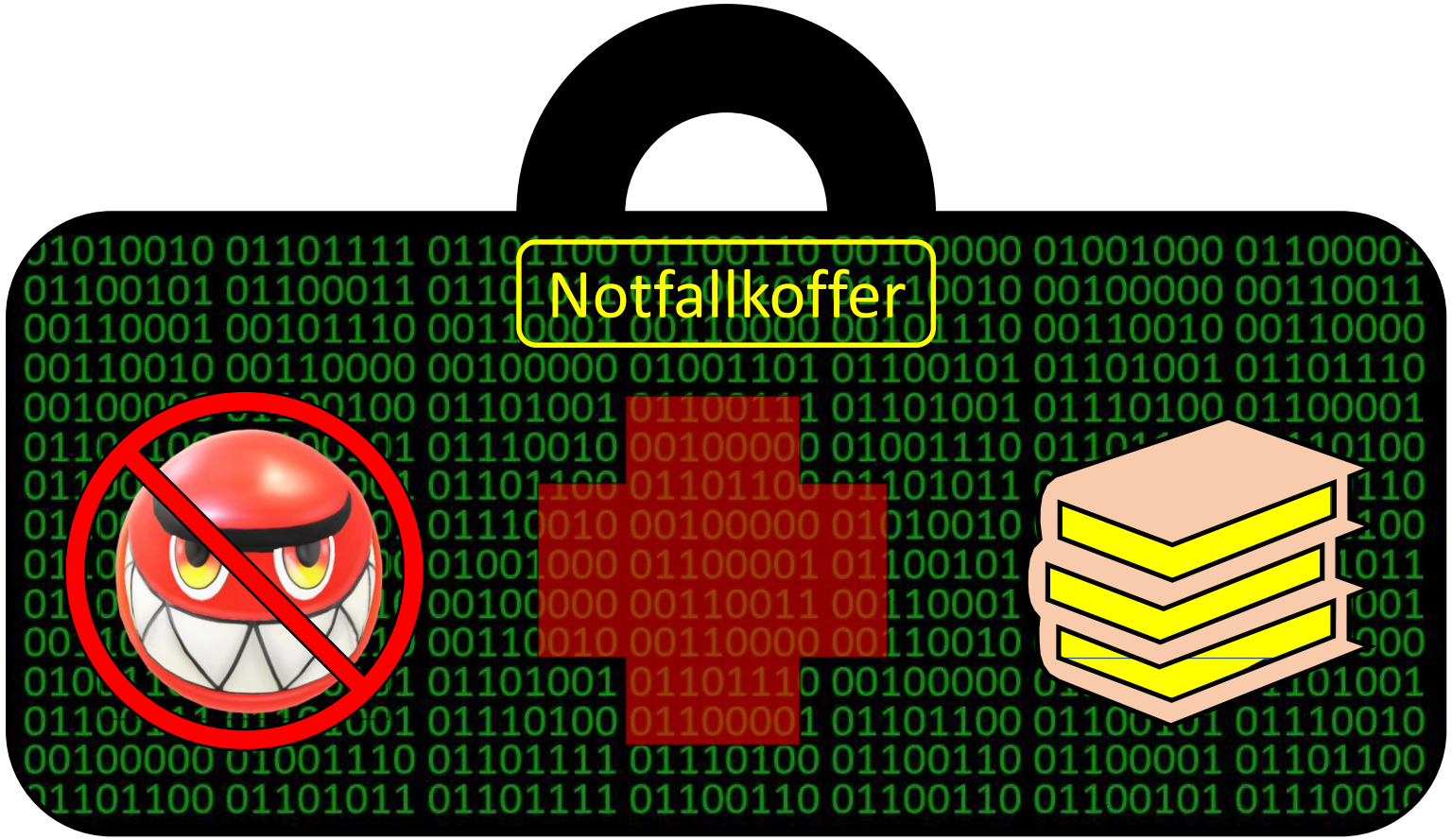
Virtuelle No-Spy Konferenz #NSKonline am 31.10.2020

Mein digitaler Notfallkoffer

Rolf Häcker

Mein digitaler Notfallkoffer



Mein digitaler Notfallkoffer

Was ist drin?

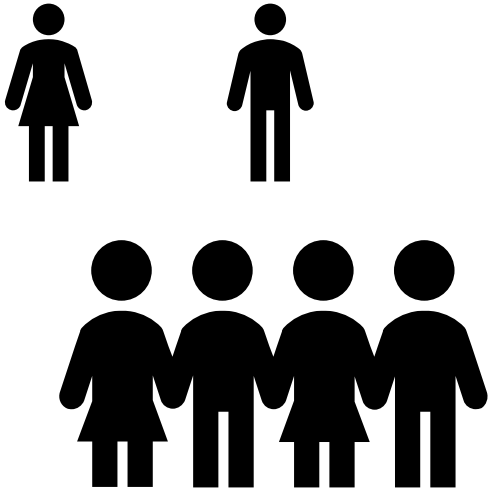
Verschiedene Facetten des Notfallmanagements

- Notwendigkeit
- Notfallvorsorge
- Notfallbehandlung

Adressatenkreis

Zielgruppen

- Privatpersonen
- Kleine Unternehmen und
- Sonstige Organisationen



Handlungsbedarf IT-Notfall

Zunehmende IT-Nutzung

- Abhängigkeit
- Grundwerte der Informationssicherheit
  - Vertraulichkeit — Confidentiality (C)
  - Integrität — Integrity (I)
  - Verfügbarkeit — Availability (A)
- Bei Unternehmen/Organisationen auch Rechtliche Anforderungen §

Auslösung IT-Notfall

- Was ist ein IT-Notfall?
- Wer entscheidet?
- Wie schnell?
- Was passiert dann?

IT-Notfall-Behandlung

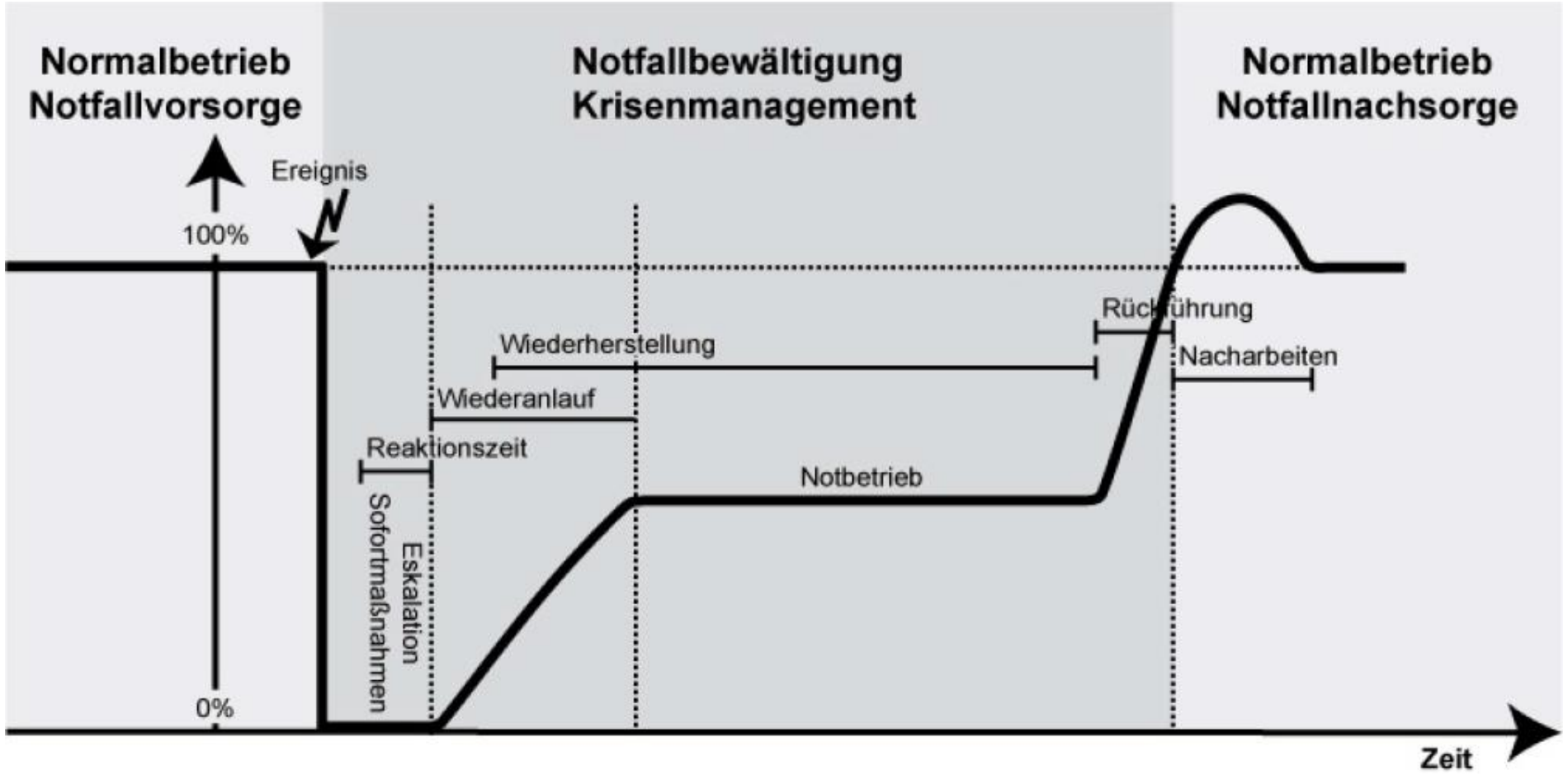
Wir brauchen einen Plan!

Abgrenzung Störung, Notfall und Krise

Vorfallsart	Erläuterung	Behandlung
Störung	Kurzzeitiger Ausfall von Prozessen oder Ressourcen mit nur geringem Schaden	Behandlung ist Teil der üblichen Störungsbehebung.
Notfall	**Länger andauernder Ausfall von Prozessen oder Ressourcen mit hohem oder sehr hohem Schaden**	**Behandlung verlangt besondere Notfallorganisation.**
Krise	Im Wesentlichen auf die Institution begrenzter verschärfter Notfall, der die Existenz der Institution bedroht oder die Gesundheit oder das Leben von Personen beeinträchtigt.	Da Krisen nicht großflächig die Umgebung oder das öffentliche Leben beeinträchtigen, können sie, zumindest größtenteils, innerhalb der Institution selbst behoben werden.
Katastrophe	Räumlich und zeitlich nicht begrenztes Großschadensereignis, zum Beispiel als Folge von Überschwemmungen oder Erdbeben	Aus Sicht einer Institution stellt sich eine Katastrophe als Krise dar und wird intern durch deren Notfallorganisation in Zusammenarbeit mit den externen Hilfsorganisationen bewältigt.

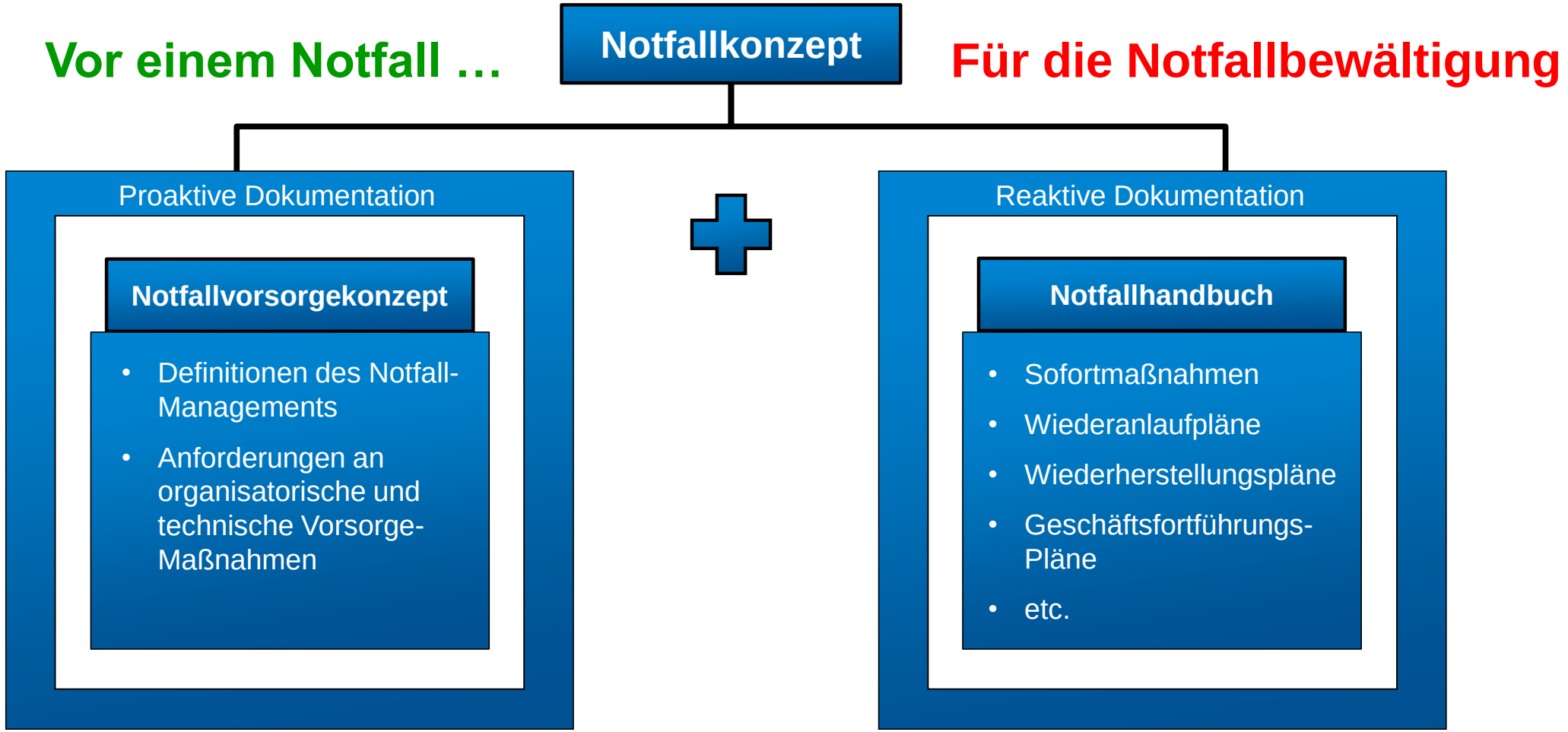
Störungen, Notfälle, Krisen und Katastrophen im Verständnis des BSI-Standards 100-4

Notfallbewältigungsphasen schematisch

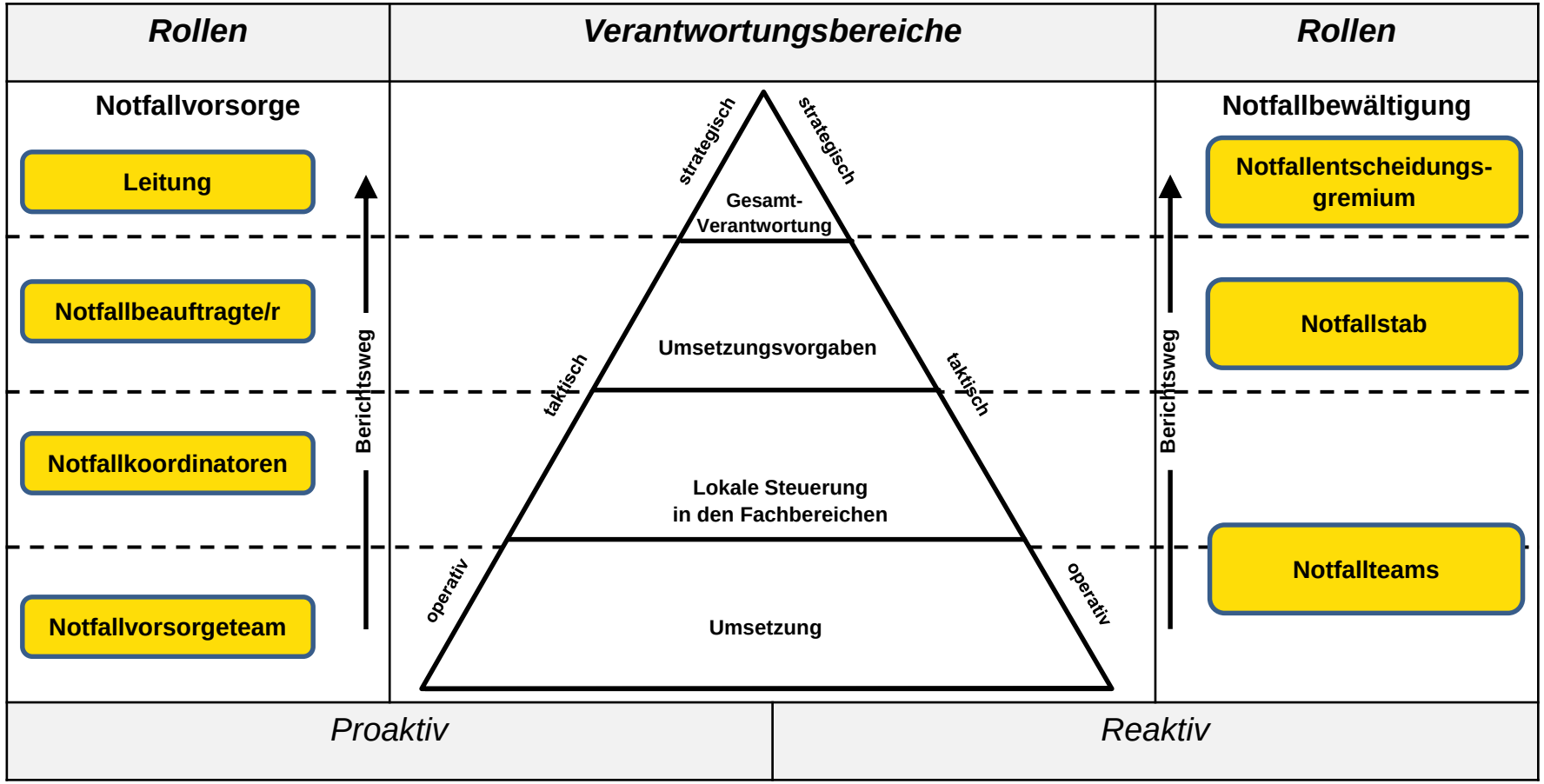


Aus BSI 100-4

Notfallvorsorgekonzept und Notfallhandbuch bilden das Notfallkonzept



Rollen und Verantwortungsbereiche

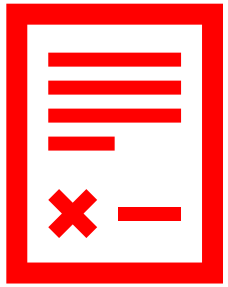


Notfallvorsorge

- Unterlagen des BSI:
- **Notfallkoordinator**
- Notfallvorsorge-Team
- Notfallvorsorgekonzept erstellen

Notfallvorsorge

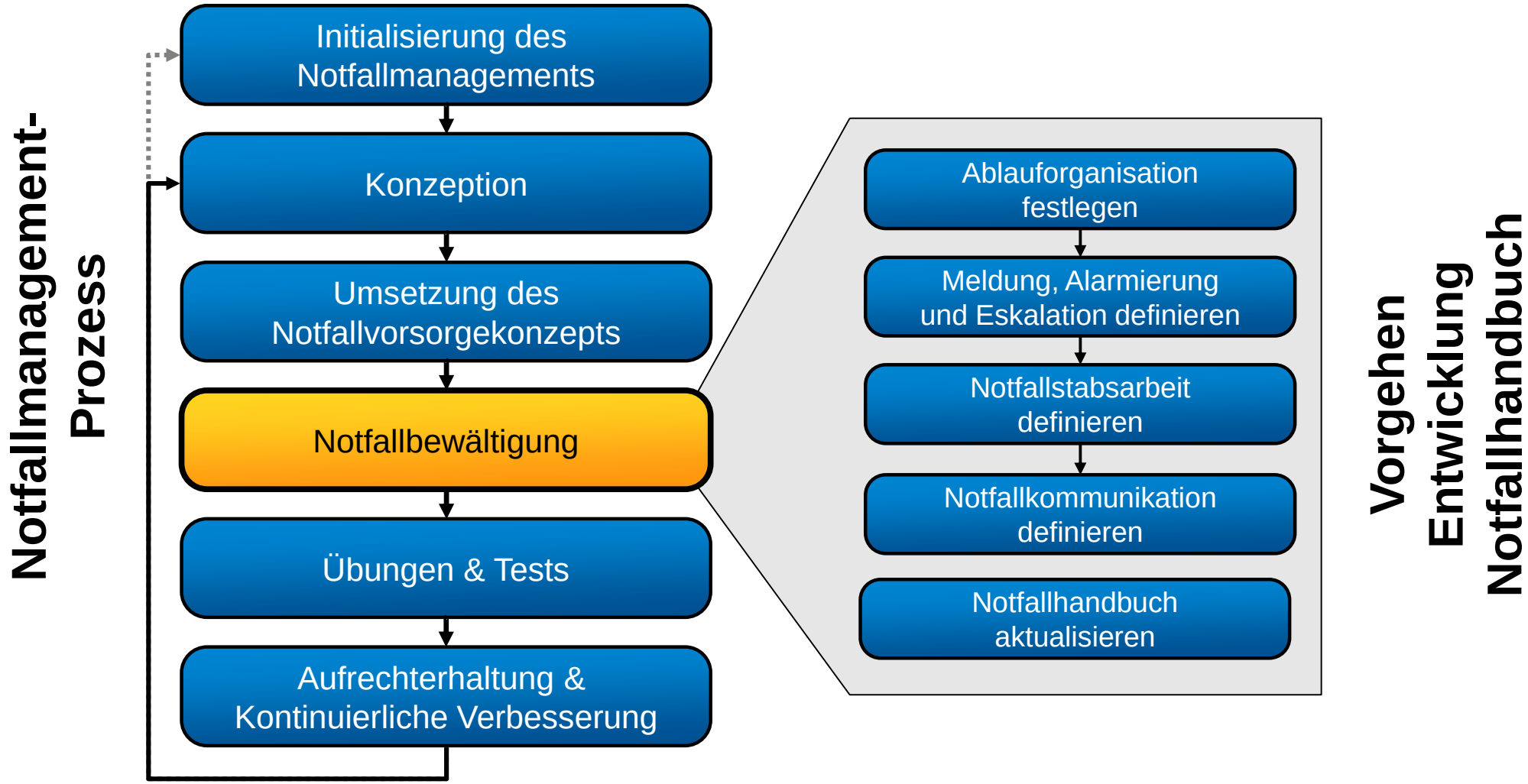
- Auftrag
- Notfallleitlinie oder Notfallrichtlinie
- Notfallvorsorgekonzept
  - Definitionen,
  - Abgrenzungen,
  - Ziele



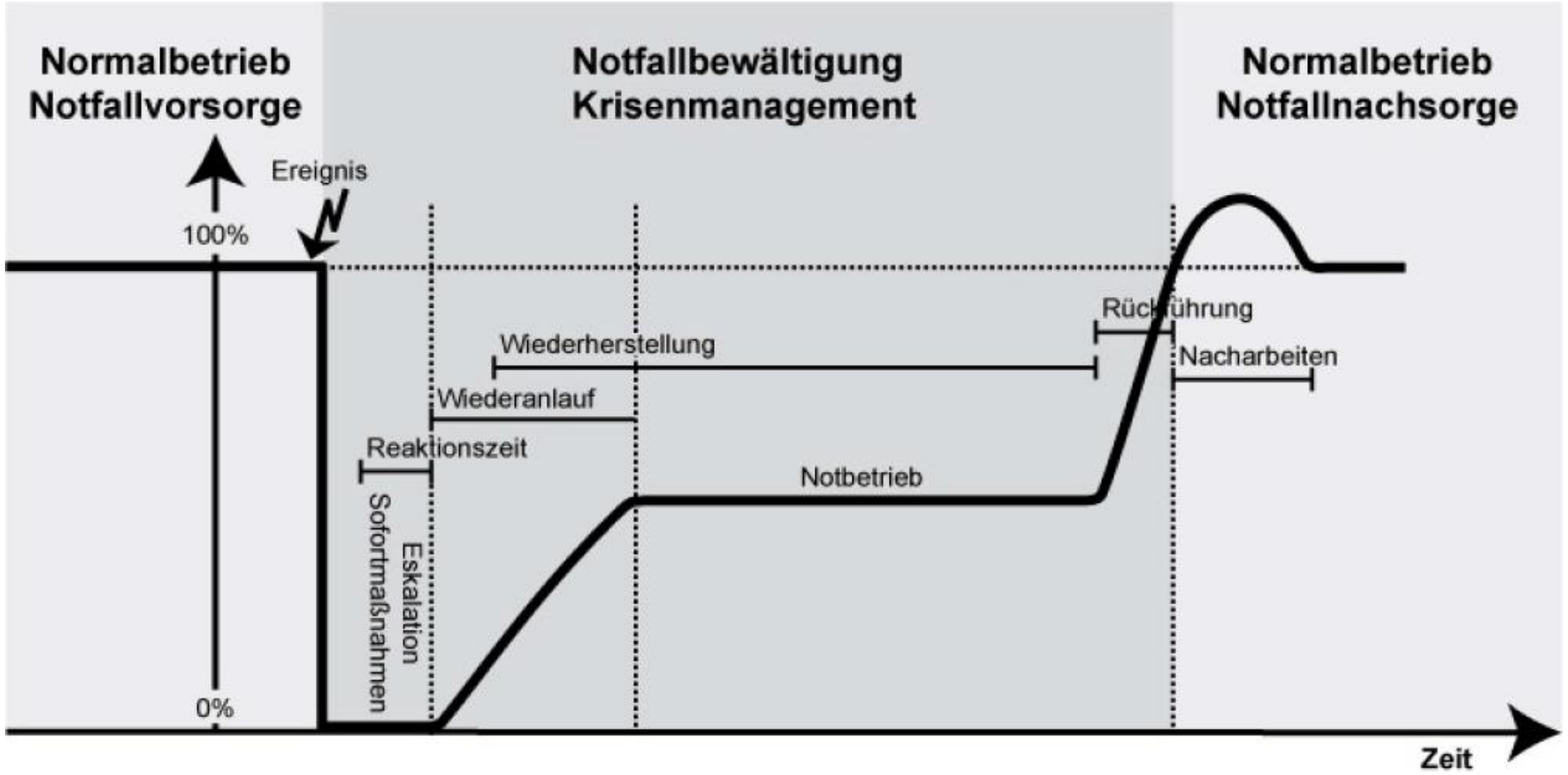
Notfallbewältigung

- Unterlagen des BSI:
- Notfallhandbuch
- **Notfall-Manager**
- Notfall-Team
- Erweitertes Notfall-Team

Die Notfallbewältigung ist Teil der Konzeptionsphase des BSI 100-4 Prozess

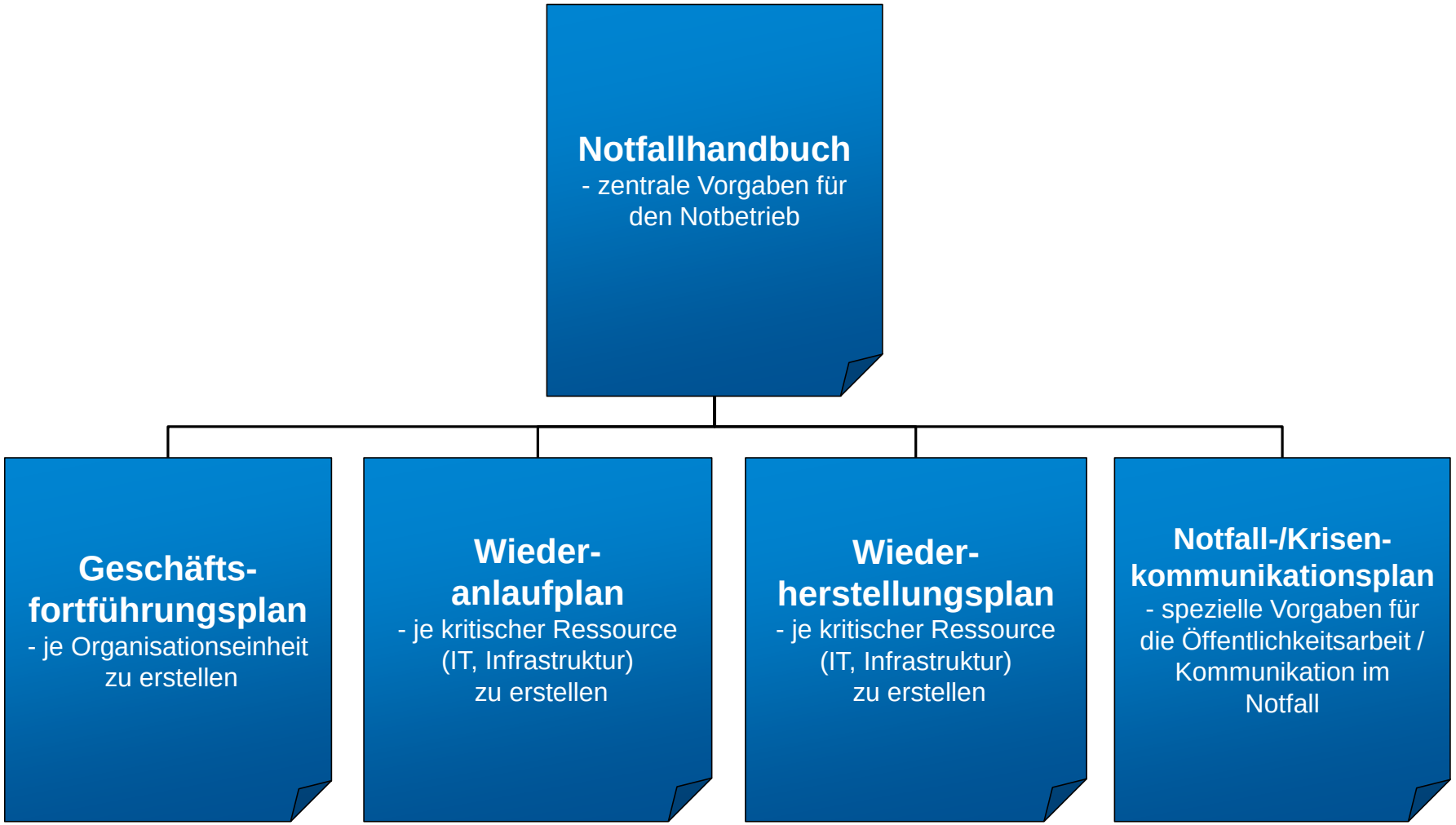


Notfallbewältigungsphasen schematisch

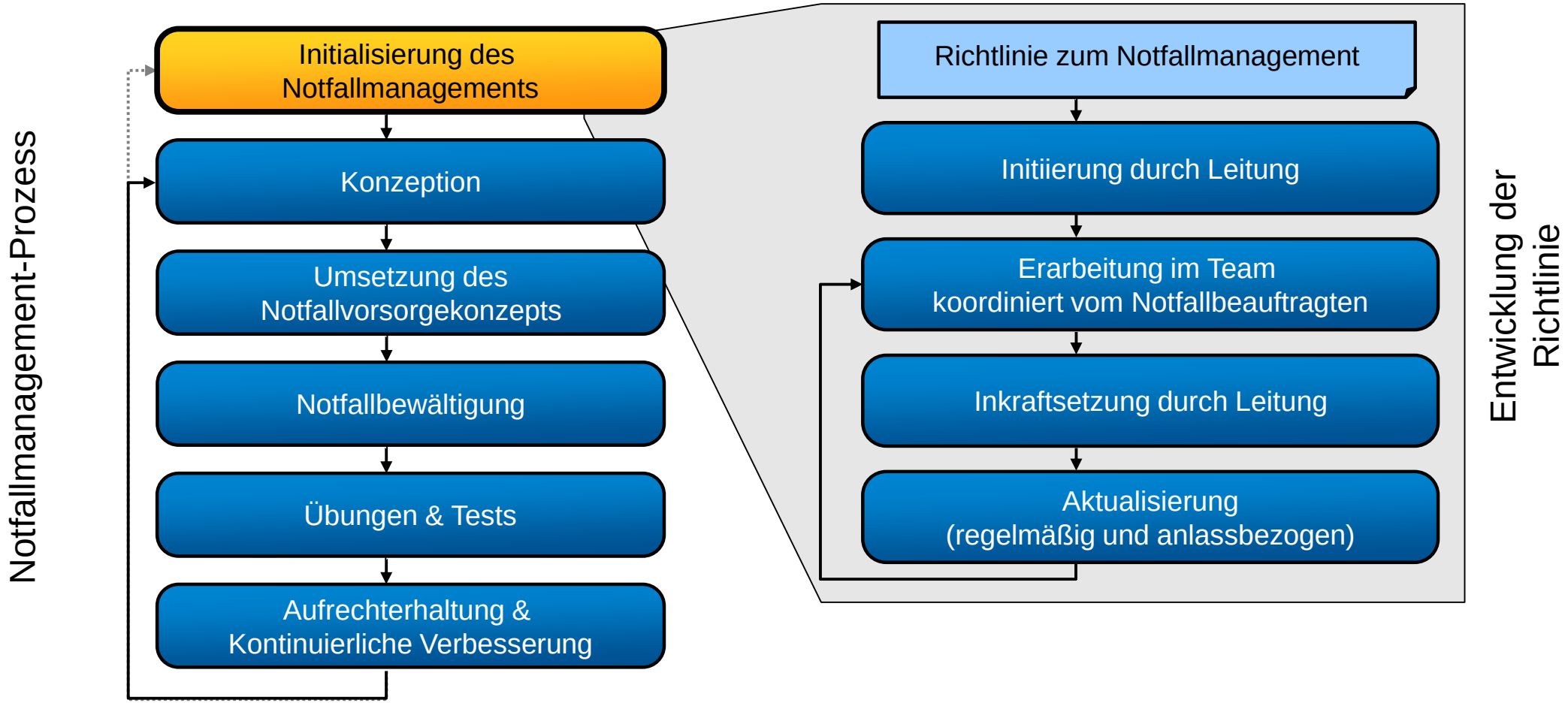


Aus BSI 100-4

Notfallhandbuch Dokumentübersicht (grafische Übersicht)

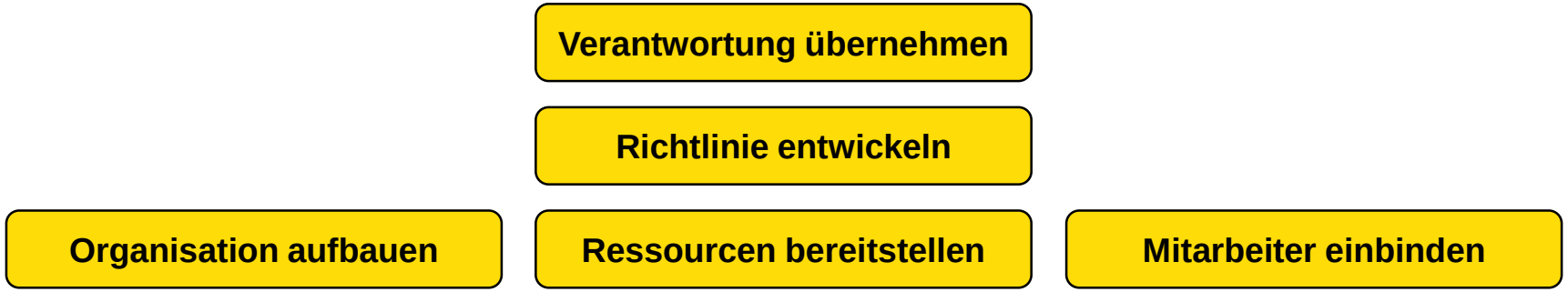


Die Richtlinie ist Teil der Initiierungsphase des Notfallmanagement-Prozesses



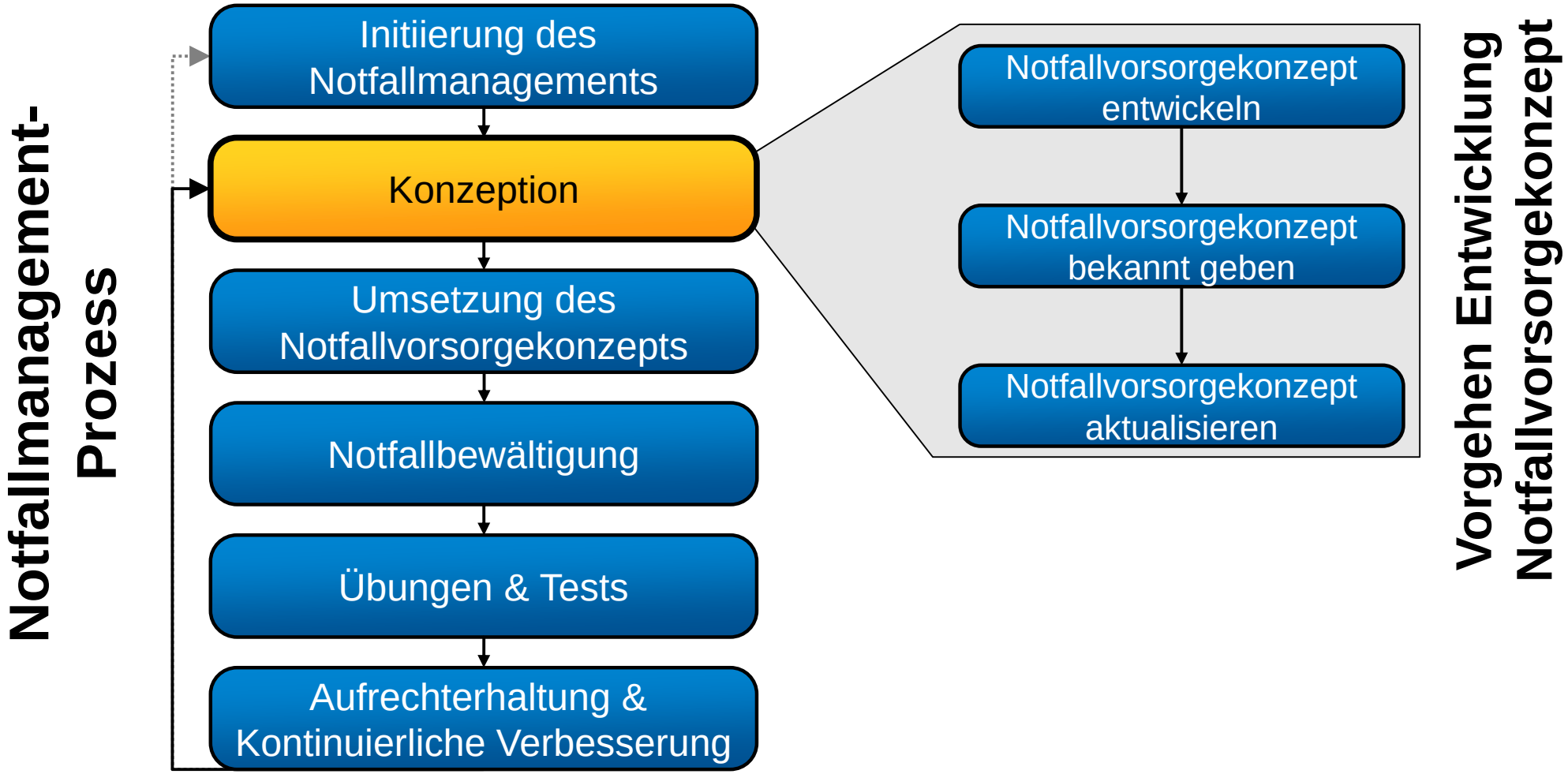
aus BSI 100-4

Notfallmanagement initiieren



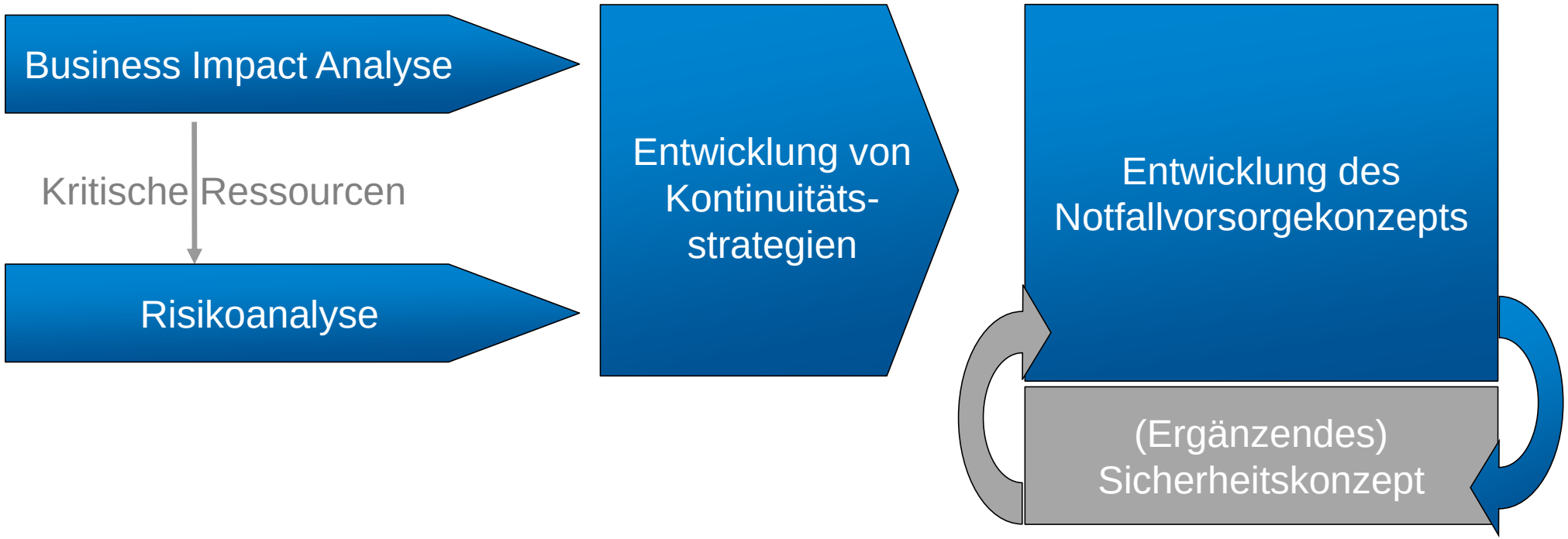
- Die Institutionsleitung übernimmt die Gesamtverantwortung für den Notfallmanagement-Prozess.
- Die Richtlinie zum Notfallmanagement wird entwickelt.
- Eine Organisationsstruktur wird aufgebaut.
- Es werden Ressourcen für die anstehenden Aufgaben bereitgestellt.
- Die Mitarbeiter werden in den Notfallmanagement-Prozess eingebunden.

Das Notfallvorsorgekonzept ist Teil der Konzeptionsphase des BSI 100-4 Prozesses



Grundlagen des Notfallvorsorgekonzepts

Achtung: Anforderungen der Sicherheit und des Datenschutzes im Notfallvorsorgekonzept berücksichtigen



Grenzwerte für Schutzbedarfskategorien

„A“	**Die Schadensauswirkungen sind begrenzt und überschaubar.**
„B“	**Die Schadensauswirkungen können beträchtlich sein.**
„C“	**Die Schadensauswirkungen können ein existenziell bedrohliches katastrophales Ausmaß erreichen.**

Die Grenzwerte für die Kategorien werden **spezifisch für die jeweilige Organisation** konkretisiert

ISMS Schutzbedarfsfeststellung

Schutzbedarfskategorien festgelegt nach den Grundwerten der Informationssicherheit

- **Vertraulichkeit,**
- **Integrität und**
- **Verfügbarkeit**

als Maßstab für den **Schutzbedarf** der **Verfahren und Anwendungen**

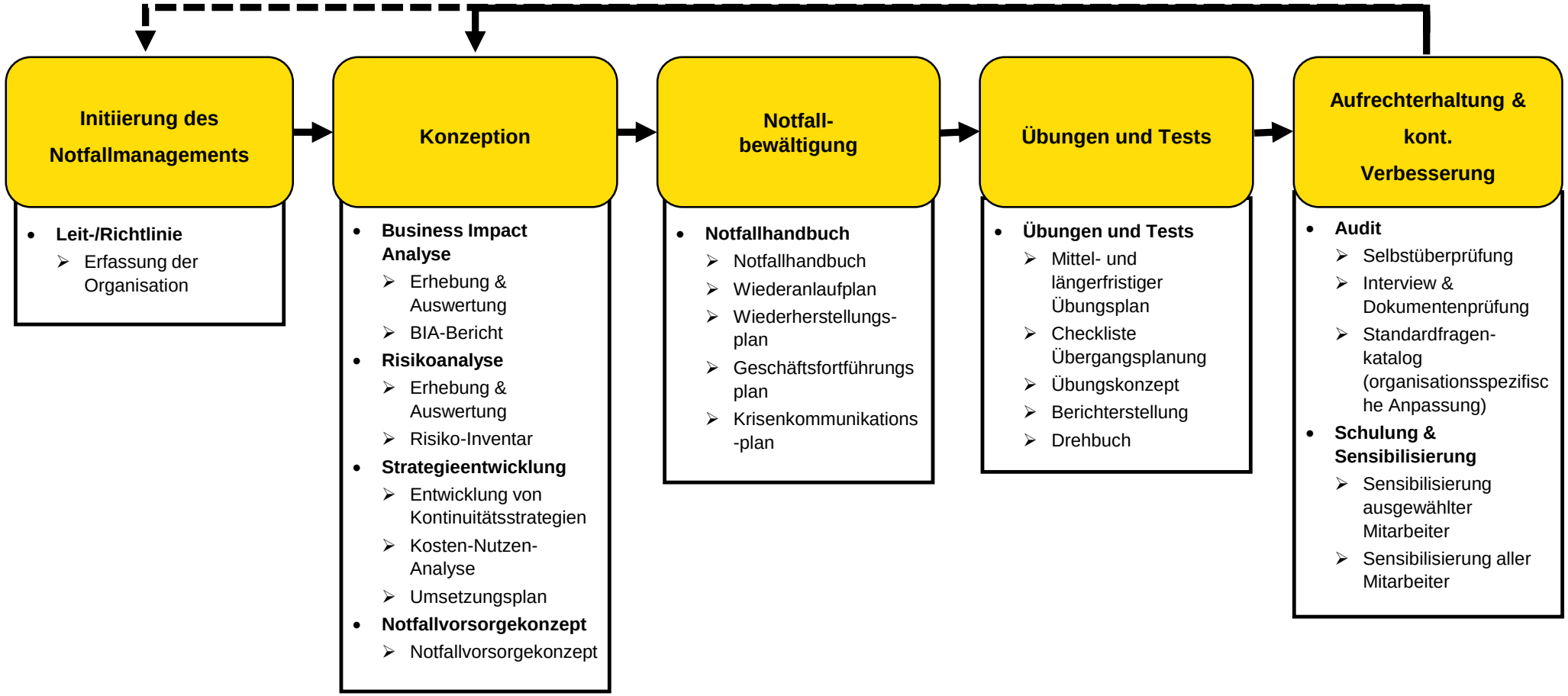
Szenarien

- Verstoß gegen Gesetze und Verträge
- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Beeinträchtigung der Aufgabenerfüllung (Maximal tolerierbare Ausfallzeit, MTA)
- Finanzielle Auswirkungen

BIA

- **Alle** (wichtigen) **Anwendungen** nach Schutzbedarfskategorien **klassifizieren** jeweils für
- Vertraulichkeit,
- Integrität und
- Verfügbarkeit
- Beispiel Anwendung „Datendrehscheibe“: **BAA**

Notfallmanagement nach BSI 100-4



https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Umsetzungsrahmenwerk/umra_node.html

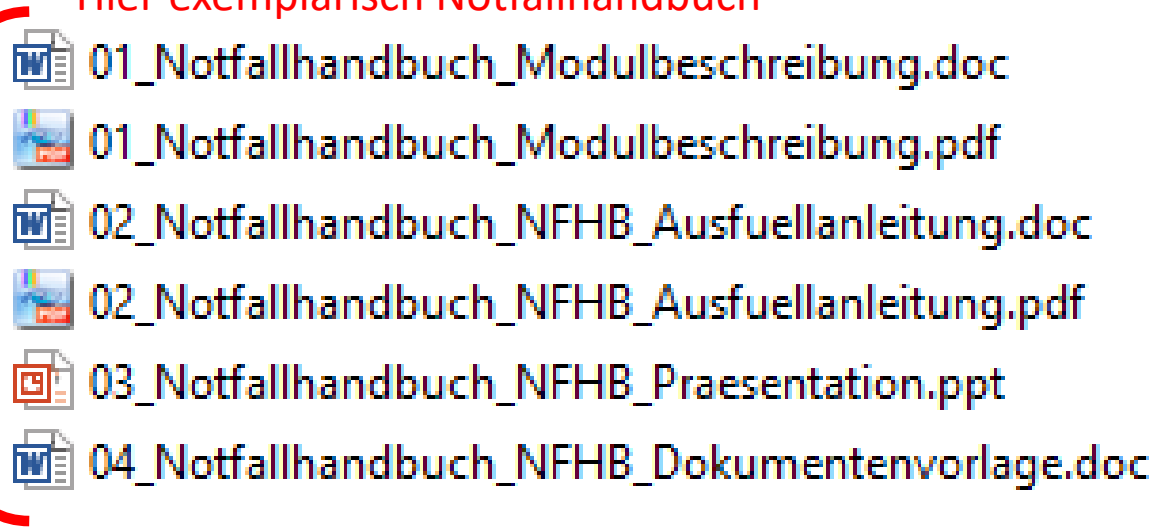
Unterlagen im Netz; BSI-Infos

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Umsetzungsrahmenwerk/umra_node.html

- **Umsetzungsrahmenwerk Hauptdokument**
- Leitfäden des Umsetzungrahmenwerks
- Modul "Leitlinie"
- Modul "Business Impact Analyse"
- Modul "Risikoanalyse"
- Modul "Strategieentwicklung"
- Modul "Notfallvorsorgekonzept"
- Modul "Notfallhandbuch"

  enthält Wiederanlauf-, Wiederherstellungs-, Geschäftsfortführungs- und Notfallkommunikationspläne
- Modul "Tests und Übungen"
- Modul "Schulung und Sensibilisierung„
- Modul "Audit"

Hier exemplarisch Notfallhandbuch



Notfallmanagement nach BSI 100-4

- **Notfallmangagement: Komplexer langwieriger Prozess!**
- Ausblick **200-4**:
  Phasen können auch parallel angegangen werden!
- **→ Bildung eines Notfallteams**
  schon vor Abschluss der BIAs

Notfall Auslösung

Was passiert dann?
Sofortmaßnahmen

- PC, Laptop Verbindungen trennen (Netzwerk-Kabel)
- Laptop in Flugmodus
- Firewall → Verbindungen deaktivieren
- Notfallteam einberufen
- Notfallteam tritt zusammen

Notfallbewältigung

- Was hat zur Notfallauslösung geführt?
- Sachstand
- Sofortmaßnahmen
- Wie ist es abgelaufen? (Wer kann das herausfinden?)
- Datenschutzverletzungen? → Datenpanne
- Kommunikationsplan
- Beweise sichern; Wer kann das gerichtsverwertbar tun?

Notfallbewältigung

- Schadensbegrenzung
- Wiederanlauf
- Notbetrieb
- Wer kann uns helfen (ggf. mehrere Alternativen)?
- Maßnahmen, Entscheidungen
- Umgebung für Normalbetrieb aufbauen
- Notfall beendet?
- Regressansprüche, Versicherung; Lessons learned, KVP

Notfallbewältigung - Kommunikation

Wer muss wie informiert werden?

- Wie sieht unser Kommunikationskonzept aus?
- Gibt es (neue) Erkenntnisse hinsichtlich **Datenpanne**?

Datenpanne

- Feststellen
- Behandeln, dokumentieren
- **Meldepflicht** nach Art. 33 DS-GVO
  Verantwortlicher meldet an Aufsichtsbehörde (LfDI)
  unverzüglich und möglichst binnen 72 Stunden!
- **Mitteilungspflicht** nach Art. 34 DS-GVO
  wenn voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen besteht
- Meldewege (Online, Fax, zu Fuß …)

Datenpanne – Meldeweg zu Fuß

Datenpanne – Meldeweg zu Fuß

Unterlagen im Netz

Allianz für Cybersicherheit (ACS)

- **BSI ACS Maßnahmenkatalog zum Notfallmanagement Fokus IT-Notfälle (3 Seiten)**
- **BSI ACS TOP_12_Massnahmen bei Cyberangriffen (1 Seite)**
- BSI-Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall (28 Seiten)
- ACS Checklisten

LfDI B-W:

- **Hackerangriffe – Empfehlenswerte Maßnahmen nach erfolgreichen Angriffen**

Unterlagen im Netz; BSI-Infos

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Angebote/IT-Notfallkarte/TOP-12-Massnahmen/top12massnahmen_node.html

Allianz für Cyber-Sicherheit

MASSNAHMEN-KATALOG ZUM NOTFALLMANAGEMENT

- Fokus IT-Notfälle -

Unterlagen im Netz; BSI-Infos

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Angebote/IT-Notfallkarte/TOP-12-Massnahmen/top12massnahmen_node.html

TOP 12
MASSNAHMEN BEI CYBER-ANGRIFFEN

Diese Fragen sollten Sie sich stellen!

Die Bewältigung eines Cyber-Angriffs ist stets individuell und Maßnahmen müssen auf die Gegebenheiten der IT-Infrastruktur vor Ort, die Art des Angriffs und die Zielsetzungen der Organisation angepasst werden. Die in den 12 als Fragen formulierten Punkten implizierten Maßnahmen dienen als Impuls und Hilfestellung bei der individuellen Bewältigung.

Das Dokument richtet sich an IT-Verantwortliche und Administratoren, in erster Linie in kleinen und mittelständischen Unternehmen.

Unterlagen im Netz; BSI-Infos

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Angebote/IT-Notfallkarte/TOP-12-Massnahmen/top12massnahmen_node.html

- Wurden erste Bewertungen des Vorfalls durchgeführt, um festzustellen, ob es sich um einen Cyber-Angriff oder lediglich um einen technischen Defekt handelt?
- Haben Sie kontinuierlich Ihre Maßnahmen abgestimmt, dokumentiert und an alle relevanten Personen und Verantwortlichen kommuniziert?
- Wurden System-Protokolle, Log-Dateien, Notizen, Fotos von Bildschirminhalten, Datenträger und andere digitale Informationen forensisch gesichert?
- Haben Sie stets die besonders zeitkritischen und damit vorrangig zu schützenden Geschäftsprozesse im Fokus gehabt?
- Wurden betroffene Systeme vom Netzwerk getrennt? Wurden Internetverbindungen zu den betroffenen Systemen getrennt? Wurden alle unautorisierten Zugriffe unterbunden?
- Wurden Backups gestoppt und vor möglichen weiteren Einwirkungen geschützt?
- Wurden Maßnahmen unternommen, um das gesamte Maß der Ausbreitung festzustellen? Wurden alle angegriffenen Systeme identifiziert?
- Wurden die beim Cyber-Angriff ausgenutzten Schwachstellen in Systemen oder (Geschäfts-) Prozessen durch relevante Maßnahmen adressiert und behoben?
- Wurden, nach Abstimmung, die Polizei oder relevante Behörden (Datenschutz, Meldepflichten, etc.) benachrichtigt?
- Wurden die Zugangsberechtigungen und Authentisierungsmethoden für betroffene (geschäftliche und ggf. private) Accounts überprüft (z.B. neue Passwörter, 2FA)?
- Wird das Netzwerk nach dem Vorfall weiter überwacht, um mögliche erneute Anomalien festzustellen?
- Wurden die betroffenen Daten und Systeme wiederhergestellt oder neu aufgebaut?

Unterlagen im Netz; BSI-Infos

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/unternehmen.html?cms_pos=1

Unternehmen: Einen Vorfall bewältigen, melden, sich informieren, vorbeugen

Inhaltsverzeichnis

1. **Ich habe einen Vorfall – Was soll ich tun?**
2. Ich habe einen Vorfall – Checkliste Organisatorisches
3. Ich habe einen Vorfall – Checkliste Technik
4. Ich möchte einen IT-Sicherheitsvorfall melden.
5. Ich suche grundsätzliche Informationen, um mich vor einem IT-Sicherheitsvorfall zu schützen
6. Ich suche aktuelle Informationen über Bedrohungen.

Notfallbewältigung

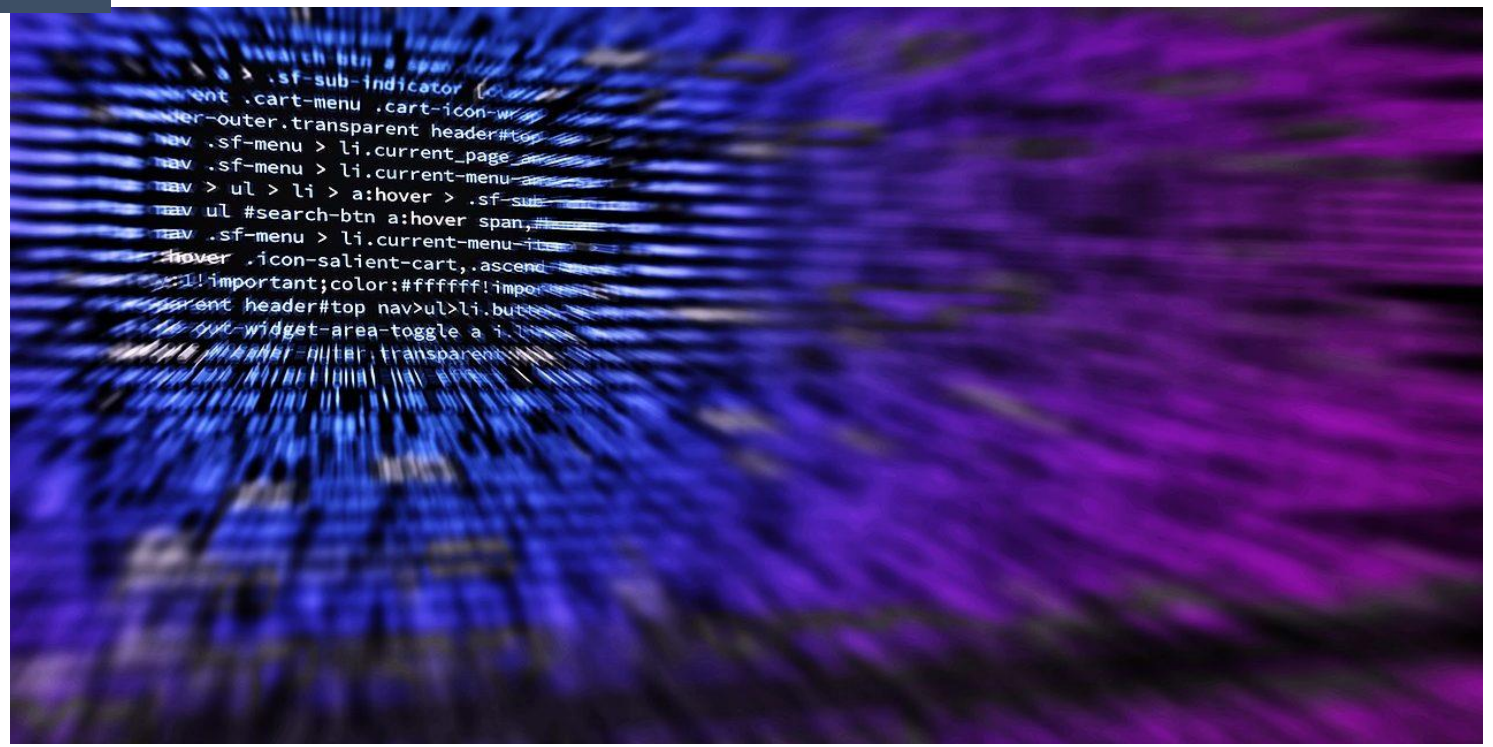
- Externe Unterstützung (Vertragspartner, ggf. mehrere Alternativen)
- Cyberwehr https://cyberwehr-bw.de/
- Zentrale Ansprechstelle Cybercrime (ZAC) für Wirtschaftsunternehmen und Behörden https://lka.polizei-bw.de/zentrale-ansprechstelle-cybercrime/
- Kommunikation
  - Spezielle Ansprechpartner (Bei KRITIS Unternehmen)
  - LfDI
  - Kunden/Lieferanten
  - Presse

Hotline: 0800-CYBERWEHR
0800-292379347

Zentrale Ansprechstelle Cybercrime (ZAC)

Hackerangriffe – Empfehlenswerte Maßnahmen nach erfolgreichen Angriffen

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg



https://www.baden-wuerttemberg.datenschutz.de/hackerangriffe-empfehlenswerte-massnahmen-nach-erfolgreichen-angriffen/

Notfallvorsorge

- Konzepte
- Sensibilisierung
- Ansprechpartner

Notfallvorsorge

Vorarbeiten (Notfallvorsorge)

- Welche Partner zur Notfallbehandlung (mehrere Alternativen)?
- Erfahrung, Reputation?
- Vertraulichkeitsvereinbarung
- Preisliste, Angebot
- Kontakt, Reaktionszeiten

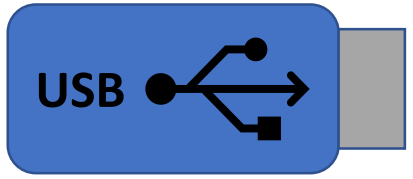
Backups

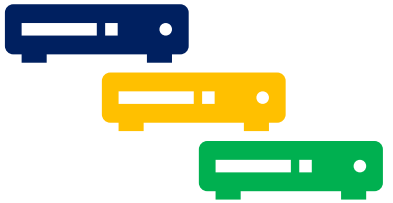
- Welche Daten sind wichtig?
- Was ist der maximal tolerierbare Datenverlust?
- Wie oft werden Backups gemacht? Passt das zusammen?
- Auf welche Medien?
- Wo werden die Backups gelagert?
- Wie viele Generationen von Backups werden gemacht?
- Wiederherstellung üben
- Wie lange wird die Wiederherstellung dauern?

Backups Privatanwender

Speichermedien

- Papier (für einzelne Dokumente evtl. sinnvoll)
- USB-Sticks
- Externe USB-Festplatten
- NAS
- Cloud
- Blu-ray-Disc
- E-Mail (u.U. für einzelne Dateien)

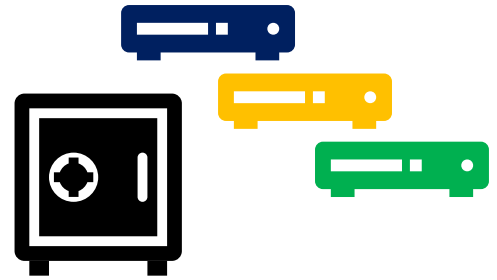




ausstecken
wegschließen

Backups Privatanwender

- **Welche Daten sind wichtig?**
- Was ist der maximal tolerierbare Datenverlust?
- Wie oft werden Backups gemacht? Passt das zusammen?
  1 x pro Woche
- Wie viele Generationen von Backups werden gemacht? Mindestens 3
- Wo werden die Backups gelagert?
  Ausstecken, wegschließen, evtl. auch außer Haus lagern
- **Wiederherstellung üben**
- **Ernstfall: In sicherer Umgebung Kopie des Backups erstellen!**
- Wie lange wird die Wiederherstellung dauern?



Sensibilisierung

- Konzept
- Maßnahmen
- Präsenz
- E-Learning
- Angriffssimulation
- Serious Gaming
- Filme/Videos
- Bücher (Blackout, Zero,…)

Fragen