IT-Blackout als Gefahr

Business Continuity Management (BCM)

für Klein- und Mittelbetriebe

DI Heidelinde Rameder & Nina Bürger, MSc
17.03.2022

T · · Systems · Let's power higher performance

Ziele

Theorie vermitteln

Sie haben einen Einblick in die Grundlagen, damit Sie durchstarten können. Sie kennen wichtige Nachschlagewerke.

Praxiserfahrung teilen

Sie verstehen die Anwendung der dargelegten Konzepte und lernen, welchen Fehlern Sie von vornherein ausweichen können.

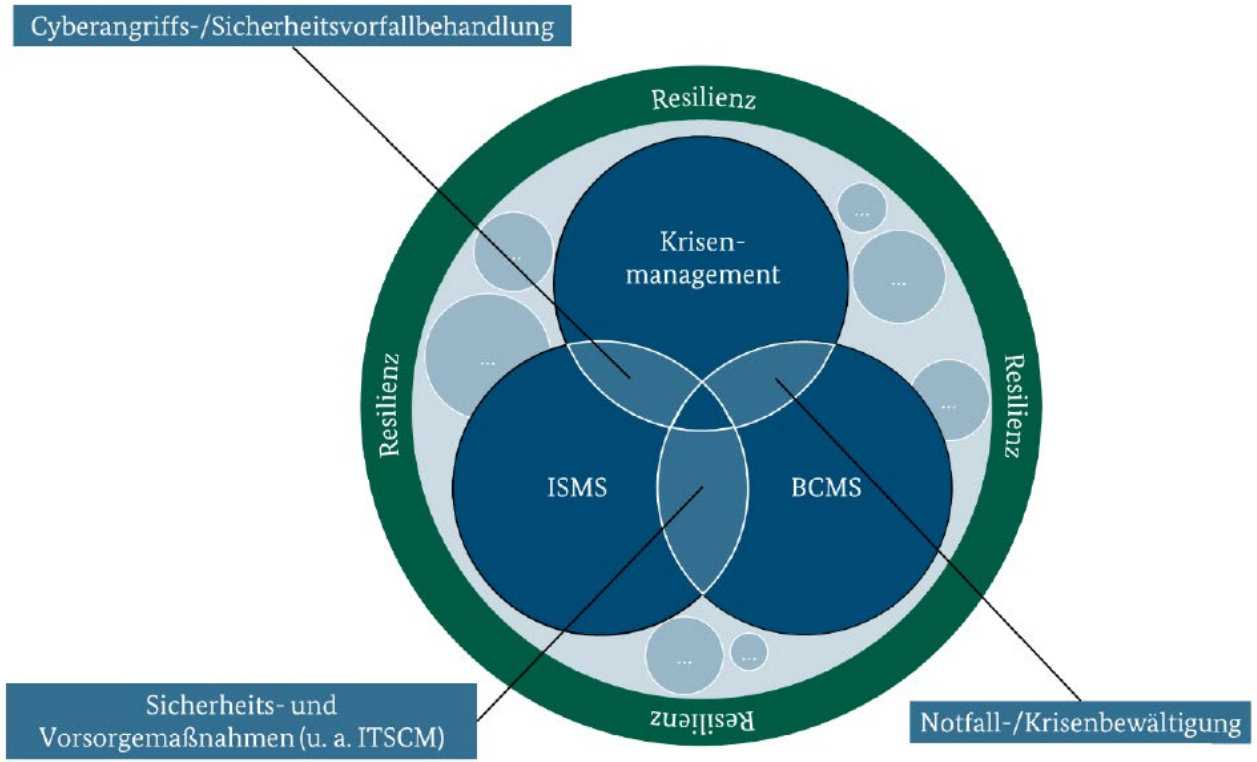
Teilnehmende empowern

Sie fühlen sich gut ausgerüstet und können z.B. mit Berater:innen auf Augenhöhe kommunizieren.

IT Resilienz

Eckpfeiler für IT Resilienz:

- Informationssicherheit (ISM)
- Business Continuity (BCM) und IT-Service Continuity Management (ITSCM)
- Krisenbewältigung



Resilienz bedeutet, dass Sie umfassend gegen Ausfälle des Geschäftsbetriebs vorgesorgt haben.

Warum Business Continuity Management?

Business Continuity Management

Was? Aufbau der organisatorischen **Widerstandsfähigkeit**

→ Sicherstellung des Tagesgeschäfts in Krisensituationen

Wozu? Prävention von und Reaktion auf Notfall-/Krisensituationen

Schnellere Wiederherstellung des Normalbetriebs

Wie? Identifikation von Risiken, Bedrohungen und Schwachstellen

99%

aller Unternehmen in der EU

gehören dem KMU Sektor an[1]

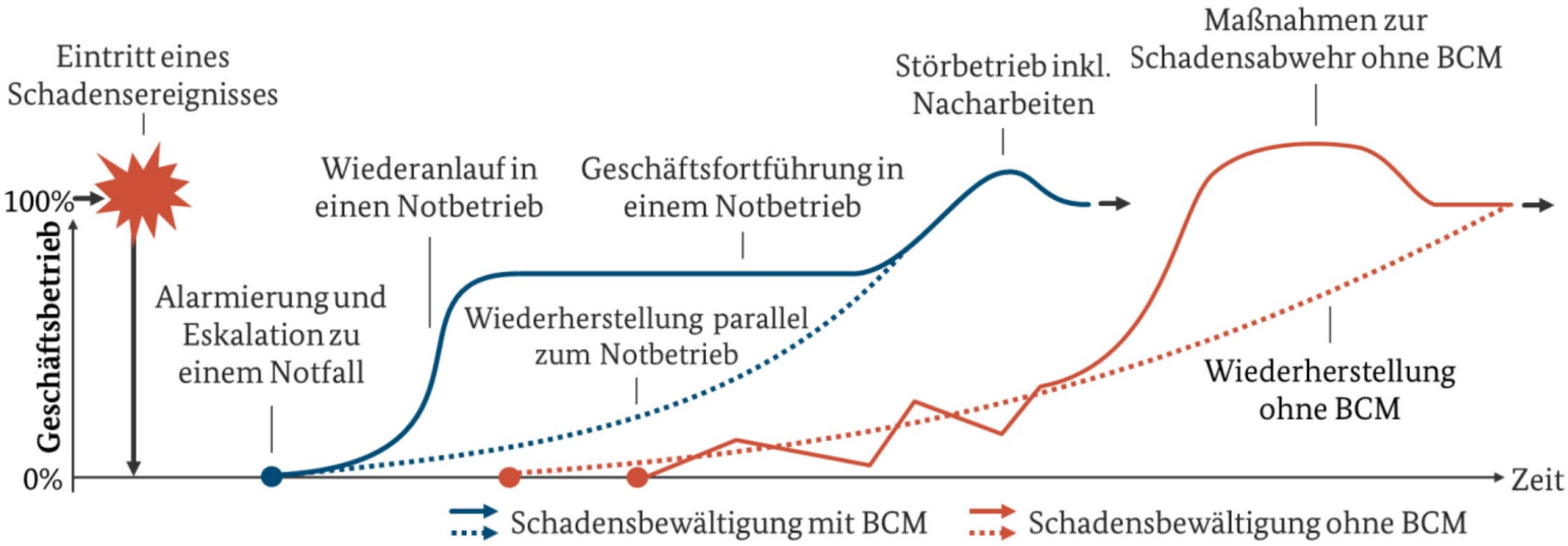
1 von 5

KMU erstellt IT-Notfallpläne[2]

Welche Geschäftsaktivität/Ressource ist essenziell zur Aufrechterhaltung des Geschäftsbetriebes?

Welche Geschäftsaktivität oder welche Ressource müsste angegriffen werden, um den größtmöglichen Schaden zu erzielen?

Schadensbewältigung mit und ohne BCM



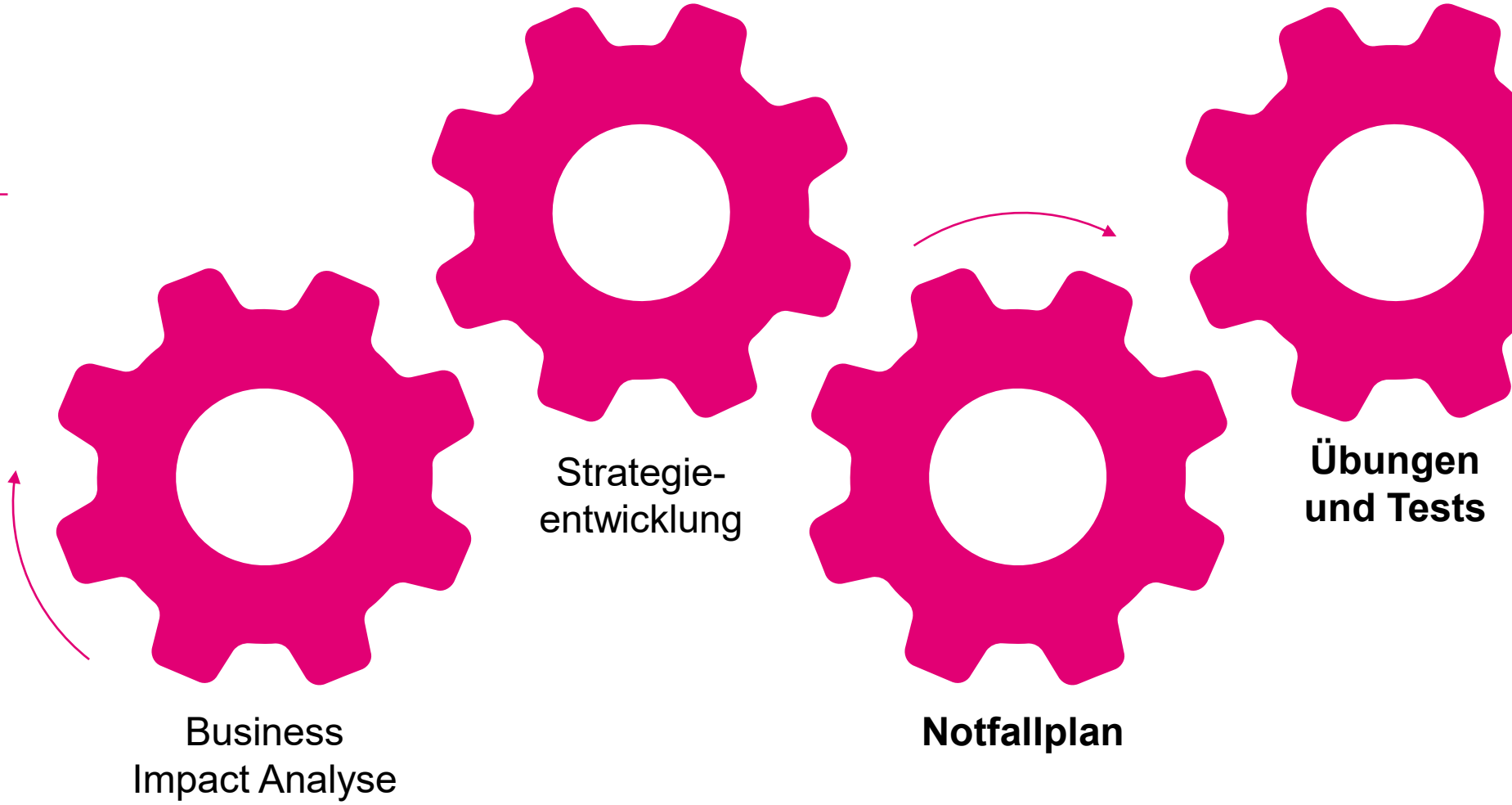
[3]

Umsetzungsleitfaden

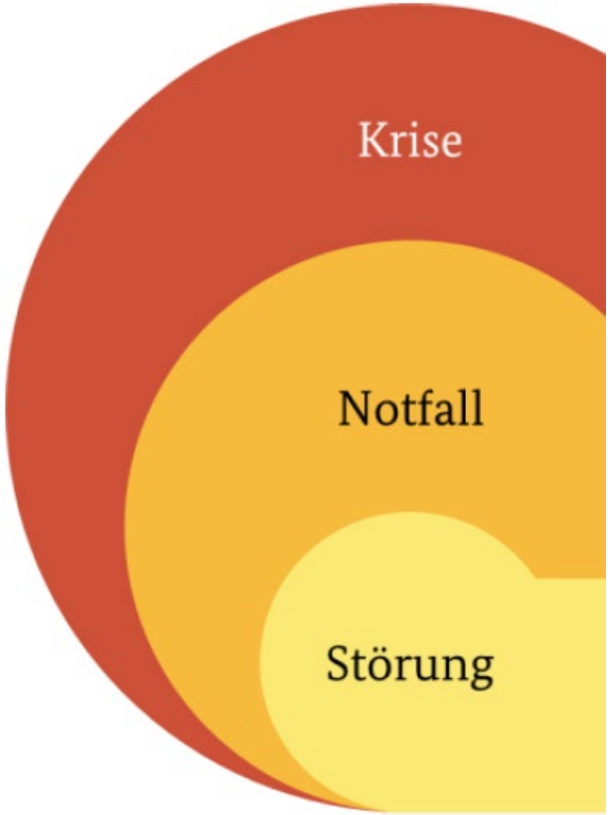
Fokussieren Sie auf das Wichtigste.

Starten Sie mit einem Grundgerüst, und gehen Sie dann in die Tiefe.

Die vier rechts dargestellten Eckpfeiler helfen Ihnen bei der ersten Orientierung.



Wichtige Begriffe[3]



- **Massive Unterbrechung** eines (zeit-)**kritischen Geschäftsprozesses**
- Es liegen **keine** (ausreichenden) **Notfallpläne** vor
- **Erweiterung der BAO** erforderlich

- **Erhebliche Unterbrechung** eines zeitkritischen Geschäftsprozesses
- **Notfallpläne** liegen vor
- **BAO** erforderlich

- Prozesse/Ressourcen stehen nicht wie vorgesehen zur Verfügung
- Innerhalb des **Normalbetriebs behebbar** (Notfallpläne **nicht** erforderlich)
- **Keine BAO** erforderlich

Besondere Aufbauorganisation (BAO)

Zeitlich Begrenzte Organisationsform (d.h. im Gegensatz zur Organisation im „Normalbetrieb“, besondere Zuständigkeiten, Entscheidungswege, etc.), um auf außergewöhnliche Situationen angemessen und schnell zu reagieren

Wichtige Begriffe[3]

Maximum Tolerable Period of Disruption (MTPD)
deutsch: Maximal tolerierbare Ausfallzeit (MTA)

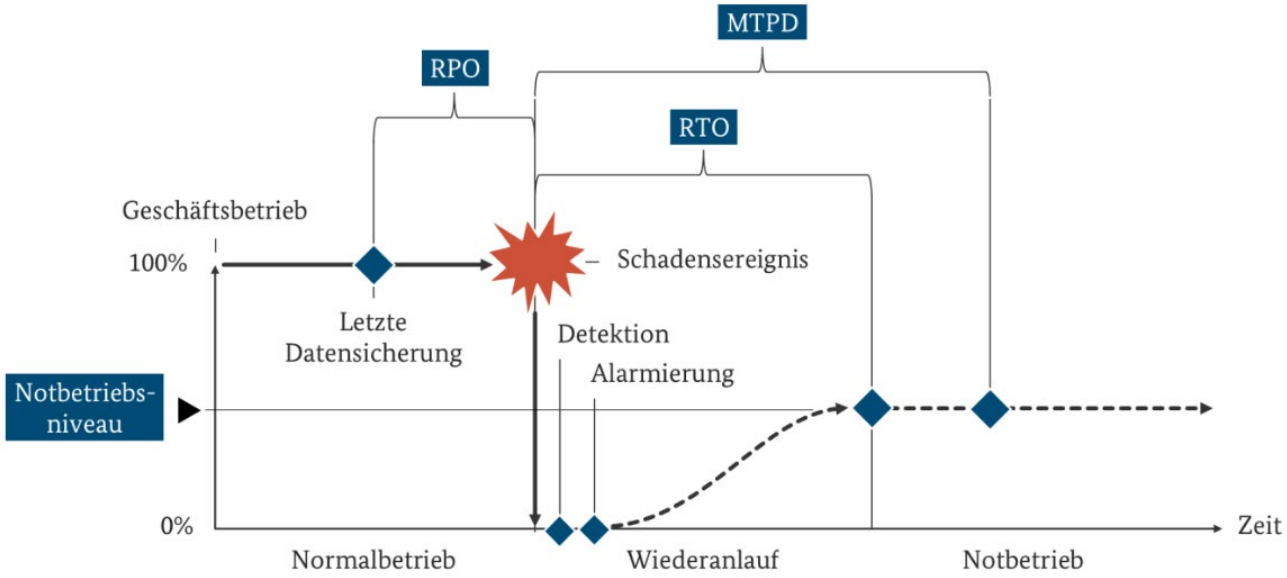
Maximale Ausfalldauer eines Geschäftsprozesses, bis nicht tolerierbare Auswirkungen auftreten

Recovery Time Objective (RTO)
deutsch: Geforderte Wiederanlaufzeit (WAZ)

Zeitraum vom Zeitpunkt des Ausfalls einer Ressource bis zur Inbetriebnahme der Notfalllösung (z.B. durch Zurücksetzen eines IT-Systems auf den letzten gesicherten Zustand)

Recovery Point Objective (RPO)
deutsch: Maximal zulässiger Datenverlust

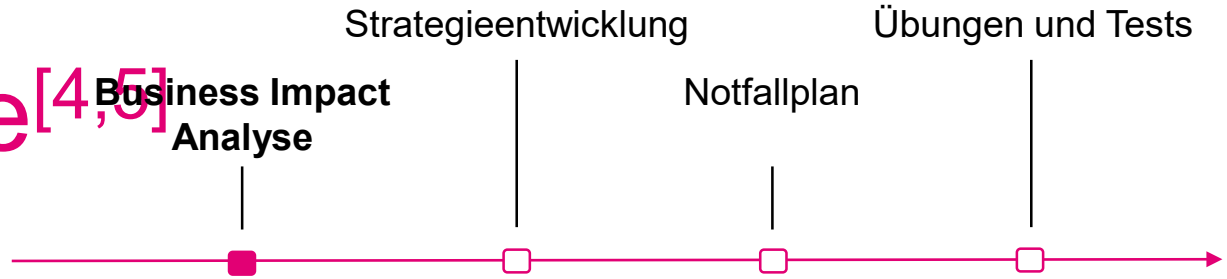
maximales Alter verfügbarer Daten für sinnvollen Notbetrieb (bestimmt minimal notwendige Datensicherungszyklen)



Notbetriebsniveau

Definierte Leistungsfähigkeit des Notbetriebs, um sinnvollen Geschäftsbetrieb zu ermöglichen. Wird je Geschäftsprozess festgelegt, z.B. prozentual.

Business Impact Analyse[4,5]
BIA



Ziel
Erhebung Ihrer geschäftskritischen Prozesse und Abhängigkeiten

Methode
Bewertung der Prozesse hinsichtlich der Auswirkungen eines Ausfalles mit unterschiedlichen **Zeithorizonten**

- Finanzielle Auswirkungen
- Beeinträchtigung der Aufgabenerfüllung
- Verstoß gegen Gesetze, Vorschriften und Verträge
- Negative Innen- und Außenwirkungen (Imageschaden)
- Beeinträchtigung der persönlichen Unversehrtheit

BSI-Standard 200-4 | Schadensszenarien und -kategorien

Schadens-kategorie	Allgemeine Beschreibung	Beeinträchtigung der Aufgaben-erfüllung	Negative Innen- und Außen-wirkung (Imageschaden)	Finanzielle Auswirkungen	Verstoß gegen Gesetze, Vorschriften und Verträge	Beeinträchtigung der persönlichen Unversehrtheit
1 - Gering	Ausfall hat geringe, kaum spürbare Auswirkungen.	Der Geschäftsbetrieb wird unwesentlich beeinträchtigt.	In Einzelfällen ist eine geringe, nicht nachhaltige Ansehensbeeinträchtigung zu erwarten.	Der finanzielle Schaden ist für die Institution unerheblich.	Es wird nur in einem geringen Maß gegen interne Vorgaben und Anweisungen verstoßen. Verstöße führen zu keinen negativen Auswirkungen.	Eine Beeinträchtigung der persönlichen Unversehrtheit ist ausgeschlossen.
2 - Mittel	Ausfall hat spürbare Auswirkungen.	Der Ausfall hat spürbare Auswirkungen auf den Geschäftsbetrieb. Mit Arbeitsrückständen ist zu rechnen.	Eine geringe Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.	Der finanzielle Schaden ist für die Institution tolerabel.	Es wird ausschließlich gegen interne Vorgaben und Anweisungen verstoßen.	Eine Beeinträchtigung der persönlichen Unversehrtheit ist unwahrscheinlich.
3 - Hoch	Allgemeine Beschreibung: Ausfall hat nicht tolerierbare Auswirkungen.	Der Geschäftsbetrieb ist massiv eingeschränkt. Arbeitsrückstände sind nur mit erhöhtem Arbeitsaufwand zu kompensieren.	Eine erhebliche, nachhaltige Ansehens- oder Vertrauensbeeinträchtigung ist intern und extern zu erwarten.	Der finanzielle Schaden ist für die Institution erheblich und nachhaltig spürbar.	Es wird gegen Gesetze verstoßen. Verstöße führen zu erheblichen Konsequenzen, z. B. hohe Bußgelder. Vertragsverletzungen führen zu hohen Konventionalstrafen oder Konsequenzen.	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden.
4 - Sehr hoch	Allgemeine Beschreibung: Ausfall führt zu existentiell bedrohlichen Auswirkungen.	Der Ausfall hat fundamentale und langfristige Auswirkungen auf den Geschäftsbetrieb. Arbeitsrückstände können nicht mehr aufgeholt werden.	Eine fundamentale, nachhaltige, in der breiten Öffentlichkeit vorhandene Ansehens- oder Vertrauensbeeinträchtigung, bis hin zu existenzgefährdender Art, ist zu erwarten.	Der finanzielle Schaden hat existenzbedrohende Ausmaße.	Es wird im hohen Maß gegen Gesetze verstoßen. Verstöße haben strafrechtliche Konsequenzen. Vertragsverletzungen führen zu ruinösen Konventionalstrafen oder Konsequenzen.	Es besteht akut Gefahr für Leib und Leben oder gravierende Beeinträchtigungen der persönlichen Unversehrtheit.

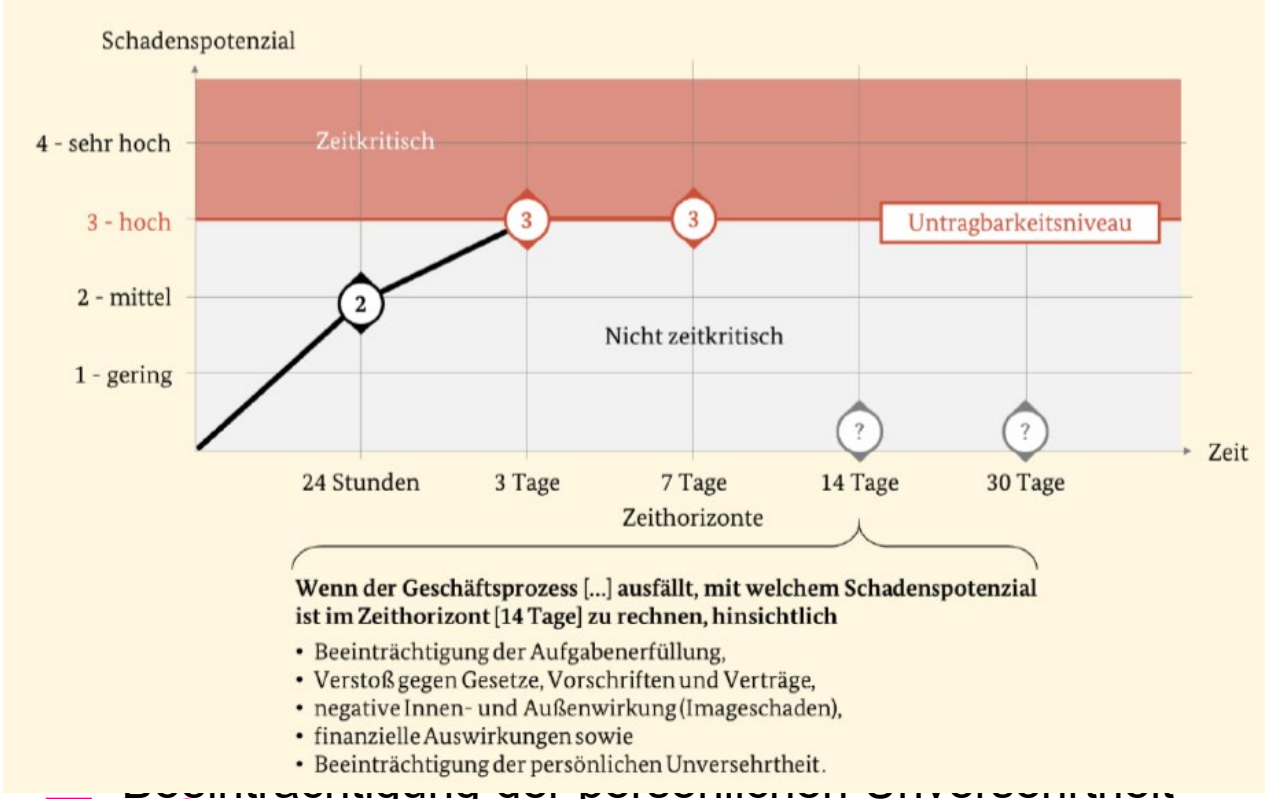
[5]

Business Impact Analyse[4,5]
BIA

Strategieentwicklung | Übungen und Tests

Business Impact Analyse | Notfallplan

Ziel
Erhebung Ihrer geschäftskritischen Prozesse und Abhängigkeiten



BSI-Standard 200-4 | Schadensszenarien und -kategorien

Schadens-kategorie	Allgemeine Beschreibung	Beeinträchtigung der Aufgaben-erfüllung	Negative Innen- und Außen-wirkung (Imageschaden)	Finanzielle Auswirkungen	Verstoß gegen Gesetze, Vorschriften und Verträge	Beeinträchtigung der persönlichen Unversehrtheit
1 - Gering	Ausfall hat geringe, kaum spürbare Auswirkungen.	Der Geschäftsbetrieb wird unwesentlich beeinträchtigt.	In Einzelfällen ist eine geringe, nicht nachhaltige Ansehensbeeinträchtigung zu erwarten.	Der finanzielle Schaden ist für die Institution unerheblich.	Es wird nur in einem geringen Maß gegen interne Vorgaben und Anweisungen verstoßen. Verstöße führen zu keinen negativen Auswirkungen.	Eine Beeinträchtigung der persönlichen Unversehrtheit ist ausgeschlossen.
2 - Mittel	Ausfall hat spürbare Auswirkungen.	Der Ausfall hat spürbare Auswirkungen auf den Geschäftsbetrieb. Mit Arbeitsrückständen ist zu rechnen.	Eine geringe Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.	Der finanzielle Schaden ist für die Institution tolerabel.	Es wird ausschließlich gegen interne Vorgaben und Anweisungen verstoßen.	Eine Beeinträchtigung der persönlichen Unversehrtheit ist unwahrscheinlich.
3 - Hoch	Allgemeine Beschreibung: Ausfall hat nicht tolerierbare Auswirkungen.	Der Geschäftsbetrieb ist massiv eingeschränkt. Arbeitsrückstände sind nur mit erhöhtem Arbeitsaufwand zu kompensieren.	Eine erhebliche, nachhaltige Ansehens- oder Vertrauensbeeinträchtigung ist intern und extern zu erwarten.	Der finanzielle Schaden ist für die Institution erheblich und nachhaltig spürbar.	Es wird gegen Gesetze verstoßen. Verstöße führen zu erheblichen Konsequenzen, z. B. hohe Bußgelder. Vertragsverletzungen führen zu hohen Konventionalstrafen oder Konsequenzen.	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden.
4 - Sehr hoch	Allgemeine Beschreibung: Ausfall führt zu existentiell bedrohlichen Auswirkungen.	Der Ausfall hat fundamentale und langfristige Auswirkungen auf den Geschäftsbetrieb. Arbeitsrückstände können nicht mehr aufgeholt werden.	Eine fundamentale, nachhaltige, in der breiten Öffentlichkeit vorhandene Ansehens- oder Vertrauensbeeinträchtigung, bis hin zu existenzgefährdender Art, ist zu erwarten.	Der finanzielle Schaden hat existenzbedrohende Ausmaße.	Es wird im hohen Maß gegen Gesetze verstoßen. Verstöße haben strafrechtliche Konsequenzen. Vertragsverletzungen führen zu ruinösen Konventionalstrafen oder Konsequenzen.	Es besteht akut Gefahr für Leib und Leben oder gravierende Beeinträchtigungen der persönlichen Unversehrtheit.

[5]

Beispiel | Business Impact Analyse (BIA)

Welche sind die kritischen Geschäftsprozesse und Ressourcen?
Welche Abhängigkeiten gibt es?

TIERÄRZTIN

- Telefonische Terminvereinbarung und Erreichbarkeit (Notfall)
- Diagnose & Therapie
  - Verfügbarkeit von Daten (Anamnese, Allergien, etc.)
  - Physische Verfügbarkeit der Praxis
- Zulieferung von Medikamenten, Nahrungsmitteln, Ausstattung
- Fakturierung

WERBEAGENTUR

- Vertrieb
  - MS Office
- Auftragsabwicklung
  - Internetzugriff
  - Cloud Services, Online Tools
  - Datenablagen (lokal, online)
- Fakturierung

Top Szenarien

- Datenverlust
- Ausfall von Kommunikationsnetzen (Telefonie, Daten)
- Personalausfall
- Probleme mit Dienstleistern und Lieferanten
- Physische Aspekte (z.B. Wasserschaden, Einbruch)

BIA | Kernprozess[6]

Fragestellung

Welche Auswirkungen (1 - niedrig, 2 - mittel, 3 - hoch, 4 - sehr hoch) hat es auf das Unternehmen, wenn der Kernprozess ausfällt?

Ausfall <1d	Ausfall <3d	Ausfall >3d
Niedrig	*Mittel*	*Hoch*

Welche Auswirkungen (1 - niedrig, 2 - mittel, 3 - hoch, 4 - sehr hoch) hat ein Datenverlust auf das Unternehmen?

Geringer Verlust	Teilweiser Verlust	Vollständiger Verlust
Mittel	*Hoch*	*Sehr hoch*

Welche IT-Systeme sind für einen Notbetrieb des Prozesses zwingend erforderlich?

Arbeitsplatz-PC mit Textverarbeitung und E-Mail-Kommunikation

E-Mail-Server mit Internetanbindung

Welcher der IT-Systeme enthalten Daten, die bei einem Verlust nicht wiederbeschafft werden können?

E-Mail-Server

Gibt es Alternativen oder alternative Arbeitsabläufe zu diesen IT-Systemen?

Web-Mail-Accounts zum Versand von Angeboten

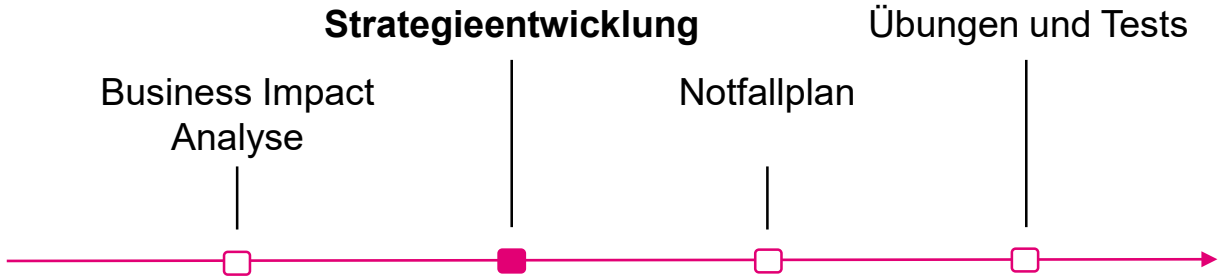
Welche IT-Dienstleister sind für einen Notbetrieb des Prozesses zwingend erforderlich?

Web-Mail-Provider

Gibt es Alternativen oder alternative Arbeitsabläufe zu diesen IT-Dienstleistern?

Ein kurzfristiger Wechsel zu einem anderen Web-Mail-Provider ist grundsätzlich möglich.

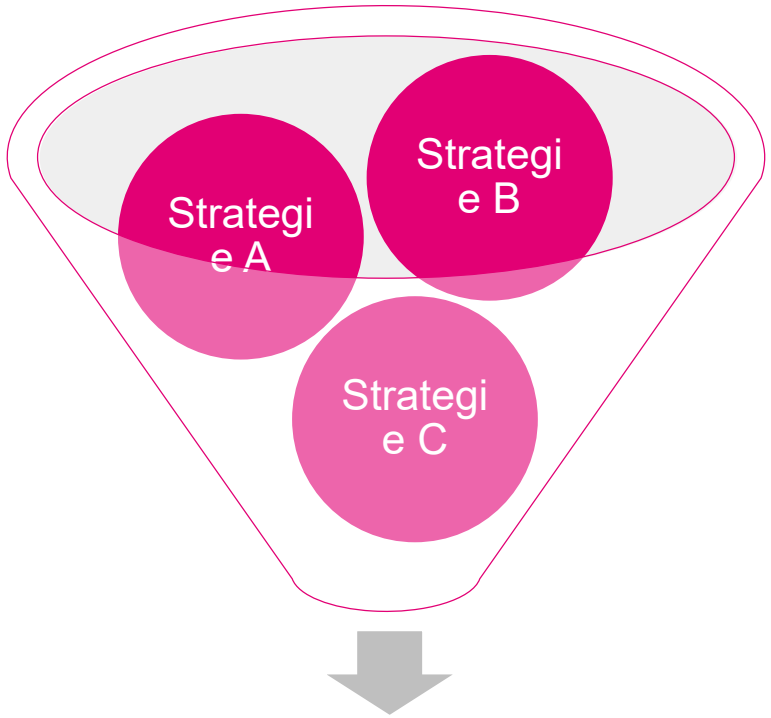
Strategieentwicklung



Ziel
Reduzierung möglicher Auswirkungen bei Ausfällen von z.B. Arbeitsplätzen, Personal, IT, Informationen, Dienstleistern, Lieferanten

Methode
Identifikation, Bewertung und Umsetzung von wirksamen und angemessenen Vorgehensweisen, z.B. in den Kategorien:

- Informationstechnik
- Personal
- Infrastruktur
- Dienstleistungen



Angemessene und wirksame Strategien zur Umsetzung

Beispiel | Strategieentwicklung

Welche (vorbereitenden) Aktivitäten & Maßnahmen setze ich?
Wie kann ich einen Notfall verhindern?

TIERÄRZTIN

- Redundante **Telefonleitung**, Umleitung
- Redundante und alternative **Lieferanten**
  - **Lieferkette** berücksichtigen: Beziehen die Lieferanten vom selben Drittlieferanten?
- **Datenbackups**
- **Vertretungsregelung**
- **Alarmanlage**

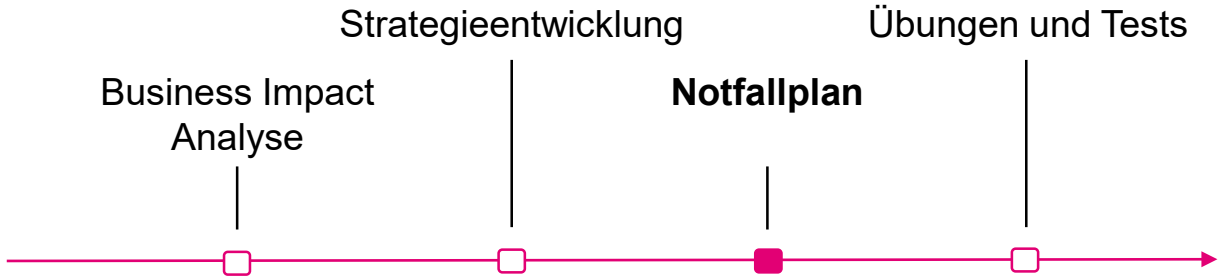
WERBEAGENTUR

- Redundanter und alternativer **Internetzugriff**
- **Datenbackups**
  - Lagerung von Backups in separatem Netzwerk bzw. physisch getrennt **Vertretungsregelung, Trainings, Wissensmanagement**
- **Hot/Warm/Cold Sites**

Top Vorschläge

- Redundanz
- Datensicherungen
- Wissensaustausch & Vertretungsregelungen
- Vereinbarungen mit externen Dienstleistern (SLAs)

Notfallplan

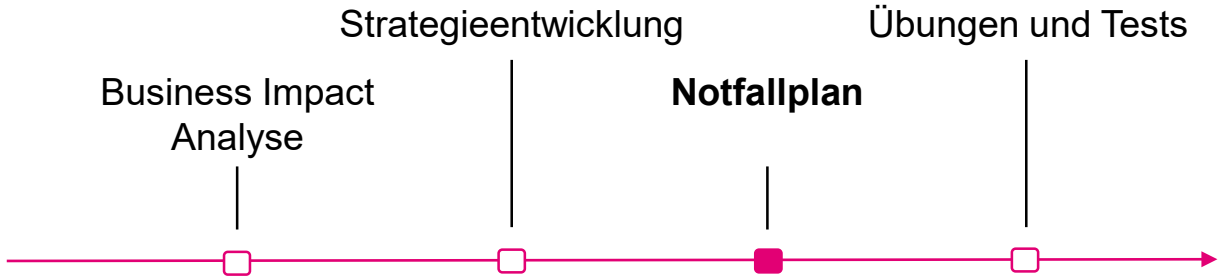


Ziel
Dokumentation der Vorgehensweise im Notfall, um kritische Geschäftsprozesse fortführen zu können

Methode
Beschreibung von Notfallszenarien und der unmittelbaren Reaktion auf ein Schadensereignis

- Aktivitäten für die Einleitung und Aufrechterhaltung eines Notbetriebs für jedes Szenario
- Rollen und deren Zuständigkeiten (BAO)
- wesentliche Kontaktinformationen (intern und extern)

Notfallplan



Schritt 1: Vorbereitung der Notfallpläne

- Wie sollen die Notfallpläne dokumentiert werden? Welche Informationen sind bereits bekar
- Wer erstellt Notfallpläne? Wann und in welchem Modus sollen sie erstellt werden?
- Aufbewahrungsort(e)

Schritt 2: Erstellung der Notfallpläne – Notfallmaßnahmen

- Übersicht zeitkritischer Prozesse und Ressourcen
- Notfallmaßnahmen je Ressource
- Notfallrelevante Dokumente sowie interne/externe Kontakte (inkl. Verantwortlichkeiten / BAC)

Schritt 3: Qualitätssicherung & Freigabe

- Prüfung ob vollständig, plausibel, aktuell (regelmäßig)
- (Formale) Freigabe

Beispiel | Notfallplan

Was muss ich im Notfall griffbereit haben? Wo liegt der Notfallplan? Wissen alle darüber Bescheid?

TIERÄRZTIN

Telefonausfall

Szenario: Ausfall der VOIP Leitung

Sofortmaßnahme/Notbetrieb: Rufumleitung Notfalltelefon (Mobil)

Kontaktaufnahme VOIP Betrieb

Verantwortlich: Person(n) A,B

WERBEAGENTUR

Datenverlust

Szenario: Datenverlust

Sofortmaßnahme:

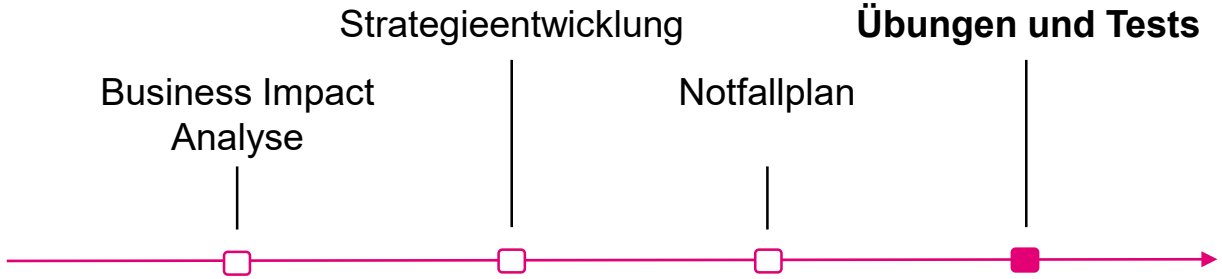
- Etablierung des Notbetriebs
  - Schritt 1, Schritt 2…
- Wiederherstellung
  - Schritt 1, Schritt 2…

Verantwortlich: Person C

TIPPS

- Vorlage verwenden
- So genau wie möglich und klar dokumentieren.
  Im Notfall bleibt weder Zeit noch Nerv, um lange zu überlegen.

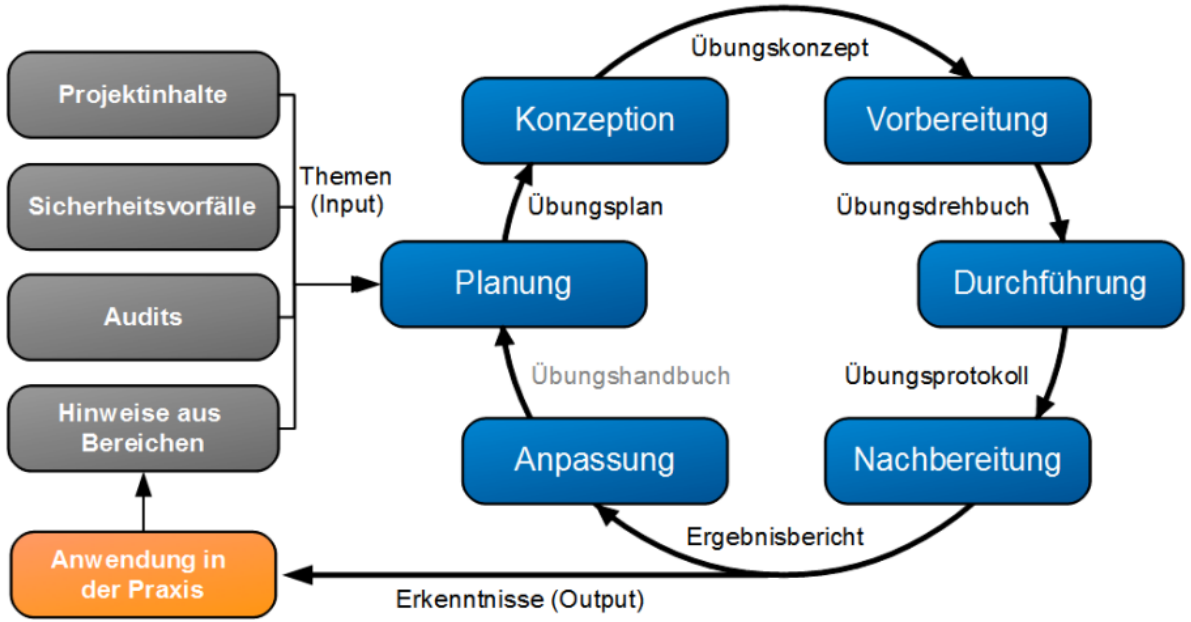
Übungen & Tests[7]



Ziel
Verifizieren erstellter Pläne und Abläufe der Notfallplanung Überprüfung der Beteiligung der Mitarbeiter:innen
Aufzeigen möglicher Optimierungspotentiale

Methoden (Beispiele)

- **Funktionstest**: Validierung der Maßnahmen aus dem Notfallplan (vor allem Sofortmaßnahmen)
- **Test technischer Maßnahmen**: z.B. redundante IT-Komponenten und Leitungen, Datenwiederherstellung
- **Kommunikations- und Alarmierungsübung**: Überprüfung der Meldung, Eskalation und Alarmierung



Beispiel | Übungen & Tests

Wie stelle ich sicher, dass meine Vorbereitungen angemessen sind?

Datenwiederherstellung

- **Notbetrieb**:
  - Verifizierung, dass alternative Datenablagen verfügbar sind
  - Verifizierung, dass alle involvierten Mitarbeiter:innen wissen, wie sie sich im Notfall zu verhalten haben

- **Wiederherstellung**:
  - Aktive Durchführung aller im Notfallplan gelisteten Schritte
  - Verifizierung, dass Daten vollständig wiederhergestellt werden können
  - Ggf. Korrektur/Erweiterung des Notfallplan durch Erkenntnisse aus dem Test

TIPPS

- Übungen ernst nehmen: Nur Übungen bereiten auf den Ernstfall vor
- Unterschiedliche Übungstypen planen
- Übungsdurchführung in einem Zyklus etablieren
- Übungen sind nicht zwangsweise aufwändig

BCM vs. kein BCM

Aufwand zur Initiierung von Business Continuity Management

Initiale und laufende Aufwände erscheinen hoch, machen sich im Notfall aber bezahlt.

Aufwand und Schaden im Notfall ohne Business Continuity Management

Ohne Business Continuity Management lebt es sich bequemer, bis etwas passiert.

Fazit

01

Sie investieren in die Zukunft Ihres Unternehmens.

Niemand ist zu hundert Prozent vor (IT-)Schwierigkeiten, Krisen/Notfällen gefeit.

Bereiten Sie sich vor und seien Sie sich sicher, dass Ihr Unternehmen einen Notfall übersteht.

02

Es gibt viele Ressourcen.

Alles, was Sie zum Anfangen brauchen, steht Ihnen zur Verfügung.

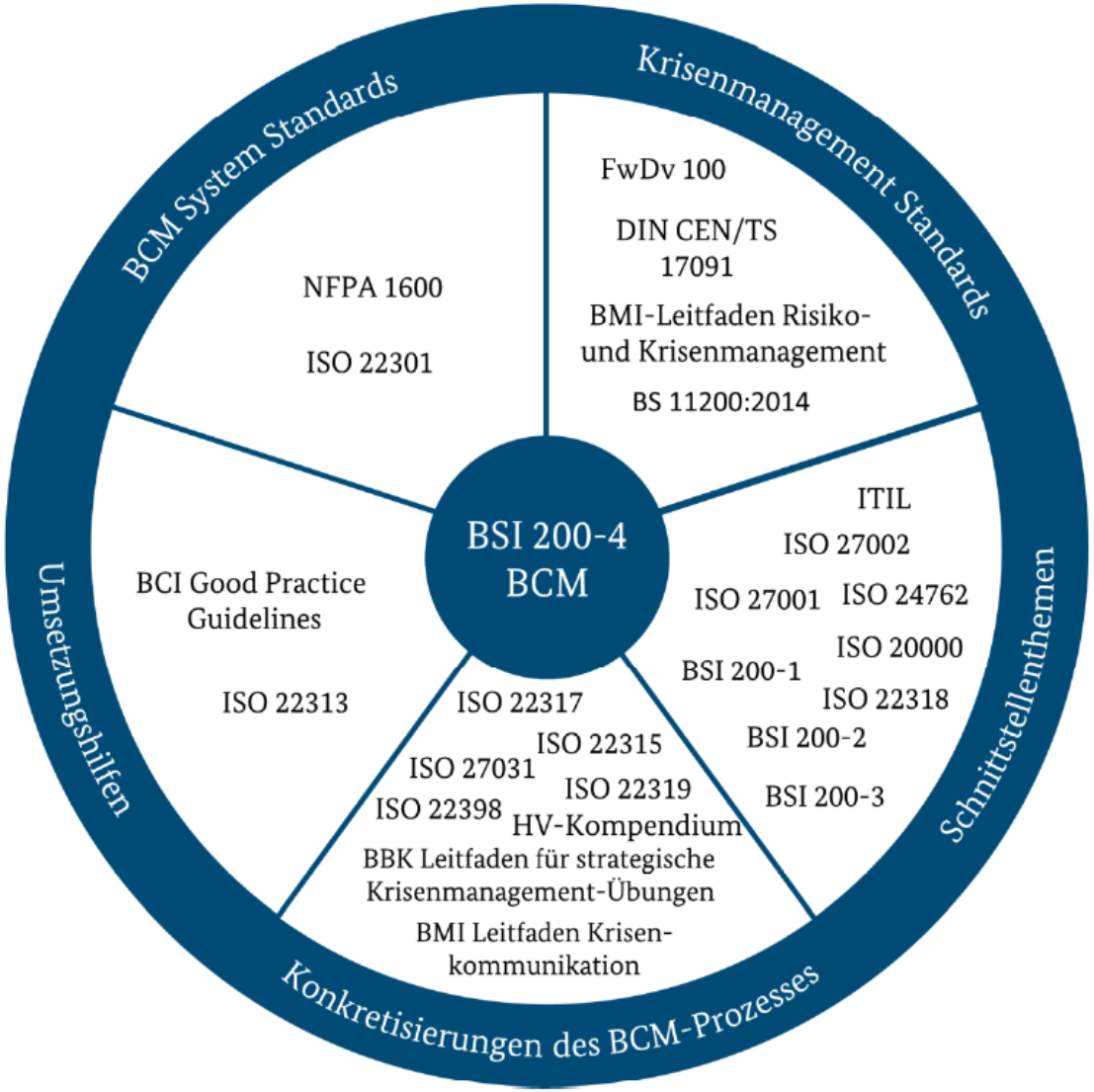
Das Wichtigste finden Sie in unserer Ressourcensammlung.

03

Holen Sie sich Unterstützung

Sie müssen nicht alles wissen. Konzentrieren Sie sich auf Ihr Kerngeschäft und holen Sie sich professionelle Unterstützung in anderen Bereichen.

Überblick Normen und Standards



Ressourcensammlung

Kostenfrei

BSI-Standard 200-4 (Business Continuity Management)

BSI-Standard 200-4 Hilfsmittel (Dokumentenvorlagen und Beispieltexte)

BSI Umsetzungsrahmenwerk zum Notfallmanagement

Kostenpflichtig

ISO/IEC 22301:2019 Security and resilience — Business continuity management systems

Weitere Quellen

1 Kurzdarstellungen zur Europäischen Union: Kleine und mittlere Unternehmen

2 handwerk.com - 81 Prozent: Unternehmer ohne Notfallplan

3 BSI-Standard 200-4 (Community Draft)

4 BSI Standard 100-4 Umsetzungsrahmenwerk, Modul "Business Impact Analyse“, Modulbeschreibung

5 BSI Übersicht Schadensszenarien und -kategorien

6 BSI Beispiel einer IT-BIA eines KMUs

7 BSI Standard 100-4 Umsetzungsrahmenwerk, Modul "Tests und Übungen", Modulbeschreibung