Kompatibilität zu anderen Arten von Risikoanalysen ist es nicht zwingend erforderlich, eine eigenständige Methodik für die BCM-Risikoanalyse festzulegen. Es ist empfehlenswert, in einem ersten Schritt zu prüfen, inwieweit vorhandene Risikoanalyse-Methoden der Institution angewendet werden können. Hierzu können die Anforderungen an eine BCM-Risikoanalyse mit den jeweiligen Zuständigen der bestehenden Risikoanalyse-Methoden abgestimmt werden, z. B. dem Risikomanager oder Informationssicherheitsbeauftragten.

- ...und vieles mehr.

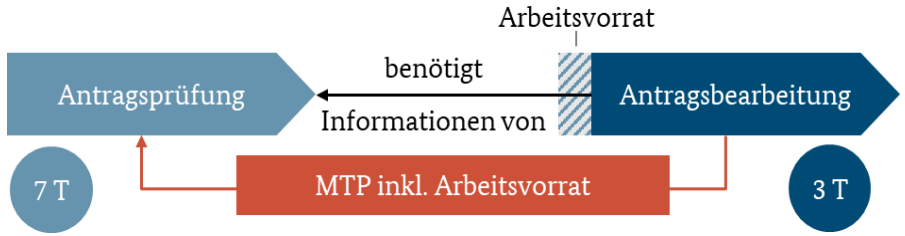
Bundesamt
für Sicherheit in der
Informationstechnik

Änderungen gegenüber dem BSI-Standard 100-4

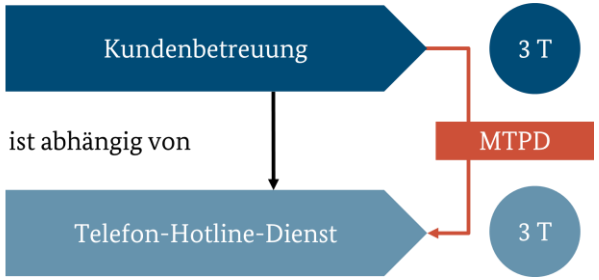
Vereinfachungen in der BIA

Vererbung von Prozessabhängigkeiten

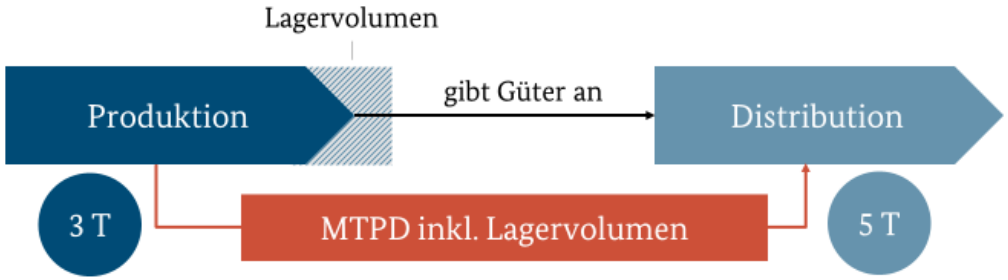
- Falls keine Prozesslandkarte vorhanden: Prozessabhängigkeiten **iterativ** über mehrere PDCA-Zyklen erfassen
- Bestimmung der MTPD/MTA der abhängigen Prozesse durch **Abstimmung** mit den relevanten Prozessen, keine Formellösung



Informationsbasierte Abhängigkeit



Parallele Abhängigkeit

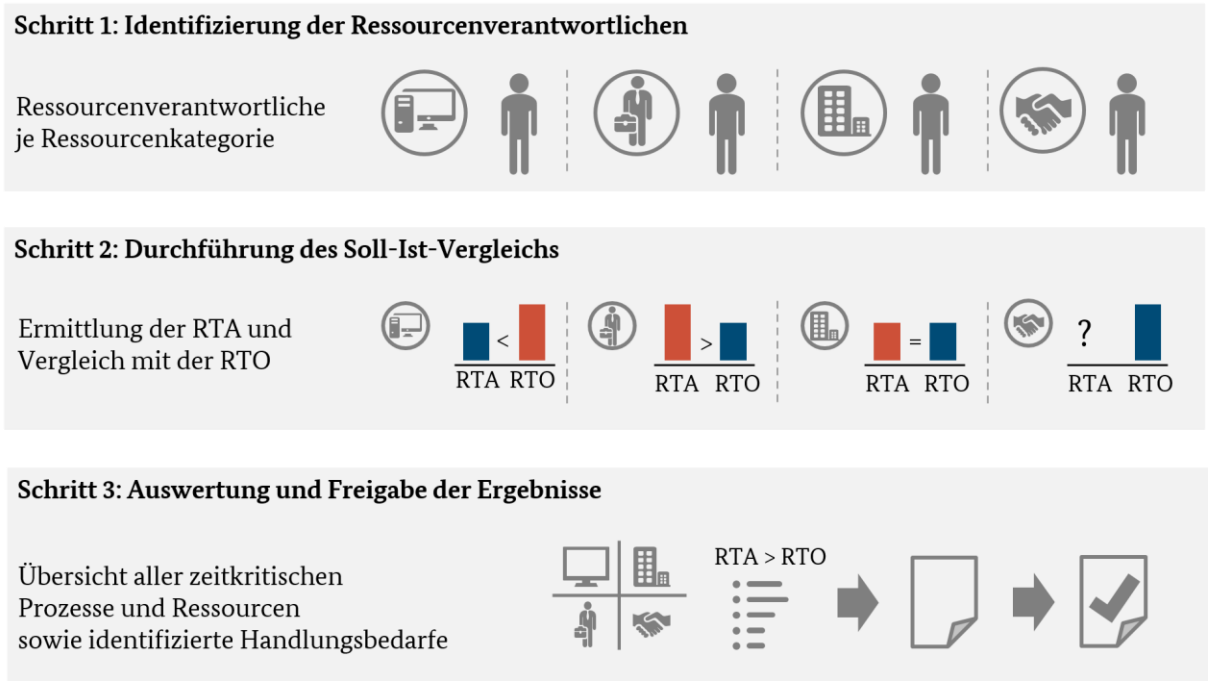


güterbedingte Abhängigkeit

Neu im BSI-Standard 200-4

Soll-Ist-Vergleich

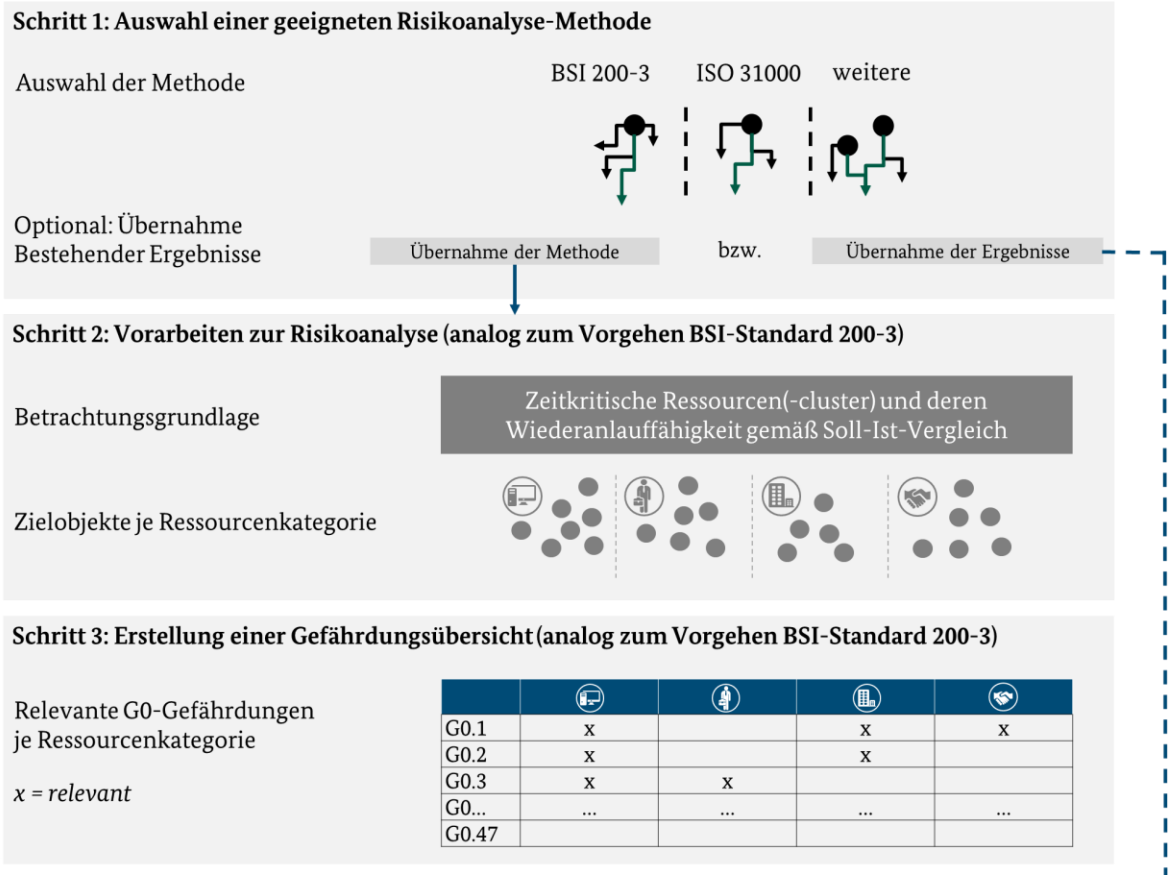
- Systematische Vorgehensweise zum Abgleich des IST-Zustandes (RTA) mit dem SOLL-Zustand (RTO)
- Neuer Begriff: Recovery Time Actual (RTA)
- Ausgangspunkt für eine zielgerichtete Risiko-Analyse



Bundesamt
für Sicherheit in der
Informationstechnik

Änderungen gegenüber dem BSI-Standard 100-4

Fokussierung auf Besonderheiten der BCM-Risiko-Analyse



Freie Auswahl der Methode:
Grundsätzlich kann die Methode/Vorgehensweise zur Risiko-Analyse frei gewählt werden, sofern diese die Anforderungen des 200-4 erfüllt.

Synergiemöglichkeit

Ergebnisse bestehender Risiko-Analyse-Methoden können – sofern geeignet – direkt weiterverwendet werden.

Bundesamt für Sicherheit in der Informationstechnik

Änderungen gegenüber dem BSI-Standard 100-4

Fokussierung auf Besonderheiten der BCM-Risiko-Analyse

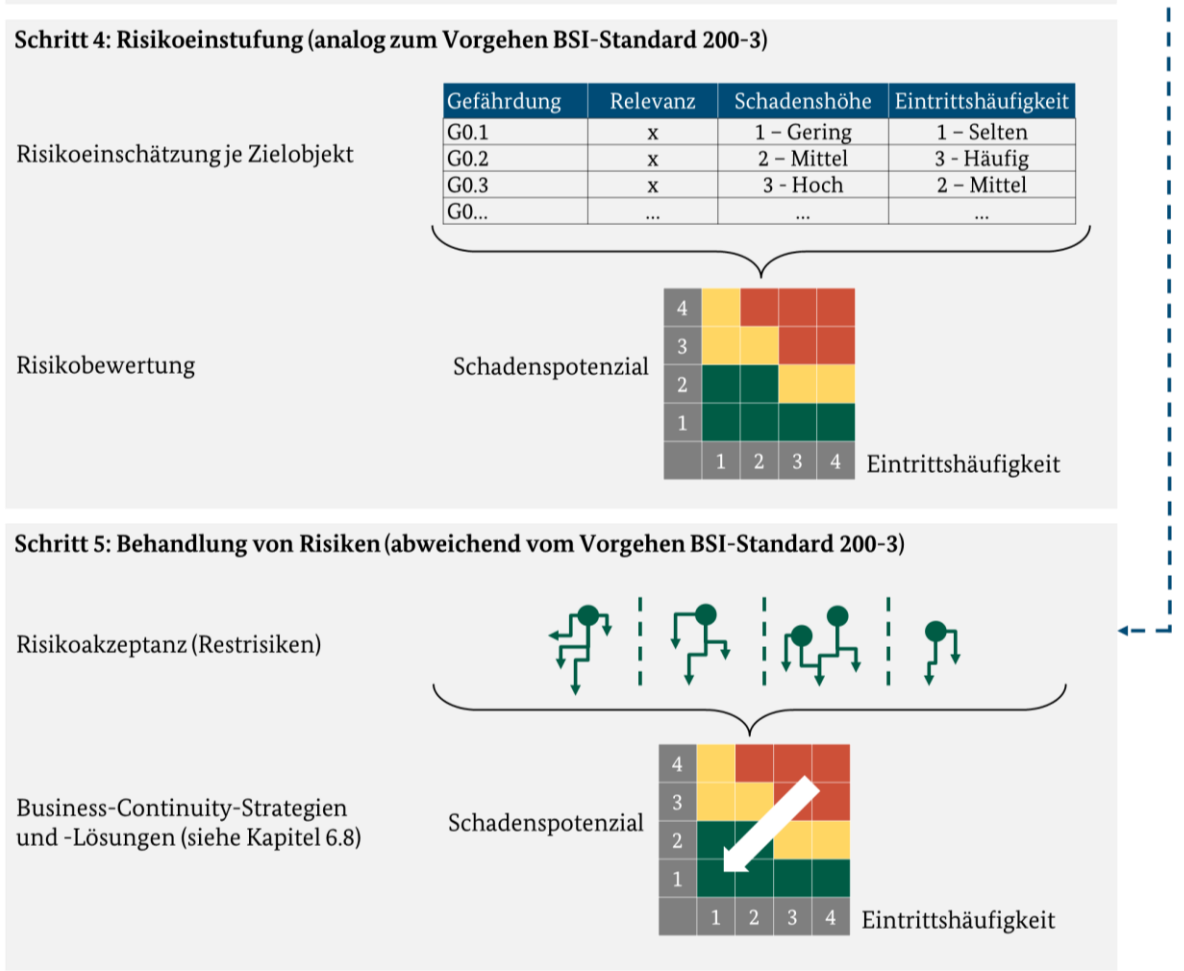
Fokussierung der Methodik am Bsp. 200-3:
Auf BCM-relevante Aspekte und auf Identifizierung und Bewertung der Risiken.

Abweichende Behandlung der Risiken

Im BCM werden Risiken in der Regel durch übergreifende BCM-Strategien und Lösungen gelöst, anstelle einzelner Insellösungen.

Fließender Übergang zum Folgeschritt

Klare Darstellung des Zusammenhangs BCM-Strategien und Ergebnisse der BCM-Risikoanalyse.



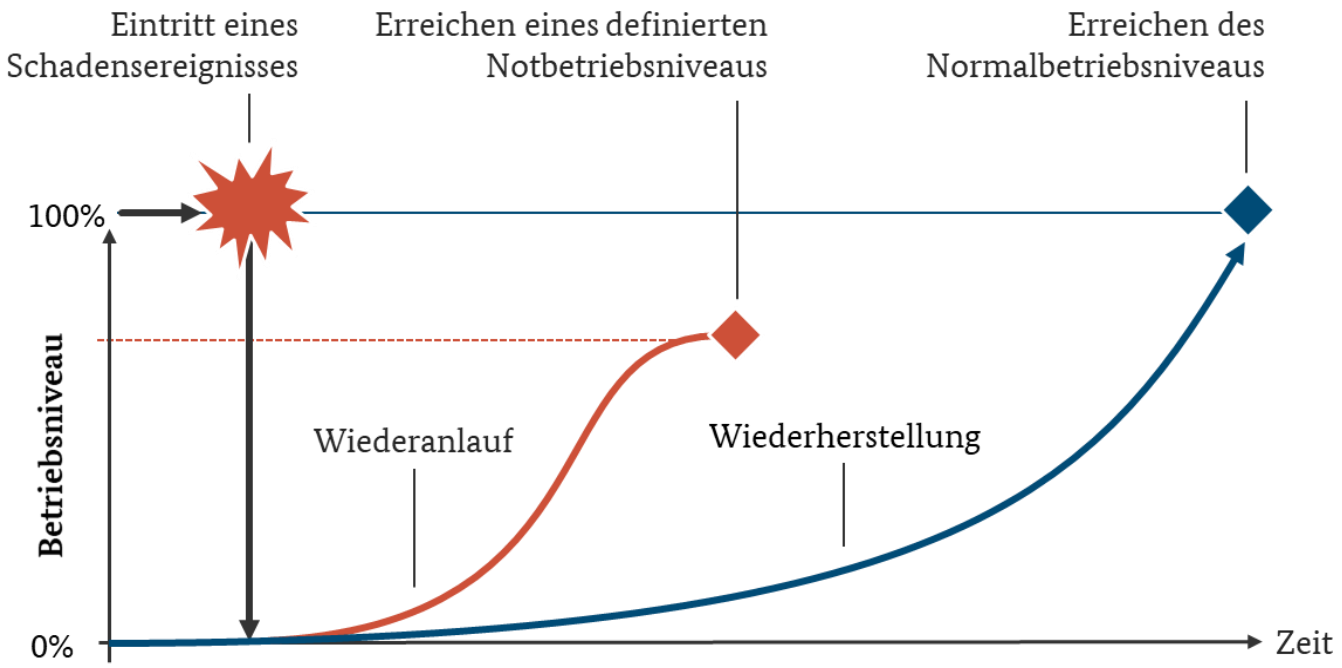
Bundesamt für Sicherheit in der Informationstechnik

Neu im BSI-Standard 200-4

Systematische Anleitung zur Erstellung der GFPs, WAPs/WHPs

Erläuterungen im BSI-Standard ermöglichen ein **Bearbeiten** der Pläne anhand der zur Verfügung gestellten Formatvorlagen aus den **Hilfsmitteln ohne weitere Anleitungen**.

Die aus dem BSI-Standard 100-4 bekannte Aufteilung in **GFPs, WAPs** und **WHPs** wird fortgeführt. Unterschied zwischen WAP und WHP:



Neu im BSI-Standard 200-4

Systematische Anleitung zur Erstellung der GFPs, WAPs/WHPs

Schritt 1: Vorbereitung der WAP/WHP

Vorlage und Terminplanung der WAP/WHP

- *Wie sollen die WAP/WHP dokumentiert werden?*
- *Welche Informationen sind bereits vorab bekannt?*
- *Wer erstellt die WAP/WHP?*
- *Wann und in welchem Modus sollen die WAP/WHP erstellt werden?*

Schritt 2: Erstellung der *WAP/WHP*

Notfallmaßnahmen

- *Allgemeine Informationen zur Ressource*
- *Technische Abhängigkeiten der Ressource*
- *Voraussetzungen für den Wiederanlauf*
- *Beschreibung der Wiederanlaufschritte*
- *Notfallrelevante Dokumente*
- *Notfallrelevante interne und externe Kontakte*

Schritt 3: Qualitätssicherung und Freigabe

Qualitätsgesicherte und freigegebene WAP/WHP

- *Prüfung, ob die WAP/WHP vollständig, plausibel und aktuell sind*
- *Formale Freigabe, um die WAP/WHP in einem Notfall nutzen zu dürfen*

Bundesamt für Sicherheit in der Informationstechnik

Neu im BSI-Standard 200-4

Systematische Anleitung zum Üben und Testen

- Systematische Vorgehensweise zum Üben und Testen
- Vereinfachung bzw. Reduzierung der Übungsarten auf:
  - Alarmierungsübungen
  - Stabsübungen
  - Stabsrahmenübungen
  - Planbesprechungen
  - Funktionstests

Bundesamt
für Sicherheit in der
Informationstechnik