Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

BSI-Standard 200-4

Business Continuity Management

-Community Draft-

Änderungshistorie

Der BSI-Standard 200-4 löst den BSI-Standard 100-4 ab.

Stand	Version	Änderungen
Januar 2021	CD 1.0	Neukonzeption basierend auf dem BSI-Standard 100-4 Im Rahmen der Neukonzeption wurde ein Stufenmodell eingeführt. Dieses unterscheidet die Stufen Reaktiv-BCMS, Aufbau-BCMS und Standard-BCMS. Erstellung praxisnaher Anleitungen, für den Aufbau, Betrieb und die kontinuierliche Weiterentwicklung eines BCMS, die auch ohne Zusatzwerke (wie das Umsetzungsrahmenwerk) oder dem Vorhandensein eines ISMS umsetzbar sind. Anpassung an ISO-Standard 22301:2019 Ganzheitliche Betrachtung des Business Continuity Management im Fokus der Resilienz Änderung des Begriffs „Notfallmanagement“ in „Business Continuity Management (BCM)“ Ergänzung der BCM-Prozessschritte Voranalyse und Soll-Ist-Abgleich Berücksichtigung der Schnittstellen und Synergien des BCM, unter anderem mit ISMS, ITSCM und Krisenmanagement Ausführlichere Beschreibung der Bewältigungsorganisation mit Ihren Strukturen

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik Postfach 20 03 63
53133 Bonn
Tel: +49 228 99 9582-5369
E-Mail: grundschutz@bsi.bund.de
Internet: https://www.bsi.bund.de

Vorwort zum Community Draft

Bei dieser vorliegenden Version des BSI-Standards 200-4 handelt es sich um einen sogenannten Community Draft. Dieses Dokument stellt noch nicht die finale Fassung des BSI-Standards 200-4 dar, sondern einen vom BSI erarbeiteten Entwurf, der von der Anwendergemeinde kommentiert werden kann. Kommentare jeglicher Art, egal ob es sich um eine orthografische oder inhaltlich-fachliche Anmerkung handelt, können an

grundschutz@bsi.bund.de

gerichtet werden. Das BSI freut sich über jeden Kommentar. Die Community Draft-Phase dauert mindestens bis zum 30.06.2021. In dieser Zeit werden die Anwenderkommentare bereits frühzeitig konsultiert und konsolidiert, sodass auch schon bedarfsweise frühzeitig überarbeitete Fassungen (CD 1.1, 1.2 usw.) auf den Webseiten des BSI zur Verfügung gestellt werden können.

Dieser Community Draft verweist bereits auf alle für den BSI Standard 200-4 konzipierten Hilfsmittel (z. B. eine Formatvorlage für die BCM-Leitlinie mit vorausgefüllten Beispieltexten). Die Hilfsmittel werden zusammen mit der Anforderungsliste aus dem normativen Anhang (siehe Kapitel *9 Anhang B: Hinweise zu den Hilfsmitteln)* kontinuierlich auf der Website des BSI während der CD-Phase veröffentlicht.

Das BSI wird über Updates zum BSI-Standard 200-4 über die bekannten Kanäle informieren (Webseite und BCM-Newsletter [BCMN]).

Inhalt

1 Einleitung

1.1 Adressatenkreis

Der BSI-Standard 200-4 richtet sich an BCM-Beauftragte bzw. BC-Manager, Krisenstabsmitglieder, Sicherheitsverantwortliche, -experten und -berater sowie alle Interessierten, die mit dem Management von Notfällen und Krisen technischen und nicht-technischen Ursprungs betraut sind.

Hinweis:

Nachfolgend wird der Begriff **Institution** in diesem Dokument als neutraler Oberbegriff für Unternehmen, Behörden und sonstige öffentliche oder private Organisationen genutzt.

Ein angemessenes BCM ist sowohl bei kleineren und mittleren als auch großen Institutionen sinnvoll. Daher richtet sich dieser Standard an alle Institutionen. Er bietet eine individuell anpassbare, ressourcenschonende und zielführende Methodik, um ein eigenes BCMS aufzubauen und zu betreiben.

Hinweis:

Alle Personalbegriffe in diesem Dokument beziehen sich in gleicher Weise auf Personen mit weiblicher, männlicher und diverser Geschlechtsidentität. Wird im Text die männliche Form verwendet, geschieht dies ausschließlich aus Gründen der leichteren Lesbarkeit.

1.2 Zielsetzung

Behörden und Unternehmen, stehen gleichermaßen vor der Herausforderung, immer effizienter und möglichst zu jeder Zeit Leistungen erbringen zu müssen. Dazu tragen verschiedene Entwicklungen und Trends in der Gesellschaft und der Wirtschaft bei, z. B. steigen die Anforderungen verschiedener Interessengruppen (wie Kunden, Aufsichtsbehörden etc.), des globalen Wettbewerbs sowie der fortschreitenden Digitalisierung. Infolgedessen werden Institutionen immer abhängiger von Informationstechnik (IT), funktionierenden Lieferketten und den Leistungen Dritter, z. B. Dienstleistern, Lieferanten und Versorgern. Die Verfügbarkeit der Geschäftsprozesse oder Fachaufgaben entwickelt sich zu einer Existenzfrage für die Institution.

Gleichzeitig nehmen Risiken zu, die den Geschäftsbetrieb oder die Aufgabenerfüllung einer Institution im hohen Maße beeinträchtigen und sogar zu einem existenzbedrohenden Schaden führen können. Hierunter fallen z. B. Cyber-Angriffe oder extreme Naturereignisse, gegen die sich Institutionen nicht komplett schützen können.

Obwohl Institutionen sich mit Informationssicherheit zu schützen versuchen, führten verschiedene Cyber-Angriffe in den vergangenen Jahren immer wieder zu Ausfällen kritischer Geschäftsprozesse (siehe jährliche Lageberichte des BSI zur IT-Sicherheit in Deutschland). Insbesondere Ransomware-Angriffe haben sich hierbei zu einer immanenten Bedrohung entwickelt.

Auf der anderen Seite sorgt die fortschreitende Effizienzsteigerung von Geschäftsprozessen dafür, dass Leerlauf- und Pufferzeiten auf ein Minimum reduziert werden. Um Lagerflächen einzusparen, werden zudem in der Logistik und der Produktion auch die benötigten Ressourcen auf ein Mindestmaß reduziert. Damit verkleinert sich in der Praxis aber auch das Zeitfenster, um auf Ausfälle der Geschäftsprozesse angemessen reagieren und unmittelbare Folgewirkungen eindämmen zu können. Entsprechend steigt die Notwendigkeit, gegen Ausfälle des Geschäftsbetriebs umfassend vorzusorgen.

Mit Hilfe eines angemessenen **Business-Continuity-Managements (BCM)** können sich Institutionen vor Schadensereignissen schützen, die sich in nicht tolerierbarer Weise auf den Geschäftsbetrieb auswirken. Ziel

des BCM ist es sicherzustellen, dass der Geschäftsbetrieb selbst bei massiven Schadensereignissen nicht unterbrochen wird (**Prävention**) oder nach einem Ausfall in angemessener Zeit fortgeführt werden kann **(Reaktion).** Das BCM umfasst organisatorische, technische, bauliche und personelle Maßnahmen. Institutionen können hierzu teilweise auf vorhandene Sicherheitsmaßnahmen weiterer Managementsysteme, wie dem ISMS, zurückgreifen oder erweitern diese gegebenenfalls.

Das BCM ist kein einmaliges Projekt, sondern bedarf eines zielgerichteten und sich kontinuierlich verbessernden **Business-Continuity-Management-Systems (BCMS)**, das sich an die stetig verändernden Rahmenbedingungen einer Institution anpasst (siehe Kapitel *2.2 Grundlagen eines Managementsystems*). So wird ein dauerhafter Prozess geschaffen, um organisatorische Resilienz (Widerstandsfähigkeit) aufzubauen.

Organisatorische Resilienz ist die Fähigkeit einer Institution, auf Veränderungen zu reagieren und sich daran anzupassen. Je „resilienter" eine Institution ist, umso besser kann sie Risiken und Chancen aus plötzlichen und allmählichen internen und externen Veränderungen erkennen sowie flexibel darauf reagieren.

Organisatorische Resilienz wird nicht durch ein eigenständiges Managementsystem aufgebaut, sondern entsteht aus der Integration verschiedener Management-Disziplinen. In diesem Standard sind die Informationssicherheit, das Business Continuity Management, die Krisenbewältigung und IT-Service Continuity (siehe Abbildung 1) die Eckpfeiler, um Resilienz zu schaffen.

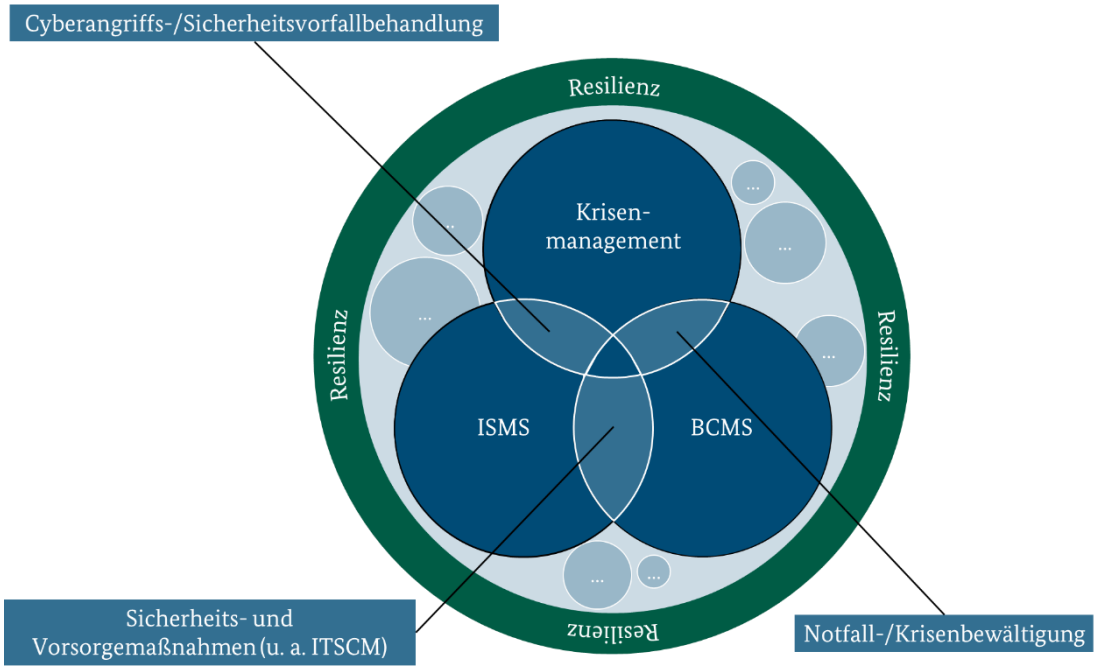

Abbildung 1: Resilienz schaffen durch verschiedene Sicherheitsthemen

Hinweis:

Neben den genannten Sicherheitsthemen können auch die Arbeitssicherheit, Perimeter- und Gebäudeschutz, personelle Sicherheit oder das IT-Berechtigungsmanagement integriert werden, um die Resilienz zu steigern.

Gemäß ISO 22316:2017 wird die Resilienz einer Institution darüber hinaus auch von Prozessen beeinflusst, die keinen direkten Bezug auf die Themen Sicherheit und Business Continuity haben, wie Qualitätsmanagement, Supply Chain Management, Finanzen, Personal und Betrugsprävention.

1.3 Anwendungsweise

Im BSI-Standard 200-4 *Business Continuity Management* wird beschrieben, mit welchen Methoden BCM in einer Institution generell initiiert und gesteuert werden kann. Der vorliegende BSI-Standard 200-4 bietet konkrete Hilfestellungen, wie ein BCMS Schritt für Schritt eingeführt werden kann. Im Fokus stehen somit einzelne Phasen dieses Prozesses sowie bewährte Best-Practice-Lösungen.

Ein ISMS wird explizit für diesen BSI-Standard nicht vorausgesetzt. Es kann jedoch den Aufbau und den Betrieb eines BCMS nach dem BSI-Standard 200-4 unterstützen und beschleunigen.

Der vorliegende BSI-Standard 200-4 setzt die Reihe der BSI-Standards 200-1 bis 200-3 konsequent fort. Er geht innerhalb der verschiedenen Kapitel auf zahlreiche Synergiepotenziale ein, insbesondere zwischen den Themen Informationssicherheit und BCM (siehe Kapitel 2.4 *Abgrenzung und Synergien*).

Zusätzlich bietet dieser Standard viele Hilfsmittel und Dokumentenvorlagen, die auf der Website des BSI heruntergeladen werden können. Die Dokumentenvorlagen beinhalten zum Teil Textbausteine und Elemente zur Strukturierung. Daher ist es sinnvoll, diese Dokumentenvorlagen zu berücksichtigen, auch wenn sie nicht als eigene Dokumentenvorlage verwendet werden.

Der vorliegende BSI-Standard 200-4 gestattet eine individuelle Anpassung an die zeitlichen, finanziellen und personellen Möglichkeiten der jeweiligen Institution. Das BCMS kann schrittweise in drei Stufen aufgebaut werden: 1. Reaktiv-BCMS, 2. Aufbau-BCMS und 3. Standard-BCMS (siehe Kapitel 2.6 *BCMS Stufenmodell*). Alle Empfehlungen dieses Standards müssen jedoch stets im Kontext der jeweiligen Institution betrachtet und an die jeweiligen Rahmenbedingungen angepasst werden.

Die Stufe Standard-BCMS ist konform zu den Anforderungen des ISO-Standards 22301:2019 (siehe [22301]). Dementsprechend erreichen Institutionen mit einem vollständig eingeführten und betriebenen Standard-BCMS die erforderliche Reife, um zertifizierungsfähig nach ISO 22301 zu sein. Das Kapitel 8 *Anhang A: Anforderungskatalog* und das Hilfsmittel *Dokumentenvergleich ISO 22301* können hierbei hilfreich sein.

Auch wenn als Grundlage für das BCMS eine andere Methodik angewendet wird, ist es trotzdem möglich, vom BSI-Standard 200-4 zu profitieren. So bietet der vorliegende Standard auch Lösungsansätze für einzelne Aufgabenstellungen, beispielsweise für die Konzeption bestimmter Methoden und Notfallpläne oder die Durchführung von Revisionen und Zertifizierungen im Bereich des BCM. Je nach Anwendungsbereich bilden bereits einzelne Umsetzungshinweise, Hilfsmittel oder Synergiepotenziale, die der BSI-Standard 200-4 zur Verfügung stellt, hilfreiche Grundlagen für die Arbeit im BCM.

Aufbau des BSI-Standards 200-4

Der Kapitelaufbau folgt der Handlungsreihenfolge, in der einzelne BCM-Prozessschritte praktisch umgesetzt werden, um ein BCMS aufbauen, betreiben und weiterentwickeln zu können. Die Vorgehensweise wird je nach gewählter BCMS-Stufe individuell beschrieben. Auf Kapitel zu einzelnen BCM-Prozessschritten, die sich in der praktischen Umsetzung überschneiden oder Abhängigkeiten zueinander besitzen, wird gesondert hingewiesen.

Für Personen, die über keine Vorerfahrung zum Aufbau eines Managementsystems im Allgemeinen sowie zum BCM im Speziellen verfügen, wurde das Kapitel 2 *Einführung in das BCM* verfasst. Es erläutert die wichtigsten Begriffe und Definitionen zum BCM sowie die die wichtigsten Schnittstellen zu anderen Managementsystemen. Personen und Institutionen mit Vorerfahrung zum BCM sollten mindestens die Kapitel 2.1 Begriffe, 2.3 *Ablauf der Bewältigung* sowie 2.6 *BCMS Stufenmodell* gelesen haben, um die im vorliegenden Standard genutzten Begriffe und deren Definitionen zu kennen.

Unabhängig von der gewählten BCMS-Stufe muss Kapitel 3 *Initiierung des BCMS* angewendet werden, da in diesem Kapitel die Grundlagen eines BCMS geschaffen werden.

Institutionsleitungen haben eine grundsätzliche Verantwortung für das BCM. Sie sollten aufgrund dieser Verantwortung mindestens die Inhalte des Kapitels 3.1 *Initiierung des BCMS durch die Institutionsleitung* kennen und beachten.

Je nachdem, welche BCMS-Stufe in der Initiierung ausgewählt wurde, muss entweder ein

- Reaktiv-BCMS nach Kapitel 4 oder ein
- Aufbau-BCMS nach Kapitel 5 oder ein
- Standard-BCMS nach Kapitel 6 aufgebaut werden.

Hinweis

Aufgrund eines besseren Leseflusses und einer besseren Verständlichkeit wiederholen sich einzelne Prozessschritte (Inhalte und insbesondere die Erläuterungen) in den Kapiteln 4 und 6. Da sich allerdings die Methoden im Detail unterscheiden, unterscheiden sich auch die Kapitel im Detail, insbesondere die Anforderungen.

Kapitel 7 setzt sich konkreter mit den besonderen Herausforderungen des BCM im Rahmen von Outsourcing und Lieferketten auseinander.

Kapitel 8 *Anhang A: Anforderungskatalog* fasst die Anforderungen zusammen, damit BCM-erfahrene Leser einen schnellen Überblick gewinnen können.

Kapitel 9 *Anhang B: Hinweise zu den Hilfsmitteln* enthält Informationen über weiterführende Hilfsmittel auf der Website des BSI.

1.4 Modalverben

Dieser Standard verbindet ausführliche Anleitungen mit konkreten Anforderungen. Zusätzlich wird in Kapitel 8 *Anhang A: Anforderungskatalog* eine reine Anforderungsliste für Prüfaspekte zur Verfügung gestellt. Die Prüfaspekte werden in den Anforderungen mit den Modalverben „muss“ und „sollte“ sowie den zugehörigen Verneinungen formuliert, um die jeweiligen Anforderungen eindeutig zu kennzeichnen. Die hier genutzte Definition basiert auf RFC 2119 (siehe [RFC2119] sowie DIN 820-2:2012, Anhang H (siehe [820-2]).

„Muss/darf nur“: Dieser Ausdruck bedeutet, dass es sich um eine Anforderung handelt, die unbedingt erfüllt werden muss (uneingeschränkte Anforderung).

„Darf nicht/darf kein“: Dieser Ausdruck bedeutet, dass etwas in keinem Fall getan werden darf (uneingeschränktes Verbot).

„Sollte“: Dieser Ausdruck bedeutet, dass eine Anforderung normalerweise erfüllt werden muss, es aber Gründe geben kann, dies doch nicht zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden.

„Sollte nicht/sollte kein“: Dieser Ausdruck bedeutet, dass etwas normalerweise nicht getan werden sollte, es aber Gründe geben kann, dies doch zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden.

2 Einführung in das BCM

Dieses Kapitel ermöglicht Institutionen ohne Vorerfahrung einen schnellen Einstieg in das Thema BCM und schafft bei allen Anwendern ein klares Verständnis über die zentralen Begriffe, Definitionen und Bestandteile dieses Standards. Innerhalb dieses Kapitels werden grundlegende, für das BCM relevante Aspekte anschaulich erläutert.

2.1 Begriffe

Im Fokus des BCM liegen die **zeitkritischen Geschäftsprozesse** der Institution, die gegen **Ausfälle** abgesichert werden sollen. Um ein einheitliches Verständnis zu schaffen, gelten innerhalb dieses Standards die nachfolgend aufgeführten Definitionen der genannten Begriffe:

Ein **Geschäftsprozess** im Sinne des BCM ist eine Menge logisch verknüpfter Einzeltätigkeiten (Aufgaben, Arbeitsabläufe), die durch Organisationseinheiten (**OEs**) ausgeführt werden, um ein bestimmtes betriebliches Ziel zu erreichen. Im behördlichen Umfeld ist der Begriff Fachaufgabe dafür geläufiger.

Hinweis:

Nachfolgend werden unter dem Begriff Geschäftsprozess auch Fachaufgaben verstanden.

Das BCM betrachtet Geschäftsprozesse ausschließlich allgemeingültig. Einzeltätigkeiten, wie sie z. B. in der Organisationsanalyse anhand einer Prozessmodellierung erhoben und dokumentiert werden, sind für das BCM nicht relevant.

Als **zeitkritisch** gelten dabei alle Geschäftsprozesse, deren Ausfall innerhalb eines zuvor festgelegten Zeitraums zu einem nicht tolerierbaren, unter Umständen existenzgefährdenden Schaden für die Institution führen kann. Falls Ressourcen wie etwa Personal, IT-Systeme oder Dienstleister benötigt werden, um die zeitkritischen Geschäftsprozesse aufrecht zu erhalten, dann müssen auch diese Ressourcen als zeitkritisch angesehen werden. Jedoch kann es in einer Institution kritische Geschäftsprozesse geben, die nicht zeitkritisch sind. Im BCM werden nur die zeitkritischen Geschäftsprozesse berücksichtigt, da bei anderen Prozessen davon ausgegangen wird, dass genügend Zeit zur Verfügung steht, darauf angemessen zu reagieren.

Üblicherweise werden Schadensereignisse durch die **Allgemeine Aufbauorganisation (AAO)** im täglichen Dienst- bzw. Geschäftsbetrieb (**Normalbetrieb**) behoben. Die **AAO** ist die ständige Organisationsform der Institution für die Aufgaben des täglichen Dienstes bzw. Geschäftsbetriebs. Für die AAO sind die Zuständigkeiten, der hierarchische Aufbau sowie die Kommunikations- und Entscheidungswege festgelegt.

Einschränkungen, Unterbrechungen oder Ausfälle des Geschäftsbetriebs können jedoch so gravierend sein, dass sie nicht mehr durch die AAO und deren Strukturen bewältigt werden können. Dazu wird in der Regel eine **Besondere Aufbauorganisation (BAO)** eingesetzt.

Die BAO ist eine zeitlich begrenzte Organisationsform, um auf außergewöhnliche Situationen angemessen und schnell zu reagieren. Innerhalb der BAO gelten dazu zeitlich begrenzte Zuständigkeiten, Hierarchien sowie Kommunikations- und Entscheidungswege, die von dem täglichen Normalbetrieb abweichen.

Um zu verdeutlichen, welche Schadensereignisse durch das BCM behandelt werden, werden die Begriffe **Störung**, **Notfall** und **Krise** voneinander abgegrenzt.

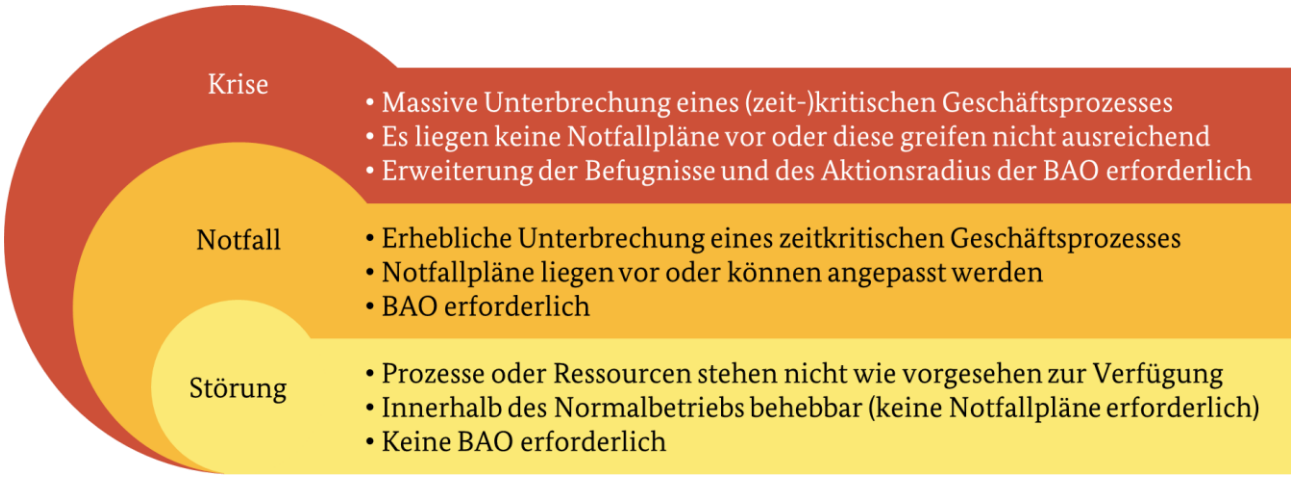

Abbildung 2: Abgrenzung Störung, Notfall, Krise

Eine **Störung** ist eine Situation, in der Prozesse oder Ressourcen nicht wie vorgesehen zur Verfügung stehen. Störungen werden in der Regel innerhalb des Normalbetriebs durch die AAO der Institution behoben. Hierzu wird auf vorhandene Prozesse zur Störungsbeseitigung oder des Incident-Managements zurückgegriffen. Daher sind Störungen nicht Betrachtungsgegenstand dieses Standards. **Störungen können jedoch zu einem Notfall eskalieren.** Es ist daher empfehlenswert, diese zeitnah zu beheben.

Notfälle sind Unterbrechungen des Geschäftsbetriebs, die mindestens einen zeitkritischen Geschäftsprozess betreffen, der nicht im Normalbetrieb innerhalb der maximal tolerierbaren Ausfallzeit (siehe Kapitel 4.3.1.1 *Konkretisierung des Begriffs zeitkritisch*) wiederhergestellt werden kann. Im Gegensatz zu Störungen wird zur Bewältigung von Notfällen eine BAO benötigt. Im Gegensatz zur Krise liegen hier geeignete Pläne zur Bewältigung vor oder bestehende Pläne können adaptiert werden. Notfälle können auch eintreten, bevor das Schadensereignis zu einer Unterbrechung des Geschäftsbetriebs führt. Es genügt die Gefahr, dass durch das Schadensereignis der Geschäftsbetrieb unterbrochen wird.

Die Kernaspekte des BCM bestehen darin, eine entsprechende BAO zu planen und die zur Bewältigung der Szenarien erforderlichen Notfallpläne zu erstellen. Es gibt auch Szenarien, die nicht im BCM planbar sind und die daher nicht als Notfälle im Kontext des BCM betrachtet werden können. Sie werden der Krise zugeordnet.

Als **Krise** im Sinne dieses Standards wird ein Schadensereignis bezeichnet, das sich in massiver Weise negativ auf die Institution auswirkt und dessen Auswirkungen auf die Institution nicht im Normalbetrieb bewältigt werden können. Im Gegensatz zu einem Notfall liegen zur Bewältigung einer Krise jedoch keine spezifischen Notfallpläne vor, vorhandene Notfallpläne können nicht oder nur bedingt adaptiert werden oder greifen schlicht nicht. Innerhalb der Institution wird die Krise durch eingeleitete Maßnahmen der BAO bewältigt.

Krisen können unmittelbar auftreten oder aus einer Störung oder einem Notfall heraus eskalieren. Das BCM trägt dazu bei, Krisen, die den Geschäftsbetrieb der Institution beeinträchtigen, mithilfe der BAO operativ zu bewältigen (siehe *Glossar,* Definition Krisenmanagement*).* Zudem können mithilfe der BAO auch die Folgen von Schadensereignissen bewältigt werden, die zwar nicht unmittelbar den Geschäftsbetrieb betreffen, jedoch aufgrund ihrer massiven Auswirkungen auf die Institution gesondert behandelt werden müssen.

Beispiel:

Ein Stromausfall in einem Gebäudeteil der Institution, z. B. einer Werkstatt, der mit den vorhandenen Möglichkeiten der AAO beseitigt werden kann und die Arbeitsfähigkeit nicht zu lange beeinträchtigt, wird als **Störung** eingestuft.

Weitet sich der Stromausfall hingegen aus, da er längerfristig ist oder einen großen Gebäudebereich umfasst, dann ist es erforderlich, das Gebäude zu räumen, da es nicht mehr einsatzfähig ist. Falls dabei zeitkritische

Geschäftsprozesse der Institution unterbrochen werden und der Wiederanlauf des Geschäftsbetriebs nicht automatisch in der erforderlichen Zeit möglich ist, liegt ein **Notfall** vor.

Wirkt ein Stromausfall sich überregional aus, weil z. B. Überlandleitungen zerstört wurden und die Ausweichstandorte ebenfalls betroffen sind, dann liegt eine **Krise** vor. Die vorhandenen Notfallmaßnahmen (in diesem Beispiel ein Notstromaggregat für 3 Tage) sind nicht mehr ausreichend und die BAO muss ad hoc über geeignete Maßnahmen entscheiden.

Hinweis:

Viele weitere Definitionen der gängigen BCM-Literatur differenzieren die Begriffe Störung, Notfall, Krise primär anhand der Auswirkungen. Im Rahmen des vorliegenden Standards werden die Auswirkungen stärker in einen zeitlichen Bezug gesetzt, um bei einem Schadensereignis schnell einen Notfall von einer Störung oder einer Krise unterscheiden zu können. Die Fragestellung, ob ein Geschäftsprozess zeitkritisch ist, berücksichtigt beide Aspekte und wird im BCM in detaillierteren Analysen beantwortet.

Im Schadensereignis muss somit nur noch festgestellt werden, ob ein zeitkritischer Geschäftsprozess betroffen ist und ob Notfallpläne vorliegen bzw. adaptiert werden können oder nicht.

- Wenn Notfallpläne vorliegen und anwendbar sind, handelt es sich um einen Notfall, der im Rahmen der BAO mit Hilfe der Notfallpläne behandelt werden sollte.
- Wenn keine vorhanden sind oder die bestehenden Notfallpläne nur bedingt angewendet werden können, handelt es sich um eine Krise, die im Rahmen der BAO situativ behandelt werden muss.

Bei Krisen kann die weitere Besonderheit vorliegen, dass sich diese nicht nur ausschließlich auf die eigene Institution, sondern auch darüber hinaus auswirken. In der Bewältigung treten gegebenenfalls weitere Parteien in Erscheinung, wie **Behörden und Organisationen mit Sicherheitsaufgaben** (BOS, z. B. Polizei, Feuerwehr) oder Aufsichtsbehörden. Krisen, wie z. B. Großschadenslagen oder Ereignisse im Spannungs- und Verteidigungsfall, werden in diesem Standard explizit nicht beschrieben. Diese Ereignisarten werden als externe Randbedingungen für die Bewältigung der eigenen Betroffenheit aufgefasst und nicht näher erläutert.

In diesem Standard wird der Begriff **Katastrophe** nicht definiert, weil es hierzu bereits Legaldefinitionen der Länder (z. B. §2 des Katastrophenschutzgesetzes des Landes Berlin (siehe [BRLN] oder §1 des Gesetzes über den Katastrophenschutz des Landes Baden-Württemberg, siehe [BW2]) und des Bundes gibt (z. B. Definition gemäß BBK Glossar, siehe [BBK1]). Da der Umgang innerhalb der Institution mit einer Katastrophe nicht anders ist, als bei einer Krise, wird innerhalb dieses Standards auch nicht zwischen Krise und Katastrophe unterschieden.

Weitere wesentliche Begriffe, die zusätzlich relevant zum Verständnis dieses Standards sind, werden innerhalb des Glossars definiert (siehe Kapitel 9 *Anhang B: Hinweise zu den Hilfsmitteln*).

2.2 Grundlagen eines Managementsystems

Ein Managementsystem umfasst alle Regelungen, die dazu dienen, eine Institution zu steuern und zu lenken und letztlich zur jeweiligen Zielerreichung zu führen (siehe BSI-Standard 200-1). Ziel jedes Managementsystems ist es, die gesteckten Ziele effektiv und effizient zu erreichen und die sich stetig verändernden Rahmenbedingungen und Anforderungen der Institution zu berücksichtigen. Durch ein Managementsystem, das sich mit Business Continuity beschäftigt und als BCMS bezeichnet wird kann sichergestellt werden, dass der Reifegrad des BCM kontinuierlich und systematisch gesteigert wird.

Anders als ein Projekt, das ein einmaliges Vorhaben mit konkretem Ziel darstellt, bedient sich ein Managementsystem verschiedener, aufeinander abgestimmter Elemente, um systematisch und fortlaufend die Ziele einer Institution zu erreichen. Ein BCMS besteht aus den nachfolgenden Elementen (siehe Abbildung 3):

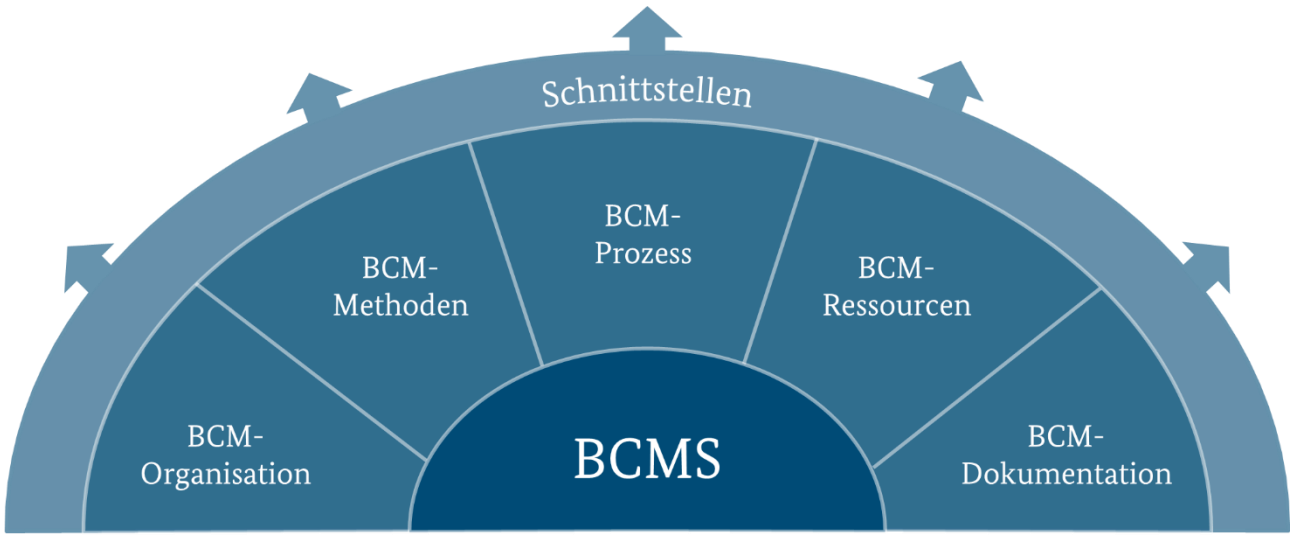

Abbildung 3: BCMS-Bestandteile

Die **BCM-Organisation** umfasst alle Rollen im BCM, die in der Notfallvorsorge sowie in der Notfallbewältigung Aufgaben und Zuständigkeiten innehaben. Grundsätzlich agieren die Rollen auf den drei nachfolgenden Ebenen innerhalb der BCM-Organisation:

- Die **Strategische Ebene** definiert den Geltungsbereich und die allgemeinen Ziele und Prioritäten.
- Die **Taktische Ebene** konkretisiert die Vorgaben, Aktivitäten und Methoden anhand des Geltungsbereichs und der Ziele.
- Die **Operative Ebene** beinhaltet konkrete Handlungen, um die gesteckten Ziele zu erreichen und berücksichtigt hierbei die definierten Vorgaben und Methoden.

Hinweis:

In anderen Standards, z. B. zur öffentlichen Gefahrenabwehr, haben die Ebenen eine andere Bedeutung, daher sollten die Begriffe taktisch und operativ stets im jeweiligen Kontext betrachtet werden.

Die **BCM-Methoden** stellen die notwendigen Werkzeuge dar, um das BCM umzusetzen. Hierzu gehören die Business Impact Analyse, die BCM-Risikoanalyse sowie Methoden, um Business-Continuity-Strategien, Lösungen und Notfallpläne zu entwickeln.

Der **BCM-Prozess** dient dazu, das BCMS aufzubauen, zu betreiben und kontinuierlich weiterzuentwickeln. Gegenüber anderen Managementsystemen weist ein BCMS die Besonderheit auf, dass es neben dem BCM-Prozess den Ablauf der Bewältigung gibt, der ebenfalls prozessual beschrieben werden kann. Die Aktivitäten der Bewältigung sind ereignisbezogen und ruhen im Normalbetrieb, bis ein Schadensereignis mit Notfall- oder Krisenpotenzial eintritt. Der BCM-Prozess regelt auch Aspekte zum Ablauf der Bewältigung und bereitet diese vor. Umgekehrt fließen Erkenntnisse aus der Bewältigung in die Weiterentwicklung und Verbesserung des BCM-Prozesses ein.

In diesem Kapitel wird nur näher auf den **BCM-Prozess** eingegangen. Der **Ablauf der Bewältigung** wird im nachfolgenden Kapitel konkreter erläutert (siehe Kapitel 2.3 *Ablauf der Bewältigung*)**.** Der **BCM-Prozess** folgt einem PDCA-Zyklus. In diesem Schema werden die Aufgaben und Aktivitäten

- nachvollziehbar geplant (PLAN),
- durchgeführt (DO),
- überwacht (CHECK) sowie
- laufend verbessert (ACT).

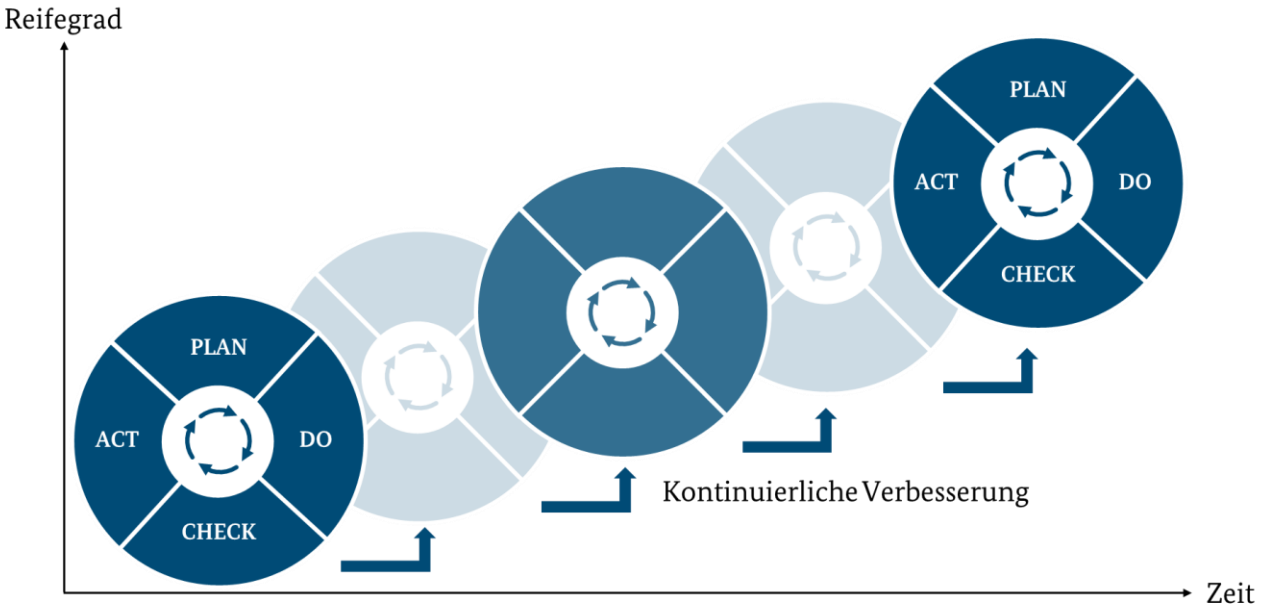

Abbildung 4: PDCA-Zyklus eines Managementsystems

Die verschiedenen Phasen PLAN, DO, CHECK, ACT werden jeweils zu einem PDCA-Zyklus zusammengefasst sowie in jedem dieser Zyklen kontinuierlich durchlaufen (siehe Abbildung 4). Der Reifegrad des Managementsystems steigert sich mit jedem weiteren PDCA-Zyklus.

In der **PLAN**-Phase werden anhand der Anforderungen der internen und externen Interessengruppen die Ziele und Rahmenbedingungen des BCM festgelegt und anschließend in Form von Leitlinien, Maßnahmen, Methoden und Vorgaben zum BCM konkretisiert.

In der **DO**-Phase werden anhand verschiedener Analysen die zeitkritischen Geschäftsprozesse und Ressourcen ermittelt und risikoorientiert durch entsprechende Maßnahmen abgesichert. Ferner werden Maßnahmen definiert, um den Geschäftsbetrieb aufrechterhalten zu können. Diese Maßnahmen werden innerhalb von Notfallplänen dokumentiert.

In der **CHECK**-Phase wird anhand von Übungen und Tests überprüft, ob die Maßnahmen zur Notfallvorsorge sowie die Notfallpläne aktuell, vollständig, wirksam und angemessen sind. Zudem werden die Vorgaben zum BCM laufend überwacht. Anhand der gewonnenen Erkenntnisse auf taktischer und operativer Ebene werden die Korrekturbedarfe und Verbesserungsmöglichkeiten des BCMS identifiziert. Durch Berichte an die Institutionsleitung zum Zustand des BCMS kann diese ihrerseits auf strategischer Ebene Korrekturbedarfe und Verbesserungsmöglichkeiten der Rahmenbedingungen, des Geltungsbereichs oder der Ziele des BCM ermitteln.

In der **ACT**-Phase werden anhand der ermittelten Bedarfe konkrete Korrektur- und Verbesserungsmaßnahmen abgeleitet. Diese stellen sicher, dass die Ziele und Rahmenbedingungen des BCM erreicht oder angepasst werden können und das BCMS verbessert wird.

Wie der BCM-Prozess anhand eines PDCA-Zyklus aufgebaut ist, hängt von der gewählten BCMS-Stufe ab (Reaktiv-, Aufbau- oder Standard-BCMS). Im vorliegenden Standard werden die drei unterschiedlichen PDCA-Zyklen daher im Einführungskapitel der jeweiligen BCMS-Stufe beschrieben.

Auf Basis der Ziele muss die Leitungsebene die erforderlichen finanziellen, personellen und zeitlichen **BCM-Ressourcen** zur Verfügung stellen. Diese werden innerhalb der Initiierung des BCMS festgelegt (siehe Kapitel 3.1 *Initiierung des BCMS durch die Institutionsleitung)*.

Die **BCM-Dokumentation** beinhaltet sowohl Dokumente, die das BCMS selbst beschreiben als auch alle Notfallpläne, die in der Notfallbewältigung eingesetzt werden. Die Besonderheiten der BCM-Dokumentation werden in Kapitel 3.2.3 *Dokumentation* näher erläutert.

Schnittstellen zu anderen Managementsystemen stellen sicher, dass die Methoden und Prozesse der unterschiedlichen Managementsysteme aufeinander abgestimmt sind. Das BCM ist anhand der Schnittstellen in die institutionsübergreifende Gesamtsicherheitsstrategie eingebunden. Zudem erzeugen Schnittstellen Synergieeffekte, um finanzielle, personelle und zeitliche Ressourcen zu sparen. Die wichtigsten Schnittstellen werden in Kapitel *2.4 Abgrenzung und Synergien* vorgestellt.

2.3 Ablauf der Bewältigung

Ein individuell angepasstes BCMS ermöglicht Institutionen, Schadensereignisse schnell und effektiv zu bewältigen.

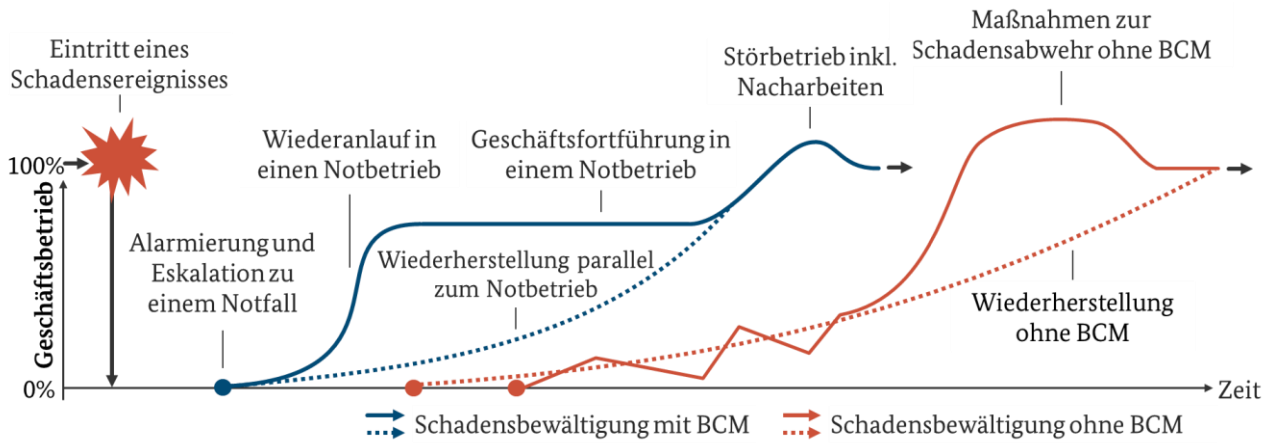

Abbildung 5: Bewältigung eines schwerwiegenden Schadensereignisses mit und ohne BCM

Ohne ein BCMS ist die Situation durch große Unsicherheit gekennzeichnet. Nachdem das Schadensereignis festgestellt und Sofortmaßnahmen eingeleitet wurden, müssen zunächst die Zuständigkeiten geklärt und alle notwendigen Informationen zusammengetragen werden. Unter Umständen müssen geeignete Kommunikationskanäle erst aufgebaut werden. Es muss geklärt werden, welche Prozesse als erstes wieder starten müssen, um die Existenz der Institution zu sichern. Falls dies nicht leicht zu ermitteln ist, besteht die Gefahr, dass unwichtigere Prozesse zuerst gestartet werden. Werden infolgedessen zeitkritische Prozesse zu spät gestartet, kann dies schnell die Existenz der gesamten Institution gefährden. Es wird deutlich mehr Zeit in Anspruch nehmen, geeignete Maßnahmen abzustimmen und auf das Schadensereignis zu reagieren. Der Geschäftsbetrieb kann nur in kleinen Schritten, anhand ad hoc entschiedener alternativer Verfahren wiederaufgebaut werden. Aufgrund des längeren Ausfalls von Geschäftsprozessen nehmen Arbeitsrückstände zu, z. B. um manuelle Arbeiten im IT-System nachzupflegen. Weitere zusätzliche Nacharbeiten werden erforderlich. Infolgedessen beginnt die Wiederherstellung ohne BCM später, da es mehr Zeit in Anspruch nimmt, das Ausmaß des Ereignisses zu erkennen und angemessen darauf zu reagieren. Zudem fehlt eine übergeordnete Koordination aller Aktivitäten, z. B. anhand von Plänen oder eines Entscheidungsgremiums.

Mit einem BCMS kann ein Schadensereignis anhand festgelegter Kriterien schnell an kompetente Entscheider gemeldet und als Notfall oder Krise identifiziert werden. Auf Grundlage der bereits vorhandenen Notfallpläne kann der Geschäftsbetrieb zeitnah wiederanlaufen und im Rahmen eines definierten Notbetriebs fortgeführt werden. Die Existenz der Institution ist gesichert. Zudem kann zur Bewältigung auf eine BAO zurückgegriffen werden. Diese ist speziell dafür etabliert und trainiert, Notfälle und Krisen zu managen.

Abbildung 6 verdeutlicht schematisch einen typischen Ablauf einer Bewältigung eines Schadensereignisses mithilfe des BCM. Die Zeitabschnitte sind zwecks besserer Lesbarkeit gestrafft dargestellt. Die wichtigsten Ereignisse und Aktivitäten der Notfallbewältigung werden nachfolgend kurz vorgestellt und in späteren Kapiteln des vorliegenden Standards näher erläutert.

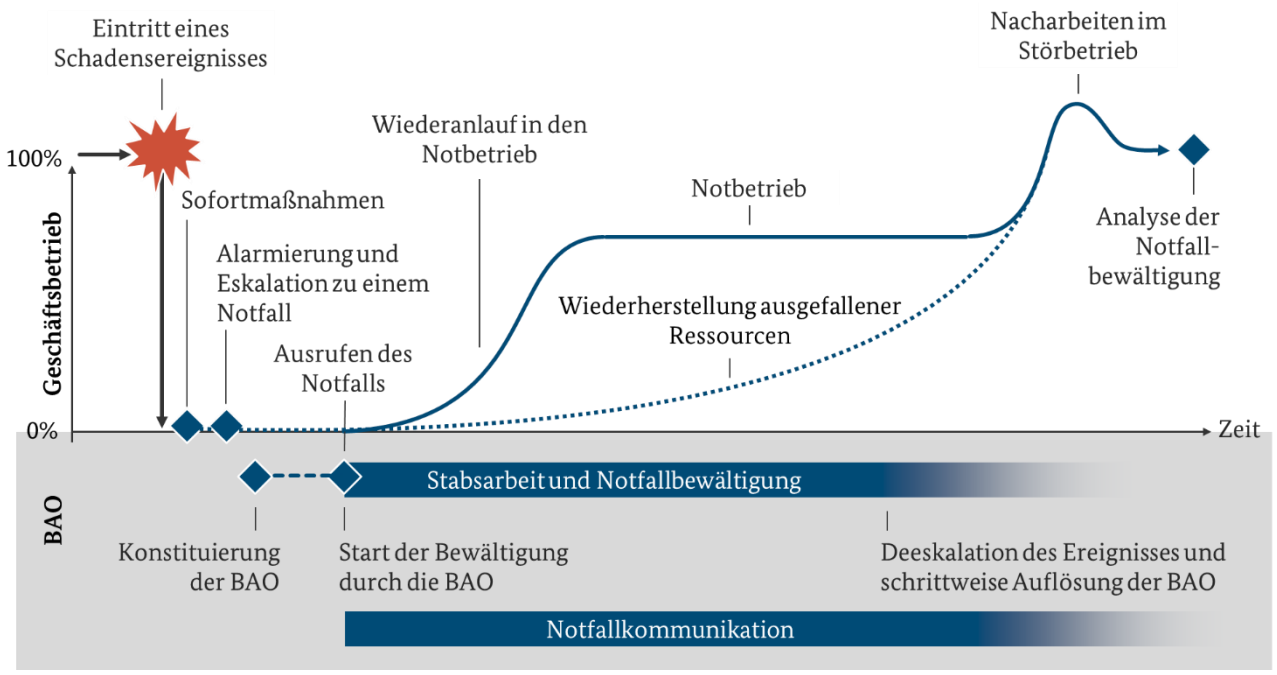

Abbildung 6: Ablauf der Bewältigung mit BCM

Hinweis:

Aufgrund der unterschiedlichen Auswirkungen von Schadensereignissen können die Ereignisse und Aktivitäten in der Bewältigung gemäß Abbildung 6 nur schematisch wiedergegeben werden. In der Praxis laufen Ereignisse und Aktivitäten nicht immer linear ab, sondern überschneiden sich oder laufen parallel zueinander. Insbesondere die Schritte Sofortmaßnahmen und Alarmierung sind situationsspezifisch und können zeitlich auch in umgekehrter Reihenfolge erfolgen.

Der **Eintritt eines Schadensereignisses** ist definiert als der Zeitpunkt, zu dem ein Schadensereignis tatsächlich passiert. Da Schadensereignisse in einigen Fällen zunächst unbemerkt bleiben, ist der Eintritt nicht immer zweifelsfrei zeitlich bestimmbar. In der Praxis kann der Eintritt des Schadensereignisses daher auch mit dem Zeitpunkt gleichgesetzt werden, zu dem das Schadensereignis erstmalig wahrgenommen wird.

Sofortmaßnahmen dienen dazu, Leib und Leben zu schützen sowie weitere Schäden in Folge des Schadensereignisses zu verhindern oder zumindest einzudämmen. So können z. B. Ausweichstandorte sofort bezogen werden. Je nach Situation können Sofortmaßnahmen bereits eingeleitet werden, noch bevor das Ereignis zu einem Notfall eskaliert wird, um weiteren Schaden aufgrund des Zeitverlustes abzuwenden. Im Einzelfall können zu Sofortmaßnahmen auch Maßnahmen gezählt werden, die keinen zeitlichen Aufschub dulden und sich daher der strukturierten Bewältigung durch die BAO entziehen, z. B. eine vorgeschriebene Sofortmeldung eines Schadensereignisses an einen Regulator.

Die **Alarmierung und Eskalation** regelt, wie ein Schadensereignis an zuvor definierte Meldestellen gemeldet werden soll. Der Standard beschreibt hierzu eine Möglichkeit, wie Meldestellen das Ereignis initial bewerten und an eine zentrale Entscheidungsinstanz melden, falls das Ereignis als potenzieller Notfall eingestuft wurde. Wird das Schadensereignis durch die Entscheidungsinstanz als Notfall bestätigt, muss diese sicherstellen, dass die BAO alarmiert wird.

Die **Konstituierung der BAO** beinhaltet alle Aktivitäten, die erforderlich sind, um die BAO arbeitsfähig zu machen. So bezieht die BAO z. B. einen Stabsraum und alle notwendigen Arbeitsmittel werden zum sofortigen Einsatz vorbereitet. Im Stab wird final darüber entschieden, ob der Notfall als solches bestätigt oder das Ereignis deeskaliert wird.

Nach Bestätigung des Notfalls erfolgt der **Start der Bewältigung durch die BAO**. Zudem wird der **Notfall in der Institution durch die BAO ausgerufen** und die BAO nimmt ihre Arbeit auf. Zunächst stellt die BAO die Lage fest und erste Maßnahmen werden festgelegt. Die verabschiedeten Maßnahmen müssen operativ umgesetzt und anschließend nachverfolgt werden, ob sie wirksam sind. Nach Ausrufen des Notfalls weist der Stab situationsbezogen die betroffenen Organisationseinheiten an, den Geschäftsbetrieb wiederanlaufen zu lassen und in einen stabilen Notbetrieb zu überführen.

Der **Wiederanlauf** beschreibt alle Maßnahmen, um strukturiert in einen vorab geregelten Notbetrieb wechseln zu können. So kann es notwendig sein, alternative Ressourcen bereitzustellen (z. B. Ausweich-IT-System, Notfallarbeitsplatz etc.), Prozesse und Tätigkeiten auf einen möglicherweise reduzierten Notbetrieb umzustellen oder die Mitarbeiter in die definierten alternativen Maßnahmen einzuweisen. Das BCM gibt Fristen vor, innerhalb derer der Wiederanlauf erfolgt sein muss (Wiederanlaufzeit).

Die Geschäftsfortführung beschreibt, wie die Geschäftsprozesse in einem **Notbetrieb** mithilfe alternativer Ressourcen bzw. alternativen Prozessschritten durchgeführt werden können. Innerhalb dieser Phase können beispielsweise Ersatzsysteme genutzt oder Tätigkeiten innerhalb von Geschäftsprozessen zurückgestellt, modifiziert oder priorisiert bearbeitet werden.

Die **Wiederherstellung** dient dazu einen Zustand zu erreichen, in dem der Normalbetrieb wieder möglich ist. Ausgefallene Ressourcen können unter anderem neu beschafft, Ersatzteile eingesetzt oder Komponenten neu installiert und konfiguriert werden. Die Wiederherstellung umfasst alle Tätigkeiten ausgehend vom Beginn der Bewältigung bis hin zur Deeskalation des Ereignisses. Sie verläuft parallel zum Wiederanlauf und zum Notbetrieb. Typischerweise erfolgt die Wiederherstellung ausgefallener Ressourcen durch die Ressourcenzuständigen Organisationseinheiten. Sie sind somit nicht Teil der BAO, sondern arbeiten parallel zu dessen Maßnahmen. Jedoch sollten die Maßnahmen zur Wiederherstellung mit den Maßnahmen zum Wiederanlauf und zum Notbetrieb abgestimmt werden, um unter anderem die Dauer des Notbetriebs ableiten zu können.

Die **Notfallkommunikation** dient dazu, Informationen während der Bewältigung zu sammeln, zu verifizieren sowie adressatengerecht nach innen und außen zu verteilen. Ferner werden im Rahmen der Notfallkommunikation vorab definierte Regeln zum Umgang mit Medien und Presse angewendet bzw. überprüft, ob diese eingehalten werden.

Die **Deeskalation des Schadensereignisses** markiert den Übergang von der Bewältigung zurück in den Normalbetrieb und kann durch die BAO ausgerufen werden, sobald sich abzeichnet, dass

- die Ursache des Schadensereignisses beseitigt wurde,
- der Schaden eingedämmt werden konnte und sich nicht weiter ausbreitet sowie
- eine Bewältigung des Schadensereignisses durch eine BAO nicht länger erforderlich ist.

In der Praxis sind zwischen der Deeskalation des Schadensereignisses und dem Erreichen des Normalbetriebs häufig weitere Aktivitäten und Nacharbeiten erforderlich.

Unter **Nacharbeiten** ist alles zu verstehen, das aufgrund des Notbetriebs nicht erledigt werden konnte, aber zur Aufgabenerfüllung nachgeholt werden muss. Dies umfasst z. B.:

- nicht bearbeitete (zeitunkritische) Aufgaben,
- Rückstand an Anfragen,
- Digitalisieren manuell erfasster Informationen,
- fehlende Berichte zu durchgeführten Aufgaben,
- Rückbau von Ersatzanlagen und -systemen,
- Rückspielen von Daten in andere Systeme oder Datenbanken sowie
- Schwenk von Ausweich- zu wiederhergestellten Hauptsystemen.

Der **Störbetrieb** umfasst alle Nacharbeiten, die sich aus dem Notbetrieb ergeben. Der Störbetrieb ist nicht unbedingt Teil der Bewältigung, da die erforderlichen Nacharbeiten teilweise bereits von den Rollen der AAO eigenverantwortlich anhand der Prozesse zur Störungsbeseitigung geplant und umgesetzt werden können.

Hinweis:

Die Praxis zeigt, dass die Zeit des Störbetriebs weiterhin eine arbeitsintensive Zeit für die Institution ist. In der Abbildung 6 ist dies durch eine „Wölbung" dargestellt, da die Institution mehr Zeit oder Ressourcen investieren muss, um diesen Rückstand aufholen zu können.

Das **schrittweise Auflösen der BAO** erfolgt innerhalb des Störbetriebs, sobald die Institution entscheidet, dass die BAO nicht mehr benötigt wird. Es kann sinnvoll sein, dass die BAO die Nacharbeiten noch eine Weile begleitet, da es z. B. dabei wieder zu einem Notfall kommen könnte.

Wenn die BAO aufgelöst wird, werden die verschiedenen Rollen innerhalb der BAO situationsbezogen aus der BAO zurück in die AAO entlassen. Zudem muss gegebenenfalls der Stabsraum zurückgebaut sowie dessen Ausstattung aktualisiert werden.

Wenn alle Arbeitsrückstände nachgearbeitet wurden und die ausgefallenen Ressourcen wiederhergestellt werden konnten ist der Normalbetrieb wieder möglich. Die **Analyse der Bewältigung** trägt wesentlich dazu bei, das BCMS weiterzuentwickeln. Anhand der gewonnenen Erfahrungen und den real angewendeten Maßnahmen und Plänen lassen sich optimal Korrekturbedarfe und Verbesserungsmöglichkeiten im BCMS identifizieren und innerhalb des kontinuierlichen Verbesserungsprozesses behandeln.

Damit eine Notfallbewältigung wie dargestellt ablaufen kann, werden im Rahmen des BCMS Vorsorge- und Notfallmaßnahmen sowie BC-Lösungen vorgeplant.

Unter **Vorsorgemaßnahmen** fallen alle Maßnahmen, die präventiv erarbeitet und umgesetzt werden und die Wahrscheinlichkeit eines Ressourcenausfalls reduzieren.

Beispiel:

In Bezug auf die Ressourcenkategorien Gebäude und Infrastruktur könnten mehrere Vorsorgemaßnahmen umgesetzt werden, um die Ausfallwahrscheinlichkeit eines Gebäudes zu senken. So können Mitarbeiter beispielsweise dahingehend sensibilisiert werden, stets auf Brandlasten wie Verpackungsmaterialien zu achten und diese umgehend zu entfernen. Zusätzliche Vorsorgemaßnahmen könnten darin bestehen, das Gebäude durch weitere Brandschutzvorkehrungen wie Brandschotte oder Feuerschutztüren gegen Feuer abzusichern.

Unter **BC-Lösungen** fallen alle Maßnahmen, die präventiv erarbeitet und umgesetzt werden, um eine Geschäftsfortführung im Notfall zu ermöglichen.

Beispiel:

„Ausweichstandort bereitstellen" stellt eine typische BC-Lösung dar. Der Ausweichstandort wird zwar bereitgestellt, aber erst im Falle eines Gebäudeausfalls von den zeitkritischen Organisationseinheiten bezogen. Auch können zusätzliche Laptops und Zugangstoken bevorratet werden. Diese ermöglichen den Mitarbeitern im Notfall ortsungebunden weiter arbeiten zu können.

Unter **Notfallmaßnahmen** fallen alle Maßnahmen, die präventiv erarbeitet jedoch erst im Notfall umgesetzt werden, um den Schaden zu begrenzen und Geschäftsprozesse fortzuführen.

Beispiel:

Die Notfallmaßnahme „Ausweichstandort beziehen“ erläutert, wie eine Organisationseinheit während eines Gebäudeausfalls an einen Ausweichstandort wechselt, welche priorisierten Tätigkeiten sie dort auf welche Weise mit den dort vorhandenen Mitteln durchführt und wie die Organisationseinheit wieder an den primären Standort zurückkehrt. Notfallmaßnahmen konkretisieren, wie zuvor erarbeitete BC-Lösungen im Notfall genutzt werden sollen.

Weitere Informationen zur Bewältigung können dem Hilfsmittel *Weiterführende Aspekte zur Bewältigung* entnommen werden.

2.4 Abgrenzung und Synergien

Ein BCMS sollte im Rahmen einer Gesamtsicherheitsstrategie in der Institution etabliert werden. Zusammen mit den nachfolgend aufgeführten Managementsystemen und Sicherheitsthemen trägt das BCM maßgeblich dazu bei, die Institution resilient gegenüber den unterschiedlichsten Arten von Risiken und Schadensszenarien zu machen. Die größten thematischen Überschneidungspunkte besitzt das BCM zu den nachfolgend aufgeführten Managementsystemen und Themen. Diese Managementsysteme werden für den Aufbau und Betrieb eines BCMS jedoch nicht vorausgesetzt.

Die nachfolgenden Kapitel erläutern die wesentlichen Gemeinsamkeiten und Unterschiede zwischen den aufgeführten Managementsystemen. Diese Informationen werden in den weiteren Kapiteln dieses Standards um grüne Synergieboxen ergänzt, die aufzeigen, welche konkreten Möglichkeiten bestehen, um die Arbeit mit den angrenzenden Managementsystemen und Themen zu erleichtern oder abzustimmen.

2.4.1 BCM und Informationssicherheit

BCM und Informationssicherheit gehören zu den wichtigsten Säulen einer ganzheitlichen Sicherheitsstrategie in einer Institution. BCM dient dazu, den Geschäftsbetrieb aufrechtzuerhalten und den Fortbestand der Institution zu sichern. Dabei profitiert BCM von den Sicherheitsmaßnahmen und den Erkenntnissen der Vorfallbehandlung aus der Informationssicherheit, welche die Verfügbarkeit der Ressourcen im Normalbetrieb sicherstellen. Durch eine zielgerichtete und möglichst frühzeitige Zusammenarbeit, z. B. bereits während die Managementsysteme initiiert werden, können Synergieeffekte genutzt und finanzielle, personelle und zeitliche Ressourcen eingespart werden. Die wichtigsten Synergieeffekte aus Sicht des BCM werden im Nachfolgenden beschrieben.

Strukturanalyse, Feststellung des Schutzbedarfs nach IT-Grundschutz und Business Impact Analyse

Im BCM bilden innerhalb der Business-Impact-Analyse die untersuchten Geschäftsprozesse und ihre für einen Notbetrieb benötigten Ressourcen die Grundlage für das weitere Vorgehen im Managementsystem. Dabei können die Ergebnisse aus der Strukturanalyse nach IT-Grundschutz als gemeinsame Datenbasis verwendet werden. Auch in einem ISMS nach ISO 27001 müssen die Geschäftsprozesse identifiziert werden. Diese können die Datenbasis für die verschiedenen Analysen im BCMS bilden.

In den darauffolgenden Analysen zum Schutzbedarf und zum Business Impact werden oftmals dieselben Ansprechpartner und ähnliche Bewertungsmethoden herangezogen. Einheitliche Stammdaten, aufeinander abgestimmte Methoden und eventuell eine gemeinsame Datenerhebung steigern die Akzeptanz in der Institution, reduzieren die Aufwände und vermeiden Missverständnisse bei den Ansprechpartnern.

Risiko-Analyse und -Behandlung

Im Hinblick auf die möglichen Ursachen eines Ausfalls des Geschäftsbetriebs oder einzelner Ressourcen können die Informationssicherheit und das BCM auf die gleichen Gefährdungen, Kriterien und Methoden zur

Risikobewertung zurückgreifen. Eine gemeinsame Übersicht der relevanten Risiken im Rahmen eines integrierten Risikobehandlungsplans erlaubt es, finanzielle, personelle und zeitliche Ressourcen einzusparen und einen umfassenden Blick auf die notwendigen Sicherheits- und BC-Lösungen zu erhalten.

Maßnahmen

Alle Maßnahmen, die darauf hinwirken die Verfügbarkeit zu optimieren, sind sowohl für das BCM als auch für die Informationssicherheit relevant. Werden Ressourcen redundant gesichert und deren Verfügbarkeit regelmäßig getestet und geübt, dann profitieren sowohl das BCM als auch die Informationssicherheit davon.

Neben dem Schutz der IT umfasst die Informationssicherheit auch den Schutz von Informationen aller Art (z. B. auch auf Papier oder in den Köpfen). Hierbei spielen neben der Verfügbarkeit die Schutzziele Vertraulichkeit und Integrität eine große Rolle. Allgemein könnte angenommen werden, dass nur Sicherheitsmaßnahmen, die die Verfügbarkeit betreffen, für das BCM relevant sind. Doch auch Sicherheitsmaßnahmen, die die Integrität und Vertraulichkeit der Informationen sicherstellen, können den Ausfall von Geschäftsprozessen verhindern oder zumindest in der Wahrscheinlichkeit reduzieren.

Informationsfluss

Beide Managementsysteme informieren regelmäßig die internen Interessengruppen über ihre Tätigkeiten, Maßnahmen und Risiken. Oftmals erfolgt diese Kommunikation an die gleichen Positionen innerhalb der Institution, durch die jeweilige Beauftragten-Funktion. Durch eine gemeinsame Berichterstattung können Zusammenhänge aufgezeigt werden, insbesondere innerhalb der Risikobewertung und Risikobehandlung. Damit werden Entscheidungen auf Grundlage einer besseren Informationsbasis getroffen, Dopplungen vermieden und somit Kosten eingespart. Anhand eines gemeinsam abgestimmten Informationsflusses können die Interessengruppen zudem für beide Themengebiete übergreifend geschult und sensibilisiert werden. Dies konkretisiert den Gedanken der Gesamtsicherheitsstrategie.

Notfallbewältigung

Auch innerhalb der Notfallbewältigung bekommt das Zusammenspiel von BCM und ISMS eine wesentliche Bedeutung. Im BCM ist die Ursache eines Ausfalls vernachlässigbar, um einen Geschäftsfortführungsplan zu aktivieren. Der Geschäftsfortführungsplan hat hauptsächlich die Aufgabe, den Ausfall zeitkritischer Ressourcen anhand alternativer Tätigkeiten in einem Notbetrieb zu überbrücken. Dennoch ergeben sich Überschneidungen, da in vielen Fällen sowohl die Business Continuity als auch die Schutzziele der Informationssicherheit betroffen sind. Wenn z. B. Teile der IT durch einen Cyberangriff kompromittiert werden und ausfallen, dann flankiert die Geschäftsfortführungsplanung des BCMS die Maßnahmen des ISMS und steigert die Resilienz der Institution.

Ausweichverfahren mit dem primären Ziel der Verfügbarkeit sollten grundsätzlich auch darauf achten, Vertraulichkeit und Integrität zu wahren und diese Schutzziele gegebenenfalls gegeneinander abzuwägen. Hier unterstützen die Erkenntnisse des ISMS, insbesondere die identifizierten Schutzbedarfe für Vertraulichkeit und Integrität, das BCM darin, geeignete Ausweichverfahren für die Notfallbewältigung zu definieren.

Unterschiede zwischen dem BCM und der Informationssicherheit

Die oben beschriebenen Überschneidungen hinsichtlich der Datenbasis und der verwendeten Methoden stehen den unterschiedlichen Zielsetzungen der Managementsysteme gegenüber. Während ein ISMS den Normalbetrieb hinsichtlich aller drei Schutzziele absichert, reduzieren die BC-Maßnahmen vor allem das Ausmaß eines eingetretenen Schadensereignisses.

Insbesondere sollten die Begriffe **Verfügbarkeit der IT gemäß ISMS** und **betriebliche Kontinuitätsanforderungen an die IT gemäß BCMS** voneinander abgegrenzt werden. Die Verfügbarkeit im Normalbetrieb muss nicht zwangsläufig der Verfügbarkeit im Notbetrieb entsprechen:

- Durch ein ISMS soll die Verfügbarkeit von Informationen soweit abgesichert werden, dass diese den Geschäftsanforderungen im Normalbetrieb entspricht. Störungsbedingte Ausfallzeiten im Normalbetrieb sollen minimiert werden. Die Anforderungen an die Verfügbarkeit werden beispielsweise innerhalb von Service oder Operation Level Agreements in durchschnittlichen Jahresverfügbarkeiten in Prozentwerten angegeben.
- Durch ein BCMS soll die Kontinuität des Geschäftsbetriebs sichergestellt werden. Im Fokus stehen die zeitkritischen Geschäftsprozesse und Ressourcen der Institution. Die umzusetzenden BCM-Lösungen dienen dazu, längere Ausfallzeiten des Geschäftsbetriebs zu verhindern. Die Anforderungen im BCM werden beispielsweise in Form von Wiederanlaufzeiten und maximalen Ausfallzeiten, bezogen auf einen Ausfall, angegeben. D. h., dass auch im Schadensfall diese Zeiten garantiert sein müssen.

Beispiel:

Ein Prozess zur Kundenbetreuung nutzt eine Anwendung, um die Kundenbeziehungen zu dokumentieren (Customer Relationship Management, CRM). Diese Anwendung erlaubt es, schnell und effizient auf Kontaktdaten zurückzugreifen und Informationen zu vorangegangen Geschäftsaktivitäten abzurufen. Auf Grund der Bedeutung der Informationen für den Geschäftsprozess erhält die Anwendung innerhalb der Schutzbedarfsanalyse des ISMS eine hohe Verfügbarkeit. Gemeinsam mit der IT-Abteilung wird eine Verfügbarkeit von 99,9%, bezogen auf das Geschäftsjahr, festgelegt. Innerhalb der Business Impact Analyse im BCM wird die CRM-Anwendung bewertet. Bezogen auf existenzbedrohende Auswirkungen auf das Unternehmen erhält diese Anwendung keine Kontinuitätsanforderung, da sie für einen Notbetrieb nicht zwingend erforderlich ist. Die Informationen können auch durch die Kontaktbetreuer als Gedankenprotokoll hergeleitet werden. Zudem befinden sich die Kontaktdaten auch in anderen Medien, wie z. B. elektronischen Adressbüchern.

Ein Prozess zur Auftragsvergabe in einem Produktionsunternehmen nutzt eine Anwendung, um die Ressourcen zu planen (Enterprise Resource Planning, ERP). Diese Anwendung erlaubt es, schnell und effizient auf Unternehmensstammdaten zurückzugreifen und den Lagerbestand in Echtzeit abzurufen. Innerhalb der Schutzbedarfsanalyse des ISMS wird deshalb eine hohe Verfügbarkeit festgestellt und gemeinsam mit der IT-Abteilung eine Verfügbarkeit von 99,9%, bezogen auf das Geschäftsjahr, für den Normalbetrieb festgelegt. Innerhalb der Business Impact Analyse erfolgt auch eine Bewertung der ERP-Anwendung. Da der Geschäftsprozess maximal 8 Stunden ausfallen darf, bevor unzumutbare Auswirkungen eintreten, wird die geforderte Wiederanlaufzeit der ERP-Anwendung auf 4 Stunden gesetzt. Die 99,9% Verfügbarkeit entspricht 8,76 Stunden maximale Ausfalldauer pro Jahr in Summe für alle Ausfälle. Hierbei wird, statistisch gesehen, nicht davon ausgegangen, dass die gesamte tolerierbare Ausfalldauer durch ein einzelnes Ereignis überschritten wird. Bei einem zeitkritischen Geschäftsprozess, der binnen 8 Stunden wiederanlaufen muss, könnte jedoch dieser schlimmste, anzunehmende Fall bereits zu nicht tolerierbaren Auswirkungen gemäß BCMS führen. Infolgedessen wird für einen Notbetrieb im BCM eine vom Normalbetrieb abweichende Wiederanlaufzeit gefordert.

2.4.2 BCM und ITSCM

In den meisten Institutionen ist der überwiegende Teil der zeitkritischen Geschäftsprozesse unmittelbar davon abhängig, dass die eingesetzte Informations- und Kommunikationstechnik wie vorgesehen funktioniert. Die Aufgabe des IT Service Continuity Managements (ITSCM) besteht darin, Risiken für den Ausfall des IT-Betriebs frühzeitig zu erkennen und effektive Gegenmaßnahmen zu etablieren. Damit sollen zeitkritische IT-Services und deren zugrundliegende IT-Systeme und IT-Ressourcen auch in einem IT-Notfall aufrechterhalten oder rasch wiederhergestellt werden können. Ein zentrales Ziel des ITSCM ist daher insbesondere, durch eine organisierte IT-Notfallbewältigung die Kontinuität der IT-Umgebungen und die Verfügbarkeit ihrer Daten auf einem für den Geschäftsbetrieb ausreichenden Leistungsniveau sicherzustellen.

Auf Basis der Anforderungen des BCM plant, implementiert und überprüft das ITSCM verschiedene präventive und reaktive IT-Notfallmaßnahmen, die baulicher, technischer, organisatorischer und personeller Natur sein können. Das ITSCM unterstützt damit das BCM, indem es sicherstellt, dass die benötigten IT-Ressourcen

die Wiederanlaufanforderungen einhalten. Darüber hinaus sorgt das ITSCM mittels Datensicherungskonzepten dafür, dass der Datenverlust in einem Notfall auf ein akzeptables Minimum reduziert wird.

Nicht jede größere IT-Störung (Major Incident) und nicht jeder größere IT-Notfall müssen automatisch als Notfall im Kontext des BCM gewertet werden. Wenn jedoch aus einem Major Incident gemäß ITSCM eine nicht tolerierbare Geschäftsunterbrechung wird, ist es von enormer Bedeutung, dass die Prozesse zur Detektion und Behandlung des Major Incidents nahtlos in die Alarmierung und Eskalation des Notfalls sowie die Notfallbewältigung übergehen (siehe Hilfsmittel *Weiterführende Aspekte zur Bewältigung*). Hierzu bedarf es entsprechender Schnittstellen zwischen dem ITSCM und dem BCM.

Beispiel:

In einer vollständig redundant aufgebauten IT-Umgebung fällt ein Rechenzentrum (RZ) nach einem lokalen Brand aus. Aufgrund von Failover-Lösungen und guter IT-Notfalldokumentation kann ohne Auswirkungen auf den Geschäftsbetrieb auf das zweite RZ umgeschaltet werden. Es handelt sich hierbei zwar aufgrund des Ausfalls der Redundanz um einen IT-Notfall, jedoch nicht unbedingt um einen Notfall im Sinne des BCM. Die BAO des BCM braucht nicht unbedingt alarmiert werden. Jedoch sollte der BCM-Beauftragte in diesem Fall zeitnah über den Vorfall informiert werden.

Hinweis:

Wie ein ITSCM unter Berücksichtigung der BCM-Anforderungen anhand eines Plan-Do-Check-Act-Zyklus aufgebaut, betrieben und weiterentwickelt werden kann, wird unter anderem in der ISO-Norm 27031 erläutert (siehe [27031]).

2.4.3 BCM und Krisenmanagement

Anhand des vorliegenden Standards können die organisatorischen Voraussetzungen geschaffen werden, um Notfälle angemessen zu bewältigen. Ein Kernelement bildet darin der Aufbau einer Besonderen Aufbauorganisation (BAO). Diese ist grundsätzlich geeignet, auch Krisen innerhalb einer Institution zu bewältigen, und stellt damit eine wesentliche Schnittstelle zu einem Krisenmanagement (KM) dar. Spezifische Anforderungen zum Aufbau eines Krisenmanagements können unter anderem den aufgeführten Standards und Normen zum Krisenmanagement in Kapitel 2.5 *Überblick über Normen und Standards* entnommen werden.

Gemäß der Definition einer Krise im Sinne des BCM geht die Krise über den Notfall hinaus (siehe Kapitel 2.1 *Begriffe*). Bei der Krise handelt es sich um eine außergewöhnliche Situation, für die keine Notfallplanung möglich ist oder für die eine vorhandene Notfallplanung nicht mehr ausreicht, um das Schadensereignis angemessen zu bewältigen. Im Krisenfall liegt daher der Fokus auf der Fähigkeit der BAO, die Lage schnell bewerten sowie Maßnahmen situativ entscheiden und umsetzen zu können. Die vorhandenen Notfallpläne werden in einer Krise soweit eingesetzt, wie diese geeignet sind, die Auswirkungen der Krise zu minimieren

Auf die spezifischen Unterschiede zwischen der Notfall- und der Krisenbewältigung sowie auf die Besonderheiten des IT-Krisenmanagements geht das Hilfsmittel *Weiterführende Informationen zur Bewältigung* näher ein. Dieses Kapitel beschreibt auch die spezifischen Unterschiede zwischen einem Notfallstab und einem Krisenstab.

Zahlreiche, mögliche Krisenszenarien erfordern eine enge Zusammenarbeit zwischen dem BCM und dem Krisenmanagement. Um sich optimal auf Krisenszenarien vorbereiten zu können, sollten daher die für das BCM und das Krisenmanagement entwickelten Verfahren und Strukturen aufeinander abgestimmt sein. Dies betrifft z. B.:

- Rollen der BAO des BCM und des Krisenmanagements
- Alarmierungs- und Eskalationsverfahren
- Informationsflüsse im Notfall und in der Krise

- Aufgabenmanagement im Notfall und in der Krise
- Notfallpläne und Krisenmanagementpläne
- Aspekte der Notfall- und Krisenkommunikation
- Schulungen, Trainings, Notfall- und Krisenübungen
- technische Infrastrukturen für die Notfall- und Krisenbewältigung

Die Kriterien, um einen Notfall von einer Krise abzugrenzen, sollten möglichst konkret für die Institution festgelegt werden. Andernfalls müssen die Kriterien bei Eintritt eines Notfalls oder einer Krise zeitraubend diskutiert werden.

2.4.4 BCM und Outsourcing sowie Lieferketten

Im Rahmen des **Outsourcings** werden Geschäftsprozesse einer Institution vollständig oder teilweise durch externe Dienstleister erbracht und somit nicht mehr ausschließlich durch die Institution selbst.

Güter, die für die Wertschöpfung einer Institution relevant sind, werden in der Praxis häufig nicht selbst durch die Institution erzeugt. Stattdessen wird die Wertschöpfung bis zum Endprodukt dadurch erreicht, indem Dienstleister bzw. Lieferanten die benötigten Güter im Auftrag der Institution erzeugen oder liefern. Dadurch entsteht eine **Lieferkette** (engl. supply chain).

Sowohl das Outsourcing als auch Lieferketten gehen für die Institution mit der Herausforderung einher, die externe Leistungserbringung steuern und kontrollieren zu müssen. In der Regel kann jedoch nur der Dienstleister sicherstellen, dass der unterbrechungsfreie Geschäftsbetrieb seiner Leistung gewährleistet wird. Die beziehende Institution hat darauf keine oder nur begrenzte Einflussmöglichkeiten.

Sofern zeitkritische Geschäftsprozesse von externen Dienstleistern erbracht oder unterstützt werden, liegt es nicht mehr allein im Einflussbereich der güter- oder leistungsbeziehenden Institution, angemessen auf Notfälle zu reagieren und diese zu bewältigen. Vielmehr müssen die relevanten Ressourcen und Geschäftsprozesse des Dienstleisters in die eigene Notfallbewältigung mit eingebunden und beide aufeinander abgestimmt werden. Zudem wirken sich Notfälle auf Seiten des Dienstleisters unmittelbar auf den Geschäftsbetrieb der leistungsbeziehenden Institution aus und müssen entsprechend im BCM des Dienstleisters abgesichert werden. Das angestrebte Leistungsniveau des Dienstleisters in einem Notfall muss dabei dem Anspruch der leistungsbeziehenden Institution gerecht werden.

Outsourcing und der Bezug von externen Gütern in Lieferketten ist heutzutage gängige Praxis in vielen Institutionen. Um die besonderen Bedingungen berücksichtigen zu können, müssen entsprechende Schnittstellen zum BCM geschaffen werden. Diese stellen sicher, dass mögliche Ausfallrisiken des Geschäftsbetriebs durch BCM-Anforderungen an den Dienstleister vermieden oder reduziert werden können. Der vorliegende Standard beschreibt diese besonderen Rahmenbedingungen explizit im Kapitel 7 *BCM im Rahmen des Outsourcings und von Lieferketten*.

2.5 Überblick über Normen und Standards

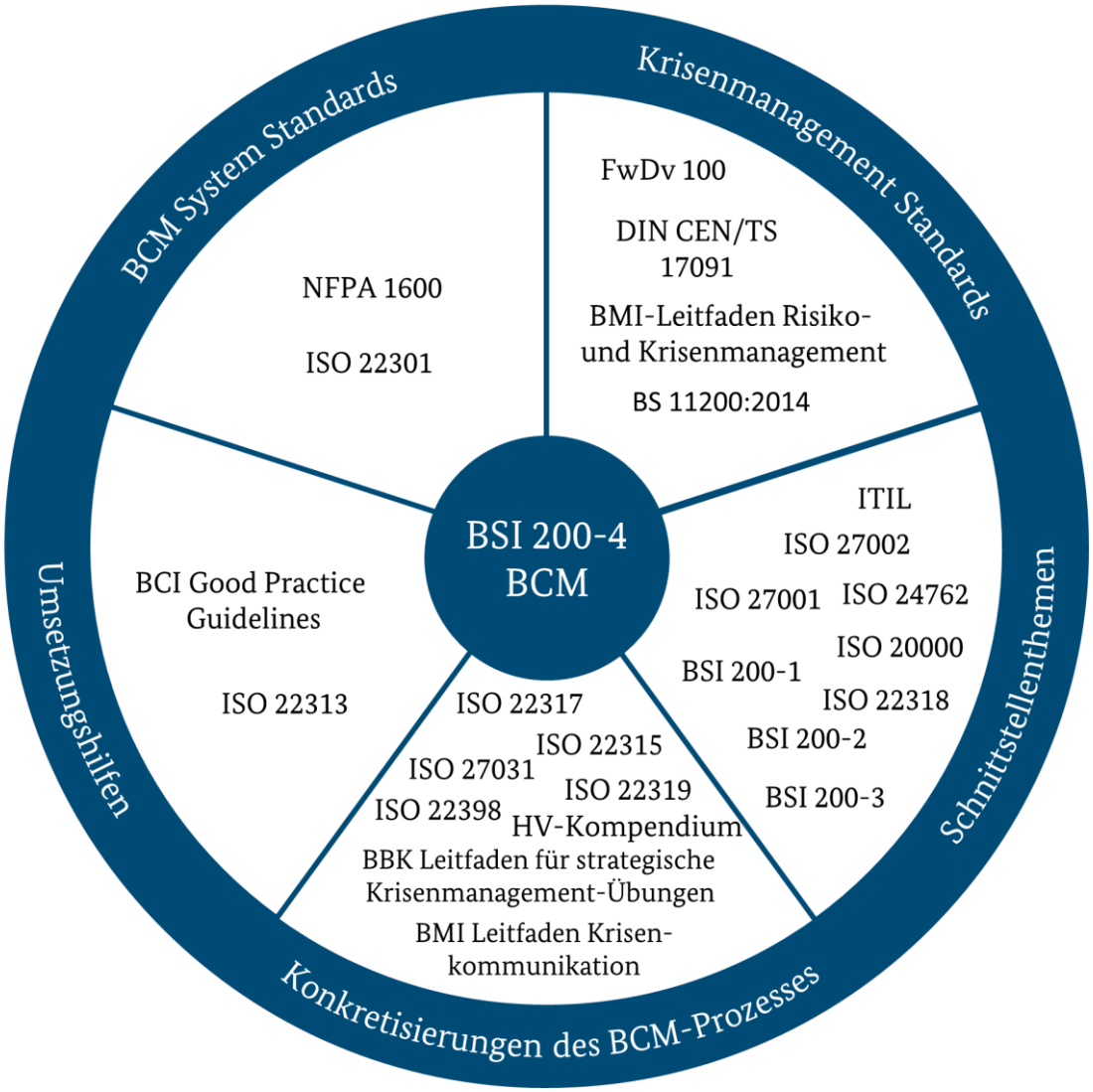

Abbildung 7: Übersicht über BCM-Standards sowie korrespondierende Sicherheitsthemen

BCM wird in verschiedenen Normen sowie nationalen und internationalen Standards behandelt. Abbildung 7 gibt einen kurzen Überblick über die wichtigsten Normen und Standards in diesem Umfeld, ohne den Anspruch auf Vollständigkeit zu erheben. Nachfolgend wird eine Auswahl der für diesen Standard relevanten Normen und Standards kurz vorgestellt.

ISO 22301:2019 (abgekürzt ISO 22301)

Der ISO-Standard 22301 „Security and resilience - Business continuity management systems - Requirements“ (siehe [22301]) ist der erste internationale Standard zum BCM, der auch eine Zertifizierung ermöglicht. Ziel des Standards ist es, Institutionen zu helfen, die Risiken von Betriebsunterbrechungen jeglichen Ursprungs zu reduzieren. Hierzu beschreibt der Standard alle Anforderungen, um ein BCMS planen, einrichten, betreiben, überwachen, überprüfen und kontinuierlich verbessern zu können.

Der internationale Standard erschien erstmalig in 2012 und ersetzte die Reihe des Britischen Standard BS 25999. Er wurde 2019 erneut überarbeitet und der BSI-Standard 200-4 ist kompatibel zu dieser überarbeiteten Version. Im Gegensatz zu diesem BSI-Standard stellt der ISO-Standard 22301 Anforderungen auf abstrakterer Ebene. Der BSI-Standard 200-4 ist deutlich konkreter und gibt an vielen Stellen Wege zur Umsetzung mit.

Ergänzende ISO-Standards der ISO 22300-Reihe konkretisieren einzelne Aspekte oder Schnittstellen zum BCM, z. B.:

- ISO 22313:2020 „Societal security and resilience – Business continuity management systems –Guidance on the use of ISO 22301“ (siehe [22313])
- ISO 22317:2015 „Societal security – Business continuity management systems – Guidelines for business impact analysis“ (siehe [22317])

BSI-Standards

Im Kapitel 2.4.1 *BCM und Informationssicherheit* wurde auf die zahlreichen Schnittstellen des BCM und der Informationssicherheit eingegangen. Entsprechend führt der BSI-Standard 200-4 die BSI-Standards der **200-x-Reihe** konsequent fort.

Der **BSI-Standard 200-1 „Managementsysteme für Informationssicherheit (ISMS)“** definiert die allgemeinen Anforderungen an ein ISMS und beschreibt, mit welchen Methoden Informationssicherheit in einer Institution generell initiiert wird (siehe [BSI1]).

Der **BSI-Standard 200-2 „IT-Grundschutz-Methodik“** beschreibt den Aufbau und den Betrieb eines Managementsystems für Informationssicherheit und erläutert die einzelnen Schritte der IT-Grundschutz-Vorgehensweise zur Erstellung einer Sicherheitskonzeption (siehe [BSI2]).

Der **BSI-Standard 200-3 „Risikoanalyse auf der Basis von IT-Grundschutz“** beschreibt, wie aufbauend auf der IT-Grundschutz-Vorgehensweise eine vereinfachte Analyse von Risiken für die Informationsverarbeitung durchgeführt werden kann. Diese basiert auf den elementaren Gefährdungen die im IT-Grundschutz-Kompendium beschrieben sind und auf deren Basis auch die IT-Grundschutz Bausteine erstellt werden Die beschriebene Methode kann auch im Rahmen der BCM-Risikoanalyse des BSI-Standard 200-4 angewendet werden (siehe [BSI3]).

Good Practice Guidelines (GPG)

Eine weitere Umsetzungshilfe im BCM sind die Good Practice Guidelines (GPG) des Business Continuity Institute (siehe [GPG]). Dessen Ziel ist es, einen hohen Standard und Kompetenz im Bereich des BCM zu setzen. Im Jahre 2002 wurden zum ersten Mal die Good Practice Guidelines herausgegeben, die von Mitgliedern des BCI entwickelt wurden und seitdem regelmäßig aktualisiert und optimiert werden. Die GPG wurden in mehrere Sprachen übersetzt.

Leitfaden Krisenkommunikation

Der Leitfaden Krisenkommunikation des Bundesministeriums des Innern (siehe [BMI1]) hilft dabei, die externe und interne Krisenkommunikation zu planen, aufzubauen und zu optimieren. Der Leitfaden beinhaltet hierfür eine Anleitung, wie die Anforderungen in der Krisenkommunikation analysiert werden können und einen Musteraufbau, um einen Krisenkommunikationsplan zu erarbeiten.

ITIL

Die „IT Infrastructure Library“ (ITIL) wird von AXELOS herausgegeben, gepflegt und weiterentwickelt (siehe [ITIL]). ITIL erläutert, wie die wesentlichen Steuerungsprozesse in der Software-Entwicklung und im IT-Betrieb gestaltet, implementiert und gemanagt werden können. Sie berücksichtigt hierzu aktuelle Trends wie Agile Softwareentwicklung, DevOps und Lean IT-Management. Von besonderer Bedeutung für das BCM ist ITIL, weil eine wichtige Komponente darin das ITSCM ist.

Leitfäden der Bundesländer zum Krisenmanagement

Verschiedene Bundesländer veröffentlichen länderspezifische Leitfäden zum Krisenmanagement, z. B. der Leitfaden Krisenmanagement durch Krisenstäbe im Lande Nordrhein-Westfalen bei Großeinsatzlagen, Krisen und Katastrophen (siehe [NRW]) oder die Verwaltungsvorschrift der Landesregierung und der Ministerien zur Bildung von Stäben bei außergewöhnlichen Ereignissen und Katastrophen des Landes Baden-Württemberg (siehe [BW1]).

2.6 BCMS Stufenmodell

Der vorliegende Standard richtet sich an Institutionen jeglicher Art, Branche, Größe und Auftrag. Entsprechend sind auch die zeitlichen, finanziellen und personellen Möglichkeiten sowie die Vorerfahrungen, um ein BCMS aufzubauen, in jeder Institution unterschiedlich ausgeprägt. Um den unterschiedlichen Rahmenbedingungen und Möglichkeiten gerecht zu werden, kann anhand des vorliegenden Standards ein BCMS in drei verschiedenen Stufen etabliert werden:

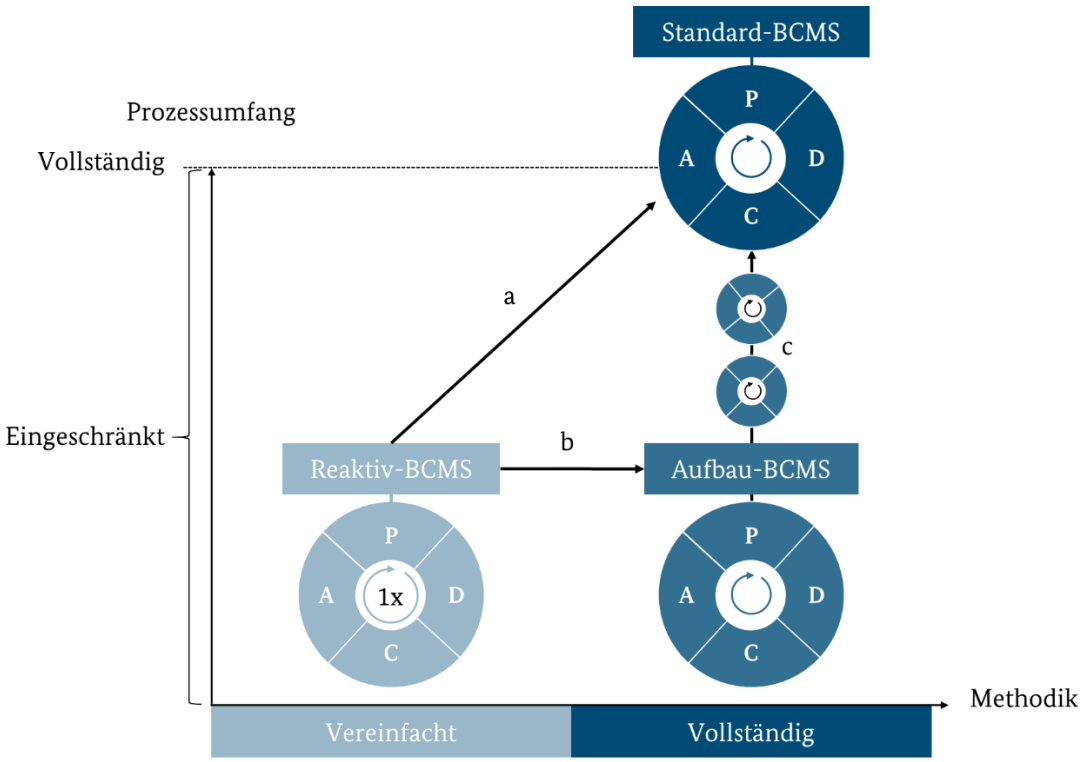

Abbildung 8: BCMS-Stufen und Übergang zwischen den Stufen

In der Initiierung des BCMS kann jede Institution die für sie optimale BCMS-Stufe auswählen. Wie in der Abbildung 8 dargestellt, bestehen verschiedene Möglichkeiten, um von jeder BCMS-Stufe zur höchsten Stufe, dem Standard-BCMS zu gelangen. Die jeweiligen Stufen unterscheiden sich hinsichtlich der anzuwendenden Methodik sowie des zu berücksichtigenden Prozessumfangs.

Methodik: Die Methodik kann im Reaktiv-BCMS vereinfacht werden, indem bestimmte Analysemethoden zeitlich zurückgestellt werden, die der detaillierteren Analyse der Rahmenbedingungen des BCMS oder der Notfallvorsorge dienen. In der vollständigen Methodik, die im Aufbau- oder Standard-BCMS angewendet wird, werden hingegen Aspekte der Notfallvorsorge und der Notfallbewältigung gleichermaßen berücksichtigt. Auch die jeweiligen Methoden der einzelnen BCMS-Prozessschritte sind erweitert, um detailliertere Ergebnisse zu ermöglichen. Zum einen kann so das BCMS deutlich effektiver und zielgerichteter aufgebaut werden. Zum anderen kann die BAO konkreter und bedarfsorientierter definiert werden.

Prozessumfang: Im Rahmen der Initiierung des BCMS wird dessen Geltungsbereich festgelegt. Unabhängig vom Geltungsbereich des BCMS kann anhand eines eingeschränkten Prozessumfangs der Ressourcenaufwand zunächst reduziert werden. Anschließend kann der Prozessumfang mit jedem weiteren Zyklus schrittweise gesteigert werden, bis alle Geschäftsprozesse im Geltungsbereich des BCMS betrachtet werden.

Tabelle 2 stellt die Eigenschaften sowie die jeweiligen Vor- und Nachteile jeder Stufe gegenüber.

Eigenschaft	Reaktiv-BCMS	Aufbau-BCMS	Standard-BCMS
Vorteile	Schnelle Fähigkeit zur Notfallbewältigung	Schrittweiser und damit ressourcenschonender Aufbau des BCMS	Vollständige Absicherung und damit Resilienz der Institution
Nachteile	Lücken in der Absicherung und Bereiche, die nicht betrachtet werden	Bereiche, die in der Absicherung der Institution nicht betrachtet werden	Erhöhter Ressourcenbedarf gegenüber den Einstiegsstufen

Tabelle 2: Vergleich der BCMS-Stufen

Das **Reaktiv-BCMS** ist besonders für Institutionen geeignet, die sich möglichst schnell in die Lage versetzen möchten, angemessen auf Notfälle reagieren zu können. Dazu wird auf vorhandene Sicherheits- und Vorsorgemaßnahmen der Institution zurückgegriffen und nur ausgewählte zeitkritische Geschäftsprozesse und Ressourcen der Institution werden priorisiert abgesichert. Weitere Maßnahmen im BCM, für die zunächst der Geschäftsbetrieb eingehender analysiert werden müsste, werden bewusst zeitlich zurückgestellt und erst durch den Wechsel zu einem Standard-BCMS (Pfad a in Abbildung 8) oder Aufbau-BCMS (Pfad b Abbildung 8) näher betrachtet. Das Reaktiv-BCMS stellt damit lediglich eine stark vereinfachte Einstiegsstufe dar, die nach Durchlaufen eines einzigen BCM-Prozess-Zyklus zu einem Aufbau- oder Standard-BCMS weiterentwickelt werden muss.

Das **Aufbau-BCMS** dient als Einstiegsvorgehensweise zum Schutz der zeitkritischen Geschäftsprozesse und Ressourcen einer Institution. Diese Vorgehensweise unterscheidet sich vom Standard-BCMS dahingehend, dass zunächst ein Ausschnitt aus dem Geltungsbereich des BCMS nämlich der Prozessumfang näher analysiert und innerhalb des BCM abgesichert wird. Gegenüber dem Standard-BCMS besteht der Vorteil, dass die Institution ihre personellen und zeitlichen Ressourcen schrittweise festlegen und mit jedem neuen Zyklus anhand der gewonnenen Erfahrungen anpassen kann (Pfad c in Abbildung 8). Damit ist das Aufbau-BCMS vor allem für Institutionen geeignet, die ein BCMS über mehrere Zyklen schrittweise und risikoorientiert aufbauen möchten oder über geringe Vorerfahrung verfügen. Gegenüber dem Reaktiv-BCMS besteht der Vorteil, dass die identifizierten zeitkritischen Geschäftsprozesse wesentlich effektiver abgesichert werden.

Das **Standard-BCMS** entspricht einem vollständigen und angemessenen BCMS, das allen Interessengruppen gerecht wird. Es werden alle Geschäftsprozesse, die sich im Geltungsbereich des BCMS befinden analysiert. Die zeitkritischen Geschäftsprozesse werden entsprechend des Ausfallrisikos anhand geeigneter Vorsorge- und Notfallmaßnahmen abgesichert. Wird ein Standard-BCMS vollständig umgesetzt, dann kann die Institution die notwendige Reife für eine Zertifizierung nach ISO-Standard 22301 erreichen.

Hinweis:

Die Stufen Reaktiv-BCMS und Aufbau-BCMS können genutzt werden, um mit geringerem Aufwand ein vorläufiges BCMS zu etablieren. Darüber hinausgehend muss grundsätzlich immer das Ziel bestehen, ein Standard-BCMS zu erreichen. Nur über ein Standard-BCMS kann sichergestellt werden, dass alle zeitkritischen Geschäftsprozesse einer Institution identifiziert und dann angemessen gegen existenzbedrohende Schadensereignisse geschützt werden.

Die folgenden Kriterien können dabei helfen, eine bestimmte BCMS-Stufe auszuwählen:

Gesetzliche oder regulatorische Anforderungen: Die Institution muss gesetzliche oder regulatorische Anforderungen erfüllen. Diese setzen voraus, dass alle Geschäftsprozesse innerhalb des Geltungsbereichs des BCMS vollständig untersucht werden.

Vorerfahrung mit Managementsystemen: Die Institution greift auf Erfahrungen zum Aufbau und Betrieb eines Managementsystems zurück, z. B. weil bereits ein ISMS gemäß ISO 27001 nach IT-Grundschutz-Vorgehensweise etabliert wurde.

Vorerfahrung mit Notfallmanagement bzw. BCM oder Krisenmanagement: Die Institution hat bereits Notfallkonzepte nach BSI-Standard 100-4 oder ISO-Standard 22301 erstellt oder sie hat bereits eine BAO zur Bewältigung von Notfällen oder Krisen etabliert.

Ressourcenausstattung: Die Institution verfügt über die erforderliche Ressourcenausstattung, um ein BCMS zu etablieren, z. B., weil bereits in ausreichender Anzahl Personal mit dem notwendigen Wissen und der Erfahrung im BCM vorhanden ist.

Um ein Reaktiv-BCMS aufzubauen, sind keine spezifischen Voraussetzungen nötig. Daher ist es für Einsteiger bestens geeignet. Mit einem Aufbau- oder Standard-BCMS einzusteigen ist dann empfehlenswert, wenn die mit X markierten Kriterien für die Institution erfüllt sind:

Kriterien bzw. Stufen	Aufbau-BCMS	Standard-BCMS
Es existieren gesetzliche bzw. regulatorische Anforderungen		X
Es existiert solide Vorerfahrung mit Managementsystemen	X	X
Es existiert Vorerfahrung mit Notfallmanagement bzw. BCM oder Krisenmanagement	X	X
Ressourcenausstattung ist gut		X

Tabelle 3: Gegenüberstellung der BCMS-Stufen anhand verschiedener Kriterien

Hinweis:

Weiterführende Informationen, wie z. B. eine vollständige Übersicht über den jeweiligen BCMS-Prozess, können den Einführungskapiteln zu den einzelnen Stufen entnommen werden.

3 Initiierung des BCMS

Ein BCM ist umso erfolgreicher, je breiter es in der Institution verankert wird und je besser es gelingt, die Motivation für die erforderlichen Tätigkeiten zu vermitteln. Die Grundlagen hierfür werden in der **Initiierung des BCMS** geschaffen. Hiermit ist eine Reihe von wichtigen Schritten gemeint, die zu Beginn der Aufbauphase des BCMS in der Institution durchgeführt werden müssen.

Darüber hinaus bedarf es einer zielgerichteten **Konzeption und Planung des BCMS**, um die gesteckten Ziele an das BCM, unter Berücksichtigung der personellen, zeitlichen und finanziellen Möglichkeiten der Institution, erreichen zu können. Die stufenspezifischen Aspekte der Planung werden abhängig von der gewählten BCMS-Stufe beschrieben.

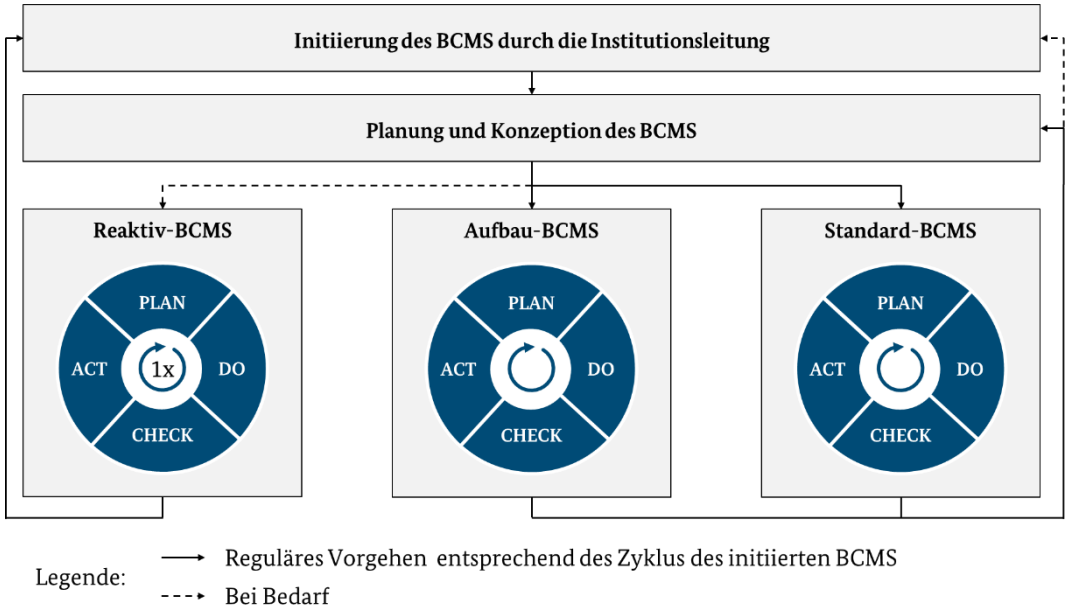

Abbildung 9: Übersicht über den Ablauf eines BCMS

3.1 Initiierung des BCMS durch die Institutionsleitung

Um ein angemessenes BCM in der Institution zu etablieren und aufrechtzuerhalten, müssen die Rahmenbedingungen und Ziele für das BCM festgelegt und in der Institution transparent kommuniziert werden. Ein BCM muss von der Institutionsleitung initiiert werden, weil die zu treffenden Entscheidungen weitreichende Konsequenzen haben. Wie in Abbildung 10 dargestellt, erläutern die nachfolgenden Unterkapitel die Zwischenschritte zur Initiierung des BCM durch die Institutionsleitung.

Abbildung 10: BCM-Prozessschritte zur Initiierung des BCMS durch die Institutionsleitung

3.1.1 Zielsetzung

Jede Institution braucht eine individuelle Zielsetzung für ein angemessenes BCM. Die Institutionsleitung, muss diese Ziele formulieren und das Ergebnis innerhalb der Institution kommunizieren. Die Leitung setzt ein klares *Startsignal*, indem sie sämtlichen Interessengruppen der Institution die Ziele des BCM bekannt gibt. Gleichzeitigt vergibt die Institutionsleitung den dafür notwendigen Arbeitsauftrag an die taktische und operative Ebene.

Die Zielsetzung sollte primär auf zwei Fragen eingehen:

- Warum benötigen wir in der Institution ein BCM? (Motivation für den Aufbau eines BCMS)
- Wie lange soll der Geschäftsbetrieb durch das BCM abgesichert werden? (Abzusichernder Zeitraum durch ein BCM)

Spätere Schritte im BCM-Prozess behandeln weitere Fragen, wie:

- „Was soll wie abgesichert werden?“
- „Wie wird das BCMS in Methoden und Prozessschritten dargestellt?“

3.1.1.1 Motivation für den Aufbau eines BCMS

Die Institution muss die spezifischen Gründe für ein BCM identifizieren und dokumentieren. Die Gründe für ein BCM ergeben sich aus bestimmten Rahmenbedingungen der Institution. Solche Rahmenbedingungen sind z. B. gesetzliche Regelungen oder bestimmte Erwartungshaltungen von Kunden oder Aufsichtsbehörden. Zudem können Erkenntnisse aus aktuellen Umfeld- und Risikoanalysen, z. B. aus dem (Informationssicherheits-)Risikomanagement, in die Zielsetzung einfließen. Ein weiterer wesentlicher Einflussfaktor sind die Geschäftsziele des Unternehmens bzw. der Auftrag der Behörde. Im Folgenden werden anhand von Beispielen typische Gründe dafür beschrieben, ein BCM einzuführen. Dabei kann grob zwischen internen und externen Gründen unterschieden werden.

Interne Gründe für BCM

BCM liegt insbesondere im Eigeninteresse einer Institution. Ein BCM trägt nachweislich dazu bei, die Überlebensfähigkeit der Institution in Notfällen zu erhöhen und ermöglicht flexible Reaktionen. Dementsprechend erfordert das BCM einen gewissen Aufwand an Arbeitszeit und zusätzlichen Ressourcen (Material und Finanzmittel). Institutionen, die ein funktionsfähiges BCMS eingeführt haben, sind insgesamt resilienter gegen Störungen und Ausfälle aller Art. Die mit dem BCM geschaffenen Voraussetzungen zur Notfallbewältigung ermöglichen es der Institution, selbst in außergewöhnlichen und weitreichenden Notfallsituationen handlungsfähig zu bleiben.

Darüber hinaus erfordert BCM auch, dass sich die Beteiligten gründlich mit den geschäftlichen Abläufen der Institution beschäftigen. Die Geschäftsprozesse und deren Abhängigkeiten werden transparenter. So können auch Verbesserungspotenziale für den Normalbetrieb sichtbar werden, was einen positiven Nebeneffekt erbringen kann.

Externe Gründe für BCM

Für die Ressorts und Einrichtungen der Bundesverwaltung gelten die Anforderungen aus dem Umsetzungsplan Bund 2017 (siehe [BMI1]). Die Bundesbehörden sind laut Kapitel 6 und Kapitel 10 dazu verpflichtet, für zeitkritische Geschäftsprozesse Maßnahmen zu entwickeln, um die Arbeitsfähigkeit sicherzustellen.

Die Konzeption Zivile Verteidigung (siehe [BMI2]) erläutert die ressortabgestimmte Aufgabenerfüllung im Bereich der Zivilen Verteidigung und zivilen Notfallvorsorge des Bundes. Diese regelt in Kapitel 5 *Aufrechterhaltung der Staats- und Regierungsfunktionen*, dass *„in einer Krise und im Verteidigungsfall […] sichergestellt sein [muss], dass Gesetzgebung, Regierung und Verwaltung sowie die Rechtsprechung funktionsfähig bleiben.*

Die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung ist im Spannungs- und Verteidigungsfall weiterhin vorrangig von den im Frieden zuständigen Behörden der Länder und des Bundes zu gewährleisten. Hierzu ist die Umsetzung von Maßnahmen zum internen behördlichen Risiko- und Krisenmanagement erforderlich."

Für viele Institutionen besteht keine unmittelbare Verpflichtung dazu, ein BCM gemäß BSI-Standard 200-4 oder einem vergleichbaren Standard zu etablieren. Aus gesetzlichen Anforderungen und aus Vorgaben einer Muttergesellschaft ergibt sich jedoch eine direkte Notwendigkeit ein BCM zu betreiben. Auch andere Verpflichtungen, wie z. B. Erwartungshaltungen von Kunden oder Geschäftspartnern, fordern ein BCMS aktiv zu betreiben.

Zusätzlich kann auch eine indirekte Notwendigkeit für BCM bestehen. Beispielsweise sind die Vorstände größerer Kapitalgesellschaften durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) zu einem angemessenen Risikomanagement verpflichtet. Dies wiederum erfordert, dass das Unternehmen ausreichend gegen Notfälle abgesichert ist.

Weitere Gesetze, Verordnungen und Richtlinien, aus denen für die betroffenen Unternehmen und Behörden Verpflichtungen zum BCM folgen, sind z. B.:

- Anforderungen an Aktiengesellschaften (z. B. EU-Richtlinie 2157/2001, Aktiengesetz (AktG)
- Anforderungen an die Kommunikation (z. B. Richtlinie (EU) 2018/1972 über den europäischen Kodex für die elektronische Kommunikation, Post- und Telekommunikationssicherstellungsgesetz (PTSG))
- das Börsengesetz (BörsG)
- das Arbeitsschutzgesetz (ArbSchG)
- die Störfallverordnung (12. BImSchV – StörfallV)
- die Gefahrstoffverordnung (GefStoffV)
- die Betriebssicherheitsverordnung (BetrSichV)
- die EU-Verordnung über die Risikovorsorge im Elektrizitätssektor (Verordnung (EU) Nr. 2019/941)
- die EU-Verordnung über Maßnahmen zur Gewährleistung der sicheren Gasversorgung (Verordnung (EU) Nr. 2017/1938)
- die Richtlinien und Verordnungen für Kritische Infrastrukturen (z. B. EU-Richtlinie 2008/114/EG, BSI-Kritisverordnung (BSI-KritisV)) und das IT-Sicherheitsgesetz
- die Solvency II-Richtlinie (Richtlinie 2009/138/EG), das Versicherungsaufsichtsgesetz (VAG) sowie Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo) in der Versicherungsbranche
- die Empfehlungen des Basler Ausschusses der Bank für Internationalen Zahlungsausgleich (BIZ) zur Regulierung von Banken (genannt Basel III) und deren europäischer Umsetzung über die europäische Bankenrichtlinie CRD IV (Richtlinie 2013/36/EU) und der CRR (Verordnung (EU) Nr. 575/2013)
- die Mindestanforderungen an das Risikomanagement im Bankenbereich (MaRisk)
- die Leitlinien der Europäischen Zentralbank (EZB) im Bankenbereich, wie z. B. die EBA Guidelines on ICT and security risk management (EBA/GL/2019/04)

Darüber hinaus sollte sich die Institutionsleitung Gedanken dazu machen, wie sie die Zielsetzung in die Institution kommuniziert. Ziel ist es, dass die Motivation für den Aufbau eines BCMS alle Mitarbeiter erreicht und von ihnen als bedeutsam wahrgenommen wird. Es ist empfehlenswert, etablierte Wege zur aktiven Führungskommunikation an die Mitarbeiter zu nutzen.

Synergiepotential:

Sofern bereits ein ISMS nach BSI-Standard 200-2 oder ISO-Standard 27001 etabliert wurde, liegen bereits verwendbare Informationen vor, wie z. B. eine Übersicht der internen und externen Parteien sowie deren Sicherheitsanforderungen. Darüber hinaus wird im IT-Grundschutz-Baustein ORP.5 *Compliance Management (Anforderungsmanagement),* bereits eine Aufstellung von gesetzlichen und regulatorischen Anforderungen verlangt. Die Institutionsleitung kann diese Informationen als Quelle für ihre Überlegungen zu den Gründen, ein BCM einzuführen, nutzen.

3.1.1.2 Abzusichernder Zeitraum durch ein BCM

Wesentlich für die Zielsetzung ist auch die Frage, wie lange der Geschäftsbetrieb durch das BCM abgesichert werden soll. Tendenziell kann davon ausgegangen werden, dass die Maßnahmen im BCM komplexer und damit auch teurer werden, je länger ein Ausfall des Geschäftsbetriebs abgesichert und überbrückt werden soll. Im selben Maße steigt jedoch auch die Resilienz der Institution, da für gewöhnlich mehr Geschäftsprozesse abgesichert werden, je länger der abzusichernde Zeitraum gewählt wird. Notfälle, die über den vom BCM abgesicherten Zeitraum andauern, führen typischerweise dazu, dass ergänzende Maßnahmen aus dem Krisenmanagement aktiviert werden müssen. Der abzusichernde Zeitraum muss für die Institution individuell festgelegt werden, da dieser stark von unterschiedlichen Gegebenheiten abhängt, wie z. B. von

- der Risikobereitschaft der Institution (Je kürzer der abzusichernde Zeitraum gewählt wird, desto eher muss das Krisenmanagement aktiviert werden),
- dem Reifegrad des BCMS,
- der vorhandenen oder avisierten Ressourcen des BCMS,
- der Art und Komplexität des Geschäftszwecks der Institution,
- der Vielfältigkeit und der Verteilung der Geschäftsprozesse über mehrere Standorte,
- dem Abhängigkeitsverhältnis des Geschäftsbetriebs von Dritten,
- dem Umfang und der Detailtiefe der Anforderungen an die Institution sowie
- branchenspezifischen Vorgaben.

Generell wird ein Zeitraum von 14 bis 30 Tagen empfohlen. Mehrwöchige Ausfälle bzw. Notfälle sind nicht unrealistisch, sondern kommen in der Praxis durchaus vor. Die Institution wird dadurch in die Lage versetzt, für diesen Zeitraum grundsätzlich handlungsfähig zu bleiben. Ist absehbar, dass ein Ausfall diesen Zeitraum überschreitet, ist es innerhalb der vom BCM abgesicherten 14 bis 30 Tage oft noch möglich, weiterführende Notfallmaßnahmen zu planen und umzusetzen.

Baut eine Institution ihr BCM erst auf und unterliegt keinen besonderen Anforderungen, wird sie wahrscheinlich zunächst einen kürzeren Zeitraum wählen. In der Praxis sind 7 bis 14 Tage als kurzer Zeitraum durchaus üblich. Im Rahmen der langfristigen Weiterentwicklung des BCMS sollte wiederkehrend geprüft werden, ob es sinnvoll und angemessen ist, den Zeitraum zu erweitern.

Hinweis:

Bei einem falsch gewählten Zeitraum besteht die Gefahr, dass das BCMS die eigenen Geschäftsprozesse nicht angemessen absichert. Deswegen sollte der Zeitrahmen immer mit Bedacht ausgewählt werden.

- Ist der Zeitraum zu kurz gewählt, werden möglicherweise zeitkritische Geschäftsprozesse nicht genug abgesichert und weniger zeitkritische, aber dennoch relevante Geschäftsprozesse gar nicht identifiziert.
- Ist der Zeitraum zu lang gewählt, sind die Aufwände zu hoch und die vorhandenen Ressourcen müssen im BCM derart verteilt werden, dass diese nicht ausreichend den zeitkritischsten Geschäftsprozessen zur Verfügung stehen.

In manchen Branchen, wie z. B. dem produzierenden Gewerbe, kann es in der Praxis auch vorkommen, dass ein Zeitraum von mehreren Monaten im BCM betrachtet wird.

Beispiel:

Ein Produktionsunternehmen erwirtschaftet seinen Umsatz primär mit Großaufträgen, die eine Laufzeit von einem Jahr oder länger haben. Eine Produktionsverzögerung von einem Monat, auf Grund eines Notfalls, hat auf dieses Unternehmen keine gravierenden Folgen, sondern wird im Normalbetrieb behandelt.

3.1.2 Geltungsbereich

Vor dem Aufbau eines BCMS muss die Institutionsleitung festlegen, welcher Bereich der Institution abgesichert werden soll. Dieser Bereich, auch Geltungsbereich des BCMS genannt, kann die gesamte Institution umfassen oder nur einzelne Standorte, Teilbereiche, Produkte oder Services. Die abzusichernden Bereiche müssen zur Zielsetzung des BCMS passen und die Hauptaufgaben der Institution abdecken.

Beispiele:

1. Eine Institution mit mehreren Standorten legt fest, dass der Geltungsbereich des BCMS zunächst nur den Hauptstandort umfasst und nicht die Nebenstandorte.
2. Ein Unternehmen aus dem produzierenden Gewerbe legt fest, dass der Geltungsbereich des BCMS initial nur die Produktion und das Lager beinhaltet. Andere Unternehmensbereiche wie Einkauf, Buchhaltung, Marketing, Vertrieb etc. werden bewusst zurückgestellt.
3. Ein IT-Dienstleister, der für die Öffentliche Verwaltung tätig ist, begrenzt den Geltungsbereich des BCMS auf ein bestimmtes Fachverfahren, das von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) zum Informationsaustausch genutzt wird.
4. Ein Konzern mit global verteilten und unabhängig agierenden Tochtergesellschaften legt je Tochtergesellschaft ein eigenes BCMS mit jeweils eigenem Geltungsbereich fest. Hierbei erstellt der Konzern zentrale Vorgaben an die einzelnen BCMS der Tochtergesellschaften, damit diese nicht zu unterschiedlich aufgebaut werden. Dies kann beispielsweise erreicht werden, indem BCM-Mindestanforderungen innerhalb einer gemeinsamen Konzern- bzw. Gruppenrichtlinie auf übergeordneter Ebene formuliert werden.

In jedem Fall muss der Geltungsbereich klar abgegrenzt und sinnvoll in sich abgeschlossen sein. Dabei sollten nur wenige, eindeutig definierte Schnittstellen vorhanden sein. Falls Teile der betrachteten Geschäftsprozesse organisatorisch von externen Partnern abhängig sind, beispielsweise im Rahmen von Outsourcing, sollten diese Schnittstellen ebenfalls klar definiert werden. Falls Einschränkungen und Abgrenzungen für das BCMS vorgenommen wurden, sollten diese in der Beschreibung des Geltungsbereichs durch die Institutionsleitung begründet werden.

Synergiepotential:

Sofern bereits ein ISMS nach BSI-Standard 200-2 etabliert wurde, kann es sinnvoll sein, sich an dem ISMS-Geltungsbereich zu orientieren. Ein zentraler Vorteil besteht hierbei darin, dass bereits der Informationsverbund und ein großer Teil der Ressourcen aus der Strukturanalyse bekannt sind. Darüber hinaus liegen bereits Ergebnisse aus Aktivitäten wie der Schutzbedarfsfeststellung, dem IT-Grundschutz-Check und der Risikoanalyse vor, die für den Aufbau des BCMS von Interesse sind. Der übernommene Geltungsbereich muss zur Zielsetzung passen.

3.1.3 Entscheidung für Vorgehensweise

Manche Vorhaben scheitern an unrealistischen oder zu ehrgeizigen Zielvorgaben. Dies ist beim Aufbau eines BCMS ebenfalls ein bedeutender Faktor. Anstelle eines groß angelegten BCM-Einführungsprojekts, kann es zu Beginn effizienter sein, ein BCMS in mehreren kleineren Schritten ohne hohe Investitionskosten in der Linie einzuführen (wie z. B. über ein Reaktiv- und anschließendes Aufbau-BCMS). In der Praxis ist es aber auch legitim, ein BCMS im Rahmen eines Projekts zu etablieren und eventuell gleich ein Standard-BCMS anzustreben. Grundsätzlich muss BCM immer in einen langfristigen, sich kontinuierlich verbessernden Prozess übergehen.

Die Institutionsleitung muss, basierend auf der Zielsetzung (siehe Kapitel 3.1.1 *Zielsetzung*) und den damit zusammenhängenden Rahmenbedingungen des BCMS sowie dem festgelegten Geltungsbereich entscheiden, wie die weiteren Schritte zum Aufbau eines BCMS aussehen sollen. Insbesondere muss die Institutionsleitung eine geeignete Stufe auswählen: Reaktiv-, Aufbau- oder Standard-BCMS. Zur Auswahl einer geeigneten Stufe sollten die Hinweise im Kapitel *2.6 BCMS Stufenmodell* berücksichtigt werden.

Falls sich die Institutionsleitung für ein Reaktiv- bzw. Aufbau-BCMS entscheidet, dann muss dies nachvollziehbar begründet und dokumentiert werden, z. B. in der Leitlinie (siehe Kapitel 4.1 *Leitlinie*). Neben den wesentlichen Einflussfaktoren, die zur Auswahl der Stufe geführt haben, sollen damit die Vor- und Nachteile sowie die zu berücksichtigenden Risiken transparent gemacht werden. Zudem muss die Institutionsleitung den langfristig angestrebten Entwicklungspfad für das BCMS aufzeigen. Das Ziel muss für jede Institution darin liegen, langfristig ein Standard-BCMS zu erreichen.

3.1.4 Übernahme der Verantwortung durch die Leitungsebene

Die Institutionsleitung ist für das zielgerichtete und ordnungsgemäße Funktionieren der Institution und damit auch für die Aufrechterhaltung des Geschäftsbetriebs in Notfällen verantwortlich. Die Institutionsleitung ist die Instanz, welche die Entscheidung über den Umgang mit Risiken trifft und die entsprechenden Ressourcen zur Verfügung stellen muss. Die Verantwortung für das BCM verbleibt bei ihr.

Die Institutionsleitung, sowie jede einzelne Führungskraft, müssen sich sichtbar zu ihrer Verantwortung bekennen und allen Mitarbeitern die Bedeutung des BCM vor Augen führen. In der Regel übernimmt ein Mitglied der Institutionsleitung die Rolle als verantwortlicher Prozesseigentümer des BCM. Die operativen Aufgaben im Kontext BCM werden an einen BCM-Beauftragten delegiert (siehe Kapitel 3.1.5 *Benennung des BCM-Beauftragten*).

Die Institutionsleitung muss im BCM eine Vorbildfunktion übernehmen. Dazu muss sie unter anderem aktiv Informationen über den Status Quo des BCM einfordern und das BCM durch Managemententscheidungen steuern. Darüber hinaus sollte sie an ausgewählten Schulungen, Trainings und Übungen teilnehmen und andere Führungskräfte bei der Ausübung ihrer Vorbildfunktion unterstützen.

Synergiepotential:

Das BCM weist vielfältige Berührungspunkte zu anderen Aufgaben auf, insbesondere dem Sicherheits-, dem Informationssicherheits- und dem Risikomanagement. Wenn die Institutionsleitung auf eine enge Zusammenarbeit mit verwandten Bereichen achtet, können Synergieeffekte, z. B. anhand einer Gesamtsicherheitsstrategie, ausgenutzt werden. Dies kann dazu beitragen, dass das BCM wirtschaftlich und effektiv umgesetzt wird.

3.1.5 Benennung des BCM-Beauftragten

Die Institutionsleitung hat in der Regel nicht ausreichend Zeit, das BCM operativ aufzubauen und aufrechtzuerhalten. Um hier die Institutionsleitung zu unterstützen, muss ein **BCM-Beauftragter (BCMB)** als Haupt-

ansprechpartner für alle Aspekte rund um das BCM ernannt werden. Er koordiniert sämtliche mit BCM zusammenhängenden Aufgaben und treibt sie innerhalb der Institution voran. Zusätzlich sollte für den BCMB ein qualifizierter Vertreter benannt werden.

Es steht jeder Institution frei, eine andere Bezeichnung für die Rolle des BCMB zu wählen. Geläufige Titel sind neben dem BCMB auch Notfallbeauftragter, Business Continuity Manager oder Notfallmanager. Aus diesen Titeln folgt aber auch manchmal ein anderes Rollenverständnis. Titel wie *Notfallmanager* führen oft dazu, dass fälschlicherweise angenommen wird, der Rolleninhaber steuere die Notfallbewältigung, obwohl die Rolle in der Regel innerhalb der Notfallvorsorge tätig ist. In diesem Standard wird diese Rolle durchgehend als BCMB bezeichnet.

Es ist empfehlenswert, die Position des BCMB organisatorisch als Stabsstelle in der AAO der Institution einzurichten, also als eine direkt der Leitungsebene zugeordnete Position, die von keinen anderen Stellen Weisungen bekommt. Zum einen muss der BCMB das direkte und jederzeitige Vorspracherecht bei der Institutionsleitung haben, um diese über BCM-relevante Ereignisse und Risiken sowie Maßnahmen zum BCM informieren zu können. Zum anderen muss er auch über das Geschehen in der Institution, soweit es einen Bezug zu seiner Tätigkeit hat, umfassend und frühzeitig unterrichtet werden. Es wird davon abgeraten, den BCMB in einer Organisationseinheit in der Linienorganisation (z. B. IT-Abteilung oder Verwaltung) zu verorten, da hierbei leicht Interessenkonflikte entstehen können.

Zeitliche Ressourcen des BCM-Beauftragten

Von hohem Stellenwert ist die Frage, mit welchen zeitlichen Ressourcen der BCMB seinen Aufgaben nachkommen soll. Hierzu gibt es keine allgemeingültigen Vorgaben. Was angemessen ist, muss für jede Institution individuell entschieden werden.

Sofern sich das BCMS noch im Aufbau befindet, besteht die Herausforderung, dass die Methoden, die Vorgaben und die Organisationsstruktur noch nicht definiert und etabliert sind. Dadurch ist der zeitliche Aufwand, um Aufgaben im BCM umzusetzen, während des Aufbaus des BCMS meist höher als im späteren Betrieb. So wird z. B. die BIA mehr Zeit in Anspruch nehmen, wenn alle Geschäftsprozesse erstmalig bewertet werden, als wenn in einem späteren Zyklus nur noch die Angaben überprüft werden müssen. Genauso ist der Aufwand Geschäftsfortführungspläne erstmalig zu erstellen, höher, als wenn sie in nachfolgenden Zyklen nur noch aktualisiert werden.

Im ersten Schritt kann eine Schätzung der Aufwände durch die Institutionsleitung vorgenommen werden, die sich an der Frage orientiert: „Was ist uns die Geschäftsfortführung im Notfall wert?“

Für eher kleine Institutionen kann es nach erfolgreichem Aufbau des BCMS ausreichend sein, eine 50 %-Stelle des BCMB für die Aufrechterhaltung und Weiterentwicklung des BCMS einzuplanen. Dem gegenüber kann es in großen oder komplexen Institutionen auch erforderlich sein, eine oder sogar mehrere Vollzeitstellen einzusetzen, um das BCMS einzuführen und aufrechtzuerhalten. Die Institution sollte sich daher bereits frühzeitig intensiv mit der Ressourcenplanung (siehe Kapitel 3.2.3 *Ressourcenplanung*) auseinandersetzen und dabei ihre Rahmenbedingungen, Anforderungen sowie ihre organisatorischen und finanziellen Möglichkeiten berücksichtigen.

Mit den gewonnenen Erkenntnissen aus dem laufenden Betrieb des BCMS können die zeitlichen Ressourcen des BCMB sukzessiv konkretisiert und angepasst werden.

Hinweis:

Es wird ausdrücklich davon abgeraten, die Position des BCMB mit weniger als einer 50%-Stelle zu besetzen. Ansonsten kann die Aufgabe nicht mit der notwendigen Sorgfalt ausgeführt werden. Dieses Mindestmaß muss immer an den individuellen Bedarf angepasst werden, sodass größere Institutionen dieser Rolle auch mehr Ressourcen zur Verfügung stellen müssen.

Synergiepotential:

Um die zeitlichen Ressourcen einzuschätzen, mit der die Rolle des BCMB ausgeübt werden kann, kann sich an den Mitarbeiterkapazitäten anderer Managementsysteme orientiert werden, wie z. B. dem Informationssicherheitsbeauftragten des ISMS.

Fachliche und persönliche Eigenschaften des BCM-Beauftragten

Um den vielfältigen Aufgaben und Anforderungen im BCM gerecht zu werden, muss der BCMB angemessene fachliche und persönliche Eigenschaften sowie Erfahrungen besitzen oder diese durch gezielte Schulungen aufbauen (siehe Kapitel 3.2.5 *Schulung*).

Die Erläuterungen in Kapitel 3.2.2 *Definition der BCM-Aufbauorganisation* decken die in der Praxis üblichen Aufgaben und Zuständigkeiten des BCMB ab. Darüber hinaus sollte der BCMB über die folgenden fachlichen und persönlichen Fähigkeiten und Kenntnisse verfügen bzw. dahingehend befähigt werden:

- Fähigkeit zur Führung von Mitarbeitern (z. B. Kooperations- und Teamfähigkeit, Selbstbewusstsein, Durchsetzungsvermögen)
- gute Kommunikationsfähigkeiten (Der BCMB sollte die Mitarbeiter und Externen von der Notwendigkeit des BCM und den damit verbundenen Aufgaben überzeugen können. Der BCMB sollte in der Lage sein, die Institutionsleitung von den Erfordernissen des BCM zu überzeugen. Dazu sind umfangreiche Transferleistungen erforderlich, um die jeweiligen Sprachwelten zu verstehen, zu respektieren und die Sachverhalte entsprechend zu übersetzen.)
- Kenntnisse allgemeiner und branchenspezifischer Vorgehensweisen und Methoden (Dies ist notwendig, um das BCMS aufzubauen, zu steuern und zu pflegen. Hierzu zählen beispielsweise etablierte BCM-Standards, in der Branche übliche Best Practices oder spezifische BCM-Anforderungen einer Aufsichtsbehörde.)
- Kenntnisse von anzuwendenden Gesetzen, Vorschriften, Standards, Leitlinien
- Kenntnisse zur Notfall-Reaktion (z. B. allgemeines Vorgehen in Notfällen, Erfahrungen in der Stabsarbeit)
- Kenntnisse von den weiteren Sicherheits- und Risikomanagementaufgaben innerhalb der Institution sowie deren Schnittstellen zum BCM
- Fähigkeit, selbstständig Richtlinien, Anweisungen, Handbücher und Verfahrensdokumentationen zu erstellen
- Kenntnisse der Geschäftsziele des Unternehmens bzw. des Auftrags der Behörde
- Kenntnisse zu Risiken für den Geschäftsbetrieb der Institution sowie die spezifischen betrieblichen Auswirkungen von Notfällen
- grundlegendes Wissen und eigene Erfahrungen hinsichtlich möglicher Maßnahmen zum BCM

Hinweis:

Der BCMB benötigt kein detailliertes Know-how zu baulichen oder technischen Notfallvorsorgemaßnahmen, wie beispielsweise IT-Redundanzkonzepten, Blitzschutz, Backup-Mechanismen und Notstromversorgung. Wenn Expertenwissen zur Erfüllung der Aufgaben erforderlich ist, kann der BCMB Mitarbeiter der AAO oder externe Spezialisten zur Unterstützung heranziehen (siehe Kapitel 3.2.2 *Definition der BCM-Aufbauorganisation*).

3.2 Konzeption und Planung des BCMS

Die Konzeption und Planung des BCMS fällt typischerweise in den Zuständigkeitsbereich des BCMB. Entsprechend sollte eine geeignete Person durch die Institutionsleitung ausgewählt und als BCMB ernannt worden sein, bevor mit den nachfolgend erläuterten Schritten begonnen wird. Die nachfolgenden Kapitel beschreiben die empfohlene Vorgehensweise, mittels derer die Konzeption und Planung des BCMS durchgeführt wird. In Abbildung 11 sind die hierfür erforderlichen Schritte in einer Übersicht dargestellt.

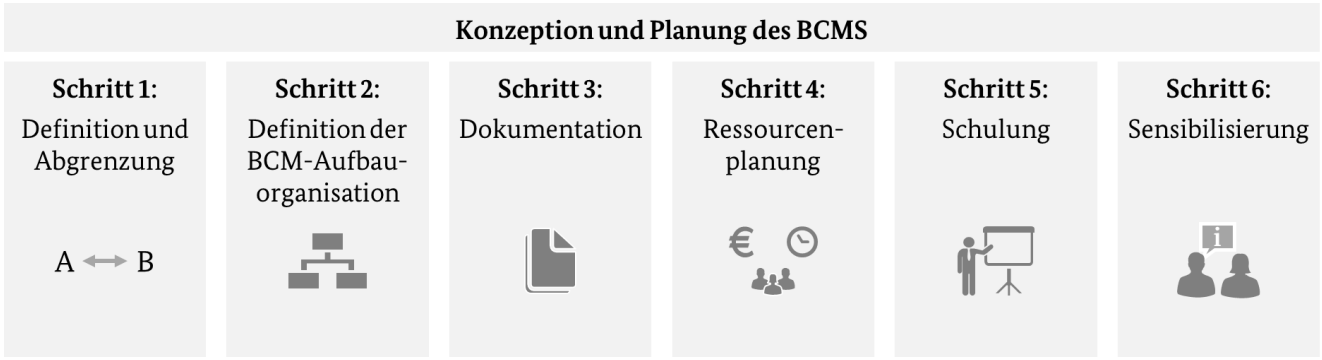

Abbildung 11: BCM-Prozessschritte zur Konzeption und Planung des BCMS

Hinweis:

Während das BCMS etabliert wird, werden zahlreiche Korrekturbedarfe und Verbesserungsmöglichkeiten identifiziert. Diese müssen in einem Maßnahmenplan dokumentiert werden. Auch wenn dieser Maßnahmenplan erst für die Weiterentwicklung des Reaktiv-BCMS (siehe Kapitel 4.8 *Weiterentwicklung des BCMS*) oder für die kontinuierliche Weiterentwicklung eines Aufbau- oder Standard-BCMS (siehe Kapitel 3.2.2 *Definition der BCM-Aufbauorganisation)* relevant ist, sollte er bereits in der Konzeption des BCMS berücksichtigt werden. So kann von vornherein sichergestellt werden, dass bereits identifizierte Korrekturbedarfe und Verbesserungsmöglichkeiten zeitnah dokumentiert werden. Dadurch werden diese nicht vergessen, bis sie zu einem späteren Zeitpunkt behandelt werden. Eine Vorlage hierfür kann den Hilfsmitteln zum Standard entnommen werden.

3.2.1 Definition und Abgrenzung

Ein BCMS besitzt vielfältige Überschneidungen und Berührungspunkte mit eventuell existierenden anderen Managementsystemen wie dem ISMS, dem Krisenmanagement oder Risikomanagement. Ferner existieren in vielen Institutionen häufig bereits Prozesse, die sich mit der Prävention, Detektion und Bewältigung von unterschiedlichen Sicherheits- und Schadensereignissen auseinandersetzen. Derartige Prozesse finden sich, z. B. im Werkschutz, Brandschutz, Arbeitsschutz, Wachschutz, der Haustechnik, dem IT Incident Management, IT Service Continuity Management oder Safety, Health and Environment.

In einem ersten Schritt sollte geprüft werden, inwiefern vorhandene Managementsysteme oder Sicherheitsprozesse bereits Aspekte des BCM und insbesondere die Bewältigung von solchen Schadensereignissen behandeln, die zu einem Ausfall des Geschäftsbetriebs führen können.

Für das BCM müssen mindestens die Begriffe *Störung, Notfall* und *Krise* eindeutig voneinander abgegrenzt werden. Hierzu kann auf die Definitionen in Kapitel 2.1 *Begriffe* zurückgegriffen werden. Liegen bereits Definitionen von Begriffen des BCM in vorhandenen Managementsystemen vor, sollte die Institution die Begriffe aufeinander abstimmen oder voneinander abgrenzen.

Hinweis:

Weitere Begriffe zum BCM können durch die Institution individuell angepasst werden und sollten ihren Rahmenbedingungen entsprechen. So kann es für eine deutsche Behörde, die bereits einen Notfallmanagementprozess etabliert hat, sinnvoll sein, den Begriff *Notfallmanagement* sowie damit korrespondierende Begriffe weiter zu nutzen anstatt sie umzubenennen. Hingegen bietet es sich für global agierende Institutionen an, den international geläufigeren Begriff BCM einzusetzen.

Ferner sollten durch die Institution die jeweiligen Zuständigkeiten zur Bewältigung von Störungen, Notfällen und Krisen klar geregelt werden. Hierbei sollten Kriterien festgelegt werden, wie bei einer möglichen Eskalation eines Schadensereignisses die Zuständigkeit von einer Management-Disziplin an eine andere übertragen werden kann (siehe Kapitel 4.2.2 *Detektion, Alarmierung und Eskalation* oder 6.4.2 *Detektion, Alarmierung und Eskalation).*

3.2.2 Definition der BCM-Aufbauorganisation

In der Regel benötigt der BCMB Unterstützung, um die angestrebten Ziele im BCM erreichen zu können.

Die Gesamtheit aller Rollen im BCM wird in der BCM-Aufbauorganisation zusammengefasst und beinhaltet sowohl die **Notfallvorsorgeorganisation** sowie die **Notfallbewältigungsorganisation**.

- Die **Notfallvorsorgeorganisation** umfasst alle Rollen, die das BCMS aufbauen, betreiben und kontinuierlich weiterentwickeln.
- Die **Notfallbewältigungsorganisation**, auch **Besondere Aufbauorganisation (BAO)** genannt, umfasst alle Rollen, die dazu dienen ein schwerwiegendes Schadensereignis, wie einen Notfall oder eine Krise, zu bewältigen.

Hinweis:

Die Besonderheiten der Notfallbewältigungsorganisation werden in den jeweiligen Kapiteln zum Aufbau und zur Befähigung der BAO näher beschrieben (siehe Kapitel 4.2.1 *Aufbau der* BAO sowie 6.4.1 *Aufbau der BAO*).

Die benötigten Rollen der BCM-Aufbauorganisation sowie deren Aufgaben und Zuständigkeiten müssen definiert werden. Anschließend müssen diese Rollen auf qualifizierte Mitarbeiter übertragen und von diesen erfüllt werden. Nur so kann gewährleistet werden, dass alle wichtigen Aspekte berücksichtigt und sämtliche anfallenden Aufgaben effektiv und effizient erledigt werden. Die gängigsten Rollen der Notfallvorsorgeorganisation werden in der Abbildung 12 beispielhaft dargestellt und in den folgenden Unterkapiteln erläutert.

Beispiel:

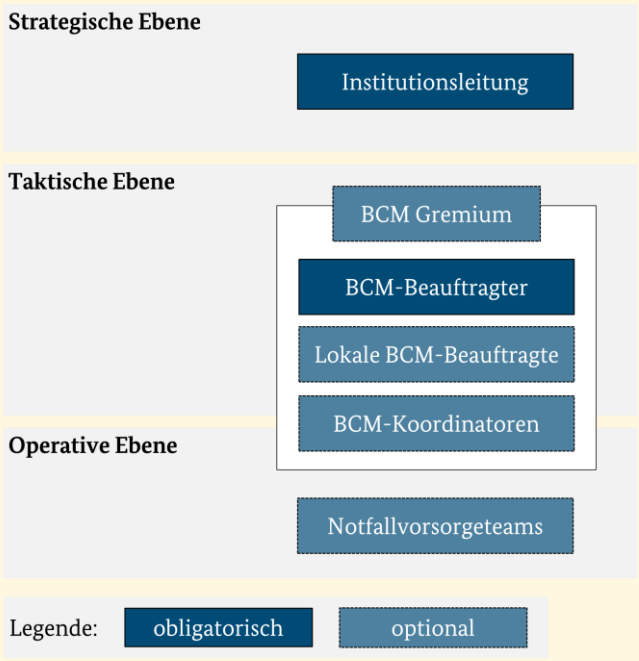

Abbildung 12: Beispiel einer BCM-Notfallvorsorgeorganisation

Allgemein können die Rollen der BCM-Aufbauorganisation drei Ebenen zugeordnet werden:

- **Strategische Ebene** (Diese legt die allgemeinen Rahmenbedingungen und Ziele fest und trägt die Verantwortung)
- **Taktische Ebene** (Diese definiert Vorgaben und Methoden anhand der Rahmenbedingungen und Ziele und überwacht die praktische Umsetzung)
- **Operative Ebene** (Diese wendet die Methoden an und setzt die Vorgaben um)

Hinweis:

In Institutionen kann diese Einteilung abweichend definiert sein. Dieser Standard verwendet konsequent obige Definition.

Die nachfolgenden Punkte stellen eine Auswahl relevanter Aspekte dar, nach denen in der Praxis eine BCM-Aufbauorganisation ausgerichtet werden kann. Die Übersicht erhebt keinen Anspruch auf Vollständigkeit:

- **Größe:** Der BCMB begleitet verschiedene Tätigkeiten innerhalb des BCM-Prozesses, die durch die Organisationseinheiten im Geltungsbereich des BCMS umgesetzt werden müssen. Sobald die Anzahl zu begleitender Organisationseinheiten zu groß wird, kann der BCMB in der Ausübung dieser Tätigkeiten durch weitere Rollen im BCM unterstützt werden.
- **Komplexität:** Viele Tätigkeiten innerhalb des BCM setzen eine gute Kenntnis der Produkte, Services sowie Strukturen und Geschäftsprozesse der Institution voraus. Mit zunehmender Komplexität einer Institution kann dieses universelle Wissen über die Abläufe und Zusammenhänge der Institution durch den BCMB allein nicht mehr sichergestellt werden. Um dieser Komplexität gerecht zu werden, kann es sinnvoll sein, dass der BCMB bestimmte Aufgaben im BCM an weitere Rollen mit entsprechenden Fähigkeiten und Kenntnissen aufteilt.
- **Geografische Verteilung:** Ist eine Institution in mehreren Ländern oder global tätig, müssen neben sprachlichen und kulturellen Unterschieden auch verschiedene ortsabhängige Rahmenbedingungen für das BCM berücksichtigt werden, z. B. aufgrund abweichender, gesetzlicher Vorgaben. Falls entschieden

wurde, keine separaten BCM-Systeme in den unterschiedlichen Ländern zu etablieren, können diese länderspezifischen Zuständigkeiten idealerweise durch Rolleninhaber abgebildet werden, die mit den Gegebenheiten vor Ort vertraut sind (siehe Kapitel 3.1.2 *Geltungsbereich*).

Dauerhaft zugewiesene Aufgaben und Zuständigkeiten im BCM sollten im Aufgaben- und Stellenprofil der jeweiligen Mitarbeiter dokumentiert werden. Bei der Festlegung der Aufgaben und Zuständigkeiten der Rollen kann sich die Institution an den nachfolgenden Vorlagen orientieren. Sofern davon abgewichen wird, muss sichergestellt werden, dass die aufgeführten Aufgaben und Zuständigkeiten über eine der Rollen abgedeckt sind.

3.2.2.1 Institutionsleitung

Die Institutionsleitung trägt die Gesamtverantwortung für das BCM. Sie muss folgende Aufgaben wahrnehmen:

- Festlegung der Ziele und Rahmenbedingungen des BCM
- Ernennung des BCMB
- Bereitstellung der angemessenen personellen, zeitlichen und finanziellen Ressourcen
- Sicherstellung, dass der BCMB sein Vorspracherecht wahrnehmen kann
- Sicherstellung, dass BCM in alle relevanten Geschäftsprozesse und Projekte integriert wird

3.2.2.2 BCM-Beauftragter

Der BCMB ist für den Aufbau, den Betrieb und die kontinuierliche Verbesserung des BCMS zuständig. Er muss die Institutionsleitung bei sämtlichen Aspekten, die für das BCM relevant sind, unterstützen und beraten. Maßgeblich für seine Tätigkeit sind die Ziele und Rahmenbedingungen, die er durch die Institutionsleitung erhält. Der BCMB hat folgende Aufgaben:

- Definition von Methoden, Vorgaben und Rollen im BCM
- fachliche Begleitung der Teilschritte im BCM-Prozess
- Überwachung der Umsetzung von Vorgaben und Einhaltung der Methoden im BCM-Prozess
- Koordination und Überwachung der Umsetzung von Verbesserungsmaßnahmen
- regelmäßige Berichterstattung an die Institutionsleitung zum Status im BCM

Für geografisch verteilte Institutionen kann es sinnvoll sein, neben einem globalen BCMB weitere **lokale BCMB** einzusetzen, welche die länderspezifischen Anforderungen kennen und die BCM-Vorgaben entsprechend anpassen können. Hierbei muss durch die Institution sichergestellt werden, dass die globalen und lokalen Vorgaben zum BCM einander nicht widersprechen.

Synergiepotenzial:

Sofern bereits ein Informationssicherheitsbeauftragte (ISB) ernannt wurde, stellt sich häufig die Frage, ob die Position des BCMB gleichzeitig vom ISB wahrgenommen werden kann. Die beiden Rollen schließen sich nicht grundsätzlich aus, es sind allerdings einige Aspekte im Vorfeld zu klären:

Es muss sichergestellt sein, dass der BCMB und ISB über ausreichend freie Ressourcen für die Wahrnehmung beider Rollen verfügt. Gegebenenfalls muss er durch entsprechendes Personal unterstützt werden.

Weiterhin sollte überlegt werden, ob konfliktträchtige Themen zur weiteren Überprüfung an die Revision übergeben werden sollten.

3.2.2.3 BCM-Koordinator (optional)

Der BCM-Koordinator (BCMK) fungiert als fachlicher Ansprechpartner und Multiplikator in seiner Organisationseinheit und stellt die Umsetzung der Vorgaben zum BCM in seinem Zuständigkeitsbereich sicher. Der BCMK hat folgende Aufgaben:

- Durchführung der Business Impact Analyse
- Erstellung, Aktualisierung oder Koordination der Geschäftsfortführungsplanung
- Durchführung von Überprüfungsmaßnahmen z. B. anhand von Übungen
- Unterstützung bei der Umsetzung von Korrektur- und Verbesserungsmaßnahmen

Der Einsatz von BCMK bietet sich insbesondere bei großen oder komplexen Institutionen an, in denen der BCMB zeitlich nicht mehr in der Lage ist, die erforderlichen Tätigkeiten in allen Organisationseinheiten zu begleiten. Der BCMB kann sich so darauf konzentrieren, die Vorgaben und Methoden zu erstellen, anzupassen und zu überwachen, ob diese eingehalten werden.

3.2.2.4 BCM-Gremium (optional)

Sofern zusätzlich zum BCMB weitere Rollen etabliert werden, die verschiedene Teilaufgaben im BCM wahrnehmen, sollten diese Tätigkeiten aufeinander abgestimmt werden. Hierzu kann beispielsweise ein BCM-Gremium aufgebaut werden, das dem kontinuierlichen Austausch zwischen den verschiedenen Rollen dient.

Synergiepotenzial:

Gibt es in der Institution bereits ein oder mehrere Gremien, die sich mit Sicherheitsfragen oder Fragen der Risikosteuerung in der Institution auseinandersetzen, können dessen Aufgaben entsprechend um BCM-spezifische Aspekte erweitert werden.

Insbesondere wenn bereits ein ISMS nach BSI-Standard 200-2 vorliegt, kann das BCM-Gremium mit dem IS-Koordinierungsausschuss kombiniert werden. Hierzu kann ein gemeinsames Gremium gebildet werden, der Teilnehmerkreis situativ um die BCM-Rollen erweitert und die Agenda der Gremiensitzungen entsprechend angepasst werden. Alternativ kann auch eine gegenseitige Vertretung in den jeweiligen Gremien eingerichtet werden.

3.2.2.5 Notfallvorsorgeteams (optional)

Bei sehr großen Institutionen, deren Organisationseinheiten eine Vielzahl von Geschäftsprozessen ausüben, kann es erforderlich sein, dass auch die BCMK durch weitere Personen im BCM unterstützt werden. Der BCMK bildet in diesem Fall zusammen mit den weiteren Personen ein Notfallvorsorgeteam. Die Notfallvorsorgeteams können temporär oder dauerhaft aufgestellt werden.

Mitglieder eines Notfallvorsorgeteams üben z. B. die folgenden typischen Tätigkeiten aus:

- Klärung spezifischer Fragestellungen zu einzelnen Geschäftsprozessen innerhalb der Durchführung der Business Impact Analyse oder BCM-Risikoanalyse
- Klärung spezifischer Fragestellungen zu einzelnen Geschäftsprozessen oder Ressourcen innerhalb der Geschäftsfortführungsplanung
- Unterstützung in der Vorbereitung und Durchführung von Übungen (siehe Kapitel 6.11.1 *Festlegung der Rahmenbedingungen zum Üben*, z. B. in der Rolle Unterstützungskräfte oder Übungsleiter)

3.2.3 Dokumentation

Im Rahmen dieses Standards werden die verschiedenen Dokumentenarten anhand von zwei Kategorien differenziert. Die hierarchische Einordnung ergibt sich aus dem Autoren- und Adressatenkreis (strategisch, taktisch oder operativ) sowie der inhaltlichen Tiefe der Dokumente. Da sich das BCM sowohl mit der Notfallvorsorge als auch mit der Notfallbewältigung auseinandersetzt, werden die Dokumentenarten zusätzlich wie folgt unterschieden:

- **Präventive Dokumente** beschreiben die Elemente des BCMS oder stellen Anforderungen an dieses. Darüber hinaus gehören alle Dokumente dazu, die in der Notfallvorsorge benötigt werden.
- **Reaktive Dokumente** werden explizit für die Notfallbewältigung erstellt und genutzt.

Beispiel:

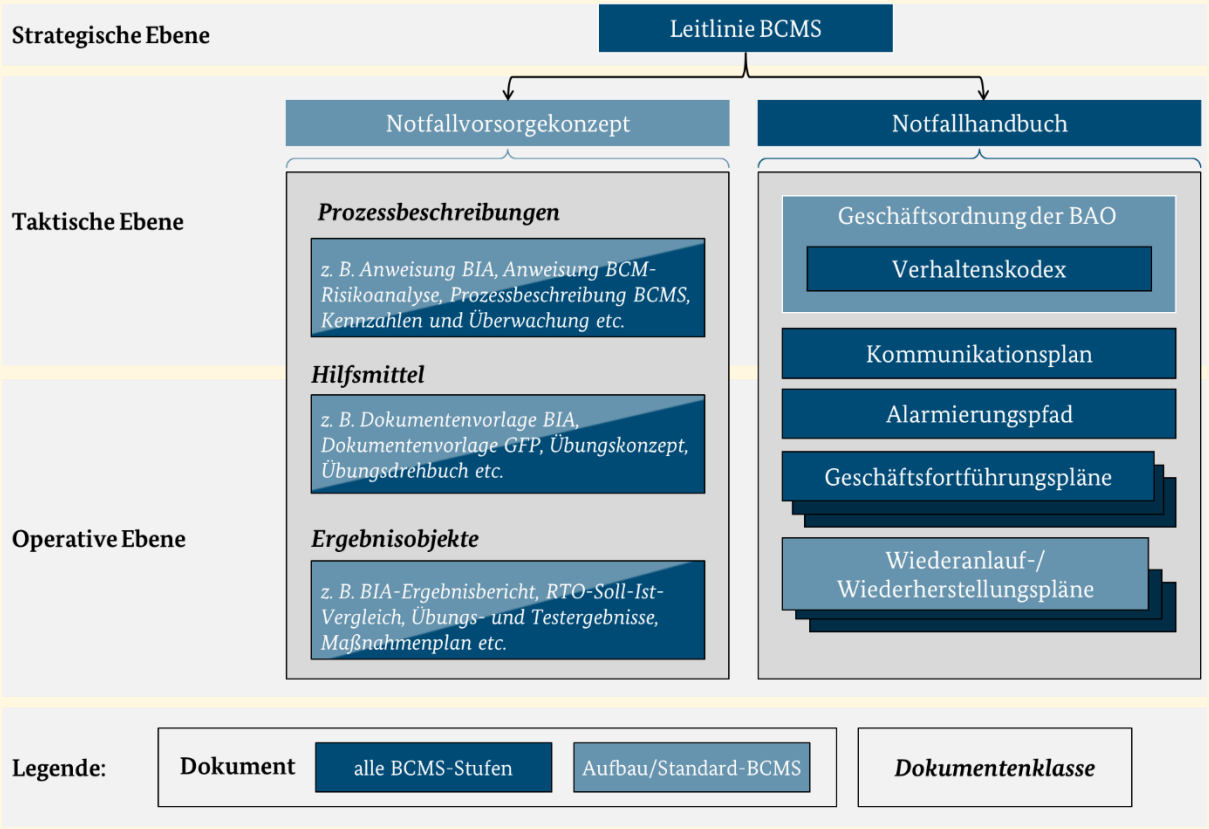

Abbildung 13: Beispiel einer Dokumentenstruktur im BCM

In Abbildung 13 werden ausgewählte in diesem Standard verwendete Dokumente und Dokumentenklassen des BCM sowie die übergreifende Dokumentenstruktur dargestellt und anhand von Beispielen erläutert. Aus Gründen der Übersichtlichkeit kann in der Abbildung nur ein Teil der Dokumente gezeigt werden.

Präventive Dokumente

Die **Leitlinie** definiert Ziele und allgemeine Vorgaben für das BCMS auf der strategischen Ebene. Damit gibt sie den verbindlichen Rahmen für alle weiteren Aktivitäten und Dokumentationen des BCMS vor. Sie beschreibt, warum und unter welchen Voraussetzungen das BCMS aufgebaut und betrieben wird, sowie die allgemeinen Zielvorgaben an das BCM.

Innerhalb des **Notfallvorsorgekonzepts** werden konkrete Informationen und Vorgaben zum BCMS dokumentiert. Diese Dokumente legen fest, wie die Ziele und allgemeinen Vorgaben der Leitlinie erreicht werden sollen. Das Notfallvorsorgekonzept enthält eine Beschreibung aller organisatorischen und konzeptionellen

Aspekte des BCMS sowie Regelungen und Vorgaben zu einzelnen BCM-Prozessschritten. Das Notfallvorsorgekonzept ist nicht notwendigerweise ein eigenes Dokument, sondern beinhaltet alle Dokumente innerhalb des BCMS, die nicht direkt zur Reaktion dienen. Hierarchisch umfasst es sowohl taktische als auch operative Elemente.

Hinweis:

Da das Notfallvorsorgekonzepts eine Vielzahl an Prozessbeschreibungen, Anweisungen, Hilfsmitteln und Ergebnisobjekten beinhaltet, werden diese jeweils unter einer Dokumentenklasse zusammengefasst.

Die Vorgaben aus dem Notfallvorsorgekonzept zu einzelnen BCM-Prozessschritten sollten in **Prozessbeschreibungen** oder **Anweisungen** konkretisiert werden. Prozessbeschreibungen geben einen allgemeinen Überblick über die verschiedenen BCM-Prozessschritte und erläutern diese. Prozessbeschreibungen können je nach Komplexität Teil des Notfallvorsorgekonzepts sein oder in separaten Dokumenten beschrieben sein. Anweisungen konkretisieren die Arbeitsschritte, die durch die definierten Rollen umgesetzt werden sollen. Anweisungen bieten sich insbesondere dann an, wenn verschiedene Rollen Schritte des BCM-Prozesses durchführen sollen. So enthält z. B. das Übungshandbuch Vorgaben, welche Übungsarten in welcher Häufigkeit durchgeführt werden sollen und welche Hilfsmittel hierfür zum Einsatz kommen sollen.

Hilfsmittel sind ergänzende Dokumente, die Anwender darin unterstützen, Aufgaben innerhalb des BCM-Prozesses umzusetzen. So können insbesondere die Analysen innerhalb des BCMS anhand von Hilfsmitteln bzw. Dokumentvorlagen strukturiert und einheitlich durchgeführt werden.

Im laufenden Betrieb des BCMS entstehen verschiedene **Ergebnisobjekte**, die unter anderem für den Aufbau, den Betrieb und die Weiterentwicklung des BCMS genutzt werden. So werden z. B. die Ergebnisse durchgeführter Übungen anhand der bereitgestellten Hilfsmittel nachvollziehbar dokumentiert. Dadurch werden die gewonnenen Informationen für nachfolgende BCM-Prozessschritte leichter auswert- und weiterverwendbar.

Reaktive Dokumente

Das **Notfallhandbuch** beinhaltet alle Informationen zur Notfallbewältigung. Die Inhalte des Notfallhandbuchs können je nach Größe und Komplexität der Institution in verschiedene Dokumente unterteilt sein. Für das Notfallhandbuch muss sichergestellt werden, dass es im Notfall der jeweiligen Zielgruppe zur Verfügung steht.

Hinweis:

Die in diesem Standard verwendete Dokumentenstruktur und die Bezeichnungen der Dokumente, wie beispielsweise Notfallhandbuch oder Notfallvorsorgekonzept, sowie die Dokumentenarten sind nicht bindend und können institutionsspezifisch festgelegt werden. Eine eigenständig entwickelte Dokumentenstruktur sollte jedoch die strategische, taktische sowie operative Ebene abdecken und die Inhalte der in diesem Standard benannten Dokumente berücksichtigen.

In der BCM-Dokumentation sind zahlreiche schützenswerte Informationen der Institution enthalten. Um einen Verlust oder die unbeabsichtigte Veröffentlichung von schützenswerten Informationen zu verhindern, sollten alle Dokumente klassifiziert werden. Die Klassifizierung eines Dokuments gibt Auskunft darüber, welcher Schutzbedarf hinsichtlich der Verfügbarkeit, Vertraulichkeit oder Integrität für die enthaltenen Informationen bestehen und wie der Anwender dementsprechend mit den Informationen umgehen muss. Weitere Informationen zur Klassifizierung von Informationen können dem BSI-Standard 200-2, Kapitel 5.1 entnommen werden. Ferner sollte für alle Dokumente des BCMS sichergestellt werden, dass diese vor dem Zugriff von nicht leseberechtigten Externen geschützt sind und keine veralteten Versionen produktiv eingesetzt werden.

3.2.4 Ressourcenplanung

Die Institutionsleitung muss gemäß ihrer Selbstverpflichtung (siehe Kapitel 3.1.4 *Übernahme der Verantwortung* durch die Leitungsebene) das BCMS mit angemessenen personellen, zeitlichen und finanziellen Ressourcen ausstatten. Der Ressourcenbedarf ist unter anderem von folgenden Faktoren abhängig:

- Geltungsbereich und Ziele des BCMS
- zeitliche Vorgaben, z. B. Meilensteine oder Fristen zur Erreichung eines definierten Zustands des BCMS
- ausgewählte Stufe des BCMS
- Größe und Komplexität der Institution
- gewählte BCM-Aufbauorganisation sowie die Aufgaben und Zuständigkeiten der Rollen

Neben den personellen und zeitlichen Ressourcen sollte der finanzielle Ressourcenbedarf im BCMS festgelegt werden. In einer frühen Phase der Etablierung des BCMS kann dieser nur geschätzt werden, da sich die konkreten Kosten umzusetzender Maßnahmen erst im weiteren Aufbau des BCMS ergeben. Der finanzielle Rahmen sollte dahingehend bereits auf zukünftige Bedarfe ausgerichtet werden. Die nachfolgende Aufzählung stellt eine Auswahl zu berücksichtigenden Posten dar:

- Schulungen und Maßnahmen zur Sensibilisierung
- Umsetzung und Betrieb von Strategien und –Lösungen zum BCM
- technische Lösungen (z. B. BCM-Tool, Alarmierungssoftware)
- Begleitung und Entwicklung besonderer BCM-Prozesse (z. B. zur Durchführung von Stabsübungen der BAO)
- Beratung, Coaching oder Zertifizierung

Die Institutionsleitung muss über die Organisationsstruktur, personelle und zeitliche Ressourcenplanung sowie finanzielle Ressourcenbedarfe entscheiden. Üblicherweise werden für die Institutionsleitung Entscheidungsvorlagen erstellt.

Nachdem die Organisationsstruktur durch die Institutionsleitung verabschiedet wurde, müssen die Rolleninhaber ernannt und in der Institution als solche bekanntgegeben werden. Ferner sollte die Rollenbesetzung anhand etablierter Medien, z. B. im Intranet, dokumentiert werden.

Im Rahmen der kontinuierlichen Verbesserung des BCMS müssen der Ressourcenbedarf sowie die Angemessenheit der Ressourcenplanung überprüft und bei Bedarf angepasst werden.

3.2.5 Schulung

Ein wesentlicher Erfolgsfaktor für den Aufbau und Betrieb des BCMS ist der Auf- und Ausbau angemessener Fähigkeiten und Kenntnisse der BCM-Rolleninhaber.

Hinweis:

Die Begriffe Fähigkeiten und Kenntnisse fassen innerhalb dieses Standards das notwendige Wissen und die Erfahrungen zusammen, um die Aufgaben einer Rolle adäquat ausüben zu können.

Anhand der Rollenbesetzungen muss festgelegt werden, welche Fähigkeiten und Kenntnisse im Rahmen von Schulungen oder Trainings aufgebaut werden müssen.

Der Schulungsbedarf richtet sich danach, inwieweit das vorhandene Wissen und die Vorerfahrung der Rolleninhaber die benötigten Fähigkeiten und Kenntnisse bereits abdecken. Durch Schulungen können die Rolle-

ninhaber gezielt auf ihre Aufgaben vorbereitet und qualifiziert werden. Die Art der Wissensvermittlung richtet sich nach der Anzahl an Rolleninhaber, deren spezifischem Bedarf sowie den festgelegten finanziellen Ressourcen.

Die Institution muss nach durchgeführten Schulungsmaßnahmen überprüfen, ob die Schulungsziele erreicht wurden. Dies kann durch Wissensabfragen oder durch Befragung der Teilnehmer im Nachgang zu Schulungsveranstaltungen sichergestellt werden. Die Institution muss dabei im Rahmen der kontinuierlichen Verbesserung des BCMS identifizierte Verbesserungsbedarfe berücksichtigen, z. B. durch Anpassung der Schulungsinhalte oder -formate.

3.2.6 Sensibilisierung

Nicht nur die BCM-Rolleninhaber müssen erforderliche Fähigkeiten und Kenntnisse erlangen. Darüber hinaus ist es von entscheidender Bedeutung für den Erfolg des BCMS, dass alle Mitarbeiter verstehen, warum ein BCM in der Institution nützlich und notwendig ist. Ziel der Sensibilisierung ist es, dass alle Mitarbeiter ein gewünschtes Verhalten aus eigenem Antrieb und eigener Überzeugung umsetzen und beibehalten.

Der Fokus der Sensibilisierung kann in der Etablierung des BCMS zunächst auf die BCM-Rolleninhaber beschränkt werden. Die Institution muss durch geeignete Maßnahmen zur Sensibilisierung sicherstellen, dass die BCM-Rolleninhaber sich ihrer Aufgaben und ihrer Verantwortung bewusstwerden.

In der kontinuierlichen Verbesserung des BCMS sollte jedoch das Bewusstsein für BCM sukzessiv bei allen Mitarbeitern der Institution angestrebt werden, um eine *BCM-Kultur* in der gesamten Institution zu erreichen. Dazu sollte die Institution durch geeignete Maßnahmen zur Sensibilisierung sicherstellen, dass allen Mitarbeitern bewusst ist,

- dass ein BCMS in der Institution etabliert ist,
- wo die für den jeweiligen Mitarbeiter relevanten Informationen zum BCM dokumentiert sind,
- welche Auswirkungen die Abweichung von Vorgaben des BCMS haben könnte,
- wie die Mitarbeiter zum Betrieb und zur Verbesserung des BCMS beitragen können,
- wie die Mitarbeiter sich in einem Notfall verhalten sollen sowie
- wo die Mitarbeiter alle relevanten Informationen zur Notfallbewältigung finden, sofern sie darin eingebunden sind.

Zur Bewusstseinsbildung kann auf die etablierten Kommunikationswege und -medien innerhalb der Institution zurückgegriffen werden, z. B. auf Führungskräftetagungen, Regeltermine, Einführungsveranstaltungen für neue Mitarbeiter, Veranstaltungen von Organisationseinheiten, Mitarbeiterzeitschriften, Poster, Newsletter, Blogs, und Apps der Institution oder soziale Medien.

Da nicht alle Interessengruppen die gleiche Intensität der Sensibilisierung benötigen, sollte die Bewusstseinsbildung zielgruppenorientiert und bedarfsgerecht gestaltet werden.

Synergiepotential:

Die Bewusstseinsbildung spielt auch in anderen Sicherheitsthemen wie der Informationssicherheit, dem Datenschutz, der physischen und personellen Sicherheit sowie dem Arbeitsschutz eine große Rolle. Durch aufeinander abgestimmte Maßnahmen können Ressourcen effizient eingesetzt und eine themenübergreifende Sicherheitskultur geschaffen werden.

4 Reaktiv-BCMS

Das Reaktiv-BCMS ermöglicht eine schnelle Notfallbewältigung für ausgewählte, als sehr zeitkritisch eingeschätzte Geschäftsprozesse. Anders als im Standard-BCMS werden nicht alle Geschäftsprozesse analysiert. Stattdessen wird in einer Voranalyse der Prozessumfang eingeschränkt. Die Methoden im Reaktiv-BCMS sind auf das Maß reduziert, das erforderlich ist, um nur die zeitkritischsten Geschäftsprozesse mit vorhandenen Mitteln der Institution abzusichern.

Das Reaktiv-BCMS wird im nachfolgenden Überblick kurz dargestellt und anschließend in den gleichnamigen Unterkapiteln ausführlich erläutert. *Abbildung 14* zeigt auch farblich, welche BCM-Prozessschritte eines Standard-BCMS ausgelassen werden können. So ist schnell ersichtlich, wo das Reaktiv-BCMS vereinfacht.

Plan-Phase

Das Reaktiv-BCMS beschränkt sich in der Plan-Phase auf die in Kapitel 3 *Initiierung des BCMS* beschriebenen Aspekte. In der **Leitlinie** dokumentiert die Institutionsleitung ihre Selbstverpflichtung und legt die Rahmenbedingungen für das BCMS (z. B. Ressourcenausstattung) fest. Anders als im Standard-BCMS wird auf eine tiefergehende Analyse der Rahmenbedingungen bewusst verzichtet.

Do-Phase

Das Kapitel **Aufbau und Befähigung der BAO** beinhaltet alle Aspekte, um eine funktionierende BAO zu etablieren, die auch im Not- und Krisenfall erreichbar und handlungsfähig ist. Die Institution kann so auf Schadensereignisse reagieren, unabhängig davon, ob bereits Notfallpläne für die Fortführung von Geschäftsprozessen vorliegen.

Alle weiteren BCM-Prozessschritte in der DO-Phase dienen der angemessenen Absicherung der zeitkritischen Geschäftsprozesse. Die Analysephase besteht aus **Voranalyse, Business Impact Analyse** und **Soll-Ist-Vergleich**. Im Vergleich zu Standard- und Aufbau-BCMS ist die Analysephase bewusst reduziert und beschränkt sich auf die zeitkritischsten Geschäftsprozesse und Ressourcen. Anhand der **Geschäftsfortführungsplanung** wird festgelegt und dokumentiert, ob und wie mit technischen und organisatorischen Lösungen sowie Notfallmaßnahmen ein Notbetrieb der zeitkritischen Geschäftsprozesse erreicht werden kann.

Im Reaktiv-BCMS werden die identifizierten Maßnahmen nicht nur geplant, sondern möglichst auch mit den gegebenen Ressourcen umgesetzt. Hierzu wird möglichst auf vorhandene Lösungen zurückgegriffen oder es werden einfache und schnell umsetzbare Lösungen geschaffen. Komplexere Probleme werden zunächst in einem Maßnahmenplan dokumentiert und anschließend in einem Folge-BCMS (Aufbau- oder Standard-BCMS) gelöst.

Check-Phase

Im Reaktiv-BCMS ist davon auszugehen, dass die Strukturen der Bewältigungsorganisation komplett neu sind. Daher ist es essenziell, dass anhand von **Übungen und Tests** überprüft wird, ob die Notfallbewältigungsorganisation in der Lage ist, angemessen und effektiv auf bestimmte Notfallszenarien zu reagieren

Act-Phase

In der **Weiterentwicklung des Reaktiv-BCMS** werden die identifizierten Korrekturbedarfe und Verbesserungsmöglichkeiten genutzt, um eine Entscheidungshilfe für die Institutionsleitung zu erstellen. Die Institutionsleitung entscheidet dann über das weitere Vorgehen.

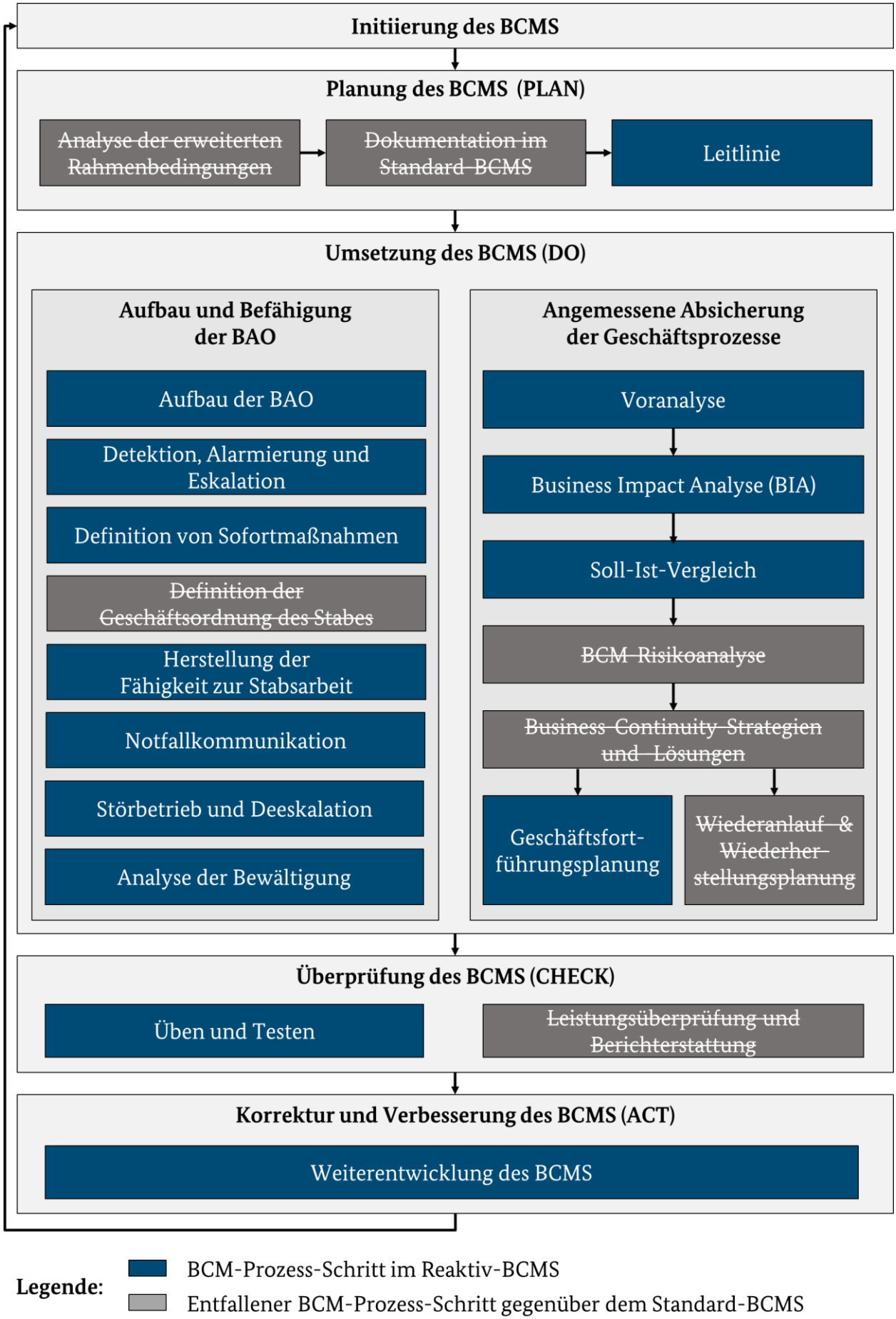

Abbildung 14: BCM-Prozess des Reaktiv-BCMS sowie Kennzeichnung der entfallenden BCM-Prozessschritte gegenüber einem Aufbau- bzw. Standard-BCMS

Hinweis:

Um vollständige Transparenz über alle zeitkritischen Geschäftsprozesse und Risiken im Geltungsbereich des BCMS zu erlangen, ist es erforderlich, entweder schrittweise ein Aufbau-BCMS oder von vornherein ein Standard-BCMS zu initiieren. Ein Reaktiv-BCMS kann nur ein erster Schritt auf dem Weg zu einem vollumfänglichen, anforderungsgerechten und angemessenen BCMS sein, das sowohl die Notfallvorsorge als auch die Notfallbewältigung umfasst.

4.1 Leitlinie

Die Institutionsleitung hat in der Initiierungsphase die zentralen Entscheidungen, um das BCMS zu implementieren, bereits getroffen. Diese Entscheidungen und Ergebnisse müssen in der Leitlinie für das Reaktiv-BCMS zusammengefasst und für die gesamte Institution dokumentiert werden. Die Leitlinie kann anhand der Dokumentenvorlage *Leitlinie* aus den Hilfsmitteln erstellt werden.

Synergiepotential:

Sofern bereits Managementsysteme, wie beispielsweise ein ISMS nach BSI-Standard 200-2, mittels einer Leitlinie in der Organisation fixiert wurden, kann auch der Aufbau dieser Leitlinien als Vorlage genutzt werden.

4.1.1 Erstellung der Leitlinie

Die Leitlinie hat drei wesentliche Funktionen:

1. Sie dient als dokumentierte Absichtserklärung der Institutionsleitung, ein BCMS aufbauen, betreiben und kontinuierlich verbessern zu wollen.
2. Sie dient dazu, die wesentlichen Rahmenbedingungen festzulegen, unter denen ein BCMS etabliert und betrieben werden soll.
3. Sie dient als verbindlicher Auftrag an alle Mitarbeiter, daran mitzuwirken, das BCMS zu etablieren, aufzubauen und kontinuierlich weiterzuentwickeln und somit die Institution gegenüber Schadensereignissen selbst und deren Auswirkungen resilienter zu machen.

Da die Leitlinie einen hohen Stellenwert im BCM hat und weitreichend wahrgenommen wird, ist sie zugleich auch eine Sensibilisierungsmaßnahme zur Schaffung einer BCM-Kultur in der Institution. Die Leitlinie sollte zu diesem Zweck leicht verständlich und präzise formuliert, sowie übersichtlich gestaltet werden. Ziel ist es, dass die Inhalte der Leitlinie von allen Mitarbeitern schnell erfasst und verstanden werden können.

Je detaillierter die Leitlinie auf konkrete Inhalte des BCMS eingeht, desto höher wird der Pflege- und Aktualisierungsaufwand, da dann bereits kleine Veränderungen im weiteren Aufbau des BCMS eine Anpassung erfordern. Zudem muss die Leitlinie mit jeder Änderung erneut durch die Institutionsleitung freigegeben werden. Ferner kann die Leitlinie bei hohem Detailgrad erst veröffentlicht werden, wenn die darin beschriebenen Inhalte definiert und etabliert sind, was einer Veröffentlichung zeitnah zur Initiierung des BCMS widerspricht. Da die Leitlinie alle strategischen Aussagen zum BCM der Institution beinhaltet, wird sie in der Praxis einem sehr großen Personenkreis bekannt gegeben werden. Auch aus Gründen der Vertraulichkeit sollte auf eine zu detaillierte Beschreibung innerhalb der Leitlinie verzichtet werden.

Es wird daher empfohlen, in der Leitlinie einen geringen Detailgrad zu wählen und lediglich „Leitplanken“ zu beschreiben, innerhalb derer das BCMS aufgebaut und betrieben werden kann.

In der Leitlinie müssen mindestens die folgenden Inhalte und Entscheidungen aus der Initiierung des BCMS beschrieben werden (siehe Kapitel 3.1 *Initiierung des BCMS durch die Institutionsleitung):*

- Motivation für den Aufbau des BCMS (siehe Kapitel 3.1.1.1 *Motivation für den Aufbau eines BCMS*)
- Abzusichernder Zeitraum durch ein BCM (siehe Kapitel 3.1.1.2 *Abzusichernder Zeitraum durch ein BCM*)

- Geltungsbereich des BCMS (siehe Kapitel 3.1.2 *Geltungsbereich*)
- Übernahme der Gesamtverantwortung der Institutionsleitung (siehe Kapitel 3.1.4 *Übernahme der Verantwortung durch die Leitungsebene*)
- institutionsspezifische Definition des Begriffs BCM und der Eskalationsstufen Störung, Notfall und Krise (siehe Kapitel 3.2.1 *Definition und Abgrenzung*)
- zentrale Rollen im BCMS (ohne Besetzung) (siehe Kapitel 3.2.2 *Definition der BCM-Aufbauorganisation*)
- Ressourcenbereitstellung (siehe Kapitel 3.2.4 *Ressourcenplanung*)

Sofern rechtliche und regulatorische Anforderungen gelten, sollten diese ebenfalls in der Leitlinie dokumentiert werden (siehe Kapitel 3.1.1 *Zielsetzung*).

4.1.2 Veröffentlichung und Aktualisierung der Leitlinie

Die Institutionsleitung muss die Leitlinie inhaltlich prüfen, freigeben und gegenüber allen Mitarbeitern bekannt geben. Um ein Bewusstsein für das BCM bei den Mitarbeitern zu schaffen und eine BCM-Kultur in der gesamten Institution zu etablieren, ist es wichtig, dass alle Mitarbeiter die Leitlinie kennen. Daher sollten auch neue Mitarbeiter auf die Leitlinie hingewiesen werden.

Es ist empfehlenswert, die Leitlinie als internes Dokument zu klassifizieren und somit nicht für die Öffentlichkeit zugänglich zu machen. Jedoch kann die Institution entscheiden, dass neben den Mitarbeitern auch weitere Gruppen die Leitlinie kennen sollen, wie z. B. zeitkritische Dienstleister oder Geschäftspartner.

Im Hinblick auf eine kontinuierliche Verbesserung im Rahmen eines Aufbau- oder Standard-BCMS sollte bereits bei der Erstellung der Leitlinie ein Überprüfungszyklus festgelegt und in der Leitlinie dokumentiert werden. Falls sich wesentliche Rahmenbedingungen, Geschäftsziele, Aufgaben und Strategien der Institution verändern, muss die Leitlinie anlassbezogen aktualisiert werden. Dafür müssen die wesentlichen Änderungen in der Institution identifiziert, die Auswirkungen der Änderung für das BCMS bewertet und die Leitlinie entsprechend angepasst werden.

Bei wesentlichen Änderungen der Inhalte, z. B. des Geltungsbereichs oder der Ziele des BCM, sollte die Leitlinie durch die Institutionsleitung erneut freigegeben werden. In der Leitlinie sollten Änderungen nachvollziehbar gekennzeichnet werden, z. B. indem ein Versionsverzeichnis oder eine -historie gepflegt wird.

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 Vorrausetzungen zur Bewältigung für Notfälle und Krisen nahezu identisch sind, wird in diesem Kapitel nicht näher zwischen Notfällen und Krisen unterschieden.

Die in *Abbildung 14* aufgezeigten Aspekte zum Aufbau und zur Befähigung der BAO werden in den folgenden Unterkapiteln aufgegriffen. Diese überlagern sich zeitlich oder stehen in Wechselwirkung zueinander. So kommt es z. B. in der Praxis häufig vor, dass der Aufbau der BAO sowie die Festlegung der Methoden und Regeln für die Stabsarbeit, die Grundlage für Schulungen, Trainings und Übungen bilden. Erkenntnisse aus durchgeführten Schulungen und Trainings führen wiederum zu Anpassungen der BAO, der Regeln oder anderen Aspekten der Stabsarbeit.

Zudem stellen die beschriebenen Aspekte nur einen von vielen möglichen Pfaden dar. Einige weitere mögliche Umsetzungsformen und Aspekte der Bewältigung können dem Hilfsmittel *Weiterführende Aspekte zur Bewältigung* entnommen werden.

Alle beschriebenen Maßnahmen sollten spezifisch auf die Institution angepasst werden und in einem Notfallhandbuch (siehe Kapitel 3.2.3 *Dokumentation*) dokumentiert werden. Das Notfallhandbuch kann anhand der Dokumentenvorlage *Notfallhandbuch* aus den Hilfsmitteln erstellt werden.

Hinweis:

In der Regel gibt die Institutionsleitung im Not- und Krisenfall bestimmte Entscheidungs- und Handlungsvollmachten an die BAO ab, wie in den nachfolgenden Kapiteln erläutert wird. Daher ist es von besonderer Bedeutung, dass sie in der Vorbereitung in allen Punkten eingebunden ist und die beschlossenen Regelungen und Maßnahmen freigibt.

4.2.1 Aufbau der BAO

In einer AAO sind Abstimmungswege häufig komplex, wodurch kurzfristige Entscheidungen in Notfällen und Krisensituationen oftmals nicht zeitgerecht getroffen werden können. Eine zielgerichtete und rasche Bewältigung erfordert daher eine besondere Aufbauorganisation (BAO).

Beispiel:

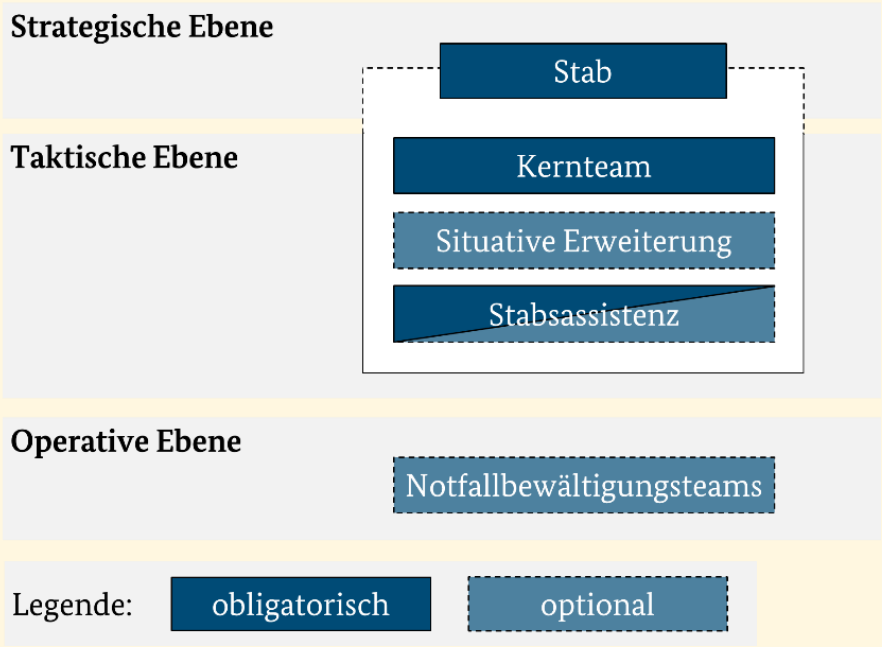

Abbildung 15: Beispiel einer BAO

Abbildung 15 erläutert ein Beispiel verschiedener Rollen einer BAO in den drei Ebenen strategisch, taktisch und operativ, wie sie im Rahmen dieses Standards definiert sind.

- Die **Strategische Ebene** legt die Ziele und Prioritäten in der Bewältigung fest.
- Die **Taktische Ebene** analysiert die Lage, beschließt dahingehend Maßnahmen und überwacht, ob diese umgesetzt wurden und wirksam sind.
- Die **Operative Ebene** setzt die beschlossenen Maßnahmen um und meldet den Erfolg oder die Wirkung der umgesetzten Maßnahmen an die taktische Ebene.

Hinweis:

In anderen Standards, z. B. zur öffentlichen Gefahrenabwehr, haben die Ebenen eine andere Bedeutung. Daher sollte im Zusammenspiel mit anderen Stäben stets geprüft werden, wie diese Begriffe belegt sind, falls sie benutzt werden.

Die BAO hat zum Ziel, komplexe Notfall- und Krisensituationen koordiniert zu bearbeiten und dabei alle relevanten Schnittstellen geeignet zu bedienen. Üblicherweise wird die BAO durch einen Stab geleitet, der komplexe Situationen beurteilen und geeignete Maßnahmen ableiten kann. Dieser agiert außerhalb der in der Alltagsorganisation etablierten Organisationsform, z. B. Linien- oder Matrixorganisation. Der Stab hat dabei innerhalb eines vorher festgelegten Rahmens Entscheidungsgewalt.

Analog zur Definition der BCM-Aufbauorganisation (siehe Kapitel 3.2.2 *Definition der BCM-Aufbauorganisation*) müssen die Aufgaben und Pflichten für alle Rollen der BAO im Vorfeld festgelegt werden. Für jede definierte Rolle der BAO kann der BCMB eine Besetzung vorschlagen. Für jedes Stabsmitglied muss mindestens ein Stellvertreter vorgesehen werden, da der Stab ad hoc und bei Bedarf über einen längeren Zeitraum handlungsfähig sein muss.

4.2.1.1 Aufbau des Stabs

Die Institution sollte in der BAO einen Stab als zentrales Führungsgremium der Bewältigung definieren. Der Stab sollte die Bewältigung lenken, koordinieren und unterstützen. Ferner sollte er an die relevanten Parteien zum Fortschritt der Notfallbewältigung kommunizieren.

Hinweis:

Verschiedene Notfall- oder Krisenstabsmodelle werden in den dem Hilfsmittel *Weiterführende Aspekte zur Bewältigung* erläutert. Um der Institution offenzulassen, mit welchem Gremium sie die Bewältigung sicherstellt, wird nachfolgend bewusst nur vom Stab gesprochen. Das Kapitel fokussiert entsprechend, welche Kriterien ein Stab grundsätzlich erfüllen soll.

Die Zuständigkeit für strategische Entscheidungen verbleibt auch in Notfällen bei der Institutionsleitung. Der Stab unterstützt die Institutionsleitung, indem er Lösungen entwickelt und alle Tätigkeiten hierzu koordiniert. Aufgabe des Stabes ist es, weitere Schäden von der Institution abzuwenden. In diesem Zusammenhang ist es empfehlenswert, dass die Institutionsleitung dem Stab Finanz- und Entscheidungsbefugnisse überträgt. Der Stab kann daher je nach Ausprägung auf der strategisch-taktischen oder nur auf der taktischen Ebene angesiedelt sein.

Es ist empfehlenswert, dass der BCMB einen ersten Vorschlag für die allgemeinen Aufgaben des Stabes erstellt. Der Vorschlag kann sich an folgender Liste orientieren:

- Lage feststellen, beurteilen und fortschreiben
- einzuleitende Maßnahmen abstimmen und darüber entscheiden

- Arbeitsaufträge an unterstützende Einheiten, z. B. Notfallbewältigungsteams, erteilen (Aufgabenmanagement)
- umgesetzte Maßnahmen auf deren Wirksamkeit überprüfen und, falls erforderlich, korrigierende Maßnahmen einleiten
- interne und externe Notfallkommunikation sowie Öffentlichkeitsarbeit (z. B. Pressestelle) steuern
- an die Institutionsleitung oder andere Zuständige eskalieren, falls die Situation die Grenzen der eigenen Zuständigkeit übersteigt

Es gibt verschiedene Möglichkeiten, wie sich Stäbe personell und funktionell zusammensetzen können. Um die in den folgenden Kapiteln aufgeführten Aufgaben der Stabsarbeit sinnvoll Personen zuordnen zu können, sollte der Stab mindestens aus einem **Kernteam** bestehen. Das Kernteam besteht jeweils aus verschiedenen Rollen, die bestimmte Aufgaben und Zuständigkeiten in der Stabsarbeit innehaben. Das Kernteam sollte lageabhängig weitere Rollen als **situative Erweiterung** hinzuziehen. Um den Stab zu unterstützen, sollte zusätzlich eine **Stabsassistenz** vorgesehen werden. Abbildung 16 zeigt beispielhaft den Aufbau eines Stabs.

Beispiel:

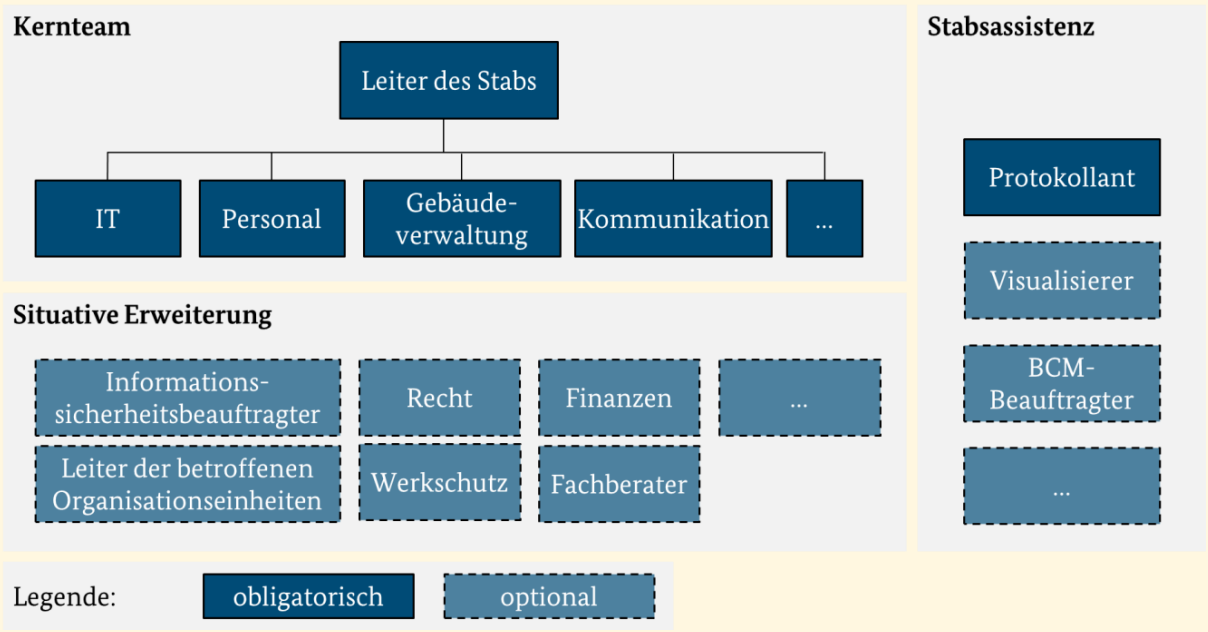

Abbildung 16: Darstellung eines Stabs

Hinweis:

Um den Informationsaustausch und damit die Entscheidungsfähigkeit des Stabs nicht durch zu viele Mitglieder zu erschweren, sollten die Rollen der situativen Erweiterung bzw. bei Bedarf auch des Kernteams, jeweils nur solange im Stab verbleiben, wie es erforderlich ist, um die Lage zu beurteilen oder Maßnahmen abzuleiten.

Der Aufbau entspricht den Empfehlungen des Reaktiv-BCMS und wird nachfolgend erläutert. Wie eingangs dargestellt, sind die Stabsstrukturen je nach Institution sehr unterschiedlich. Daher sollte das Beispiel institutionsspezifisch angepasst werden.

4.2.1.2 Aufbau des Kernteams

Das Kernteam besteht aus den ständigen Mitgliedern des Stabs und umfasst alle Rollen, die in der Regel lageunabhängig für die Bewältigung alarmiert werden. Das Kernteam sollte mindestens die folgenden Rollen beinhalten:

- Leiter des Stabs
- IT
- Personal
- Gebäudeverwaltung
- Kommunikation

Der **Leiter des Stabs** koordiniert die Aktivitäten aller Stabsmitglieder in der Bewältigung. Er trifft grundsätzlich die Entscheidungen im Stab. Für den Leiter des Stabs muss neben den Aufgaben und Zuständigkeiten zusätzlich die Verantwortung im Not- und Krisenfall definiert werden, wenn er bei Ausrufung des Not- oder Krisenfalls über die AAO hinausgehende Entscheidungsbefugnisse oder finanzielle Spielräume erhält. Die Entscheidungsbefugnis kann der Leiter an das Kernteam delegieren. Daraufhin kann jede Rolle im Kernteam nach außen in Vertretung bzw. im Auftrag des Leiters Weisungen geben.

Für den Leiter des Stabes sollten mehrere Stellvertreter benannt werden, um sicherstellen zu können, dass diese zentrale Rolle für die Bewältigung besetzt ist.

Die Rollen **IT**, **Personal** und **Gebäudeverwaltung** repräsentieren die Vertreter der Organisationseinheiten, die über die jeweilige Fach- und Sachkenntnis der Ressourcen verfügen und hierzu geeignete technische, bauliche oder organisatorische Maßnahmen in der Notfallbewältigung ableiten können. Ferner bilden die Rollen die Schnittstellen zu den Einheiten, welche die Maßnahmen umsetzen.

Die Rolle **Kommunikation** ist zuständig für die Informationssammlung sowie adressatengerechte Informationsaufbereitung und -verteilung nach innen und außen. Weiterführende Informationen können hierzu dem Kapitel 4.2.5 *Notfallkommunikation* entnommen werden.

4.2.1.3 Aufbau der situativen Erweiterung

Zum erweiterten Stab zählen Rollen, die durch ihre Expertise und Ressourcen zur Bewältigung beitragen können. Der Personenkreis beschränkt sich dabei normalerweise auf die eigene Institution. Es können beispielsweise Personen aus der AAO in den Stab beordert werden, um besondere Meldepflichten gegenüber Regulatoren wahrzunehmen.

Es können aber auch externe Mitglieder in den Stab aufgenommen werden, beispielsweise Dienstleister und Berater. In diesem Fall ist es empfehlenswert, die Punkte Vertraulichkeit von Informationen sowie Handlungs- und Entscheidungsbefugnisse explizit zu regeln.

Beispiel:

Typische Beispiele für eine situative Erweiterung:

- Informationssicherheitsbeauftragter (ISB)
- Leiter der betroffenen Organisationseinheiten
- Recht
- Werkschutz
- Finanzen
- interne und externe Fachberater

4.2.1.4 Aufbau der Stabsassistenz

Der Stab sollte durch eine Stabsassistenz unterstützt werden. Die Rollen der Stabsassistenz entlasten den Stab von organisatorischen Aufgaben und schaffen damit den Freiraum zur Handlungs- und Entscheidungsfähigkeit des Stabs.

Die Stabsassistenz muss mindestens aus der Rolle **Protokollant** bestehen. Der Protokollant führt die Nachweise über die Schadensbewältigung in der sogenannten Protokollierung zusammen und unterstützt damit den Stab, die getroffenen Entscheidungen und Ereignisse nachzuhalten. Das Protokoll dient dazu, die Institution rechtlich abzusichern, Entscheidungen zu dokumentieren und unmittelbar identifizierte Verbesserungsmöglichkeiten in der Notfallbewältigung nachzuhalten. Weiterführende Informationen zur Protokollierung sind im Kapitel 4.2.4 *Herstellung der Fähigkeit zur Stabsarbeit,* Unterpunkt Protokollierung beschrieben.

Es ist empfehlenswert, den Stab durch eine Rolle **Visualisierer** zu unterstützen. Dieser stellt das Ereignis in einem Schaubild, auch Lagebild genannt, dar und verfolgt auf diese Weise Lageveränderungen sowie die Maßnahmenumsetzung. Dies fördert das Lageverständnis des Stabs und trägt zu einer effizienteren Bewältigung bei. Weiterführende Informationen zur Visualisierung sind im Kapitel 4.2.4 *Herstellung der Fähigkeit zur Stabsarbeit,* Unterpunkt Visualisierung beschrieben.

Der **BCMB** ist eine Rolle in der präventiven BCM-Organisation. Es ist aber empfehlenswert, diesen auch in der BAO einzubinden. Dies hat den Vorteil, dass das Wissen über die zeitkritischen Geschäftsprozesse und Ressourcen sowie die Notfalldokumentation dem Stab jederzeit direkt zur Verfügung steht und falls erforderlich erfragt werden kann. Abbildung 16 zeigt ein mögliches Beispiel, in dem der BCMB der Stabsassistenz zugeordnet ist.

4.2.1.5 Aufbau von Notfallbewältigungsteams

Zur operativen Bewältigung eines Notfalls sollten Notfallbewältigungsteams aufgebaut werden.

Hinweis:

Die Größe der Teams richtet sich an der Komplexität und der Personalausstattung der Institution aus. Gerade in kleinen Institutionen kann es möglich sein, dass statt eines Teams nur ein einzelner Mitarbeiter für bestimmte Aktivitäten der Notfallbewältigung zuständig ist. Nachfolgend wird jedoch zur besseren Verständlichkeit nur vom Team gesprochen.

Die Notfallbewältigungsteams erhalten ihre Arbeitsaufträge aus dem Stab und setzen die darin beschriebenen technischen, baulichen oder organisatorischen Maßnahmen zur Notfallbewältigung um. Im Vorfeld festgelegte Notfallbewältigungsteams haben gegenüber ad hoc zusammengestellten Teams drei Vorteile:

- Sie können anhand von Trainings und Übungen auf verschiedene Notfallszenarien vorbereitet werden.
- Sie können im Ernstfall aufgrund des Trainingseffekts üblicherweise schneller und zielgerichteter im Notfall agieren.
- Die Kommunikationswege zwischen Stab und Notfallbewältigungsteams können im Vorfeld festgelegt und erprobt werden.

Die Leiter der Notfallbewältigungsteams sollten während der Notfallbewältigung dem Stab in regelmäßigen Abständen berichten. Dazu sollte er die Informationen vor Ort sammeln, an den Stab weiterleiten und koordinieren sowie kontrollieren, ob die vom Stab angeordneten Maßnahmen vor Ort umgesetzt und wirksam sind.

In der Praxis haben sich die folgenden Notfallbewältigungsteams bewährt:

- IT
- Personal
- Gebäudeverwaltung
- Notfallkommunikation

Es ist empfehlenswert, diese institutionsspezifisch durch weitere Notfallbewältigungsteams zu ergänzen. Zum Beispiel können Notfallteams in den zeitkritischsten Organisationseinheiten, die das Kerngeschäft repräsentieren, etabliert werden.

4.2.1.6 Freigabe der BAO durch die Institutionsleitung

Wie eingangs erwähnt, muss der festgelegte Aufbau der BAO von der Institutionsleitung freigegeben werden. Um der Institutionsleitung einen Gesamtüberblick über die BAO zu ermöglichen, ist es empfehlenswert, eine grafische Übersicht des Stabsaufbaus zu erstellen. Hierzu kann ein Schaubild, wie in Abbildung 16 dargestellt, erstellt werden. Anhand von Rollenkarten können zusätzlich die jeweiligen Aufgaben und Zuständigkeiten jeder Rolle im Detail vorgestellt werden. Sobald die BAO durch die Institutionsleitung freigegeben wurde, müssen die festgelegten Personen offiziell ernannt werden.

4.2.2 Detektion, Alarmierung und Eskalation

Je schneller ein Schadensereignis richtig eingeschätzt und behandelt wird, desto eher werden Folgeschäden eingedämmt und eine weitere Eskalation des Ereignisses verhindert. Wenn ein Notfall eintritt, ist es daher wichtig, dass dieser möglichst schnell erkannt und an die Entscheider gemeldet wird. Dies fällt umso leichter, je klarer die Verfahren und Wege für die Meldung von Schadensereignissen mit Notfallpotenzial vorab festgelegt und den Mitarbeitern vertraut gemacht wurden. Hierzu ist es empfehlenswert, die Art der Meldung näher zu definieren. So kann eine Meldung entweder der Information oder der Alarmierung dienen.

Die **Information** (Zustand bzw. Störung) dient ausschließlich dazu, den Sachverhalt eines Ereignisses zu übermitteln. Die Information wird in der Praxis z. B. genutzt, wenn der Leiter des Stabes über eine Störung informiert wird, die potenziell zu einem Notfall eskalieren kann. Dies erfordert von Seiten des Leiters des Stabes keine direkte Handlung, da die Störungsbeseitigung in der AAO durchgeführt wird. Durch eine transparente und frühzeitige Kommunikation ist der Leiter des Stabes für den Fall informiert, dass die Störung dennoch eskaliert und kann bei Bedarf eine schnellere und qualifiziertere Bewertung durchführen.

Die **Alarmierung** führt immer zu einer Handlung von ausgewählten Mitarbeitern in der BAO, die über das weitere Vorgehen entscheiden.

Die Detektion von Ereignissen kann bereits in anderen Prozessen der Institution geregelt sein, z. B. im IT Incident Management, in der Störungsbehandlung der Gebäudeverwaltung, in Entstörungsdiensten von Dienstleistern oder in der Sicherheitsvorfallbehandlung. Es sollte geprüft werden, ob entsprechende Prozesse zur Behandlung von Störungen und Sicherheitsvorfällen in der Institution bereits vorhanden sind. In diesem Fall ist es empfehlenswert, diese unterschiedlichen Prozesse aufeinander abzustimmen. Hierbei sollte sichergestellt werden, dass Schadensereignisse und Störungen mit Notfallpotenzial an eine zentrale Entscheidungsinstanz gemeldet werden und Reaktionszeiten aufeinander abgestimmt sind. Zusätzlich sollte die Kommunikations- und Alarmierungstechnik redundant ausgelegt sein. Es sollten außerdem Kommunikationskanäle zur Verfügung stehen, die unabhängig von der IT der Institution funktionieren.

Die Abbildung 17 stellt verkürzt mögliche Alarmierungspfade dar. Die einzelnen Aktivitäten, um ein Alarmierungs- und Meldewesen zu etablieren, werden in den nachfolgenden Unterkapiteln schrittweise beschrieben.

Beispiel:

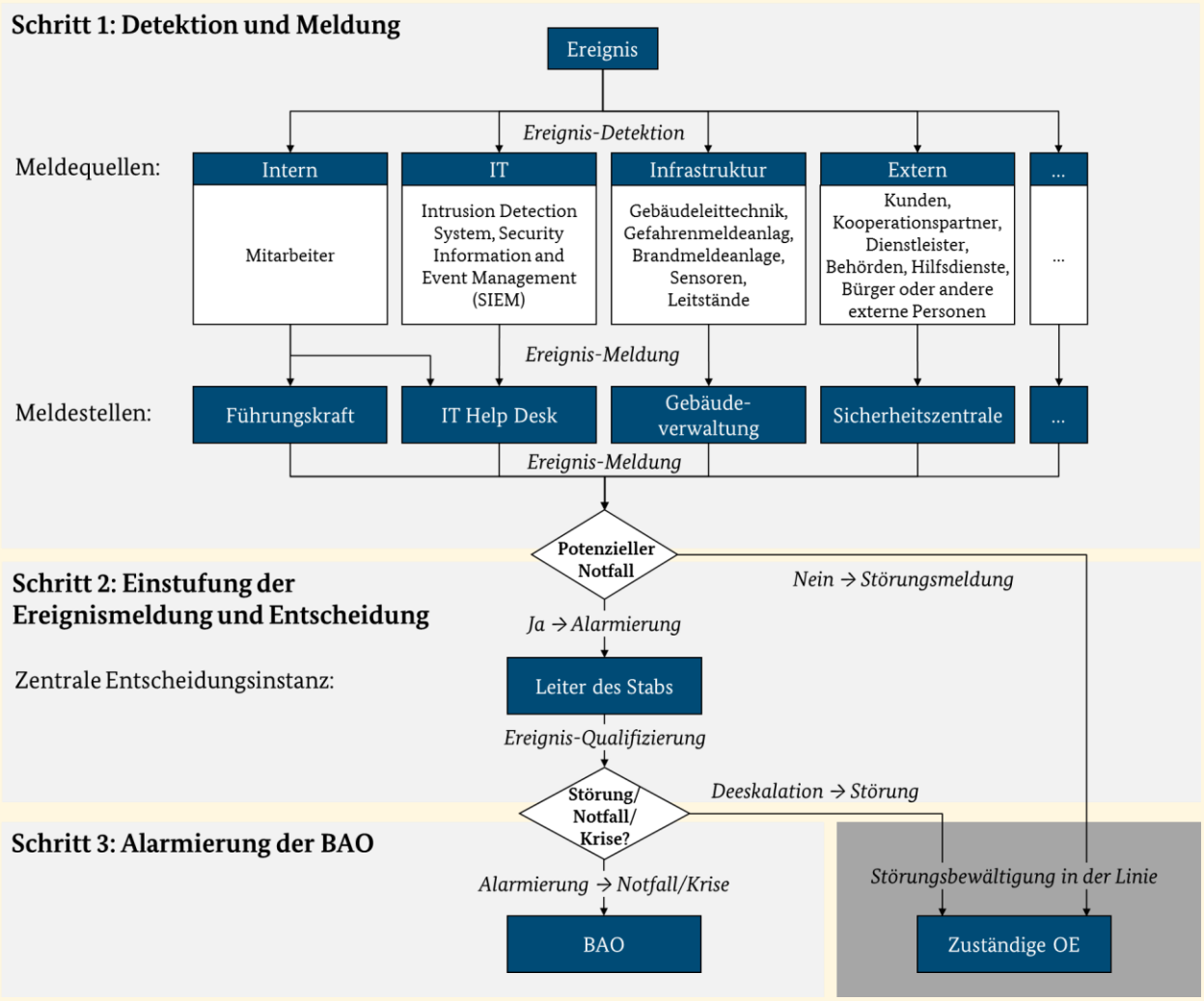

Abbildung 17: Beispiel eines Eskalations- und Alarmierungspfads

4.2.2.1 Detektion und Meldung

Die Detektion eines Schadensereignisses und die anschließende Weitergabe der Meldung können durch verschiedene interne und externe Personen oder technische Systeme erfolgen. Diese werden im Folgenden als Meldequellen bezeichnet. Typische Beispiele für Meldequellen sind:

Beispiel

- interne Mitarbeiter
- IT-Monitoring der IT-Infrastrukturen, z. B. durch den Einsatz von Intrusion Detection Systemen (IDS) oder Security Information and Event Management (SIEM)
- technisches Monitoring der Infrastruktur, z. B. mittels Gebäudeleittechnik, Gefahrenmeldeanlage (Brandschutz, Einbruchschutz etc.), Sensoren zur Überwachung der grundlegenden Versorgung (z. B. Strom, Wasser, Klimatisierung) oder Leitständen in der Produktion zur Betriebs- bzw. Werkssteuerung
- Externe, wie z. B. Kunden, Kooperationspartner, Dienstleister, Behörden, Bürger oder andere Externe

Die relevanten Meldequellen müssen in der Institution identifiziert und im Notfallhandbuch dokumentiert werden. Alle Meldungen müssen an einer dafür zuständigen, festgelegten Stelle zusammenlaufen. Dabei kön-

nen entweder genau eine Meldestelle für jegliche Meldungen festgelegt oder individuelle Stellen entsprechend dem Ereignistyp bestimmt werden. Letzteres hat den Vorteil, dass mehrere spezialisierte Meldestellen Ereignismeldungen entgegennehmen können und durch ihre jeweilige Fachkunde entscheidungs- bzw. aussagefähig sind. Ein weiterer Vorteil ist, dass durch mehrere individuelle Stellen die Last einer Vielzahl von Meldungen auf die einzelnen Meldestellen verteilt wird.

Beispiel:

In vielen Institutionen sind bereits mehrere zuständige Stellen etabliert, die Ereignismeldungen entgegennehmen und bearbeiten sowie erste Maßnahmen zum Eindämmen von Schäden einleiten:

- Ausfälle von IT-Anwendungen werden häufig an einen First-Level-Support gemeldet.
- Technische Alarme der Gefahrenmeldeanlage oder Elementarschäden laufen meist bei einer Sicherheitsleitstelle oder einem Sicherheitsdienst auf.
- Personalausfälle oder Störungen bei Dienstleistern werden dagegen über die Linienorganisation an die jeweils zuständigen Führungskräfte gemeldet.
- Oft nehmen auch der Empfang, die Telefonzentrale oder die Kundenhotline Meldungen über Schadensereignisse mit Notfallpotenzial entgegen.

Ein Meldeweg über mehrere Meldestellen ist beispielhaft in Abbildung 17 dargestellt. Die identifizierten und festgelegten Meldewege müssen mit den beteiligten, organisatorischen Schnittstellen abgestimmt werden, sodass diese bei Schadensereignissen mit Notfallpotenzial mit den definierten Wegen vertraut sind. Hierbei sollte grundsätzlich beachtet werden, dass Notfälle auch durch Schadensereignisse ausgelöst werden können, die weder aus einer Störung heraus eskalieren noch als Sicherheitsvorfall eingestuft werden. Ein Beispiel hierfür ist ein krankheitsbedingter, massiver Personalausfall in einer Organisationseinheit, der zu nicht tolerierbaren Auswirkungen auf den Geschäftsbetrieb führt. Auch für diese Ereignisse sollten Kriterien festgelegt werden, was durch wen an eine Meldestelle gemeldet werden sollte. Die im Notfallhandbuch dokumentierten Verfahren sollten den gelebten Prozessen entsprechen.

Um Ereignisse anhand vollständiger Informationen qualifiziert einschätzen zu können, sollte jede Meldestelle die Meldungen in einem einheitlichen Format erfassen (siehe Kapitel 4.2.2.2 *Einstufung der Ereignismeldung und Entscheidung*). Um die Meldung effizient weitergeben zu können, sollte diese kurzgefasst sein. Dabei sollten die Tatsachen von Vermutungen getrennt und mindestens folgende Angaben aufgenommen werden:

- Zeitpunkt und Ort des Ereignisses
- meldende Person oder Stelle
- eventuell betroffene Personen, Bereiche oder Prozesse
- mögliche Ursache oder Auslöser sowie
- die aktuellen Auswirkungen.

Unter Berücksichtigung der Rahmenbedingungen sowie der Risikobereitschaft der Institution muss definiert und dokumentiert werden, wie die Meldestellen sowohl während als auch außerhalb der üblichen Geschäftszeiten erreicht werden können. Eine Möglichkeit ist z. B. Rufbereitschaften hierzu festzulegen. Vorgaben seitens des Arbeitsschutzes sowie vorhandene Regelungen der Institution zur Arbeitszeit und Erreichbarkeit müssen beachtet werden. Die Regelungen zur Sicherstellung der Erreichbarkeit müssen mit den relevanten Stellen abgestimmt werden, z. B. der Institutionsleitung, der Personalabteilung und dem Betriebs- oder Personalrat. Falls nur eine eingeschränkte Erreichbarkeit einzelner Meldestellen realisiert werden kann, sollte dies ebenfalls im Notfallhandbuch dokumentiert werden. Durch die Institutionsleitung sollte dann eine Risikoübernahme herbeigeführt werden.

Hinweis:

Einige Institutionen unterliegen gesetzlichen oder regulatorischen Anforderungen, die vorschreiben, dass bestimmte Schadensereignisse innerhalb von wenigen Stunden an ausgewählte Interessengruppen (z. B. die zuständige Aufsichtsbehörde) gemeldet werden müssen. Wenn solche kurzfristigen Meldepflichten erfüllt werden müssen, muss für die Institution sichergestellt werden, dass die Meldepflicht z. B. durch Rufbereitschaftsregelungen oder eine durchgängige Besetzung eingehalten wird.

Jede Meldestelle muss dazu befähigt werden, bei einem Schadensereignis initial einzuschätzen, ob ein Ereignis mit Notfallpotenzial vorliegt. Dies kann im Rahmen eines gemeinsamen Termins erfolgen, in dem der aktuelle Stand erklärt und gemeinsam Kriterien zur Ersteinschätzung gefunden werden. Klare und für alle Beteiligten verständliche Kriterien sind von hoher Bedeutung, da die Ersteinschätzung möglichst schnell erfolgen muss. Dieser Zeitfaktor hängt sehr stark mit den definierten Erreichbarkeiten der Meldestellen zusammen. Wenn eine Meldestelle z. B. nur von 8 bis 17 Uhr erreichbar ist, kann ein Schadensereignis mit Notfallpotenzial um 17:30 Uhr mitunter erst am Folgetag festgestellt und weitergemeldet werden.

Durch wen die Ersteinschätzung vorgenommen wird, sollte sich an den bereits etablierten Meldestellen und Meldewegen orientieren. Die Kriterien, um ein Ereignis einschätzen zu können, sollten auch durch Personen mit nur geringen fachlichen oder technischen Kenntnissen angewendet werden können. Die Ersteinschätzung sollte deshalb nach einem einfachen Schema erfolgen, z. B. per Ja-Nein-Antwort auf allgemein verständliche Fragen. In den folgenden Tabellen ist jeweils ein allgemeingültiges Beispiel zur Ersteinschätzung eines Schadensereignisses für die häufigsten vier Ressourcenkategorien dargestellt. Für jede Institution und Meldestelle müssen diese Fragen individuell konkretisiert werden. Hierbei kann darauf hingewiesen werden, dass diese Information auch erfragt werden kann, wenn sie nicht offensichtlich ist.

Beispiele:

Meldestelle: Führungskraft Personal

Leitfragen für Schadensereignisse mit Notfallpotenzial - Personal	**Antwort Ja/Nein**
• Sind in Ihrem Zuständigkeitsbereich in Summe so viele Mitarbeiter nicht arbeitsfähig, dass Sie möglicherweise den Geschäftsbetrieb nicht mehr aufrechterhalten können? • Ist durch die Abwesenheit von Mitarbeitern mit bestimmten Berechtigungen der normale Geschäftsbetrieb eventuell nicht mehr möglich?	

Sobald mindestens eine Frage mit JA beantwortet werden kann,
bitte umgehend den Leiter des Stabs alarmieren: Telefon 1234567890

Tabelle 4: Beispiel zur Ersteinschätzung eines Schadensereignisses beim Personal

Meldestelle: Provider Management bzw. Dienstleistersteuerung

Leitfragen für Schadensereignisse mit Notfallpotenzial - Dienstleister	**Antwort Ja/Nein**
• Liegt beim Dienstleister oder dessen Subunternehmen ein nicht geplanter Ausfall bzw. Notfall vor oder ist dieser absehbar? • Hat der Dienstleister den Vertrag einseitig gekündigt und mit sofortiger Wirkung seine Leistung eingestellt?	

Sobald mindestens eine Frage mit JA beantwortet werden kann,
bitte umgehend den Leiter des Stabs alarmieren: Telefon 1234567890

Tabelle 5: Beispiel zur Ersteinschätzung eines Schadensereignisses beim Dienstleister

Meldestelle: IT-Help Desk (1st bzw. 2nd Level Support)

Leitfragen für Schadensereignisse mit Notfallpotenzial - IT	Antwort Ja/Nein
• Ist das betroffene IT-System oder die betroffene Anwendung wesentlicher Bestandteil der Sicherheitsinfrastruktur (Viren-Management, Firewall etc.)? Für nähere Details siehe IT-Servicekatalog oder IT-Anwendungsliste. • Hat der Ausfall des betroffenen IT-Systems oder der betroffenen Anwendung Auswirkungen auf einen großen Nutzerkreis oder den wesentlichen Geschäftsbetrieb der Institution? • Besteht ein dringender Verdacht auf vorsätzliche Daten- oder Systemmanipulationen (Datenabfluss), unerlaubte Ausübung von Rechten oder eines gezielten Angriffs (physisch oder virtuell) auf IT-Komponenten? • Ist zu erwarten, dass die Auswirkungen des gemeldeten Ereignisses einen Zeitraum > X Stunden übersteigen werden? Gegebenenfalls die Information im 2nd Level Support erfragen. • Hat der Ausfall des betroffenen IT-Systems oder der betroffenen Anwendung Auswirkungen auf externe Interessengruppen, wie z. B. Kunden, Medien, Aufsichtsbehörden? Gegebenenfalls die Information beim Anwender erfragen.	

Sobald mindestens eine Frage mit JA beantwortet werden kann,
bitte umgehend den Leiter des Stabs alarmieren: Telefon 1234567890

Tabelle 6: Beispiel zur Ersteinschätzung eines Schadensereignisses in der IT

Meldestelle: Gebäudemanagement/Sicherheitszentrale/Sicherheitsdienstleister/Leitstand

Leitfragen für Schadensereignisse mit Notfallpotenzial – Gebäude bzw. Infrastruktur	Antwort Ja/Nein
• Ist oder war die Räumung eines Gebäudes notwendig, z. B. aufgrund eines Brandes oder eines Sicherheitsvorfalls? • Kann oder darf mindestens ein Gebäudeteil (z. B. gesamte Etage, Brandabschnitt, Trakt) zeitweise nicht genutzt werden, z. B. aufgrund eines Gebäudeschadens oder Defekts einzelner Infrastrukturkomponenten (z. B. Brandschutzeinrichtungen oder Sanitäranlagen)? • Ist die Versorgung mit Strom, Wasser oder Klimatisierung ausgefallen und eine ausreichend schnelle Wiederherstellung bzw. Instandsetzung dieser Versorgung nicht absehbar? • Ist eine Produktionsmaschine oder -anlage ausgefallen und eine ausreichend schnelle Reparatur oder Ersatz nicht absehbar? • Ist die Sicherheit der Mitarbeiter am Standort aufgrund eines Ereignisses (z. B. Unwetterwarnung, politische Demonstration oder Schadensereignis im Umfeld) möglicherweise gefährdet?	

Sobald mindestens eine Frage mit JA beantwortet werden kann,
bitte umgehend an den Leiter des Stabs melden: Telefon 1234567890

Tabelle 7: Beispiel zur Ersteinschätzung eines Schadensereignisses am bzw. im Gebäude

Wenn es sich um ein Schadensereignis mit Notfallpotenzial handelt, muss die zuständige Stelle unverzüglich eine vordefinierte zentrale Entscheidungsinstanz alarmieren. Hierbei müssen alle Details zum Schadensereignis, die bisher bekannten Auswirkungen und bereits eingeleitete Maßnahmen zur Bewältigung des Ereignisses übermittelt werden.

Falls die Meldestelle bei der Ersteinschätzung unsicher ist, gilt der Grundsatz „Lieber zu viel melden, als zu wenig". Dementsprechend sollte die zentrale Entscheidungsinstanz von der Meldestelle alarmiert werden. Eventuelle Fehlmeldungen können im Nachgang untersucht und der Prozess *Alarmierung und Eskalation* entsprechend angepasst werden, z. B. indem die Kriterien anhand der gewonnenen Erkenntnisse geschärft werden.

Um eine möglichst verzugslose Alarmierung sicherzustellen, muss festgelegt werden, wie Alarmmeldungen übermittelt werden sollen, z. B. per Telefon, Alarm-SMS mit Lesebestätigung oder Alarmierungstool. Es wird empfohlen, Kommunikationsmittel einzusetzen, die den direkten, verzugslosen Dialog erlauben und damit zusätzlich sicherstellen, dass Informationen aufgenommen und verstanden wurden.

Hinweis:

Alarmmeldungen über E-Mail erzeugen nicht genügend Aufmerksamkeit für Schadensereignisse mit dringendem Handlungsbedarf und sind grundsätzlich hierfür ungeeignet. Besser geeignet sind z. B. manuelle oder automatisierte Anrufe auf Mobiltelefonen oder Alarm-Apps.

4.2.2.2 Einstufung der Ereignismeldung und Entscheidung

Die Einstufung und Entscheidung, ob es sich bei dem Schadensereignis um eine Störung, einen Notfall oder eine Krise handelt, sollte durch eine **zentrale Entscheidungsinstanz** getroffen werden. Eine zentrale Entscheidungsinstanz verhindert, im Gegensatz zu dezentralen Entscheidungsinstanzen, zeitaufwendige Abstimmungen, unklare Entscheidungsbefugnisse und ermöglicht so eine schnelle Entscheidungsfindung. Dies ist von hoher Bedeutung, da die Entscheidung über das Ereignis weitreichende Auswirkungen auf das weitere Geschehen der Bewältigung hat. Stellt sich heraus, dass ein Schadensereignis als Störung bewertet wurde, es sich aber um einen Notfall handelt, wäre wertvolle Zeit verloren gegangen. Deshalb sollte die zentrale Entscheidungsinstanz geschult, erfahren und befugt sein.

Geschult bedeutet hier, dass die zentrale Entscheidungsinstanz über die hierzu erforderliche Sachkenntnis verfügen muss, z. B. um die Begriffe Störung, Notfall und Krise unterscheiden zu können (siehe Kapitel 2.1 *Begriffe*) und den Alarmierungsprozess kennen muss.

Die Entscheidungsinstanz muss auch erfahren sein und einen guten Überblick über die Institution haben, damit sie die Auswirkungen unmittelbar einschätzen kann. In den meisten Fällen liegen zu einem Schadensereignis nur eingeschränkte Informationen vor. Die Entscheidungsinstanz sollte auch bei spärlicher Informationslage entscheidungsfreudig sein.

Als letzter Punkt muss die Entscheidungsinstanz entsprechend befugt sein, eigenständig die Ereignismeldung zu qualifizieren und eine Entscheidung zu fällen. Dies verkürzt die Zeitspanne, die bis zum Beginn der Bewältigung verstreicht.

Hinweis:

Aufgrund ihrer Aufgaben, Fähigkeiten und Erfahrungen sind in der Praxis häufig der Leiter des Stabs oder der BCMB geeignete Rollen, um die Ereignismeldung qualifizieren zu können.

Um die Entscheidung zu vereinfachen und sie transparent zu machen, sollte der zentralen Entscheidungsinstanz eine Checkliste mit Kriterien zur Verfügung gestellt werden. Auf deren Basis kann eine nachvollziehbare und dokumentierte Entscheidung zur Einstufung des Ereignisses getroffen werden. Um Kriterien ableiten zu können, können zunächst folgende Punkte als Grundlage herangezogen werden:

- Ist der normale Geschäftsbetrieb der gesamten Institution oder einzelner Teile unterbrochen?
- Steht ein Ausfall des Geschäftsbetriebs unmittelbar bevor oder ist er absehbar?
- Erfordert die Bewältigung eine BAO, z. B. für kurze Entscheidungswege und schnellen Zugriff auf Spezialisten?

Wenn zu einem späteren Zeitpunkt durch die Institution konkreter festgelegt wird, wie der Stab final über einen Notfall oder Krise entscheidet, können die dort festgelegten Kriterien bereits in der ersten Einstufung hinzugezogen werden (siehe Kapitel 4.2.4.2 *Konstituierung und Auflösung* der BAO).

Das Ergebnis der Ersteinschätzung kann zwei Ausgänge haben:

- Das Ereignis wird als **Störung** qualifiziert.

  Dann muss das Ereignis als Störung gemeldet und durch die entsprechende Fachabteilung innerhalb der AAO behoben werden. Da ein Schadensereignis jederzeit durch Lageveränderungen eskalieren kann, sollte sich die Entscheidungsinstanz über den Verlauf der Störungsbeseitigung durch die zuständige Fachabteilung informieren lassen.

- Das Ereignis wird als **Notfall** oder Krise qualifiziert.

  Dann muss die Entscheidungsinstanz die BAO unverzüglich alarmieren (siehe Kapitel 4.2.2.3 *Alarmierung der BAO*).

In jedem Fall muss die zentrale Entscheidungsinstanz die getroffene Entscheidung mit den notwendigen Details dokumentieren, wie z. B. Zeitpunkt und Auswirkung des Ereignisses, Begründung der Entscheidung und Beteiligte an der Entscheidung.

In der Konstituierung der BAO muss diese Entscheidung durch den Stab anhand weiterer Kriterien überprüft und bestätigt bzw. deeskaliert werden (siehe Kapitel 4.2.4.2 *Konstituierung und Auflösung* der BAO).

4.2.2.3 Alarmierung der BAO

Um sicherzustellen, dass die BAO unverzügliche alarmiert werden kann, muss die Institution dafür sorgen, dass die hierfür notwendigen organisatorischen und technischen Voraussetzungen geschaffen und dokumentiert werden. Organisatorisch sollte festgelegt werden,

- wie die BAO innerhalb und außerhalb der üblichen Geschäftszeiten erreicht wird,
- welche Personen durch die zentrale Entscheidungsinstanz alarmiert werden,
- welche weiteren Personen durch die zuerst alarmierten Personen alarmiert werden,
- welche Kommunikationskanäle hierzu eingesetzt werden sowie
- welche Informationen vermittelt werden.

Analog zu dem beschriebenen Vorgehen für die zentrale(n) Meldestelle(n) sollten Rufbereitschaften der BAO eingerichtet werden. Für Zeiten, in denen eine Erreichbarkeit der BAO nicht garantiert ist, sollten Risikoübernahmen durch die Institutionsleitung schriftlich fixiert werden.

Die Benachrichtigung der Rolleninhaber der BAO sollte kurz und präzise sein. Diskussionen und längere Ausführungen zur Lage müssen bei der Alarmierung vermieden werden. Zum einen können zu viele Informationen den Einzelnen verwirren. Zum anderen wird die Alarmierung unnötig verzögert. Detaillierte Informationen werden in der ersten Lagebesprechung für alle Anwesenden gemeinsam vorgestellt und besprochen.

In der Nachricht sollte klar erkennbar sein, welche nächsten Schritte der Alarmierte unternehmen muss, beispielsweise sich im Stabsraum oder einer virtuellen Arbeitsumgebung (z. B. Telefonkonferenz) einzufinden. Der Alarmierte muss dem Aufruf zeitnah folgen. Leben im Haushalt des Alarmierten weitere Personen, die den Anruf entgegennehmen könnten, so sollten diese für den Umgang mit empfangenen Alarmmeldungen sensibilisiert werden.

Je nach Größe der BAO kann es zeitaufwändig sein, alle Rolleninhaber einzeln persönlich zu benachrichtigen. Zur Unterstützung der Alarmierung kann es sinnvoll sein, eine Alarmierungssoftware oder eine Alarm-App einzusetzen (siehe Hilfsmittel *Tools*). Diese IT-Anwendungen ermöglichen es, auf Knopfdruck die zur Bewältigung erforderlichen Personen zu benachrichtigen. Neben der Alarmauslösung bieten die IT-Anwendungen oft wichtige Zusatzfunktionen, wie z. B.:

- eine Alarmnachverfolgung
- eine automatische Benachrichtigung der Stellvertreter bei Nicht-Erreichbarkeit
- die Möglichkeit, dass die Alarmierten dem Leiter des Stabs den erwarteten Zeitpunkt des Eintreffens am Notfalltreffpunkt mitteilen können, falls dies der nächste Schritt ist.

Der vollständig definierte Eskalations- und Alarmierungsprozess sollte visualisiert und im Notfallhandbuch dokumentiert werden. Dafür kann z. B. die Abbildung 17 vom Beginn des Kapitels angepasst werden. Diese ist auch in den Hilfsmitteln hinterlegt.

Dokumentierte Vorgaben und begleitende Maßnahmen stellen sicher, dass die definierten Meldewege, wie vorgesehen, eingehalten werden. Als begleitende Maßnahme ist unter anderem empfehlenswert, dass Meldestellen und Kommunikationswege organisationsweit bekannt gegeben werden. Dazu können z. B. Aushänge oder andere Informationsmaterialen genutzt werden. Die Notfallkarte in den Hilfsmitteln stellt ein mögliches Beispiel dafür dar. Des Weiteren sollten Schulungen und Sensibilisierungsmaßnahmen für die Mitarbeiter geplant und veranlasst werden, um eine schnelle Alarmierung und Eskalation zu gewährleisten.

4.2.3 Definition von Sofortmaßnahmen

Mit Sofortmaßnahmen sind solche gemeint, die keinen zeitlichen Aufschub dulden und möglichst unmittelbar nach Eintritt eines Schadensereignisses eingeleitet werden müssen. Alle diese Maßnahmen stellen den Schutz von Leib und Leben von Personen sicher und wenden weitere Schäden ab. Zu Sofortmaßnahmen zählen z. B. die Räumung des Gefahrenbereichs, die aus Sicherheitsgründen erforderliche Abschaltung der Stromversorgung oder die vorgeschriebene Sofortmeldung an einen Regulator.

In einem Notfall gilt der Grundsatz, dass der Schutz von Leib und Leben vor dem Schutz von Sachwerten und Gütern steht. Entsprechend muss die Institution dafür sorgen, dass entsprechende Anweisungen und konkrete Aufgaben festgelegt werden. Es muss klar sein, wer welche Sofortmaßnahmen durchführen darf oder muss. Insbesondere ist es empfehlenswert, Sofortmaßnahmen für Notfallszenarien festzulegen, bei denen „Gefahr im Verzug“ besteht. Hierunter fallen z. B.:

- Maßnahmen zur Ersten Hilfe
- Maßnahmen zur Rettung und Bergung von Verletzten
- Maßnahmen zur Räumung von Gebäuden und Betriebsstätten
- Handlungsanweisungen für spezielle, wahrscheinliche Schadensereignisse, wie z. B.
    - Brand
    - Wassereinbruch
    - Ausfall der Strom-, Wasser oder Gas-Versorgung
    - Gefahr durch einen Sicherheitsvorfall, z. B. herrenloser Koffer im Gebäude
    - Großereignis im unmittelbaren Umfeld, z. B. Demonstrationen

Je nach Branche der Institution kann davon ausgegangen werden, dass es weitere spezielle Schadensereignisse gibt, für die Sofortmaßnahmen festgelegt werden müssen.

Synergiepotenzial:

Häufig existieren bereits gesetzliche Vorgaben für die oben genannten Punkte, die durch die jeweiligen Berufsgenossenschaften konkretisiert werden. Somit sollten entsprechende Anweisungen für Sofortmaßnahmen bereits in der Institution vorhanden sein, z. B. seitens der Fachkraft für Arbeitssicherheit.

Die Sofortmaßnahmen sollten in geeigneter Form in die Ablauforganisation der Notfallbewältigung integriert werden. Entsprechend müssen die im Notfallhandbuch dokumentierten Sofortmaßnahmen zum Schutz von Leib und Leben zwischen dem BCMB und der Fachkraft für Arbeitssicherheit abgestimmt werden. Im Notfallhandbuch sollte auf vorhandene Regelungen und Rollen verwiesen werden, z. B. die Aufgaben und Zuständigkeiten der Ersthelfer, Betriebssanitäter, Brandhelfer, Evakuierungshelfer oder Einsatzteams sowie entsprechende Aushänge in den Gebäuden. Die Dokumentation der Sofortmaßnahmen sollte in Form von Checklisten erfolgen. Dies ermöglicht auch unter Zeitdruck eine strukturierte Vorgehensweise.

Hinweis:

Häufig wird unter Sofortmaßnahmen die Evakuierung des Gebäudes verstanden, beispielsweise bei einem Brand. BCM-relevante Sofortmaßnahmen greifen jedoch in der Regel erst ab dem Zeitpunkt, wenn die Mitarbeiter das Gebäude nach einem Brand verlassen haben und beim Sammelpunkt eingetroffen sind. Deswegen sollten die vorhandenen Regelungen und Sofortmaßnahmen geprüft und festgelegt werden, welche Inhalte aus anderen Themenfeldern in das BCM einbezogen und dokumentiert werden sollten.

Tabelle 8 und Tabelle 9 zeigen ein Beispiel für Sofortmaßnahmen bei einem Gebäudeausfall aufgrund von Stromausfall.

Beispiel:

Grau hinterlegte Zeilen stellen übliche Sofortmaßnahmen der AAO dar, während weiß hinterlegte Zeilen Sofortmaßnahmen des BCM wiedergeben.

Nr.	Aktivität	Zuständig
1	Meldung des Schadensereignisses an Gebäudemanagement	Feststellende Person
2	Fehlersuche und Schadensbegrenzung	Mitarbeiter Gebäudemanagement
3	Beauftragung eines Wartungs- bzw. Reparaturdienstes	Mitarbeiter Gebäudemanagement
4	Ermitteln der konkreten Auswirkungen bzw. betroffenen Gebäude(teile)	Mitarbeiter Gebäudemanagement
5	Aktuellen Arbeitsstand der zeitkritischen Geschäftsprozesse prüfen und Aufgaben priorisieren	Führungskräfte betroffener OEs
6	Droht Gebäudeausfall mobile Arbeitsfähigkeit herstellen Mitarbeiter des Notfallteams sollen Laptops mitnehmen (Sicherheit geht jedoch vor!) Schlüsselpersonen mit Token ausstatten	Führungskräfte betroffener OEs
7	Meldestelle informieren	Mitarbeiter Gebäudemanagement

Tabelle 8: Beispiel für Sofortmaßnahmen bei einem Gebäudeausfall

Nach Eskalation zu einem Notfall:

8	Ausweichstandorte aktivieren und arbeitsfähig machen	Notfallteam Gebäude
9	Sofortigen Umzug auf Ausweichstandorte anordnen	Führungskräfte betroffener OEs

Tabelle 9: Beispiel für Sofortmaßnahmen bei einem Gebäudeausfall nach Eskalation zu einem Notfall

4.2.4 Herstellung der Fähigkeit zur Stabsarbeit

Für eine funktionierende Bewältigung ist es wichtig, dass die Methoden und Abläufe der Stabsarbeit durch die BAO-Rolleninhaber verstanden und verinnerlicht werden. Daher sollten die Stabsmitglieder hinsichtlich der geschaffenen BAO-Strukturen und ihrer Aufgaben im Notfall **geschult** werden (**Schulung der Stabsmitglieder**). Neben theoretischem Wissen sollten die Stabsmitglieder möglichst eigene Erfahrungen in geschützter Umgebung sammeln können, wie Stabsarbeit in der Praxis funktioniert. Dies kann am besten über Trainings und Übungen erreicht werden.

Zudem müssen die **Methoden und Regeln für die Stabsarbeit** festgelegt werden, damit es ein einheitliches Verständnis über die Abläufe und Besonderheiten in der Zusammenarbeit gibt. So kann eine „Chaosphase" im Notfall weitestgehend vermieden werden. Außerdem muss festgelegt werden, in welchem **Stabsraum** und mit **welcher Ausstattung** die Stabsarbeit stattfindet, damit diese Infrastruktur im Notfall verfügbar und einsatzbereit ist. Anschließend müssen diese Schritte durch **die Institutionsleitung freigegeben** werden.

Im Nachfolgenden werden die einzelnen Schritte in eigenen Unterkapiteln erläutert. Die Unterkapitel reflektieren keine zeitliche Abfolge, sondern weisen Wechselwirkungen untereinander auf. So kommt es z. B. in der Praxis häufig vor, dass Erkenntnisse aus Schulungen und Trainings zu Anpassungen der dokumentierten Methodik zur Stabsarbeit oder zu Veränderungen an der Ausstattung des Stabsraums führen. Die veränderten Methoden und Regeln der Stabsarbeit fließen wiederum in die Schulungen, Trainings und Übungen für den Stab oder seine Unterstützungsrollen ein.

4.2.4.1 Festlegung der Methoden und Regeln für die Stabsarbeit

Die Arbeitsweise im Stab unterscheidet sich deutlich von der gewohnten Zusammenarbeit im Normalbetrieb. Aufgrund der außergewöhnlichen Herausforderungen im Notfall, wie z. B. hoher Handlungsdruck, gestörte Kommunikationswege, unvollständige oder widersprüchliche Informationen etc., ist die Stabsarbeit häufig sehr belastend für die Stabsmitglieder.

Sind in einer solchen Situation Rollen- und Aufgabenverteilung im Stab und die Mitsprache- und Entscheidungsrechte unklar oder die Kommunikation zwischen den Mitgliedern unstrukturiert, kann die Stabsarbeit stark beeinträchtigt werden. Um dies zu vermeiden, müssen die Methodik und die Regeln für die Stabsarbeit schon in der Notfallvorsorge erarbeitet, abgestimmt und festgelegt werden. Dieser sogenannte **Verhaltenskodex** stellt sicher, dass der Stab im Notfall seine Arbeit direkt aufnehmen kann und handlungsfähig ist. Es wird empfohlen, dass der BCMB aufgrund seiner Sachkenntnis einen Vorschlag für den Verhaltenskodex erstellt. Damit der Verhaltenskodex von allen Stabsmitgliedern akzeptiert wird, empfiehlt es sich jedoch, die Stabsmitglieder möglichst frühzeitig mit einzubinden.

Hinweis:

Insbesondere, wenn die Mitglieder des Stabes noch nicht gemeinsam in Übungen oder realen Vorfällen zusammengearbeitet haben, ist es entscheidend, dass allen Personen klar ist, wer welche Funktion im Stab einnimmt. Zu diesem Zweck ist es empfehlenswert, wenn sich jede Person in der ersten Lagebesprechung namentlich vorstellt, ihre Rolle oder Funktion nennt und die Lage kurz aus der eigenen Position heraus beschreibt.

Im Nachfolgenden wird ein einfaches Beispiel für einen Verhaltenskodex dargestellt. Dies muss von jeder Institution an die eigenen Bedürfnisse und Anforderungen angepasst werden. Das Hilfsmittel *Weiterführende Aspekte zur Bewältigung* kann als Nachschlagewerk verwendet werden, um die einzelnen Punkte genauer nachzuvollziehen oder detaillierter auszugestalten (z.B. für den Führungszyklus FOR-DEC).

Beispiel:

1. Der Stab richtet seine Arbeitsweise anhand der vorliegenden Notfallpläne (Geschäftsfortführungspläne) aus. Liegen keine Notfallpläne vor oder greifen diese nicht, wird die Arbeitsweise am **Führungszyklus** FOR-DEC ausgerichtet.
2. Der Stab hat Arbeits- und Besprechungsphasen (**Lagebesprechungen**). Diese müssen eindeutig festgelegt und allen Stabsmitgliedern kommuniziert werden.
3. Lagebesprechungen
   - dauern nie länger als 30 Minuten,
   - brauchen immer einen Moderator,
   - dürfen ihren Fokus nicht durch Einzeldiskussion zu Spezialthemen verlieren (diese Diskussionen können im Nachgang geklärt werden),
   - müssen immer eindeutig beendet werden,
   - müssen immer zeitlich klar terminiert und angesagt werden.
4. Es muss immer ein **Protokoll** geführt werden, aus welchem die Meldungen bzw. Ereignisse und Beschlüsse des Stabs mit den notwendigen Angaben zu Ort, Zeit und Status nachvollziehbar dokumentiert werden. Im Protokoll muss zudem erfasst werden, wer wann anwesend war.
5. Fakten müssen von Gerüchten getrennt und Informationen immer verifiziert werden. In komplexen Lagen sollte dazu ein **Informationsmanagement** aufgebaut werden.
6. Die **Visualisierung** sollte regelmäßig genutzt und aktualisiert werden.
7. Aufgaben müssen klar benannt, terminiert und delegiert werden (Zielstellung, Aufgabenstellung, Zuständigkeiten, Umsetzungsfrist bzw. Wiedervorlage) und im **Aufgabenmanagement** festgehalten werden.
8. Damit allen anwesenden Personen bewusst ist, wer welche Rolle oder Funktion in der BAO einnimmt, muss sich jeder in der ersten Lagebesprechung mit Namen und Rolle bzw. Funktion vorstellen.

Hinweis:

Ein Verhaltenskodex kann die Form der Zusammenarbeit nur auf einer eher generellen Ebene regeln und stellt kein abgeschlossenes detailliertes Regelwerk dar. Wenn die Zusammenarbeit auch schon im Reaktiv-BCMS detailliert festgelegt werden soll, kann hierzu eine *Geschäftsordnung* erstellt werden. Dies wird unter Kapitel 6.4.4 *Definition der Geschäftsordnung des Stabs* näher beschrieben.

Zusätzlich zur Erstellung des Verhaltenskodex sollte der BCMB die nachfolgenden Aspekte klären und schriftlich regeln.

Arbeitsbedingungen

Die Stabsarbeit erfolgt unter Stress und ist physisch wie psychisch belastend. Zudem endet die Stabsarbeit oft nicht zum Ende eines regulären Arbeitstages. Daher ist es empfehlenswert, die Möglichkeiten eines Schichtbetriebs für den Stab zu prüfen, organisatorisch zu regeln und zu dokumentieren. Falls ein Schichtbetrieb gewählt wird, sollte bereits im Vorfeld die Übergabe zwischen den Schichten geregelt werden.

Falls die institutionsspezifischen Arbeitszeit- und Überstundenregelungen keine Vorgaben für einen Notfall beinhalten, wird empfohlen abweichende Regelungen für den Notfall festzulegen. Diese sollten vorab mit den relevanten Stellen, wie z. B. der Rechtsabteilung, Personal- oder Betriebsrat sowie der Institutionsleitung abgestimmt werden.

Protokollierung

Grundsätzlich müssen alle wesentlichen durchgeführten Aktivitäten und Entscheidungen des Stabs protokolliert werden. Die Arbeit im Stab muss dabei so dokumentiert werden, dass im Nachhinein nachvollzogen werden kann, auf welcher Grundlage jede Entscheidung im Stab getroffen wurde und welche Stabsmitglieder an der Entscheidung beteiligt waren.

Mit der Protokollierung werden zwei unterschiedliche Zielsetzungen verfolgt: Zum einen dient das Protokoll als Nachweis bei einer möglichen späteren Revision oder Ermittlung zu den Entscheidungen im Stab. Zum anderen ist das Protokoll die Basis für eine Auswertung im Nachgang, um Lücken und Verbesserungspotenziale für das BCMS und die Ereignisbewältigung identifizieren zu können.

Die Protokollierung kann in elektronischer Form oder in Papierform erfolgen. Zur Arbeitserleichterung sollte eine Dokumentvorlage bzw. ein Hilfsmittel für die Protokollierung entwickelt werden. Hierbei sollte ein Kompromiss zwischen den Nachweispflichten der Institution, der Nachvollziehbarkeit von Entscheidungen und der Arbeits- und Entscheidungsfähigkeit des Stabs gefunden werden. Hierüber sollten sich der BCMB, die Rolleninhaber Protokollant und der Leiter des Stabs abstimmen.

Hinweis:

In der Praxis hat es sich bewährt, wenn die Rolle Protokollant die zu dokumentierenden Sachverhalte proaktiv im Stab erfragt, anstatt nur im Hintergrund zu agieren. Dadurch können Maßnahmen und Entscheidungen noch einmal im Stab durchdacht und eventuelle Fehlerquellen identifiziert werden. Des Weiteren kann so sichergestellt werden, dass alle wichtigen Informationen im Protokoll enthalten sind und dass die Formulierung von kritischen Sachverhalten im Stab abgestimmt wurde.

Lagebeobachtung und -visualisierung

Notfälle und Krisen sind dadurch gekennzeichnet, dass sich die Lage laufend verändert. Hierbei gibt es erwünschte Lageänderungen, z. B. aufgrund eingeleiteter Notfallmaßnahmen sowie unerwünschte Lageänderungen, z. B. aufgrund einer Eskalation des Ereignisses infolge nicht wirksamer Gegenmaßnahmen.

Lageänderungen können darüber hinaus aus neu gewonnenen Erkenntnissen heraus entstehen, z. B. weil Ursachen des Ereignisses ermittelt wurden. Lageänderungen können auch zu neuen Herausforderungen in der Notfallbewältigung führen, z. B. weil das Ereignis extern bemerkt wurde.

Mithilfe der Lagebeobachtung können diese Veränderungen der Lage schnell erfasst und darauf reagiert werden, z. B. indem angepasste oder neue Notfallmaßnahmen abgeleitet und umgesetzt werden.

Für eine effektive **Lagebeobachtung** ist es empfehlenswert, folgende Punkte vorab festzulegen.

- zuständige Rollen in der Lagebeobachtung
- Schwerpunkte der Lagebeobachtung, z. B.
    - bisher umgesetzte Sofortmaßnahmen
    - bekannte Fakten zum Ereignis
    - jegliche, bisher ergriffene Maßnahmen und deren Wirksamkeit
- Sicherstellung der Erreichbarkeit der Personen am Ort des Geschehens, z. B.
    - Personen, die Sofortmaßnahmen ausgeführt haben

- Notfallteams, welche die Notfallmaßahmen operativ ausführen.

Die **Lagevisualisierung** hat das Ziel, eine einheitliche und schnelle Übersicht über die Lage zu geben und den Stab bei Lagebesprechungen sowie bei der Schichtübergabe zu unterstützen. Je mehr in der Stabsarbeit visualisiert wird, desto besser ist grundsätzlich das gemeinsame Lagebild des Stabs. Folgende Elemente zur Lagevisualisierung sollten vorab geplant werden:

- fortlaufendes Lagebild (z. B. eingehende Meldungen, Übersichten zum Schadensereignis, Zeitstrahl)
- Übersicht aller Aufgaben mit Status und Priorisierung (Aufgabenmanagement)
- Besetzung des Stabs (z. B. mit Schichtplan)
- Übersicht zur internen und externen **Notfallkommunikation**

Abbildung 18 veranschaulicht exemplarisch die Visualisierung eines fortlaufenden Lagebildes anhand eines Zeitstrahls.

Beispiel:

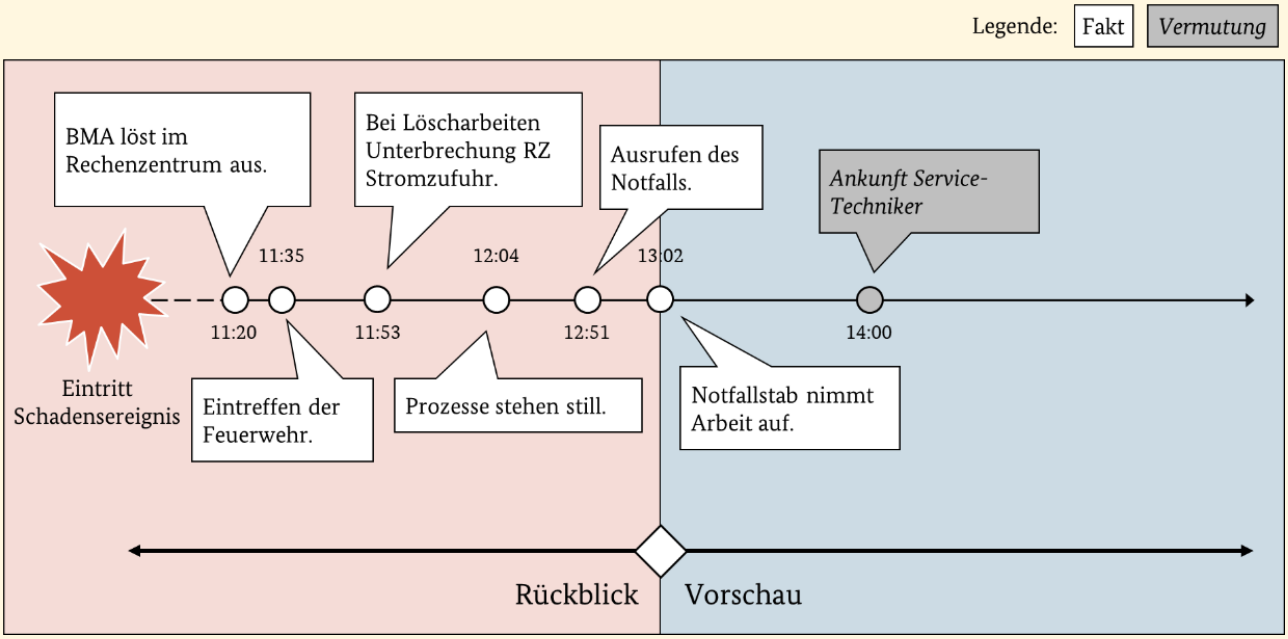

Abbildung 18: Beispiel eines Zeitstrahl zur Visualisierung von Ereignissen

Es sollten bevorzugt gesicherte Informationen visualisiert werden. Vermutungen und Annahmen müssen als solche kenntlich gemacht werden. Falls die Rolle Visualisierer eingesetzt wird, sollte diese für die Elemente zur Lagevisualisierung ausführlich sein (siehe Kapitel 4.2.4.3 *Schulung der Stabsmitglieder*). Dabei sollte auch gemeinsam mit dem Leiter des Stabes besprochen werden, wie mit dem Stab und der Protokollierung zusammengearbeitet werden soll. Wird keine separate Rolle Visualisierer eingesetzt, sollten alle Mitglieder des Kernteams mit den Grundsätzen der Lagevisualisierung vertraut gemacht werden.

4.2.4.2 Konstituierung und Auflösung der BAO

Die Konstituierung und Auflösung der BAO markiert den jeweiligen Übergang vom Normal- in den Notbetrieb bzw. vom Not- und Störbetrieb in den Normalbetrieb. Die Konstituierung der BAO schließt sich dem Alarmierungs- und Eskalationsprozess unmittelbar an (siehe Kapitel 4.2.2 *Detektion, Alarmierung und Eskalation).*

Bereits in der Notfallvorsorge sollte sich die Institution Gedanken dazu machen, welche Einzelschritte in der Startphase der Notfallbewältigung erforderlich sind, damit die Stabsarbeit im Notfall zeitnah aufgenommen

werden kann. Insbesondere sollten Kriterien festgelegt werden, die der Stab nutzt, um final über einen Notfall zu entscheiden. Hierzu können folgende Kriterien angewendet werden.

Beispiel:

- Das Leben und die Gesundheit von Personen ist durch das Ereignis selbst gefährdet.
- Das Leben und die Gesundheit von Personen ist durch die Geschäftsunterbrechung gefährdet.
- Das Ansehen der Institution in der Öffentlichkeit ist gefährdet.
- Der zu erwartende finanzielle Schaden des Ereignisses ist wahrscheinlich hoch, unter Umständen sogar existenzbedrohend (siehe Kapitel 3.1.4 Selbstverpflichtung der Institutionsleitung).
- Es wurde ein bedeutsamer Verstoß gegen Gesetze, Vorschriften oder Verträge festgestellt, der zu Meldepflichten an Dritte oder zu rechtlichen Konsequenzen führen kann.

Die meisten dieser Kriterien können in der Regel anhand der Ergebnisse der BIA beantwortet werden. Liegen noch keine Ergebnisse der BIA vor, dann müssen die genannten Kriterien ad hoc durch den Stab überprüft werden.

Die Institution sollte im Vorhinein Abläufe festlegen, sowohl um einen Notfall auszurufen als auch um ein Ereignis zu deeskalieren. Im Falle eines Schadensereignisses können dann diese Abläufe unmittelbar eingeleitet werden, nachdem der Stab entschieden hat, ob es sich um einen Notfall, eine Krise oder eine Störung handelt. Zudem ist es empfehlenswert, folgende Schritte zu klären:

- Wie erfolgt eine Prüfung der Vollständigkeit, Handlungs- und Entscheidungsfähigkeit des Stabes?
- Wie erfolgt eine erste Lagebesprechung? (z. B. Vorstellung anwesender Personen in Rollen, die vom Normalbetrieb abweichen, oder Regelungen zur Redezeit je Teilnehmer)
- Wie wird über die erforderlichen Mitglieder im Kernteam bzw. hinsichtlich einer situativen Erweiterung des Stabes entschieden?
- Wie wird die finale Entscheidung, ob es sich um einen Notfall handelt, dokumentiert und in der Institution kommuniziert?
- Wer entscheidet, wann die Wiederanlauf- und Geschäftsfortführungspläne (siehe Kapitel 4.6 Geschäftsfortführungsplanung) aktiviert werden?
- Unter welchen Voraussetzungen wird die Stabsarbeit beendet und die BAO schrittweise aufgelöst?

Beispiel:

Checkliste zum Konstituieren des Stabes:

- Wie werden die Stabsmitglieder alarmiert?
- Wie wird die Anfahrt und der Zugang zum Stabsraum sichergestellt?
- Wie wird der Ablageort der Ausstattung des Stabsraums dokumentiert, eventuell inklusive Hinweisen zum Zugang?
- Wo und wie wird der Aufbau der Ausstattung des Stabsraums dokumentiert?
- Welche Rollen sind für den Aufbau der Ausstattung des Stabsraums zuständig?
- Wie erfolgt die erste Lagebesprechung durch den Stab?

Checkliste zum Auflösen der BAO:

- Wodurch entscheidet es sich, wann die letzte Lagebesprechung durchgeführt wird?

- Wann beendet jede Rolle offiziell ihre Mitarbeit in der BAO?
- Wurden alle notwendigen Beschlüsse für den Störbetrieb getroffen?
- Ist die Maßnahmenverfolgung (auch für Aufgaben im Störbetrieb) vollständig dokumentiert bzw. durch wen wird diese in der AAO fortgeführt?
- Ist das Protokoll der Stabsarbeit vollständig, vertraulich und wiederauffindbar abgelegt?
- Wann und durch wen erfolgt der Rückbau des Stabsraums?

4.2.4.3 Schulung der Stabsmitglieder

Alle Stabsmitglieder, einschließlich der Stellvertreter, müssen für ihre Aufgaben und Zuständigkeiten im Notfall befähigt werden. Dies kann auf unterschiedliche Weise erreicht werden, z. B. durch Übungen, Trainings oder durch die reale Bewältigung eines Schadensereignisses.

Insbesondere bei unerfahrenen Personen, die ihre Rolle erst verinnerlichen müssen, ist es empfehlenswert zunächst die theoretischen Grundlagen der Notfallbewältigung zu schulen. Die **Grundlagenschulung** kann dazu folgende Aspekte beinhalten:

1. In welchen Phasen läuft eine Notfallbewältigung ab?
2. Warum gibt es eine BAO?
3. Wie interagieren die verschiedenen Rollen in der BAO miteinander?
4. Welche Rollen übernehmen die zu schulenden Personen darin?

Bei erfahrenen Personen, die über ein grundsätzliches Verständnis der Notfallbewältigung und der Besonderheiten einer BAO verfügen, bietet es sich hingegen an, zunächst die **Methoden und Regeln der Stabsarbeit** in ihrer Institution zu entwickeln, bevor die Stabsmitglieder darin geschult und trainiert werden. So wird sichergestellt, dass die Stabsmitglieder genau die Methoden und Abläufe verinnerlichen, die auch in der Institution angewendet werden sollen.

Weiter ist es empfehlenswert, verschiedene Schulungen für Stabsmitglieder anzubieten, die sich am jeweiligen Erfahrungsstand orientieren, z. B.:

- Schulung zu den institutionsspezifischen Aspekten der Notfallbewältigung und Stabsarbeit für neue Stabsmitglieder
- Rollenspezifische, praktische Trainings für einzelne Rollen innerhalb des Stabs (z. B. Visualisierer, Protokollanten)

Das **praktische Training zur Stabsarbeit** kombiniert inhaltliche und methodische Aspekte der Stabsarbeit. Ziel des Trainings ist es, dass die Rolleninhaber ihre individuellen Aufgaben verstehen und die für ihre Aufgaben festgelegten Methoden und das Notfallhandbuch sicher anwenden können. Im Training werden die rollenspezifischen Aufgaben detailliert erläutert und im Rahmen kurzer Trainingsszenarien durch die Teilnehmer praktisch angewendet. Entsprechend sollte das Training durch einen erfahrenen Trainer für Stabsarbeit moderiert und geleitet werden.

Hinweis:

Gerade, wenn sich das BCMS noch im Aufbau befindet, liegen häufig noch nicht ausreichend eigene Erfahrungen und Kenntnisse vor, um Schulungen, Trainings und Übungen selbstständig vorzubereiten und durchzuführen. In diesem Fall empfiehlt es sich, externe Fachexperten einzubeziehen oder Seminarangebote zu nutzen.

Mögliche weiterführende Schulungen und Trainings, unter anderem zur Protokollierung und Visualisierung sowie „Führung im Notfall“, können nach Bedarf zusätzlich eingeplant werden. Im Anschluss an diese Schulungen sollte eine Stabsübung durchgeführt werden, um die Fähigkeiten und Kenntnisse zu vertiefen und praktische Erfahrungen aufzubauen. Die hierzu erforderlichen Schritte sind im Kapitel 4.7.2 *Stabsübung* beschrieben. In der weiteren Entwicklung des BCMS können sich einzelne Aspekte zur Stabsarbeit verändern bzw. weiter konkretisieren. Daher sollten die Schulungsinhalte für die Stabsmitglieder regelmäßig geprüft und angepasst werden.

4.2.4.4 Festlegung eines Stabsraums

Eskaliert ein Ereignis zu einem Notfall, werden die Mitglieder des Stabs umgehend informiert und treffen sich an einem zuvor festgelegten Ort, dem Stabsraum. Der Stabsraum dient dem Stab als Arbeitsumgebung, an die besondere Anforderungen gestellt werden, die im Nachfolgenden näher erläutert werden.

Hinweis:

Je nach dem Bedarf und den baulichen Möglichkeiten der Institution kann es sich bei einem Stabsraum um genau einen Raum handeln oder verschiedene Bereiche umfassen. Verschiedene Bereiche bieten sich an, um die Arbeits-, Ruhe- und Besprechungsphasen örtlich voneinander zu trennen. Nachfolgend wird nur von Stabsraum gesprochen, ohne die Anzahl an Bereichen konkret festzulegen.

Erreichbarkeit und Zutritt

In einem Notfall muss der Stabsraum von allen Mitgliedern des Stabs in einem angemessenen Zeitraum erreichbar sein. Daher muss der Stabsraum auch außerhalb der üblichen Arbeitszeiten jederzeit für diese zugänglich sein. Hierzu muss geprüft werden, welche Zutrittsregelungen bestehen oder benötigt werden. Die Stabsmitglieder sowie ihre Stellvertreter müssen mit den entsprechenden Zutrittsmitteln und -rechten für alle notwendigen Räumlichkeiten ausgestattet sein. Da eine Lageänderung im Notfall jederzeit zu einer situativen Erweiterung des Stabs führen kann, sollten die Zutrittsregelungen für neue Mitglieder des Stabs zeitnah erweitert werden können. Anhand von Begehungen oder Stabsübungen sollte überprüft werden, ob der Stabsraum für alle Mitglieder jederzeit zugänglich ist, damit es im Notfall nicht zu unnötigen Verzögerungen kommt.

Verfügbarkeit

Ein Stabsraum sollte so geplant werden, dass er im Notfall verfügbar ist. Dies kann dadurch erreicht werden, dass ein Raum als dedizierter Stabsraum festgelegt wird und damit allein für diesen Zweck zur Verfügung steht. Aufgrund mangelnder räumlicher Ressourcen und fehlender finanzieller Mittel kann ein Stabsraum häufig jedoch nicht dauerhaft für diesen Zweck allein vorgehalten werden, sondern wird als Besprechungsraum oder Ähnliches im Normalbetrieb genutzt. In diesem Fall muss durch entsprechende organisatorische Regelungen sichergestellt werden, dass in einem Notfall der Einsatz als Stabsraum immer Vorrang hat und anderweitig geplante Einsatzzwecke, wie Besprechungen oder Veranstaltungen, gegebenenfalls verdrängt werden. Außerdem sollte verhindert werden, dass der Raum bei Zweitnutzung zu stark verändert oder wichtige Ausstattung entfernt wird.

Ein weiterer Aspekt der Verfügbarkeit ist das Szenario, dass der Stabsraum vom Schadensereignis selbst betroffen ist und damit nicht wie vorgesehen genutzt werden kann. Aus diesem Grund sollte ein alternativer Raum an einem Ausweichstandort definiert werden. Dies kann z. B. ein ähnlicher Raum in einem Gebäude mit ausreichendem Abstand sein, aber auch ein Konferenzcenter, ein Hotelbesprechungsraum etc. Der Ausweichstandort sollte möglichst vergleichbare Gegebenheiten bieten wie der Hauptstabsraum. Zudem ist es empfehlenswert, dass der Stabsraum gegen Ausfälle der Grundversorgung abgesichert wird, z. B. durch eine eigene Notstromversorgung.

Liegen keine geeigneten alternativen physischen Räume vor, kann eine Sekundärlösung auch aus einem virtuellen Konferenzraum bestehen, der z. B. über ein Webkonferenz- oder ein Krisenmanagement-Tool bereitgestellt wird. Hierbei muss die Vertraulichkeit in der Planung mitberücksichtigt werden.

Größe

Die Größe des Stabsraums sollte nicht zu knapp bemessen sein, da keine abschließende Vorhersage über die Anzahl der Stabsmitglieder gemacht werden kann, die für ein bestimmtes Notfallereignis hinzugezogen werden. Es ist empfehlenswert, dass der Raum über ausreichend Arbeitsplätze, über Bereiche für Visualisierungstechnik und über abgetrennte Besprechungszonen verfügt.

Einhaltung von Sicherheitsanforderungen

Für alle definierten Stabsräume muss sichergestellt werden, dass die geltenden Sicherheitsanforderungen der Institution, z. B. im Umgang mit vertraulichen Informationen, auch im Notfall eingehalten werden. Es ist grundsätzlich empfehlenswert, dass der Stabsraum nicht von außen und von angrenzenden Flächen aus einsehbar ist.

4.2.4.5 Ausstattung des Stabsraums

Neben den räumlichen Anforderungen an den Stabsraum ist es im Notfall entscheidend, dass dieser mit allen erforderlichen Materialen und Technik ausgestattet ist, damit der Stab schnell arbeitsfähig ist. Die Ausstattung sollte regelmäßig auf ihre Vollständigkeit, Aktualität oder Funktionsfähigkeit hin überprüft werden. Dies gilt insbesondere, wenn der Stabsraum im Normalbetrieb anderweitig genutzt wird. Die notwendige Ausstattung für die Notfallbewältigung lässt sich in die folgenden Kategorien unterteilen:

- Kommunikationsausstattung
- Visualisierungsausstattung
- Battleboxen mit BCM-Equipment und -Dokumentation (siehe auch das Hilfsmittel *Weiterführende Aspekte zur Bewältigung*)

Kommunikationsausstattung

Der Raum, in dem der Stab sich bespricht, sollte weitgehend frei von Kommunikationsausstattung gehalten werden. Zum einen handelt es sich um einen Raum, der im Schwerpunkt für die Besprechungsphasen des Stabs genutzt wird, in denen keine ständige Kommunikation nach außen notwendig ist. Zum anderen stört jede Kommunikation, egal ob Telefongespräche oder die Bearbeitung von E-Mails, die konzentrierte Arbeitsumgebung. Es ist jedoch empfehlenswert, ein zentrales Konferenztelefon („Telefonspinne“) als Grundausstattung im Stabsraum vorzuhalten. Hiermit können Mitglieder des Stabs oder Fachexperten, die nicht vor Ort sind, telefonisch zu den Besprechungen hinzugezogen werden. Zudem ist es hilfreich ein Notfall-Laptop vorzuhalten, welches autark funktioniert und auf dem unter anderem die BCM-Dokumentation hinterlegt ist. Je nach eingesetzter Methodik zur Dokumentation und Visualisierung kann es erforderlich sein, weitere Laptops oder PC-Arbeitsplätze vorzusehen.

Im Gegensatz zu der stark reduzierten Kommunikationsausstattung des Stabsraums sollte ein zusätzlicher Raum in der Nähe dauerhaft mit allen etablierten Kommunikationskanälen ausgestattet sein. Dieser sollte entsprechend vorbereitet werden. Dazu zählen:

- Telefonie (mehrere Leitungen, unter Umständen auch Videotelefonie)
- E-Mail (z. B. durch vorbereitete Funktionspostfächer für einzelne Rollen)
- Fax
- Funk, Satellitentelefonie oder kryptografische Kommunikationsinfrastruktur

Dieser Raum sollte ebenfalls die räumlichen Anforderungen an die Verfügbarkeit und Sicherheit erfüllen, wie der Stabsraum selbst. Falls ein zweiter Raum aus wirtschaftlichen oder anderen Gründen nicht bereitgestellt werden kann, kann auch der Stabsraum entsprechend ausgestattet werden. In diesem Fall sollte in der Stabsarbeit strikt zwischen Besprechungsphasen ohne Außenkommunikation und Arbeitsphasen, in denen die Kommunikation aus dem Stab heraus erfolgt, unterschieden werden. Eingehende Meldungen und Anrufe während einer Besprechungsphase sollten entsprechend durch die Stabsassistenz angenommen werden.

Hinweis:

Bei der Planung muss unbedingt auf Ausfallsicherheit und Redundanz der Ausstattung geachtet werden, damit die Notfallbewältigung nicht durch den Ausfall eines Kommunikationsmittels zusammenbricht. Dies kann z. B. neben dem normalen Telefon ein Notfallmobiltelefon oder ein Laptop mit SIM-Karte sein.

Visualisierungsausstattung

Im Stabsraum sollten ausreichende und geeignete Materialien zur Visualisierung der Lage, also für das *Lagebild*, vorgehalten werden. Neben ortsfesten Materialien, wie Beamern, digitalen Tafeln, Monitoren und Whiteboards, sollte auch folgende Ausstattung im Vorfeld beschafft werden:

- Moderationskoffer mit Visualisierungsflächen (z. B. Flipcharts)
- Vorlagen, um unter anderem folgende Inhalte darzustellen (nicht abschließende Aufzählung)
    - Stand der Visualisierung (Datum, Uhrzeit)
    - nächste Sitzung (Datum, Uhrzeit, Gäste)
    - Kartenmaterial (Gebietskarte, Werkgelände etc.)
    - Aufgabenliste (Was? Durch wen? Bis wann?)
    - Zeitstrahl (bisherige Ereignisse und Prognose im fortlaufenden Lagebild)
    - Schadensübersicht und -schwerpunkte (Wo? Wann? Was und wer?)
    - Besetzung der BAO (falls erforderlich mit Schichtplan)
    - Kommunikationsübersicht (Was? Wer? Wann? Mit wem?)

Battlebox

Im Rahmen der Stabsarbeit greifen die verschiedenen Rollen auf unterschiedliche Pläne, Checklisten und Hilfsmittel zurück, insbesondere auf das Notfallhandbuch. Sämtliche für den Notfall relevante BCM-Dokumentation sollte daher einerseits im Stabsraum und andererseits zentral zugänglich vorgehalten werden. So bleibt sie auch verfügbar, z. B. bei physischer Zerstörung des Stabsraums, der Dokumentation an sich oder des Notfall-Laptops. Diese doppelte Vorhaltung kann z. B. durch weitere physische oder digitale Kopien erfolgen. Hierbei muss auf Aktualität und die Anforderungen der Informationssicherheit und des Datenschutzes geachtet werden. So müssen papierhafte Dokumente bei jeder Aktualisierung der Dokumentation neu ausgedruckt und an den Ablageorten ausgetauscht werden. Andererseits sind sie auch ohne Vorhandensein von Strom oder IT verfügbar und einsetzbar. Elektronische Informationen haben wiederum den Vorteil, dass sie schneller aktualisiert bzw. ausgetauscht werden können. Ergänzend zur oben genannten BCM-Dokumentation kann es hilfreich sein, eine Checkliste im Stabsraum zu hinterlegen, die erläutert, wie die Materialien

und Technik in Betrieb genommen und genutzt werden. Zusätzlich dazu können die Checklisten im Anhang des Notfallhandbuchs hinterlegt werden, damit im Bedarfsfall eine Kopie verfügbar ist.

Beispiel:

Die Checkliste „Einrichtung des Stabsraums“ kann im Detail beschreiben, welche Tätigkeiten erforderlich sind und wer dafür zuständig ist.

Mögliche Tätigkeiten können sein:

- Raum aufschließen und lüften
- Visualisierungsflächen vorbereiten, wie z. B. Maßnahmenverfolgung oder Ereigniszeitstrahl
- Tische und Stühle U-förmig in Richtung Visualisierungsflächen aufstellen
- Namenskarten entsprechend des Sitzplans aufstellen
- BCM-Dokumentation sortiert nach den Rollen im Raum verteilen
- Telefonkonferenzschaltung bereitstellen
- Kommunikationsmittel und Technik auf Einsatzfähigkeit testen
- Verpflegung und Getränke bereitstellen

4.2.4.6 Freigabe durch die Institutionsleitung

Die erarbeiteten, abgestimmten und dokumentierten Aspekte zur Stabsarbeit sowie nachfolgend zur Alarmierung und Eskalation (siehe Kapitel 4.2.2 *Detektion, Alarmierung* und Eskalation), sollten der Institutionsleitung vorgestellt und durch diese freigegeben werden. Dies stellt sicher, dass die Institutionsleitung diese wichtigen Aspekte der Notfallbewältigung beeinflussen und die erforderlichen personellen und finanziellen Ressourcen freigeben kann. Insbesondere die zentrale Entscheidungsinstanz im Alarmierungsprozess muss durch die Institutionsleitung freigegeben werden. Anschließend müssen die hierfür erforderlichen Maßnahmen umgesetzt und im Maßnahmenplan nachverfolgt werden (siehe Kapitel 4.8 *Weiterentwicklung des BCMS*).

4.2.5 Notfallkommunikation

Wie die Institution im Notfall wahrgenommen wird und ob Vertrauen in die Notfallbewältigung gesetzt wird, hängt im Wesentlichen auch davon ab, wie gut die Notfallkommunikation gelingt. Daher muss die Notfallkommunikation im Vorfeld gut vorbereitet und geplant werden. Dabei ist es wichtig, dass in der Institution präventiv überlegt wird, wann Meldungen an die Mitarbeiter und an externe Interessengruppen erforderlich sind und wie die externe Notfallkommunikation kontrolliert werden kann, um Reputationsschäden zu vermeiden. Weitere Informationen zur Notfallkommunikation können Hilfsmittel *Weiterführende Aspekte zur Bewältigung* entnommen werden.

4.2.5.1 Allgemeine Regelungen zur Kommunikation

Aus den zuvor genannten Gründen ist die Notfallkommunikation einer der zentralen Erfolgsfaktoren in der Notfallbewältigung. Sowohl die interne als auch externe Kommunikation bedarf einer systematischen Vorbereitung. Für die Rolle Kommunikation sollten im Vorhinein verbindliche Regeln für folgende Aufgaben definiert werden:

- interne Kommunikation (Was dürfen oder müssen die Mitarbeiter wann erfahren?)
- externe Kommunikation durch Mitarbeiter (Was dürfen die Mitarbeiter wann und wie gegenüber der Presse und in sozialen Medien äußern und was nicht?)

- externe Kommunikation durch Rolle Kommunikation (Was soll die Rolle Kommunikation wann und wie gegenüber der Presse und in sozialen Medien bekannt geben?)
- Regelungen für den Kontakt mit Polizei und anderen Behörden sowie Hilfsorganisationen
- Meldepflichten der Institution, die sich aus einem Notfall ergeben
- Regelungen zum Medienmonitoring

Um im Notfall alle Interessengruppen auf geeignetem Weg und innerhalb einer angemessenen Zeit zu erreichen, müssen die Möglichkeiten zur Kommunikation bekannt und die Kommunikationstechnik einsatzbereit sein. Dies umfasst:

- Ausfallsicherheit (z. B. Notstrom), Redundanz (z. B. Ersatz-TK-Anlage) und alternative Kommunikationsmittel
- Schutzmaßnahmen bei vertraulicher Kommunikation
- Berechtigungen zur Nutzung der Kommunikationstechnik

Ferner sollten die anzuwendenden Kommunikationskanäle (z. B. Telefon, E-Mail, Chat, Webseiten, Fax) und Medienformate (z. B. Pressemitteilung, Pressekonferenz, Stellungnahme auf der Webseite oder über soziale Medien) vorab festgelegt werden. Sofern innerhalb der Institution mehr als eine Person für die Notfallkommunikation zuständig ist, müssen die jeweiligen Aufgaben und Zuständigkeiten innerhalb des Notfallkommunikationsteams festgelegt und dokumentiert werden, damit diese Arbeit effektiv koordiniert werden kann.

4.2.5.2 Interne Kommunikation

Eine kontinuierliche interne Notfallkommunikation ist entscheidend, um Unsicherheit unter den Mitarbeitern während eines Notfalls zu minimieren. Durch eine sachliche interne Notfallkommunikation soll das Vertrauen geschaffen werden, dass die Institutionsleitung und die BAO in der Lage ist, die Situation zu kontrollieren. Es ist oft nicht notwendig, dass die Mitarbeiter jedes Detail des Notfallereignisses kennen. Falls eine Information jedoch die persönliche Situation oder die Sicherheit betrifft, sollte diese in jedem Fall kommuniziert werden. Wenn die Mitarbeiter frühzeitig und angemessen in die Notfallbewältigung einbezogen werden, steigt deren Bereitschaft, erforderliche Maßnahmen umzusetzen und mit Informationen sorgsam umzugehen.

Zudem sollten relevante Informationen im Zusammenhang mit dem Status der Notfallbewältigung insbesondere für die Mitarbeiter bereitgestellt werden, die in Kontakt mit externen Interessengruppen stehen, z. B. Kunden, Behörden, Dienstleister.

Hinweis:

In der Praxis hat es sich bewährt, dass alle Mitarbeiter zeitlich mindestens dieselben Informationen erhalten wie die allgemeine Öffentlichkeit. Das bedeutet, dass die Informationen aus der externen Notfallkommunikation auch intern kommuniziert werden sollten. Somit wird vermieden, dass Mitarbeiter erst durch Medien über das Notfallereignis selbst oder über Neuigkeiten in dessen Zusammenhang erfahren und sich dadurch vernachlässigt fühlen. Außerdem wird Gerüchten und Mutmaßungen vorgebeugt. Gleichzeitig gilt: Informationen, die auf keinen Fall nach außen kommuniziert werden dürfen, sollten in der Regel auch nicht intern an alle Mitarbeiter kommuniziert werden.

4.2.5.3 Externe Kommunikation

In jedem Notfallszenario sind diverse Interessengruppen direkt oder indirekt involviert, welche die Institution in Bezug auf die Kommunikation berücksichtigen muss. Typische Beispiele hierfür sind Journalisten, Medien, Kunden, Dienstleister, Aufsichtsbehörden, Polizei und Angehörige von Mitarbeitern.

Die externe Kommunikation hat die Aufgabe, alle relevanten externen Interessengruppen adressatengerecht und unter Beachtung der Grundsätze für die Notfall- und Krisenkommunikation zu informieren. Oberstes Ziel ist es, die Kommunikation zu kontrollieren, um Reputationsschäden zu minimieren. Für die externe Notfallkommunikation bieten sich z. B. folgende Kanäle an:

- E-Mail
- Telefon
- Notfall-Hotline
- Website der Institution mit Informationen über den Notfall und FAQs
- alternative Notfall-Website („Dark Site“)
- Public Relations Agentur
- Soziale Medien
- persönliches Interview
- Fernseh- oder Radio-Interview
- Pressemitteilung
- Pressekonferenz

Für mögliche Presseanfragen sollte eine Person sowie ein Stellvertreter als Notfallsprecher namentlich benannt und innerhalb der Institution sowie extern veröffentlicht werden. Dies stellt eine einheitliche und offizielle externe Kommunikation sicher.

Die externe Notfallkommunikation begrenzt sich nicht auf die einseitige Kommunikation der Institution mit Dritten sowie der Öffentlichkeit, sondern sollte auch die Kommunikation Dritter untereinander betrachten. Dies betrifft vor allem die Medienberichterstattung. Notfälle, die durch die Medien aufgegriffen werden, können eine kritische Berichterstattung nach sich ziehen, die sich schnell verbreiten kann und durch Diskussionen in sozialen Medien weiter verschärft wird. Es ist daher zum Schutz der Reputation der Institution empfehlenswert, dass auch im Notfall situativ Medien beobachtet werden. So können kommunikative Gegenmaßnahmen frühzeitig eingeleitet werden.

4.2.6 Störbetrieb und Deeskalation

Ist das Schadensereignis überwunden, sollte der Stab den Notfall offiziell für beendet erklären und diese Entscheidung innerhalb der Institution kommunizieren. Hierzu können die gleichen Kommunikationskanäle verwendet werden wie beim Ausrufen des Notfalls. Dies stellt sicher, dass allen Beteiligten und Betroffenen bewusst ist, dass nun wieder die Prozesse des Normalbetriebs greifen.

Störbetrieb

Abhängig von der Art und dem Ausmaß des Schadensereignisses kann es sein, dass zwar die Ursachen und Auswirkungen des Ereignisses vollständig unter Kontrolle gebracht wurden, aber noch kein Normalzustand für die zeitkritischen Prozesse erreicht ist. Die Institution befindet sich übergangsweise im sogenannten Störbetrieb, der dadurch gekennzeichnet ist, dass die Wiederherstellungsmaßnahmen oder Nacharbeiten noch nicht abgeschlossen sind, sodass noch nicht von einem Normalbetrieb gesprochen werden kann.

Beispiel:

Ein IT-System muss inklusive der Daten vollständig wiederhergestellt sein, bevor der Normalbetrieb erreicht werden kann. Ein Gebäude kann je nach Schadensszenario teilweise, z. B. etagenweise, wiederhergestellt werden. Der Normalbetrieb kann darüber schrittweise erreicht werden. In dieser Zeit befindet sich jedoch die Institution im Störbetrieb, bis das ganze Gebäude wiederhergestellt ist.

Hierzu kann eine Checkliste mit konkreten Prüfpunkten oder zu treffenden Entscheidungen für die Rückführung in den Normalbetrieb entwickelt werden. Neben den direkt ersichtlichen Aspekten, wie z. B. der Reihenfolge der wieder in den Normalbetrieb zu versetzenden Geschäftsprozesse, sollten auch die durch den Notbetrieb entstandenen Folgen betrachtet werden.

Beispiel:

Checkliste zur Rückführung in den Normalbetrieb:

- Wie und wann wird die BAO aufgelöst und in die normale Linienorganisation überführt?
- Welche Arbeitsrückstände sind entstanden und wie können diese am besten abgearbeitet werden?
- Durch wen erfolgt die interne und externe Kommunikation für die Dauer des Störbetriebs?
- Wie, durch wen und in welchen zeitlichen Intervallen werden die Mitarbeiter über den Fortschritt der Rückführung in den Normalbetrieb informiert?
- An wen sollen die Organisationseinheiten in dieser Zeit ihre Erkenntnisse und Fortschritte melden? Dies umfasst z. B.:
    - Schäden oder Verluste durch den Notbetrieb,
    - aktueller Stand der Arbeitsrückstände sowie
    - erwartete Dauer im Störbetrieb bis zur Rückkehr in den Normalbetrieb.

Hierbei ist es empfehlenswert, dass die Organisationseinheiten bereits präventiv einschätzen und dokumentieren, ob Arbeitsrückstände im Notfall zu erwarten sind und welche Optionen sie haben, diese abzuarbeiten. Die Informationen sollten im Geschäftsfortführungsplan dokumentiert werden (siehe Kapitel 4.6.2 *Erstellung der GFPs*).

Deeskalation und Auflösen der BAO

Üblicherweise erreichen in der Praxis die betroffenen Organisationseinheiten den Normalbetrieb schrittweise. Auch die BAO kann schrittweise aufgelöst werden, wenn es die jeweiligen Umstände erforderlich machen. Jedoch sollte zu einem spezifischen Zeitpunkt an alle Interessengruppen kommuniziert werden, wenn der Notfall für beendet erklärt wird. Dieser Zeitpunkt wird als Deeskalation des Ereignisses definiert. Ab diesem Zeitpunkt gelten wieder die üblichen Zuständigkeiten der AAO.

Für die Deeskalation sollten geeignete Kriterien und Zuständigkeiten definiert werden. Hierbei kann sich bei der Ausgestaltung der Kriterien an den Anforderungen der Eskalation orientiert werden (siehe Kapitel 4.2.2.2 *Einstufung der Ereignismeldung und Entscheidung*). Folgende Fragen können hilfreich sein, um die Kriterien für die Deeskalation festzulegen:

- Sind sämtliche Ereignisse bewältigt, die eine BAO benötigen?
- Können die restlichen Probleme vollständig durch die AAO gelöst werden?
- Kann eine erneute Verschärfung der Lage bei einer schrittweisen Überführung in den Normalbetrieb ausgeschlossen werden?
- Kann die interne und externe Kommunikation wieder vollständig durch die AAO erfolgen?

4.2.7 Analyse der Bewältigung

Der Verlauf der Bewältigung sollte analysiert werden, um aus Notfällen und Krisen zu lernen. Nur durch eine strukturierte Analyse kann ermittelt werden, was gut funktioniert hat und an welchen Stellen Optimierungsbedarf besteht. Daraus kann abgeleitet werden, was noch präventiv getan werden sollte, damit die Bewältigung sowie die Resilienz der Institution weiter verbessert werden können.

Der BCMB sollte durch entsprechende Vorgaben sicherstellen, dass im Nachgang die Verläufe jedes Notfalls und jeder Krise untersucht werden, inwieweit Korrekturbedarfe oder Verbesserungsmöglichkeiten für das BCMS abgeleitet werden können. Der BCMB sollte diese Analyse der Bewältigung zentral regeln, z. B. in Form von Workshops mit den Beteiligten. Diese Workshops sollten möglichst zeitnah zum Notfallereignis erfolgen. Weitere Informationen zur Analyse der Bewältigung können dem Hilfsmittel *Weiterführende Information zur Bewältigung* („hot wash-up“) entnommen werden. Die Workshops können anhand eines vorab festgelegten Frageschemas aufgebaut sein, sodass die Informationen vollständig abgefragt werden können.

Beispiel:

Fragenkatalog – Analyse der Bewältigung

- Wie kam es zu dem Ereignis?
- Welche Auswirkungen hatte das Ereignis?
- Wie schnell und wie effektiv erfolgte die Reaktion auf das Ereignis?
- Welche Elemente der BAO haben gut funktioniert und welche weniger gut?
- Gab es Unterschiede zu der geplanten Notfallbewältigung?
- Waren alle zeitkritischen Geschäftsprozesse und Ressourcen bekannt?
- Welche Notfallmaßnahmen wurden ergriffen bzw. neu eingeführt?
- Wie gut haben die vorbereiteten Notfallpläne funktioniert?
- Wurden Notfallpläne neu erstellt oder angepasst?
- Wie gut hat die Notfallkommunikation funktioniert?

Ferner sollte durch entsprechende Vorgaben sichergestellt werden, dass die Ergebnisse der Analyse dokumentiert und an die Institutionsleitung berichtet werden. Falls bei der Analyse konkrete Mängel und Verbesserungsmöglichkeiten identifiziert werden, können so zeitnah Korrektur- und Verbesserungsmaßnahmen initiiert werden. Hierbei stehen Verbesserungsbedarfe der Prozesse, Methoden und Hilfsmittel im BCM im Fokus, die in der Weiterentwicklung des BCMS berücksichtigt werden können (siehe Kapitel 4.8 *Weiterentwicklung des BCMS*). Es geht in der Mängel-Analyse nicht darum, mögliche Fehlentscheidungen einzelner Personen zu bewerten.

4.3 Voranalyse

In der Initiierung des BCM wurde durch die Institutionsleitung entschieden, welcher Geltungsbereich und welcher Zeitraum durch das BCM abgesichert werden soll (siehe Kapitel *3.1.2 Geltungsbereich*). Zu diesem frühen Zeitpunkt konnte jedoch noch keine Aussage darüber getroffen werden, wie viele Geschäftsprozesse aufgrund des gewählten Geltungsbereichs im Rahmen einer Business Impact Analyse (BIA) untersucht werden müssen (siehe Kapitel 4.4 *Business Impact Analyse (BIA)*). Mitunter kann daher eine hohe Anzahl zu berücksichtigender Geschäftsprozesse den weiteren Fortschritt im BCM deutlich verlangsamen und somit dem Ziel eines Reaktiv-BCMS, schnellstmöglich eine Reaktionsfähigkeit zu erlangen, entgegenstehen. Je nachdem, wie viele Geschäftsprozesse im Rahmen der BIA als zeitkritisch identifiziert werden, reichen zudem die initial festgelegten Ressourcen unter Umständen nicht aus, um diese adäquat absichern zu können. Die Voranalyse

hat daher das Ziel, bereits vor Beginn der BIA eine Vorauswahl zu treffen und auf die potenziell zeitkritischsten Geschäftsprozesse einzugrenzen.

Hinweis:

Auf Anhieb mag die Voranalyse aufwendig und redundant zur BIA wirken. Aufgrund des reduzierten Detailgrads und der vereinfachten Fragestellung kann damit aber schnell und effektiv der Analysebereich der BIA eingegrenzt werden, was zu einer deutlichen Aufwands- und Zeitersparnis in den nachfolgenden BCM-Prozessschritten führt.

Es gibt viele Möglichkeiten eine Vorauswahl zu treffen, um den Aufwand in der BIA zu reduzieren. Für ein Reaktiv-BCMS ist es empfehlenswert, die Vorauswahl anhand der Organisationseinheiten zu treffen, die erwartungsgemäß die zeitkritischsten Geschäftsprozesse abdecken. Die meisten Institutionen verfügen über ein Organigramm, das die Aufbauorganisation hierarchisch wiedergibt, z. B. anhand von Abteilungen, Fachbereichen oder Unterabteilungen und Referaten oder Teams. Zudem stellt das Organigramm eine nachvollziehbare Datengrundlage für die Voranalyse dar, da die Organisationseinheiten systematisch über die Hierarchie-Ebenen betrachtet werden können und die zu befragenden Personen in der Regel mit dem Organigramm vertraut sind. Sollte die Institution über keine hierarchischen Strukturen in ihrer Aufbauorganisation verfügen (z. B. agile Organisationen) kann die Vorauswahl anhand anderer hierarchischer Aspekte getroffen werden, z. B. Geschäftsprozesse, Produkte, Services oder Standorte.

Hinweis:

Das Ergebnis der Voranalyse erlaubt lediglich eine pauschale Aussage darüber, ob eine Organisationseinheit zeitkritisch ist oder nicht. Konkrete Aussagen über die möglichen Schäden bei Ausfall der Geschäftsprozesse einer Organisationseinheit können erst mit Hilfe der BIA getroffen werden. Somit ist auch eine Notfallplanung erst möglich, wenn die Ergebnisse der BIA vorliegen.

Abbildung 19 verdeutlicht die empfohlenen Schritte, um eine Voranalyse basierend auf den Organisationseinheiten durchzuführen. Die einzelnen Schritte werden in den nachfolgenden Unterkapiteln näher erläutert. Nachdem das Ergebnis der Voranalyse durch die Institutionsleitung freigegeben wurde, kann mit der BIA anhand der getroffenen Vorauswahl begonnen werden.

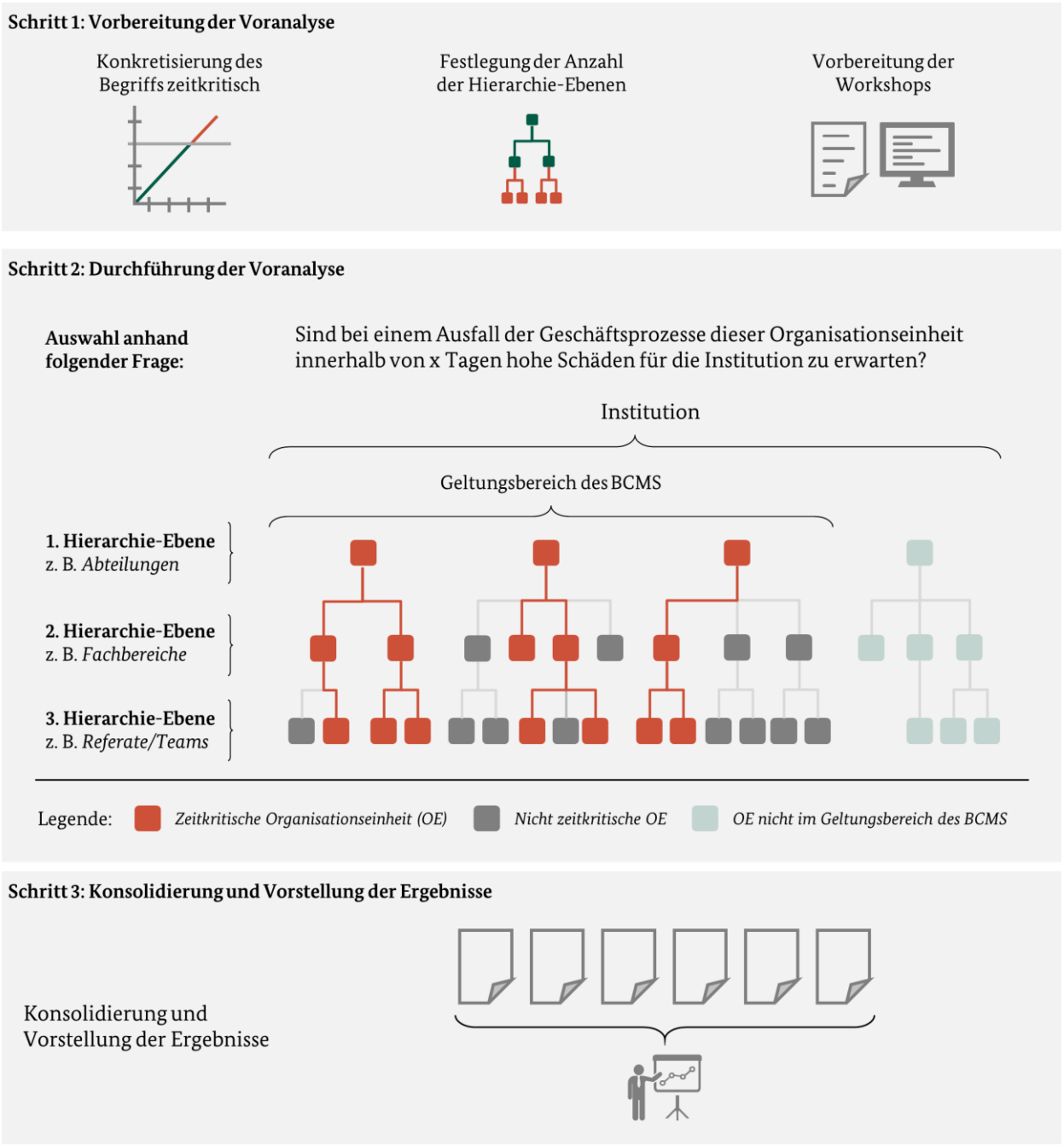

Abbildung 19: BCM-Prozessschritte der Voranalyse

Hinweis:

Die Herausforderung besteht darin, einerseits den Aufwand innerhalb der BIA zu reduzieren, indem in der Voranalyse möglichst effizient potenziell zeitkritische Organisationseinheiten im Geltungsbereich des BCMS herausgefiltert werden. Andererseits entstehen durch die Voranalyse Bereiche, die in der Absicherung nicht betrachtet werden, da für die als nicht zeitkritisch eingestuften Organisationseinheiten keine systematische Schadensbewertung im Rahmen der BIA durchgeführt wird und so zeitkritische Geschäftsprozesse unentdeckt bleiben könnten. Die Ergebnisse der Voranalyse haben damit weitreichende Konsequenzen für alle weiteren Schritte des BCM. Entsprechend muss die Institutionsleitung in der Voranalyse aktiv eingebunden sein, um das damit einhergehende Risiko der unberücksichtigten Bereiche tragen zu können.

4.3.1 Vorbereitung der Voranalyse

Eine effektive **Vorbereitung der Voranalyse** schafft die Voraussetzungen dafür, dass

- die Voranalyse möglichst effizient, valide und vergleichbar durchgeführt werden kann,
- die Teilnehmer optimal auf die Fragestellungen vorbereitet werden sowie
- die Ergebnisse möglichst nahtlos in der BIA weiter genutzt werden können.

Die Methodik der Voranalyse sollte festgelegt und die Voranalyse organisatorisch vorbereitet werden. Anhand der Methodik wird sichergestellt, dass die Voranalyse nachvollziehbar, einheitlich und wiederholbar durchgeführt werden kann. Eine gute Vorbereitung beschleunigt den Ablauf und reduziert die Aufwände für alle weiteren Beteiligten. Idealerweise führt der BCMB die Voranalyse durch, um selbst einen Überblick zu erhalten und die Ergebnisse vergleichbar zu halten.

Er kann vorbereitende Tätigkeiten ganz oder teilweise an weitere Rollen im BCM delegieren, z. B. an lokale BCMB oder ein Notfallvorsorgeteam (siehe Kapitel *3.2.2 Definition der BCM-Aufbauorganisation*). Die Aufgaben in der Vorbereitung der Voranalyse werden in den nachfolgenden Unterkapiteln näher erläutert. Die Kapitel folgen einer logischen Reihenfolge, jedoch können sich verschiedene darin beschriebene Aufgaben in der Praxis zeitlich überlagern.

4.3.1.1 Konkretisierung des Begriffs zeitkritisch

Unabhängig, ob eine Organisationseinheit in der Voranalyse oder ein Geschäftsprozess in der BIA untersucht wird, muss die Frage, wann etwas als *zeitkritisch* gilt, einheitlich in der Institution beantwortet werden können. Daher müssen die Parameter aus der eingangs formulierten Leitfrage (siehe Abbildung 19) durch den BCMB definiert und mit der Institutionsleitung abgestimmt sein, bevor mit der Voranalyse begonnen wird. Abbildung 20 stellt in einem Beispiel die nachfolgend erläuterten Parameter der Voranalyse in den Zusammenhang mit der Leitfrage.

Beispiel:

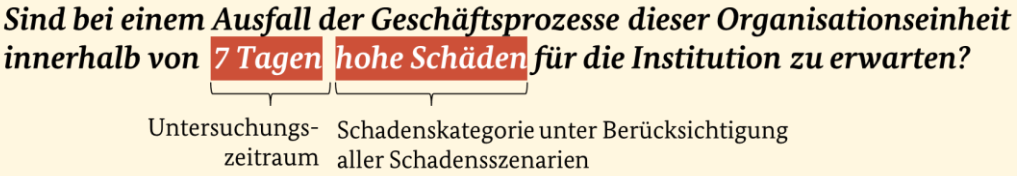

Abbildung 20: Zusammenhang zwischen Leitfrage und Parametern der Voranalyse

Untersuchungszeitraum

Der Untersuchungszeitraum legt fest, für welche mögliche Ausfalldauer ein Schaden für die Institution bewertet werden soll. Der Untersuchungszeitraum repräsentiert das „***innerhalb von x Tagen***“ in der eingangs genannten Leitfrage. Er sollte kleiner oder gleich dem abzusichernden Zeitraum des BCMS sein (z. B. 14-30 Tage gemäß Kapitel *3.1.2 Geltungsbereich*), jedoch einen relativ kurzen Zeitraum umfassen, z. B. 7 Tage oder kürzer, um die Vorauswahl auf die zeitkritischsten Organisationseinheiten einzuschränken und so den Aufwand in der BIA deutlich zu reduzieren.

Schadensszenarien

Um die Schäden besser einschätzen zu können, werden die potenziellen Auswirkungen von Ausfällen anhand von Schadensszenarien untersucht. Die Schadensszenarien sollten sich an den Rahmenbedingungen der Institution ausrichten und sowohl direkte als auch indirekte Schäden berücksichtigen. Direkte Schäden umfassen beispielsweise entgangene Gewinne, Verluste durch Rechtsfolgen sowie unmittelbare Auswirkungen auf

Leib und Leben oder die persönliche Unversehrtheit von Menschen. Indirekte Schäden berücksichtigen z. B. Verluste durch entgangene Aufträge, Verlust an Marktanteil, Imageschäden oder negative Auswirkungen auf Dritte. Die Schadensszenarien sind sowohl für die Voranalyse als auch für die BIA relevant. Die Schadensszenarien können daher in der anschließenden BIA ohne Änderungen übernommen werden.

Innerhalb der Voranalyse und BIA eines Reaktiv-BCMS sollten die folgenden Schadensszenarien berücksichtigt werden, wie sie aus dem BSI Standard 200-2 bekannt sind:

- Beeinträchtigung der Aufgabenerfüllung,
- Verstoß gegen Gesetze, Vorschriften und Verträge,
- negative Innen- und Außenwirkung (Imageschaden),
- finanzielle Auswirkungen sowie
- Beeinträchtigung der persönlichen Unversehrtheit.

Hinweis:

Auch Behörden können durch einen Ausfall des Geschäftsbetriebs von finanziellen Auswirkungen betroffen sein. Neben Strafzahlungen aufgrund nicht eingehaltener Fristen gehören hierzu Ausgaben für nicht einsatzfähige Ressourcen und Personal oder entgangene Beiträge, Forderungen oder Steuern. Im Regelfall sollten diese finanziellen Schäden für Behörden keine existenzbedrohenden oder nicht tolerierbaren Auswirkungen haben. Um mögliche Ausnahmefälle zu identifizieren, wird empfohlen, die finanziellen Auswirkungen in der Schadensbewertung dennoch mit zu berücksichtigen und gegebenenfalls als nicht relevant zu markieren.

Schadenskategorien

Die festgelegten Schadensszenarien erlauben noch keine Schadensbewertung, da hierbei für den Anwender nicht klar ersichtlich ist, wonach er den Schaden bewerten soll. Zu diesem Zweck muss für alle Schadensszenarien anhand verschiedener Schadenskategorien definiert werden, welcher mögliche Schaden eintreten kann (**Schadenspotenzial**). Die Anzahl an Schadenskategorien muss für alle Schadensszenarien einheitlich definiert werden. Üblicherweise wird mit drei bis fünf Schadenskategorien gearbeitet.

Für den Aufbau eines Reaktiv-BCMS werden beispielshaft die nachfolgend aufgeführten Schadenskategorien zugrunde gelegt:

1 - Gering

2 - Mittel

3 - Hoch

4 - Sehr hoch

Tabelle 10 erläutert beispielhaft, wie die Schadenskategorien je Schadensszenario konkretisiert werden können. Die Definitionen sollten individuell für die Institution angepasst werden. Die angepasste *Tabelle 10* kann gleichzeitig als Hilfsmittel eingesetzt werden, um bei der Durchführung von Voranalyse und BIA die Schadensbewertung zu unterstützen. Hierbei bietet es sich an, wie in der *Tabelle 10* aufgezeigt, die Schadensbewertungen gesammelt je Schadenskategorie aufzuführen, nicht je Schadensszenario.

Beispiel:

Schadens-kategorie	Erläuterung des Schadenspotenzials je Schadensszenario
1 - Gering	**Allgemeine Beschreibung:** Ausfall hat geringe, kaum spürbare Auswirkungen. • **Beeinträchtigung der Aufgabenerfüllung:** Der Geschäftsbetrieb wird unwesentlich beeinträchtigt. • **Verstoß gegen Gesetze, Vorschriften und Verträge:** Es wird nur in einem geringen Maß gegen interne Vorgaben und Anweisungen verstoßen. Verstöße führen zu keinen Konsequenzen. • **Negative Innen- und Außenwirkung (Imageschaden):** In Einzelfällen ist eine geringe, nicht nachhaltige Ansehensbeeinträchtigung zu erwarten. • **Finanzielle Auswirkungen:** Der finanzielle Schaden ist für die Institution unerheblich. • **Beeinträchtigung der persönlichen Unversehrtheit:** Eine Beeinträchtigung ist ausgeschlossen.
2 - Mittel	**Allgemeine Beschreibung:** Ausfall hat spürbare Auswirkungen. • **Beeinträchtigung der Aufgabenerfüllung:** Der Ausfall hat spürbare Auswirkungen auf den Geschäftsbetrieb. Mit Arbeitsrückständen ist zu rechnen. • **Verstoß gegen Gesetze, Vorschriften und Verträge:** Es wird ausschließlich gegen interne Vorgaben und Anweisungen verstoßen. • **Negative Innen- und Außenwirkung (Imageschaden):** Eine geringe Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten. • **Finanzielle Auswirkungen:** Der finanzielle Schaden ist für die Institution tolerabel. • **Beeinträchtigung der persönlichen Unversehrtheit:** Eine Beeinträchtigung ist unwahrscheinlich.
3 - Hoch	**Allgemeine Beschreibung:** Ausfall hat nicht tolerierbare Auswirkungen. • **Beeinträchtigung der Aufgabenerfüllung:** Der Geschäftsbetrieb ist massiv eingeschränkt. Arbeitsrückstände sind nur mit erhöhtem Arbeitsaufwand zu kompensieren. • **Verstoß gegen Gesetze, Vorschriften und Verträge:** Es wird gegen Gesetze verstoßen. Verstöße führen zu erheblichen Konsequenzen, z. B. hohe Bußgelder. Vertragsverletzungen führen zu hohen Konventionalstrafen oder Konsequenzen. • **Negative Innen- und Außenwirkung (Imageschaden):** Eine erhebliche, nachhaltige Ansehens- oder Vertrauensbeeinträchtigung ist intern und extern zu erwarten. • **Finanzielle Auswirkungen:** Der finanzielle Schaden ist für die Institution erheblich und nachhaltig spürbar. • **Beeinträchtigung der persönlichen Unversehrtheit:** Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden.

Schadens-kategorie	Erläuterung des Schadenspotenzials je Schadensszenario
4 - Sehr hoch	**Allgemeine Beschreibung:** Ausfall führt zu existentiell bedrohlichen Auswirkungen. • **Beeinträchtigung der Aufgabenerfüllung:** Der Ausfall hat fundamentale und langfristige Auswirkungen auf den Geschäftsbetrieb. Arbeitsrückstände können nicht mehr aufgeholt werden. • **Verstoß gegen Gesetze, Vorschriften und Verträge:** Es wird im hohen Maß gegen Gesetze verstoßen. Verstöße haben strafrechtliche Konsequenzen. Vertragsverletzungen führen zu ruinösen Konventionalstrafen oder Konsequenzen. • **Negative Innen- und Außenwirkung (Imageschaden):** Eine fundamentale, nachhaltige, in der breiten Öffentlichkeit vorhandene Ansehens- oder Vertrauensbeeinträchtigung, bis hin zu existenzgefährdender Art, ist zu erwarten. • **Finanzielle Auswirkungen:** Der finanzielle Schaden hat existenzbedrohende Ausmaße. • **Beeinträchtigung der persönlichen Unversehrtheit:** Es besteht akut Gefahr für Leib und Leben oder gravierende Beeinträchtigungen der persönlichen Unversehrtheit.

Tabelle 10: Beispiel für Schadenskategorien und Erläuterung je Schadensszenario

Neben harten Faktoren wie Liquidität oder Risikotragfähigkeit können auch Vorgaben der Institutionsleitung oder Anforderungen aus dem Risikomanagement Basis für die Ausprägung der Schadenskategorien sein. So können z. B. anhand konkreter Euro-Werte die Schadenskategorien zu finanziellen Auswirkungen voneinander abgegrenzt werden. Solche Schadenskategorien werden im Risikomanagement einer Institution definiert und orientieren sich am jeweils aktuellen Umsatzziel oder Haushaltsbudget.

Synergiepotenzial:

Sofern bereits ein ISMS nach BSI-Standard 200-2 vorliegt, können die in der Schutzbedarfsfeststellung definierten Schadensszenarien und Schadenskategorien als Grundlage genutzt werden. Dies fördert die Vergleichbarkeit von Ergebnissen zwischen dem BCMS und ISMS. Aus dem übergeordneten Risikomanagement können die Schadenskategorien zu den finanziellen Auswirkungen übernommen werden.

Untragbarkeitsniveau

Das Untragbarkeitsniveau stellt eine definierte Grenze dar, ab der die Auswirkungen eines Ausfalls durch die Institution nicht länger toleriert werden. Anhand dessen muss festgelegt werden, ob ein Geschäftsprozess zeitkritisch ist oder nicht. Das Untragbarkeitsniveau wird anhand der Schadenskategorien definiert. Gemäß den oben angeführten Beispielen von Schadenskategorien wird im Rahmen des Reaktiv-BCMS für alle folgenden Beispiele die Schadenskategorie *3 – Hoch* als Untragbarkeitsniveau zugrunde gelegt.

4.3.1.2 Festlegung der Hierarchie-Ebenen

Anhand eines Organigramms werden hierarchische Strukturen in der Aufbauorganisation einer Institution ersichtlich und nachvollziehbar dokumentiert.

Beispiel:

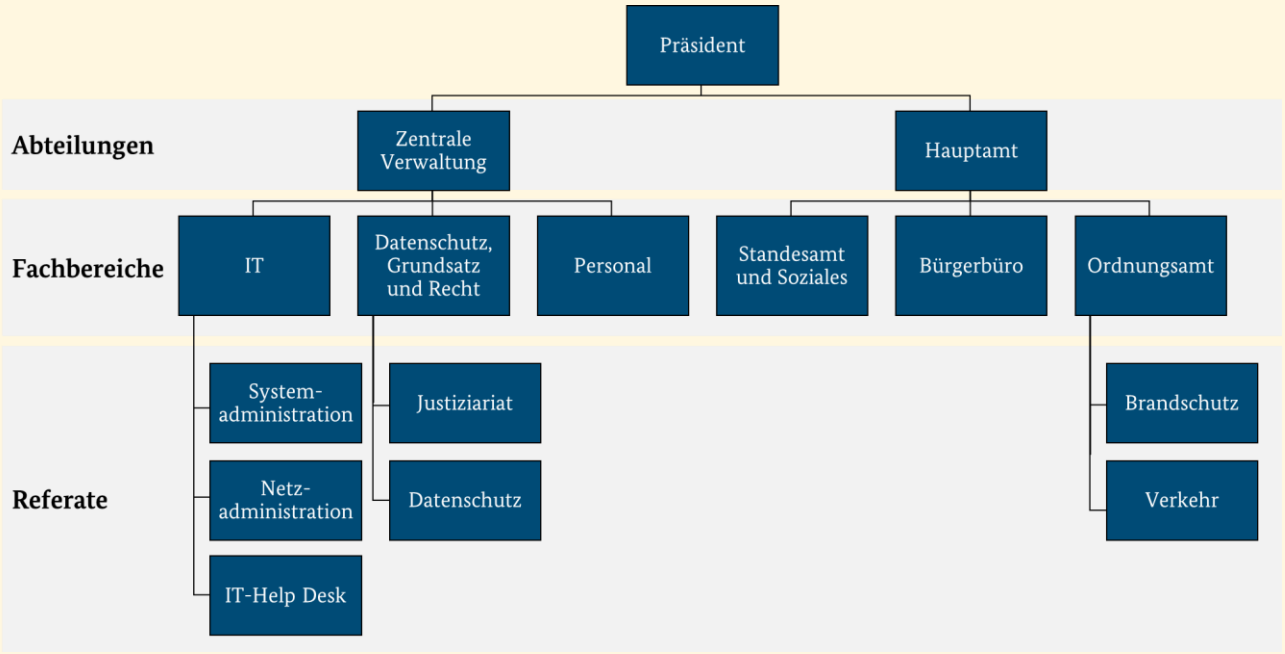

Abbildung 21: Hierarchisch angeordnete Organisationseinheiten am Beispiel einer Behörde

Abbildung 21 stellt ein Beispiel ausgewählter Organisationseinheiten anhand einer Behörde mit den Hierarchie-Ebenen Abteilungen, Fachbereiche und Referate dar. Je nach Größe und Komplexität der Institution kann es sehr viele Hierarchie-Ebenen geben. Bevor die Voranalyse durchgeführt wird, kann durch den BCMB festgelegt und mit der Institutionsleitung abgestimmt werden, wie viele Hierarchie-Ebenen darin berücksichtigt werden sollen. Dies dient einerseits dazu, die Voranalyse zeitlich exakter planen zu können, da die maximal mögliche Anzahl zu berücksichtigender Organisationseinheiten definiert ist. Zum anderen kann darüber gesteuert werden, wie detailliert die Voranalyse erfolgen soll.

Je mehr Hierarchieebenen berücksichtigt werden, desto detaillierter kann eine Aussage über (nicht) zeitkritische Organisationseinheiten getroffen werden. Jedoch steigt im selben Maße die Menge erforderlicher Termine, um die Informationen zu erheben. Die Institution sollte daher ein ausgewogenes Verhältnis aus Detailgrad und Aufwand abstimmen, um Informationen zu ermitteln. Eine Voranalyse anhand der in Abbildung 21 dargestellten drei Hierarchie-Ebenen stellt oft einen guten Kompromiss zwischen Detailgrad und der maximal notwendigen Anzahl Termine dar. Unabhängig von der Anzahl der Hierarchie-Ebenen muss die Voranalyse immer top-down erfolgen, d. h. von der obersten Hierarchie-Ebene beginnend bis zur festgelegten, untergeordneten. Nur so kann sichergestellt werden, dass keine Organisationseinheiten übersehen oder ausgelassen werden.

4.3.1.3 Vorbereitung der Workshops zur Voranalyse

Die Voranalyse sollte im Reaktiv-BCMS durch den BCMB anhand von Einzelterminen (Workshops) mit den Ansprechpartnern je Hierarchieebene durchgeführt werden. Der Workshop bietet verschiedene Vorteile gegenüber Formaten, in denen die Ansprechpartner die Informationen selbstständig erheben:

- Durch den BCMB kann näher erläutert werden, wieso die Voranalyse für die Folgeschritte im BCM bedeutend und sinnvoll ist.
- Der Workshop lässt Raum für Fragen und gestattet es, mögliche Unsicherheiten und Bedenken der Teilnehmer auszuräumen.
- Der BCMB sollte sorgfältig vermitteln, dass die wichtigsten Organisationseinheiten nicht zwangsläufig die zeitkritischsten sind und umgekehrt.

- Der BCMB kann sicherstellen, dass die Ergebnisse einheitlich erhoben werden.
- Fehleingaben oder fehlende Angaben können bereits im Workshop vermieden werden, sodass Nacharbeiten geringer ausfallen.

Um die Workshops effektiv zu gestalten, sollten Hilfsmittel durch den BCMB vorbereitet werden, die den Ansprechpartnern die Bewertung vereinfacht.

Workshop-Präsentation

Mit der Workshop-Präsentation kann der BCMB die Ansprechpartner thematisch auf die Schadensbewertung vorbereiten. Insbesondere sollte das Ziel der Voranalyse vorgestellt und verdeutlicht werden, welche Auswirkungen die Antworten der Teilnehmer auf die weitere Voranalyse sowie auf die nachfolgenden Schritte im BCM-Prozess haben.

Beispiel:

Sind bei einem Ausfall der Geschäftsprozesse dieser Organisationseinheit innerhalb von 7 Tagen hohe Schäden für die Institution zu erwarten?

Betrachtungszeitraum

Schadenskategorie unter Berücksichtigung aller Schadensszenarien

Allgemeine Beschreibung: Ausfall hat nicht tolerierbare Auswirkungen.

Beeinträchtigung der Aufgabenerfüllung: Der Geschäftsbetrieb ist massiv eingeschränkt. Arbeitsrückstände sind nur mit erhöhtem Arbeitsaufwand zu kompensieren.

Verstoß gegen Gesetze, Vorschriften und Verträge: Es wird gegen Gesetze verstoßen. Verstöße führen zu erheblichen Konsequenzen, z. B. hohe Bußgelder. Vertragsverletzungen führen zu hohen Konventionalstrafen oder Konsequenzen.

Negative Innen- und Außenwirkung (Imageschaden): Eine erhebliche, nachhaltige Ansehens- oder Vertrauensbeeinträchtigung ist intern und extern zu erwarten.

Finanzielle Auswirkungen: Der finanzielle Schaden ist für die Institution erheblich und nachhaltig spürbar.

Beeinträchtigung der persönlichen Unversehrtheit: Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden.

Abbildung 22: Beispiel für die Erläuterung des Zusammenwirkens der Parameter

Die Vorgehensweise sowie das Zusammenwirken der Parameter kann anhand der jeweiligen Leitfrage für die einzelnen Termine in den jeweiligen Organisationseinheiten erläutert werden. Abbildung 22 gibt hierzu beispielhaft eine zusammenfassende Übersicht.

Erhebungsbogen Voranalyse

Um die Informationen einheitlich und vollständig zu erheben, ist es hilfreich, für jeden Termin eine Dokumentenvorlage zu nutzen. Diese wird mit den relevanten Angaben zur Organisationseinheit vorausgefüllt. So kann im Termin direkt mit der Beantwortung der Leitfrage begonnen werden. Ein Beispiel für einen Erhebungsbogen kann der Tabelle 11 im nächsten Kapitel entnommen werden.

Liste der Organisationseinheiten und Geschäftsprozesse

Zu jedem Workshop-Termin sollte eine Übersicht der Organisationseinheiten anhand des Organigramms bereitgestellt werden. Hierbei ist es empfehlenswert, dass die Übersicht nur die Organisationseinheiten umfasst, die sich im Geltungsbereich des BCMS befinden und für den Workshop-Termin relevant sind.

Sofern in der Institution bereits Geschäftsprozesse definiert und dokumentiert wurden, z. B. anhand einer Prozesslandkarte, wird empfohlen, auch diese Übersicht für die Voranalyse bereitzustellen. Auch wenn in der Voranalyse noch keine einzelnen Geschäftsprozesse untersucht werden müssen, kann eine Übersicht der Geschäftsprozesse einer Organisationseinheit die Teilnehmer dabei gut unterstützen, die Leitfrage zu beantworten.

Übersicht zu Schadenskategorien und Schadensszenarien

Um eine vergleichbare Schadensbewertung zu erhalten, sollten die Ansprechpartner die Schadensszenarien und Schadenskategorien kennen. Hierzu kann auf die Abbildung 22 sowie ergänzend auf Tabelle 10, jeweils angepasst, zurückgegriffen werden.

Synergiepotenzial:

Sofern bereits ein ISMS nach der Standard- oder Kern-Absicherung nach BSI-Standard 200-2 besteht, kann für die Schutzbedarfsfeststellung bereits eine Übersicht der Schadenskategorien und Schadensszenarien erstellt worden sein, die für die Voranalyse adaptiert werden kann.

4.3.2 Durchführung der Voranalyse

In der Voranalyse muss zuerst die Institutionsleitung befragt werden. Zum einen hat die Institutionsleitung den besten Gesamtüberblick über die Institution. Zum anderen kennt so die Institutionsleitung die Ergebnisse der Voranalyse gut, da sie diese selbst erarbeitet hat.

Zu Beginn des Workshops sollten die Vorgehensweise und Methodik sowie die festgelegten Parameter in leicht verständlicher Form, z. B. unterstützt durch die Workshop-Präsentation, dargestellt werden. Dadurch werden die Teilnehmer des Workshops sensibilisiert, welche Auswirkungen die jeweiligen Antworten auf das Ergebnis und die folgenden Schritte im BCMS haben. Der BCMB sollte den Workshop moderieren und sicherstellen, dass valide und vergleichbare Ergebnisse entstehen.

In der ersten Hierarchie-Ebene müssen alle Organisationseinheiten dieser Ebene innerhalb des Geltungsbereichs des BCMS berücksichtigt werden (im Beispiel der Abbildung 21 sowie Tabelle 11 Abteilungen). Die Institutionsleitung sollte anhand der Leitfrage beantworten, welche der betrachteten Organisationseinheiten als zeitkritisch angesehen werden. Die Leitfrage sollte anhand der Übersicht zu den Schadenskategorien gemäß Tabelle 10 beurteilt werden. Wenn mindestens eine der genannten Schadenskategorien die Leitfrage erfüllt, kann die betrachtete Organisationseinheit als potenziell zeitkritisch angesehen werden. Um die Antworten zu dokumentieren, kann der Erhebungsbogen für die Voranalyse genutzt werden. Tabelle 11 zeigt beispielhaft den Aufbau eines Erhebungsbogens für die Voranalyse und greift hierzu die Beispiele aus Abbildung 21 auf.

Beispiel:

Hierarchie-Ebene: 1 – Abteilungen

Organisationseinheit der übergeordneten Hierarchie-Ebene: -/-

Ansprechpartner: Institutionsleitung

Datum des Workshops: 24.01.2020

Leitfrage: Sind bei einem Ausfall der Geschäftsprozesse dieser Organisationseinheit innerhalb von 7 Tagen hohe Schäden (Schadenskategorie 3) für die Institution zu erwarten?

Organisationseinheiten der Hierarchie-Ebene	Zeitkritisch?	Begründung anhand der Schadensszenarien und -kategorien
Zentrale Dienste	Teilweise	Der Ausfall der zentralen Dienste kann zu erheblichen Beeinträchtigungen des Geschäftsbetriebs führen. Zudem sind bei bestimmten untergeordneten Organisationseinheiten (z. B. Datenschutz) nicht tolerierbare, gesetzliche Verstöße möglich.
Hauptamt	Teilweise	Der Ausfall des Hauptamts kann zu erheblichen Beeinträchtigungen des Geschäftsbetriebs sowie zu massiver Außenwirkung führen. Zudem sind bei bestimmten untergeordneten Organisationseinheiten (z. B. Brandschutz) nicht tolerierbare, gesetzliche Verstöße möglich.

Tabelle 11: Erhebungsbogen zur Voranalyse am Beispiel der Abteilungen

Die Leitfrage kann auf drei verschiedene Arten beantwortet werden:

- **Vollständig zeitkritisch:** Alle untergeordneten Organisationseinheiten müssen in der BIA einbezogen werden. Untergeordnete Organisationseinheiten müssen in der Voranalyse daher nicht detaillierter untersucht werden.
- **Teilweise zeitkritisch:** Die Organisationseinheit hat zeitkritische Geschäftsprozesse. Die untergeordneten Organisationseinheiten müssen in weiteren Voranalyse-Workshops auf der jeweiligen Hierarchie-Ebene näher untersucht werden.
- **Nicht zeitkritisch:** Auf die Geschäftsprozesse dieser Organisationseinheit kann notfalls x Tage (=Untersuchungszeitraum) verzichtet werden. Untergeordnete Organisationseinheiten müssen daher nicht detaillierter in der Voranalyse untersucht werden.

Die Anzahl der Workshops für die folgenden Hierarchie-Ebenen richtet sich jeweils am Ergebnis der Befragung aus. Die nachfolgend benötigten Workshops sollten analog zur Hierarchie-Ebene 1 durch den BCMB vorbereitet, terminiert und moderiert werden. Hierbei ist es wichtig, dass die Ansprechpartner der nachfolgenden Workshops aussagefähig zu Auswirkungen von Ausfällen der Organisationseinheit der jeweiligen Hierarchie-Ebene sind. Im Falle von Organisationseinheiten sind dies üblicherweise die jeweiligen Leitungsfunktionen, gegebenenfalls unterstützt durch Prozesseigentümer oder Prozessexperten.

Tabelle 12 greift das Ergebnis der vorangegangenen Bewertung gemäß Tabelle 11 auf. Entsprechend der dargestellten Bewertung würde die Voranalyse für die Fachbereiche IT und Datenschutz, Grundsatz und Recht fortgesetzt, für den Fachbereich Personal hingegen ausgeschlossen werden.

Beispiel:

Hierarchie-Ebene: 2 – Fachbereiche

Organisationseinheit der übergeordneten Hierarchie-Ebene: Zentrale Dienste

Ansprechpartner: Leiterin Zentrale Dienste

Datum des Workshops: 03.02.2020

Leitfrage: Sind bei einem Ausfall der Geschäftsprozesse dieser Organisationseinheit innerhalb von 7 Tagen hohe Schäden (Schadenskategorie 3) für die Institution zu erwarten?

Organisationseinheiten der Hierarchie-Ebene	Zeitkritisch?	Begründung anhand der Schadensszenarien und -kategorien
IT	Teilweise	Nicht erkannte oder behandelte Störungen der IT können sich massiv auf den Geschäftsbetrieb auswirken und in der Folge zu nicht tolerierbaren finanziellen Verlusten oder Reputationsverlusten führen. Jedoch steht der IT-Betrieb im Fokus, hingegen nicht die IT-Entwicklung.
Datenschutz, Grundsatz und Recht	Teilweise	Datenschutzverstöße müssen zeitnah erkannt und gemeldet werden, sodass diese aufgrund des möglichen Verstoßes gegen Gesetze zeitkritisch sind. Grundsatz und Recht sind hingegen nicht zeitkritisch.
Personal	Nicht	Der Ausfall kann zur Beeinträchtigung der Aufgabenerfüllung führen, aber es kommt binnen 7 Tagen zu keinen hohen Schäden.

Tabelle 12: Erhebungsbogen zur Voranalyse am Beispiel der Fachbereiche

Die Voranalyse sollte so lange fortgesetzt werden, bis die definierte unterste Hierarchie-Ebene erreicht oder alle Organisationseinheiten der aktuell betrachteten Hierarchie-Ebene insgesamt als nicht oder als vollständig zeitkritisch bewertet wurden.

4.3.3 Konsolidierung und Vorstellung der Ergebnisse

Da in der Voranalyse verschiedene Personen mitwirken, kann der Detailgrad, das sprachliche Niveau und die Aussagekraft der Informationen schwanken. Daher sollte der BCMB die Ergebnisse dahingehend überprüfen, ob diese vollständig und plausibel dokumentiert wurden. Dies trifft umso mehr zu, wenn die Voranalyse nicht wie empfohlen im Rahmen von moderierten Workshops durchgeführt wird, sondern beispielsweise per Selbstauskunft der Teilnehmer erfolgte. Der BCMB sollte daher überprüfen, ob die Ergebnisse der Voranalyse plausibel und vollständig sind. Anschließend sollte dieser die zeitkritischen Organisationseinheiten der einzelnen Hierarchie-Ebenen in einer Gesamtübersicht zusammenfassen.

Beispiel:

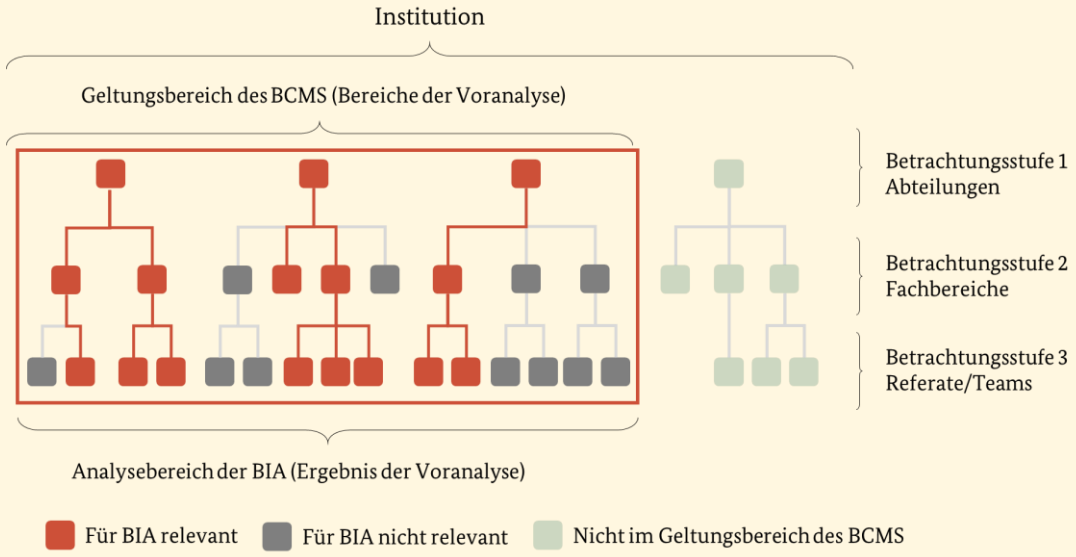

Abbildung 23: Beispiel für ein Ergebnis der Voranalyse

Der BCMB muss der Institutionsleitung die Ergebnisse der Voranalyse vorstellen. Nur so kann sichergestellt werden, dass die Institutionsleitung darüber entscheidet, ob der Analysebereich in der BIA, abweichend vom Geltungsbereich des BCMS, wie dargestellt eingeschränkt werden soll. Die Institutionsleitung muss sich des damit verbundenen Risikos bewusst sein und es tragen.

Die Institutionsleitung sollte ihrerseits überprüfen, ob der Analysebereich der BIA angemessen eingegrenzt wurde. Z. B. wenn ein zu geringer oder sehr hoher Prozentsatz der im Geltungsbereich des BCMS liegenden Organisationseinheiten als potenziell zeitkritisch ermittelt wurden. Falls durch die Institutionsleitung entschieden wird, dass die Eingrenzung des Analysebereichs nicht angemessen ist, sollten die Parameter sowie Hierarchie-Ebenen überarbeitet und die Voranalyse wiederholt werden. Die Voranalyse ist abgeschlossen, wenn die Institutionsleitung die Ergebnisse freigegeben hat.

4.4 Business Impact Analyse (BIA)

Anhand der Voranalyse wurden die potenziell zeitkritischen Organisationseinheiten ermittelt, die den eingegrenzten Analysebereich der BIA vorgeben. Das Ziel der BIA besteht darin, die Voranalyse zu verfeinern, um die zeitkritischen Geschäftsprozesse im Analysebereich und die ihnen zugeordneten Ressourcen zu ermitteln.

In der BIA wird dazu untersucht, welche Geschäftsprozesse innerhalb des Untersuchungsbereichs zeitkritisch sind und ab wann deren Ausfälle nicht tolerierbare Auswirkungen haben. Dies bestimmt, ob und ab wann für diese Geschäftsprozesse ein Notbetrieb zur Verfügung stehen sollte. Zusätzlich werden für zeitkritische Geschäftsprozesse die Ressourcen für den Notbetrieb sowie deren Wiederanlaufzeiten ermittelt.

Die BIA erfolgt stets bezogen auf die **Auswirkungen** eines Geschäftsprozessausfalls, nicht auf die Ursachen. Ob ein Geschäftsprozess aufgrund der Nichtverfügbarkeit des Gebäudes durch Feuer, Hochwasser, Stromausfall oder aufgrund der Nichtverfügbarkeit einer für den Geschäftsprozess zwingend benötigten IT-Anwendung ausfällt, spielt daher für die Schadensbewertung keine Rolle. Innerhalb der BIA muss vom Totalausfall des Geschäftsprozesses ausgegangen und in dessen Folge die zu erwartenden Schäden bewerten werden.

In einer BIA wird nicht nur bewertet, welche Auswirkungen ein Ausfall eines Geschäftsprozesses für die Institution hat, sondern auch wie sich der Schaden zeitlich entwickelt. Das Ergebnis der BIA legt fest, welche Geschäftsprozesse und Ressourcen zeitkritisch sind und daher in den nachfolgenden Schritten des BCM berücksichtigt werden müssen. Da die BAO schon aufgebaut wurde, helfen diese Informationen der BAO zudem,

- die zeitkritischen Geschäftsprozesse und Ressourcen in einem Notfall zu priorisieren,
- früh zu erkennen, ob ein Schadensereignis eskaliert werden muss sowie
- den Geschäftsbetrieb aufrechtzuerhalten.

Während in der Voranalyse anhand einer vereinfachten Fragestellung nur sehr allgemein zwischen zeitkritischen und nicht zeitkritischen Organisationseinheiten unterschieden wurde, wird innerhalb der BIA präziser anhand verschiedener Kenngrößen abgeleitet, wie zeitkritisch ein Geschäftsprozess ist.

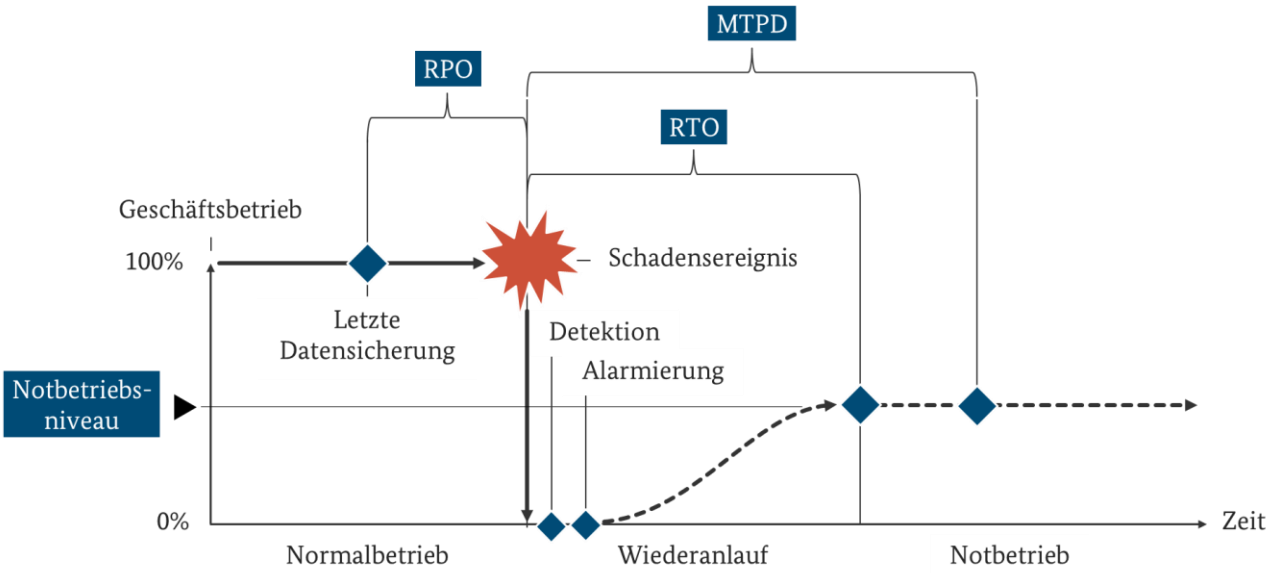

Abbildung 24: Erläuterung der Kenngrößen MTPD, RTO, RPO sowie Notbetriebsniveau

Abbildung 24 verdeutlicht anhand eines vereinfachten Beispiels einer Notfallbewältigung die Zusammenhänge zwischen den Kenngrößen. Die verkürzte Darstellung besteht hier nur aus den Phasen Normalbetrieb, Wiederanlauf einer zeitkritischen Ressource und Notbetrieb eines zeitkritischen Geschäftsprozesses.

1. Die **Maximum tolerable Period of Disruption** (**MTPD**, deutsch: Maximal tolerierbare Ausfallzeit, MTA) legt fest, wie lange ein Geschäftsprozess maximal ausfallen darf, bevor nicht tolerierbare Auswirkungen für die Institution auftreten. Sie wird anhand einer Schadensbewertung je Geschäftsprozess ermittelt.
2. Die **Recovery Time Objective (RTO,** deutsch: Geforderte Wiederanlaufzeit, WAZ) wird aus der MTPD abgeleitet und den Ressourcen zugeordnet, die relevant sind für die Aufrechterhaltung der zeitkritischen Geschäftsprozesse. Die RTO einer zeitkritischen Ressource umfasst den Zeitraum vom Zeitpunkt des Ausfalls der Ressource bis zum Zeitpunkt der geforderten Inbetriebnahme der Notfall-Lösung, z. B. durch Schwenk auf eine Ausweich- oder Ersatzressource oder durch Zurücksetzen eines IT-Systems auf den letzten gesicherten Zustand. Die RTO der Ressource muss zwingend kürzer sein als die MTPD des relevanten Geschäftsprozesses, um zwischen Eintritt eines Schadensereignisses und der Detektion sowie Alarmierung bis hin zum Einleiten der Maßnahme zum Wiederanlauf über ausreichend zeitlichen Puffer zu verfügen.
3. Der **Recovery Point Objective** (**RPO**, deutsch: Maximal zulässige Datenverlust) legt fest, wie alt verfügbare Daten maximal sein dürfen, um im Notbetrieb sinnvoll damit arbeiten zu können. Diese Kenngröße dient auch dazu, die minimal notwendigen Datensicherungszyklen daraus abzuleiten.
4. Das **Notbetriebsniveau** definiert, wie leistungsfähig der Notbetrieb sein soll, um einen sinnvollen Geschäftsbetrieb gewährleisten zu können. Das Notbetriebsniveau wird je Geschäftsprozess individuell festgelegt. Hierzu kann die Leistungsfähigkeit des Notbetriebs z. B. prozentual angegeben werden oder alternativ Aktivitäten priorisiert werden. In der Abbildung 24 wird das Notbetriebsniveau nur schematisch dargestellt.

Um eine BIA durchzuführen, kann die Dokumentenvorlage *BIA-Auswertungsbogen* aus den Hilfsmitteln verwendet werden. Anhand dieser Dokumentenvorlage werden einige der nachfolgend aufgeführten Beispiele und Hinweise dargestellt. Die nachfolgenden Kapitel beschreiben die empfohlene Vorgehensweise, mittels derer die BIA vorbereitet, durchgeführt und ausgewertet werden kann. In Abbildung 25 sind die hierfür erforderlichen Schritte in einer Übersicht dargestellt.

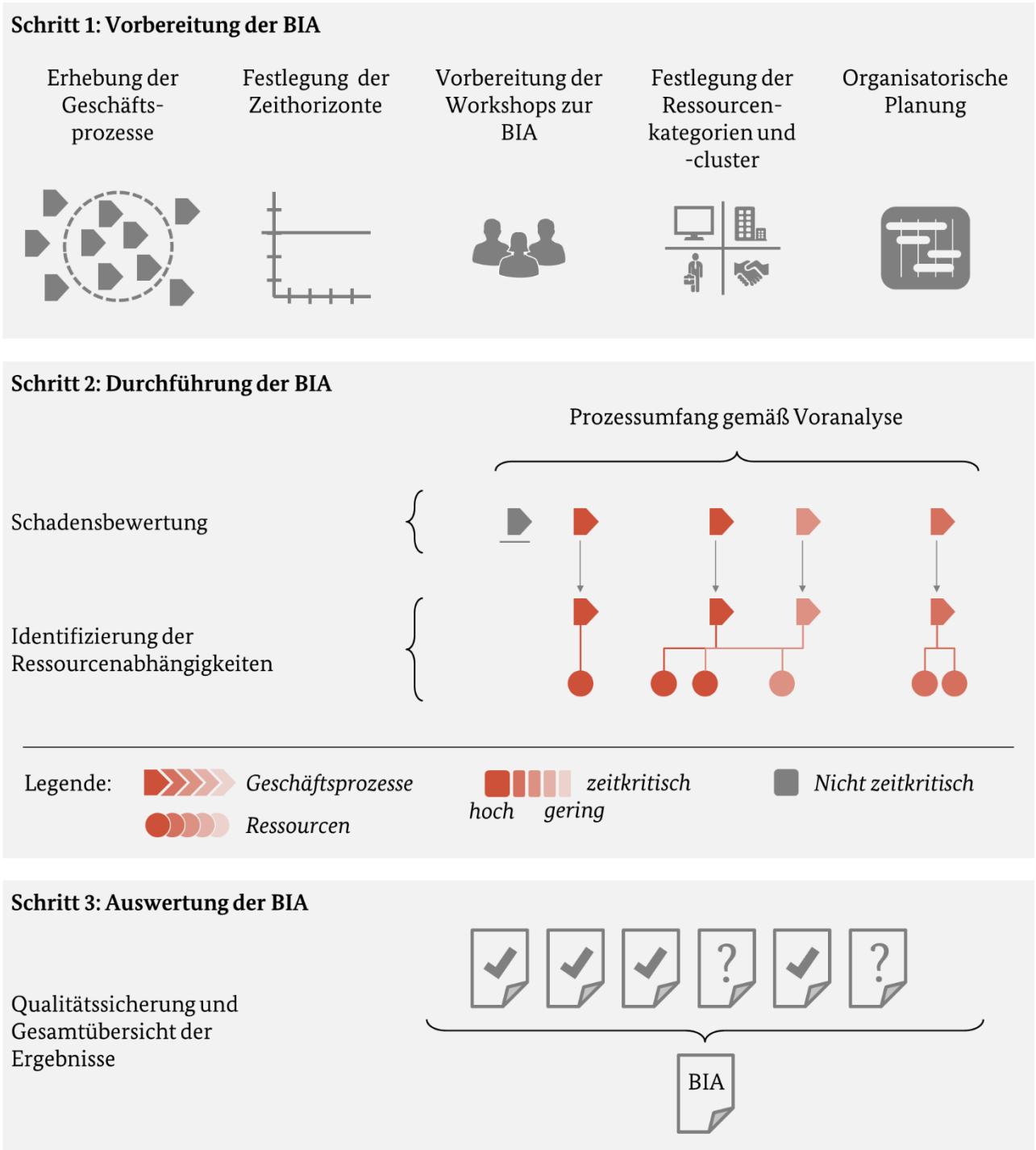

Abbildung 25: BCM-Prozessschritte der Business Impact Analyse

4.4.1 Vorbereitung der BIA

Ähnlich wie in der Voranalyse ist auch hier die Vorbereitung der BIA essenziell, um die Daten einheitlich zu ermitteln und die Akzeptanz bei den Mitarbeitern zu stärken. Der BCMB sollte die Methodik der BIA festlegen und die BIA organisatorisch vorbereiten. Dies ist sinnvoll, da er über das notwendige Fachwissen verfügt und den BCM-Prozess zeitlich steuert. Er kann vorbereitende Tätigkeiten ganz oder teilweise an weitere Rollen im BCM delegieren. Die Aufgaben in der Vorbereitung der BIA werden in den nachfolgenden Unterkapiteln näher erläutert. Die Kapitel folgen einer logischen Reihenfolge, jedoch können sich verschiedene darin beschriebene Aufgaben in der Praxis zeitlich überlagern.

4.4.1.1 Erhebung der Geschäftsprozesse

Für die in der Voranalyse als zeitkritisch identifizierten Organisationseinheiten müssen die jeweiligen Geschäftsprozesse identifiziert werden, da auf deren Grundlage der Schaden innerhalb der BIA bewertet wird. Jede Institution sollte hierzu möglichst auf eine vollständige und aktuelle Übersicht ihrer Geschäftsprozesse zurückgreifen. Eine solche Übersicht wird häufig in einem Prozessmanagement erstellt oder durch Querschnittsfunktionen wie zentrale Dienste, Betriebsorganisation oder Vorstandsstab. Liegt keine Übersicht vor, so muss diese im Rahmen der BIA erhoben oder aktualisiert werden.

Hinweis:

Während in einer Prozesslandkarte häufig eine sehr große Anzahl an Informationen vorliegen, werden im Rahmen der BIA nur die Prozessbezeichnung sowie die zuständige Organisationseinheit benötigt. Eine kurze Beschreibung der Aktivitäten oder Ergebnisse des Geschäftsprozesseses kann für die Schadensbewertung hilfreich sein. Liegt keine Prozesslandkarte vor, so können in den BIA-Workshops die Ansprechpartner zu ihren Geschäftsprozessen befragt werden. Diese können sich ihrerseits an den bestehenden Geschäftsverteilungsplänen, Aufgabenbeschreibungen oder anderen organisationsbeschreibenden Dokumenten der Organisationseinheit orientieren.

Synergiepotenzial:

Liegt ein ISMS nach BSI-Standard 200-2 oder nach ISO-Standard 27001 vor, so kann auf die dort identifizierten Geschäftsprozesse zurückgegriffen werden.

Das Verfahrensverzeichnis für den Datenschutz kann möglicherweise ebenfalls als Grundlage genutzt werden. Es fast alle Geschäftsprozesse zusammen, in denen personenbezogene Daten verarbeitet werden.

Je nach Größe und Komplexität der Institution kann es unterschiedliche Detailebenen der Geschäftsprozesse geben. Bevor die BIA durchgeführt wird, sollte durch den BCMB festgelegt werden, auf welcher Detailebene der Geschäftsprozesse die BIA durchgeführt werden soll. Dies dient einerseits dazu, die BIA zeitlich exakter planen zu können, da die maximal mögliche Anzahl zu berücksichtigender Geschäftsprozesse definiert ist. Zum anderen kann darüber gesteuert werden, wie detailliert die Schadensbewertung erfolgen soll.

Als Vorgabe für den Detailgrad der zu berücksichtigenden Geschäftsprozesse sollte ein goldener Mittelweg zwischen zu starker Zusammenfassung von Geschäftsprozessen und einer zu detaillierten Betrachtung gefunden werden. Eine zu starke Bündelung von Geschäftsprozessen führt zu einer mangelnden Aussagekraft hinsichtlich der zeitkritischen Aktivitäten innerhalb des Geschäftsprozesses. Eine zu detaillierte Betrachtung führt zu einer nicht zu bewältigenden Anzahl zu betrachtender Geschäftsprozesse. Ein wesentliches Merkmal dieses Mittelweges liegt darin, dass die Planung des Notbetriebs und Erstellung von geeigneten GFPs mit den Ergebnissen der BIA erreicht werden können.

Eine Schadensbewertung der in Abbildung 26 dargestellten Prozessebene 3 stellt einen guten Kompromiss hinsichtlich aussagekräftigem Detailgrad und der Menge an Geschäftsprozessen dar. Die beschriebenen Geschäftsprozesse sind als Beispiele zu verstehen und decken nur einen kleinen Teil der üblichen Geschäftsprozesse innerhalb einer Institution ab.

Beispiel:

Prozessebene 1	Prozessebene 2	Prozessebene 3	...
Personalmanagement	Personalbeschaffung	Personalrekrutierung	...
		Einstellungsverfahren	...
		...	...
	Personalbetreuung	Personalservice	...
		Personalentwicklung	...
		Personalaustritt	...
		...	...
IT	IT-Steuerung	IT-Strategie	...
		IT-Ressourcenmanagement	...
		...	...
	IT-Betrieb	Sicherstellung IT-Betrieb	...
		Berechtigungsmanagement	...
		Incident Management	...
		Problem Management	...
		...	...
	IT-Anwendungsentwicklung	Softwareauswahl	...
		Softwaretest	...
		...	...

Abbildung 26: Beispiele hierarchisch angeordneter Geschäftsprozesse

4.4.1.2 Festlegung der Zeithorizonte

In der Voranalyse konnte die Leitfrage beantwortet werden, ob eine Organisationseinheit zeitkritisch ist (siehe Kapitel 4.3.1.1 *Konkretisierung des Begriffs zeitkritisch*). Die Bewertung erfolgte

- anhand des Untersuchungszeitraums,
- der Schadensszenarien und -kategorien (Schadenspotenzial) sowie
- des Untragbarkeitsniveaus.

Anders als in der Voranalyse, die nur einen definierten Untersuchungszeitraum betrachtet, wird in der BIA der Schaden über mehrere Zeithorizonte bewertet. Zu diesem Zweck müssen zusätzlich zu den oben aufgeführten Parametern, Zeithorizonte festgelegt werden. Die Leitfrage kann anschließend lauten:

> **Wenn ein Geschäftsprozess ausfällt, mit welchem Schadenspotenzial (y) ist im Zeithorizont (x) zu rechnen?**

Die nachfolgende Abbildung 27 stellt beispielhaft die **Schadensbewertung** für einen Geschäftsprozess grafisch dar und fasst die relevanten Parameter zusammen. Im Unterschied zur Voranalyse wird der Schaden nun pro Zeithorizont bewertet, d.h. die Vorgehensweise sowie das Zusammenwirken der Parameter kann anhand der Leitfrage des Termins erläutert werden.

Beispiel:

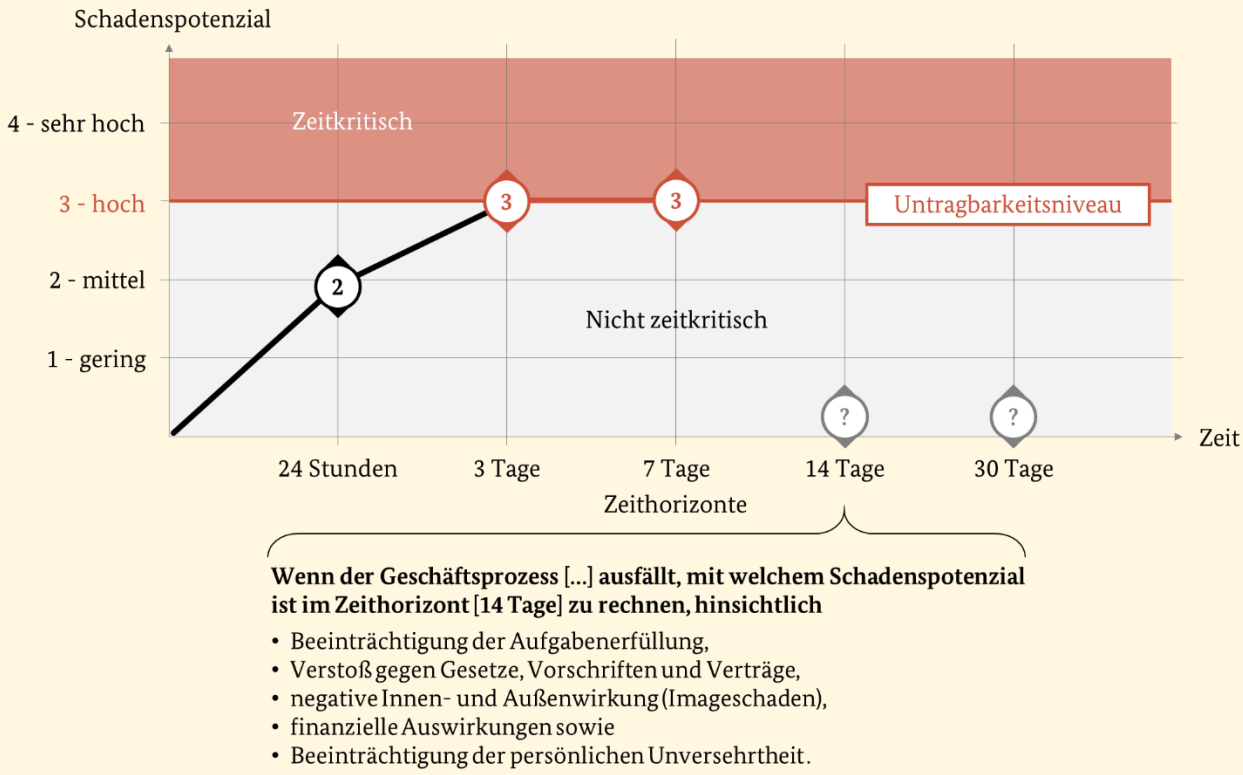

Abbildung 27: Beispiel für das Zusammenwirken der Parameter in der BIA-Schadensbewertung

Die **Zeithorizonte** (im Beispiel-Diagramm auf der Zeit-Achse aufgetragen) legen den jeweiligen Zeitpunkt fest, zu dem ein Schaden bewertet wird. Die Zeitpunkte x (24 Stunden, 3 Tage, 7 Tage etc.) markieren je einen Zeitraum von 0 bis x und sind zu verstehen als *„Der Geschäftsprozess ist ausgefallen bis zum Zeitpunkt x"*.

- Das **Schadenspotenzial** (im Beispiel-Diagramm als Kreis auf dem Koordinatensystem dargestellt) lässt sich aus den Schadensszenarien und Schadenskategorien ableiten.
- Die **Schadensszenarien** (im Beispiel unter dem Diagramm dargestellt) beschreiben die Szenarien, in denen ein Schaden entstehen könnte.

Die **Schadenskategorien** (im Beispiel-Diagramm auf der Schadenspotenzial-Achse aufgetragen) klassifizieren den Schaden, der je Schadensszenario entstehen kann.

Das **Untragbarkeitsniveau** wird im Beispiel-Diagramm als horizontale rote Linie dargestellt. Oberhalb der Schadensstufe 3 (hoch) erzeugt der Ausfall des Geschäftsprozesses Schäden, die durch die Institution nicht toleriert werden, d. h. der Prozess wird zeitkritisch.

Der Verlauf des Graphen, d. h. der dickeren, schwarzen Linie im Beispiel-Diagramm, zeigt die Entwicklung des Schadenspotenzials über die Zeit. Der Graph verdeutlicht, wann ein Geschäftsprozess zeitkritisch wird und ob das Schadenspotenzial über den Zeitverlauf stagniert oder mit längerer Ausfallzeit weiter ansteigt.

Sowohl die Anzahl als auch die genaue Unterteilung der Zeithorizonte müssen sich an den Gegebenheiten der Institution ausrichten. Deswegen sollten Zeithorizonte festgelegt werden, zu denen sich typischerweise der Schadensverlauf in der Institution wesentlich verändert.

Hinweis:

Die Wahl der Zeithorizonte wird unter anderem beeinflusst durch

- die Zyklen, in denen Produkte hergestellt oder Services bereitgestellt werden,
- die Erwartungshaltung von Interessengruppen,
- interne oder gesetzliche Vorgaben,
- branchenübliche Standards sowie
- den Risikoappetit der Institution.

Entsprechend können z. B. dynamische Branchen, wie der Onlinehandel, sehr kurze Zeithorizonte wählen, sowie Institutionen mit sehr langen Produktions- oder Bearbeitungszeiten längere Zeithorizonte.

Beispiel:

Die Beispiele erläutern, wie die Zeithorizonte anhand branchen- oder institutionsspezifischer Vorgaben sowie besonderer Termine und Ereignisse abgeleitet werden können.

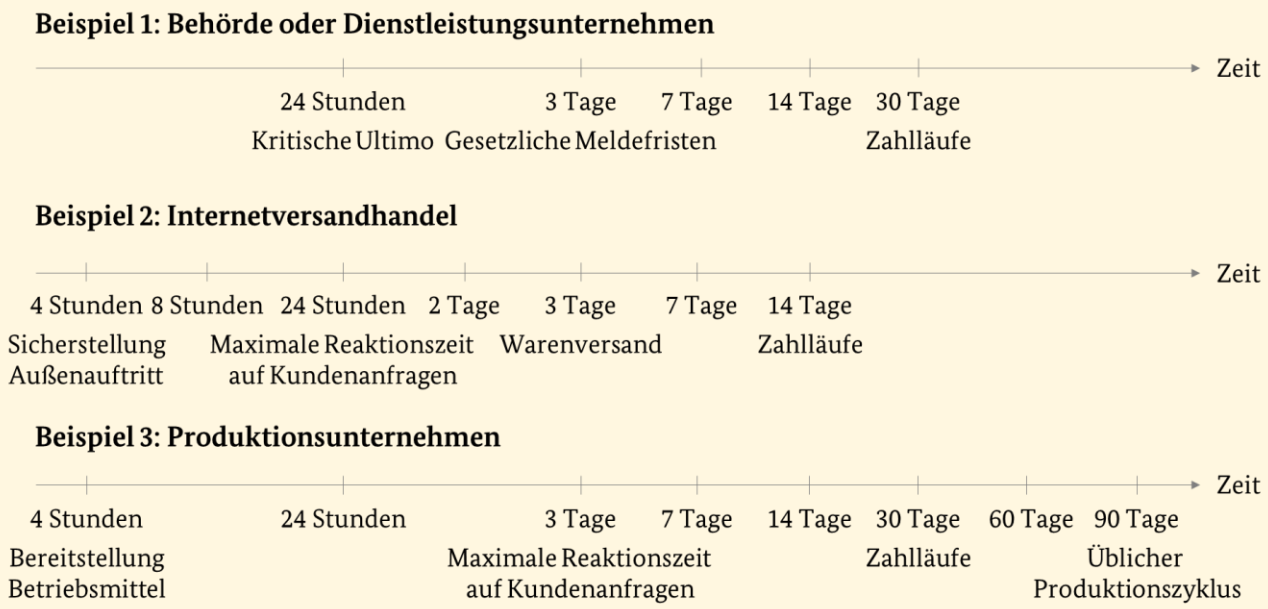

Abbildung 28: Beispiele für Zeithorizonte

In der Praxis hat sich eine Einteilung in fünf bis acht Zeithorizonte bewährt. Der längste zu betrachtende Zeithorizont sollte am Zeitraum ausgerichtet sein, der in der Initiierung des BCMS (siehe Kapitel 3.1.2 *Geltungsbereich*) festgelegt wurde.

4.4.1.3 Festlegung der Ressourcenkategorien und -cluster

Da der Ausfall eines Geschäftsprozesses immer auf den Ausfall einer notwendigen Ressource zurückzuführen ist, müssen im zweiten Schritt der BIA die Ressourcenabhängigkeiten der zeitkritischen Geschäftsprozesse erhoben werden. Hierzu muss vorbereitend festgelegt werden, welche Ressourcenkategorien in der Institution relevant sind. Darauf aufbauend müssen die Ressourcen(-cluster) der jeweiligen Kategorie ermittelt werden.

Einheitliche Namen und damit einheitlich definierte Ressourcenkategorien und Ressourcen(-cluster) stellen sicher, dass die benötigten Ressourcen einheitlich erhoben werden können. Dann können auch die Informationen zu RTO und RPO den Ressourcen richtig zugeordnet und so nach der BIA unmittelbar mit dem Soll-Ist-Vergleich begonnen werden.

Ressourcenkategorien

Grundsätzlich benötigt eine Institution für ihren Geschäftsbetrieb Strom, Wasserversorgung, Klimatechnik etc. Es ist jedoch nicht zweckmäßig diese Ressourcen für jeden Geschäftsprozess einzeln zu erheben, da diese für die Aufrechterhaltung des gesamten Geschäftsbetriebs vorausgesetzt werden. Diesen Ressourcen kann der kleinste, zeitkritische Zeithorizont zugeordnet werden, der für die Institution vorgegeben wird.

Werden darüber hinaus spezifische Ressourcen für einen Geschäftsprozess benötigt, so müssen diese in der BIA ermittelt werden. Die Ressourcen können in verschiedene Ressourcenkategorien unterteilt werden. Es müssen mindestens die folgenden in *Tabelle 13* beschriebenen Ressourcenkategorien berücksichtigt werden:

- IT
- Personal
- Infrastruktur
- Dienstleistungen.

Für das produzierende Gewerbe sollten zusätzlich die folgenden in *Tabelle 13* beschriebenen Ressourcenkategorien verwendet werden:

- Maschinen/Geräte/Anlagen/Fahrzeuge
- Betriebsmittel (Sonstige)

Die Institution sollte die Anzahl und Beschreibung der Ressourcenkategorien an ihre Bedürfnisse anpassen.

Beispiel:

Ressourcenkategorie	Beschreibung
IT	IT umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen.
Personal	Um Geschäftsprozesse durchführen zu können, werden Mitarbeiter benötigt, die Entscheidungen treffen, Aufgaben ausführen, Maschinen bedienen oder sonstige Arbeitsschritte durchführen. Die Mitarbeiter verfügen hierzu über spezielle Fähigkeiten und Kenntnisse. Die jeweiligen Aufgaben, Pflichten, Fähigkeiten und Kenntnisse werden in Form von Rollen und Funktionen definiert. Ferner sind an Rollen Berechtigungen für Zugang, Zutritt und Zugriff sowie Stellvertreterregelungen geknüpft.
Dienstleistungen	Unter dem Begriff Dienstleistungen werden alle intern und extern bezogenen Leistungen zusammengefasst, die einen Input liefern oder benötigte Ressourcen für einen Geschäftsprozess bereitstellen.

Ressourcenkategorie	Beschreibung
Informationen	Für gewöhnlich werden aus Endanwendersicht Anwendungen inklusive der darin gespeicherten oder verarbeiteten Daten betrachtet (siehe Ressourcenkategorie IT). In der Praxis können aber auch Daten in elektronischer Form vorliegen, die keiner Anwendung zugeordnet werden. Hierzu gehören z. B. gespeicherte Daten auf mobilen Datenträgern, in Dateisystemen oder Cloudlösungen. Neben elektronischen Daten können auch papierhafte Dokumente der Ressourcenkategorie Informationen zugeordnet werden. Abweichend zum *Glossar des IT-Grundschutz-Kompendiums* werden Informationen, die in Köpfen gespeichert sind, der Ressource Personal zugeordnet.
Infrastruktur	Zur Infrastruktur zählen z. B. Gelände, Grundstücke, Gebäude inklusive Lager, Produktionshallen, Parkgaragen, Aktenarchive, Server- oder Büroräume sowie Strom-, Gas-, Wasser oder Fernwärmeversorgung sowie und (TV-, Internet-, Telefon-Verbindung), die für einen oder mehrere Geschäftsprozesse benötigt werden.
Maschinen/ Geräte/ Anlagen/ Fahrzeuge	Insbesondere im produzierenden Gewerbe stellen Maschinen, Geräte und Anlagen eine wesentliche Komponente in Geschäftsprozessen dar. Unter Fahrzeuge fallen Transport- und Verkehrsmittel (PKW, LKW, Zug, Flugzeug, Schiff etc.). Auch spezielle Bürogeräte wie Plotter oder Scanner können unter dieser Kategorie zusammengefasst werden.
Betriebsmittel (Sonstige)	Unter Betriebsmittel sind alle weiteren Ressourcen zu verstehen, die in keiner vorherigen Ressourcenkategorie erfasst wurden. Dies kann auch Rohstoffe für eine Produktion oder Kleinmaterial (z. B. Büromaterial, Büroausstattung, Zugangstoken etc.) umfassen.

Tabelle 13: Übersicht über die Ressourcenkategorien (Beispiele)

Ressourcencluster

Innerhalb bestimmter Ressourcenkategorien, wie z. B. der IT, können mitunter sehr viele einzelne Ressourcen vorhanden sein, die in der BIA berücksichtigt werden müssen. Wenn alle Ressourcen einzeln erfasst werden, besteht jedoch die Gefahr, dass diese aufgrund der Menge und der Komplexität nicht handhabbar sind. Ressourcen sollten deshalb sinnvoll zu Clustern zusammengefasst werden. Das gängigste Beispiel für ein Cluster ist der Arbeitsplatz.

Ein **Arbeitsplatz** fasst alle Arbeitsmittel und Geräte zusammen, die für eine spezifische Aufgabenstellung innerhalb eines Geschäftsprozesses benötigt werden. Hierbei kann allgemein zwischen einem Standard-Arbeitsplatz und Spezial-Arbeitsplätzen unterschieden werden. Ein Arbeitsplatz kann Teil einer größeren Infrastruktur sein und wiederum aus einer Menge an Maschinen, Geräten, Anlagen oder Betriebsmitteln zusammengesetzt sein.

Beispiel:

Ein **Standard-Arbeitsplatz** wird definiert als ein Schreibtisch mit Bürostuhl und PC sowie ein Telefon. Der Standard-Arbeitsplatz wird mit den Medien Strom und Internet versorgt. Auf dem PC sind die gängigen Anwendungen der Institution installiert, z. B. E-Mail und Textverarbeitung. Weitere Ausstattung muss rollen- oder funktionsspezifisch definiert werden.

In einer Bank wird ein **Handels-Arbeitsplatz** definiert, der zusätzlich zu einem Standard-Arbeitsplatz mit mehreren großformatigen Monitoren, einer speziellen Tastatur und einem Kartenlesegerät ausgestattet sowie an eine Telefonanlage mit Sprachaufzeichnung angeschlossen ist. Auf dem PC sind neben Standardprogrammen spezielle Bankanwendungen installiert, für die spezifische Berechtigungen erforderlich sind.

In einem Logistikbetrieb wird abweichend zu einem Standard-Arbeitsplatz ein **Kommissionier-Arbeitsplatz** definiert, der aus einem Arbeitstisch, einem PC mit Zugang zum Lieferketten- und Lagerverwaltungssystem (Supply Chain und Warehouse Management), einem Touchpad zur Dateneingabe, einem Label-Drucker sowie Handscanner, Verpackungsmaterial und Transportboxen besteht.

Synergiepotenzial:

Liegt ein ISMS nach BSI-Standard 200-2 vor, können Informationen aus der Strukturanalyse für die Bezeichnung verschiedener Ressourcen übernommen werden. Allerdings kann die Gruppenbildung gemäß BSI-Standard 200-2 voraussichtlich nicht für die Ressourcencluster im BCM angewendet werden, da diese einem abweichenden Zweck dienen.

Ist der IT-Betrieb nach ITIL ausgerichtet, kann der Bedarf an Informationstechnik anhand des IT-Servicekatalogs ermittelt werden.

Auf Grund von Datenschutz-Vorgaben werden kontinuierlich die IT-Anwendungen ermittelt, die personenbezogene Daten verarbeiten. Diese Ergebnisse können ebenfalls als Grundlage für eine IT-Anwendungsliste dienen.

Über die Gebäudeverwaltung können häufig Arbeitsplatz-Definitionen sowie Raumlisten übernommen werden.

Im produzierenden Gewerbe liegen meist Maschinen- und Geräte-Inventarlisten vor, die für die Ressourcenkategorie Maschinen/Geräte/Anlagen/Fahrzeuge herangezogen werden können.

4.4.1.4 Organisatorische Planung

Vor Beginn der BIA sollte festgelegt werden, wie die Informationen zur BIA erhoben werden sollen. Analog zur Voranalyse ist das Format von Workshops empfehlenswert. Der Workshop bietet verschiedene Vorteile gegenüber Formaten, in denen die Ansprechpartner die Informationen selbstständig erheben:

- Durch den BCMB kann näher erläutert werden, welche Auswirkung die BIA auf spätere Folgeschritte im BCM hat, unter anderem auf die Geschäftsfortführungsplanung.
- Durch den BCMB kann spezifisch darauf hingewiesen werden, dass die BIA nicht der Organisationsoptimierung dient. Anhand der Ergebnisse sollen weder Umstrukturierungen, Arbeitsplatzverdichtung oder Ähnliches abgeleitet werden, da die Fragestellungen sich auf einen temporären Notbetrieb beziehen.
- Der BCM-Beauftragte sollte sorgfältig vermitteln, dass die Geschäftsprozesse, die für die Organisationseinheit die wichtigsten sind, nicht zwangsläufig die zeitkritischsten sind und umgekehrt.

Ferner bestehen dieselben Vorteile eines Workshops, wie in der Voranalyse:

Innerhalb eines BIA-Workshops wird durch eine BCM-sachkundige Person, zumeist dem BCMB, die BIA-Methodik erläutert und durch die einzelnen Schritte moderiert. Weiter nehmen am BIA-Workshop ein oder mehrere Prozesseigentümer teil. Die Ansprechpartner können hierbei die gleichen Personen wie in der Voranalyse sein. Diese können durch einzelne Prozessexperten im Rahmen des BIA-Workshops unterstützt werden.

Um die BIA-Workshops zeitlich planen zu können, ist es hilfreich, den maximal erwünschten Gesamtzeitraum der BIA inklusive Nachbereitung und Auswertung festzulegen. Dadurch können die notwendigen personellen und zeitlichen Ressourcen eingeplant werden (siehe Kapitel 3.2.4 *Ressourcenplanung*).

Die Anzahl der Termine für die BIA-Workshops richtet sich nach der Anzahl zu berücksichtigender Organisationseinheiten im Analysebereich sowie der Anzahl zu berücksichtigender Geschäftsprozesse je Organisationseinheit. Um alle Geschäftsprozesse im Analysebereich der BIA abzudecken, müssen die BIA-Workshops alle Hierarchie-Ebenen der Organisationseinheiten berücksichtigen, nicht nur die unterste Ebene.

Beispiel:

Die Managementprozesse *IT-Strategie* und *IT-Ressourcenmanagement* werden durch die IT-Abteilung verantwortet. Der Unterstützungsprozess *IT Incident Management* wird hingegen durch das Referat IT Help Desk verantwortet. Um alle Geschäftsprozesse in der BIA zu berücksichtigen, ist es empfehlenswert, sowohl einen BIA-Workshop mit einem Ansprechpartner der Abteilung sowie einem Ansprechpartner aus dem Referat IT Help Desk durchzuführen oder die jeweiligen Ansprechpartner gemeinsam in einem Termin zu befragen.

4.4.1.5 Vorbereitung der BIA-Hilfsmittel

Der BCMB muss sicherstellen, dass die Ergebnisse des BIA-Durchlaufs einheitlich und nachvollziehbar dokumentiert werden. Hierzu sollten Hilfsmittel durch den BCMB vorbereitet werden, die den Ansprechpartnern die Schadensbewertung vereinfacht. Da die Schadensbewertung die Parameter aus der Voranalyse nutzt, kann als Übersicht zu Schadenszenarien und Schadenskategorien auf die Hilfsmittel aus der Voranalyse zurückgegriffen werden.

Präsentation zur Erläuterung der BIA

Mit der Präsentation zur Erläuterung der BIA können die Ansprechpartner thematisch auf die Schadensbewertung vorbereitet werden. Dazu ist es empfehlenswert, das Ziel der BIA und die Vorgehensweise zur Schadensbewertung vorzustellen (siehe Abbildung 27). Zudem ist es hilfreich zu erläutern, welche Auswirkungen die Antworten auf die Folgeschritte im BCM-Prozess haben, unter anderem auf die Geschäftsfortführungsplanung. Um die BIA-Methodik vorzustellen, kann die *Präsentationsvorlage Voranalyse/BIA* aus den Hilfsmitteln verwendet werden.

Dokumentenvorlage BIA

Um die Informationen einheitlich und vollständig zu erheben, sollte eine Dokumentenvorlage für die BIA genutzt werden. Diese sollte je Workshop mit den bekannten Informationen zur Organisationseinheit, und sofern bereits bekannt mit den Geschäftsprozessen, im Vorfeld befüllt werden. Dadurch kann im Termin direkt mit der Schadensbewertung begonnen werden. Hierzu kann auf die nachfolgend vorgestellte Liste der Organisationseinheiten und Geschäftsprozesse zurückgegriffen werden. Die Dokumentenvorlage *BIA-Auswertungsbogen* aus den Hilfsmitteln zeigt eine Variante auf, wie eine BIA einheitlich und vollständig erhoben werden kann.

Synergiepotenzial:

Sofern bereits ein ISMS nach der Standard- oder Kern-Absicherung nach BSI-Standard 200-2 besteht, könnten für die Schutzbedarfsfeststellung bereits Hilfsmittel erstellt worden sein, die für die BIA adaptiert werden können.

Liste der Organisationseinheiten und Geschäftsprozesse

Die Institution sollte, sofern noch nicht vorhanden, die Organisationseinheiten mit ihren jeweiligen Geschäftsprozessen definieren und dokumentieren. Die Dokumentation kann z. B. anhand einer Prozesslandkarte oder anderen organisationsbeschreibenden Dokumente stattfinden. Es wird empfohlen, diese Übersicht für die BIA zu nutzen. Dies stellt sicher, dass die Bezeichnungen der Geschäftsprozesse einheitlich verwendet werden und damit eindeutig identifizierbar sind. Ferner ergibt sich aus der Prozesslandkarte, für wie viele Geschäftsprozesse eine Organisationseinheit zuständig ist. Dies kann für die Anzahl oder Dauer der Workshop-Termine mit den Ansprechpartnern relevant sein. Sofern keine Prozesslandkarte vorliegt, können die organisationsbeschreibenden Dokumente helfen, die Geschäftsprozesse im Workshop zu erheben.

Übersicht zu Schadenskategorien und Schadensszenarien

Um eine vergleichbare Schadensbewertung zu erhalten, sollten die Ansprechpartner die Schadensszenarien und Ausprägungen je Schadenskategorie kennen. Wie in Tabelle 10 dargestellt, sollten beide Parameter in einer gemeinsamen Übersicht zusammengefasst und dem Ansprechpartner während des Workshops zur Verfügung gestellt werden.

4.4.2 Durchführung der BIA

Sind die notwendigen Vorbereitungen abgeschlossen, kann mit der BIA begonnen werden. Hierzu müssen die Ansprechpartner der zeitkritischen Organisationseinheiten zum Workshop-Termin eingeladen und befragt werden. Die Durchführung der BIA unterteilt sich in die nachfolgenden zwei Teilprozessschritte **Schadensbewertung** und **Identifizierung der Ressourcenabhängigkeiten**:

4.4.2.1 Schadensbewertung

Die Schadensbewertung umfasst die im Nachfolgenden vorgestellten Teilprozessschritte.

Festlegung des Schadenspotenzials

Durch die Ansprechpartner muss das Schadenspotenzial aller Geschäftsprozesse der Organisationseinheit für alle definierten Zeithorizonte bewertet werden. Hierzu kann auf die Leitfrage zurückgegriffen werden, die z. B. in der Workshop-Präsentation dokumentiert wurde (siehe Kapitel 4.4.1.5 Vorbereitung der BIA-Hilfsmittel).

Tabelle 14 zeigt beispielhaft eine Schadensbewertung für einen Geschäftsprozess anhand der verschiedenen Schadensszenarien. Hierzu werden die Parameter zugrunde gelegt, die in der Voranalyse (siehe Kapitel *4.3.1.1 Konkretisierung des Begriffs zeitkritisch)* festgelegt und um die Zeithorizonte erweitert wurden (siehe Kapitel *4.4.1.2 Festlegung der Zeithorizonte*).

Beispiel: Schadensbewertung des Geschäftsprozesses „Sicherstellung IT-Betrieb“ anhand verschiedener Schadensszenarien

Leitfrage: Wenn der Geschäftsprozess **Sicherstellung IT-Betrieb** ausfällt, mit welchem Schadenspotenzial *[1-gering, 2-mittel, 3-hoch, 4-sehr hoch]* ist bei einem Ausfall bis zu *[24 Stunden, 3 Tage, 7 Tage, 14 Tage, 30 Tage]* zu rechnen?

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

Tabelle 14: Beispiel einer Schadensbewertung anhand der verschiedenen Schadensszenarien

Die Einzelbewertungen je Schadensszenario müssen nicht gesondert dokumentiert werden, um im folgenden Schritt die MTPD (Maximum Tolerable Period of Disruption) festlegen zu können. Um den Dokumentationsaufwand zu reduzieren, kann das Schadenspotenzial anhand des schlimmsten, anzunehmenden Falls (engl.: *worst case*) dokumentiert werden. Entsprechend muss nur das Schadensszenario mit dem jeweils höchsten Schadenspotenzial in einem Zeithorizont dokumentiert werden. Hierzu wurde in der Voranalyse auch das Hilfsmittel *Übersicht zu Schadensszenarien und Schadenskategorien* so aufgebaut, dass dieses die worst-case-Betrachtung erleichtert.

Tabelle 15 greift das Beispiel von Tabelle 14 auf, reduziert jedoch die Schadensbewertung auf eine worst case-Sicht, die alle Schadensszenarien beinhaltet. Neben dem Vorteil, dass die Schadensbewertung beschleunigt wird, ermöglicht diese Sicht einen Gesamtüberblick über die Geschäftsprozesse und deren Schadensbewertung.

Beispiel:

Wenn der nachfolgend aufgeführte Geschäftsprozess ausfällt, mit welchem Schadenspotenzial [1-gering, 2-mittel, 3-hoch, 4-sehr hoch] ist bei einem Ausfall bis zu … zu rechnen?

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

Tabelle 15: Beispiel einer Schadensbewertung nach dem worst case-Prinzip

In der Schadensbewertung muss berücksichtigt werden, dass ein einmal eingetretener Schaden nur gleichbleiben oder weiter steigen, nicht jedoch im Laufe der Zeit wieder abnehmen kann.

Geschäftsprozess	24 Stunden	3 Tage	7 Tage	14 Tage	30 Tage
Geschäftsprozess RICHTIG	2 - mittel	3 - hoch	3 - hoch	4 - sehr hoch	4 - sehr hoch
Geschäftsprozess FALSCH	2 - mittel	2 - mittel	3 - hoch	3 - hoch	2 - mittel

Tabelle 16 zeigt hierzu beispielhaft ein korrektes („Geschäftsprozess RICHTIG“) und ein fehlerhaftes Ergebnis („Geschäftsprozess FALSCH“). Die fehlerhafte Angabe ist rot hervorgehoben.

Beispiel:

Geschäftsprozess	24 Stunden	3 Tage	7 Tage	14 Tage	30 Tage
Geschäftsprozess RICHTIG	2 - mittel	3 - hoch	3 - hoch	4 - sehr hoch	4 - sehr hoch
Geschäftsprozess FALSCH	2 - mittel	2 - mittel	3 - hoch	3 - hoch	2 - mittel

Tabelle 16: Beispiel einer korrekten und fehlerhaften Schadensbewertung

Festlegung der MTPD

Um die MTPD eines Geschäftsprozesses zu bestimmen, muss der kleinste Zeithorizont gewählt werden, bei dem das Untragbarkeitsniveau erreicht wird. Tabelle 17 zeigt einige Beispiele, wie die MTPD anhand des Schadenspotenzials festgelegt wird. Der jeweils relevante, kleinste Zeithorizont, zu dem das Untragbarkeitsniveau erreicht wird, ist rot umrandet.

Beispiel:

Leitfrage: Wenn der Geschäftsprozess ausfällt, mit welchem Schadenspotenzial [1 - gering, 2 - mittel, 3 - hoch, 4 - sehr hoch] ist bei einem Ausfall bis zu … zu rechnen?

Geschäftsprozess	24 Stunden	3 Tage	7 Tage	14 Tage	30 Tage	MTPD
Sicherstellung IT-Betrieb	2-mittel	3 - hoch	4 – sehr hoch	4 – sehr hoch	4 - sehr hoch	3 Tage
Berechtigungsmanagement	1 - gering	2 - mittel	3 - hoch	3 - hoch	3 - hoch	7 Tage
Incident Management	3 - hoch	3 - hoch	3 - hoch	4 - sehr hoch	4 - sehr hoch	24 Stunden
Problem Management	1 - gering	1 - gering	1 - gering	1 - gering	1 - gering	Keine

Tabelle 17: Beispiele für die Festlegung der MTPD (Untragbarkeitsniveau 3-hoch)

Begründung der Schadensbewertung

Die Schadensbewertung muss je Geschäftsprozess begründet und dokumentiert werden. Dies hat drei wesentliche Gründe:

- Wenn die BIA in einem neuen BCMS-Zyklus aktualisiert wird, kann auf die bestehenden Informationen zurückgegriffen werden. In der Zwischenzeit könnten jedoch die Ansprechpartner der BIA gewechselt haben. Damit die Schadensbewertung auch zu einem späteren Zeitpunkt nachvollziehbar ist, sollte diese begründet werden.
- Regulatoren setzen eine Begründung voraus, um auch als außenstehende Dritte die Schadensbewertung dahingehend überprüfen zu können, ob diese plausibel ist.
- Die Begründung dient als Entscheidungshilfe, um geeignete Maßnahmen für die Geschäftsfortführung auszuwählen. Wenn die einzusetzenden finanziellen oder personellen Ressourcen für diese Maßnahmen zu hoch erscheinen, dann hilft eine Begründung aus der BIA mehr als die reine Angabe einer zu erreichenden MTPD.

Die Schadensszenarien, die maßgeblich in der Schadensbewertung zur MTPD beigetragen haben, sollten in der Begründung benannt werden. Wird die BIA aktualisiert, kann so besser überprüft werden, ob die für die Schadensbewertung getroffenen Annahmen noch aktuell sind oder angepasst werden müssen.

Tabelle 18 greift das Beispiel aus Tabelle 15 auf und erweitert dieses um die Begründung der Schadensbewertung. Aus Platzgründen wird die Schadensbewertung ausgeblendet.

Beispiel:

Geschäftsprozess	~	MTPD	Begründung des Schadenspotenzials
Sicherstellung IT-Betrieb	~	3 Tage	Bei Ausfall des Prozesses ist kein IT-Monitoring und keine Wartung der IT-Systeme möglich. Zudem können keine IT-Arbeitsplätze bereitgestellt oder defekte Geräte ausgetauscht werden. Ein kurzfristiger Ausfall des Prozesses bis 24 h führt zu Arbeitsrückständen, wird jedoch nur intern bemerkt. Fällt der Prozess bis zu 3 Tage aus ist eine massive Beeinträchtigung der Aufgabenerfüllung in der gesamten Institution zu spüren, da kein reibungsloser IT-Betrieb garantiert werden kann. Nicht eingespielte Patches bergen zudem ein zunehmendes Sicherheitsrisiko. Ab 7 Tagen ist sowohl mit internem Ansehensverlust als auch mit einer erheblichen negativen Außenwahrnehmung zu rechnen.

Tabelle 18: Beispielhafte Begründung einer Schadensbewertung

Für nicht zeitkritische Geschäftsprozesse entfallen die nachfolgenden Schritte, da diese im Rahmen der Geschäftsfortführungsplanung nicht weiter betrachtet werden

Festlegung des Notbetriebsniveaus

Um im folgenden Schritt die für einen Notbetrieb zwingend erforderlichen Ressourcen ermitteln zu können, sollte vorab festgelegt werden, welches Notbetriebsniveau in einem zeitkritischen Geschäftsprozess erreicht werden soll. Zur Dokumentation des Notbetriebsniveaus genügt eine stichpunktartige Beschreibung, welche Aktivitäten des Geschäftsprozesses innerhalb des Notbetriebs aufrechterhalten werden sollen bzw. welche Aktivitäten zurückgestellt werden können. Je nach Aufgaben- bzw. Geschäftszweck ist auch eine prozentuale Angabe des Notbetriebsniveaus möglich, z. B. im produzierenden Gewerbe. Die Informationen zum Notbetriebsniveau können anschließend in der Geschäftsfortführungsplanung weiter konkretisiert werden (siehe Kapitel *4.6 Geschäftsfortführungsplanung*).

Beispiel:

Geschäftsprozess	~	Notbetriebsniveau
Sicherstellung IT-Betrieb	~	Der Fokus liegt auf dem IT-Monitoring sowie Patchen von IT-Systemen. Wartungsarbeiten, die nicht der Sicherheit oder Stabilität des IT-Betriebs dienen, werden zurückgestellt. Anfragen von Organisationseinheiten zum Austausch fehlerhafter Geräte oder dem Bereitstellen neuer Geräte werden nach Dringlichkeit bearbeitet und unter Umständen zurückgestellt.
Incident Management	~	Der Fokus liegt auf der Bearbeitung von Major Incident-Tickets. Wenn der Notbetrieb nur wenige Tage andauert, können bei 50% Arbeitsvolumen die entstehenden Arbeitsrückstände leicht kompensiert werden. Da mit jedem weiteren Tag auf Notbetriebsniveau jedoch Tickets unbearbeitet bleiben, muss das Notbetriebsniveau schrittweise auf 80% Arbeitsvolumen gesteigert werden.

Tabelle 19: Beispiel eines Notbetriebsniveaus als Beschreibung

Zudem kann es hilfreich sein, nicht nur den Zielzustand des Notbetriebsniveaus zu beschreiben, sondern auch mögliche kurz- und langfristige Ziele, z. B. was soll in den ersten Stunden, Tagen oder bis Zeitraum x im Notbetrieb erreichen werden? Wenn das Notbetriebsniveau über einen zeitlichen Verlauf betrachtet wird, kann die Information dabei helfen den Ressourcenbedarf im Notbetrieb zeitlich differenziert zu erheben.

Die Schadensbewertung ist abgeschlossen, wenn

- die Geschäftsprozesse im Prozessumfang hinsichtlich ihres Schadenspotenzials bewertet,
- die MTPD je zeitkritischem Geschäftsprozess festgelegt und begründet sowie
- für zeitkritische Geschäftsprozesse das erforderliche Notbetriebsniveau definiert wurde.

4.4.2.2 Identifizierung der Ressourcenabhängigkeiten

Für alle Geschäftsprozesse mit einer MTPD müssen anhand der festgelegten Ressourcenkategorien (siehe Kapitel 4.4.1.3 *Festlegung der Ressourcenkategorien und -cluster*) die für einen Notbetrieb erforderlichen Ressourcen ermittelt und den entsprechenden Geschäftsprozessen zugeordnet werden.

Erfahrungsgemäß wird nicht jede Ressource, die von einem Geschäftsprozess im Normalbetrieb genutzt wird, auch per se in einem Notbetrieb benötigt. Zum einen können Ressourcen entfallen, die lediglich für zurückgestellte Aktivitäten gemäß dem definierten Notbetriebsniveau benötigt werden. Zum anderen werden in der Praxis häufig Ressourcen eingesetzt, die einen Geschäftsprozess im Normalbetrieb effizienter oder einfacher gestalten, aber nicht zwingend erforderlich sind, um das gewünschte Prozessergebnis auf dem definierten Notbetriebsniveau zu erreichen. Da im BCM prinzipiell nur die für einen Notbetrieb erforderlichen Ressourcen besonders abgesichert und in der weiteren Notfallplanung berücksichtigt werden sollen, kann auf die Angabe von Ressourcen, die nur im Normalbetrieb eingesetzt werden, bewusst verzichtet werden.

Beispiel:

Ein Mitarbeiter kann über ein *Customer-Relationship-Management (CRM)-System* schnell Kontakte identifizieren und Zusatzinformationen abrufen. Im Notbetrieb genügt es aber möglicherweise nur über die Kontaktdaten aus einem Adressbuch zu verfügen, die hilfreich sind um den Geschäftsprozess aufrechtzuerhalten.

Die Ressourcen(-cluster) sollten anhand vorgegebener Listen ermittelt und dokumentiert werden. So werden unterschiedliche Namen oder Schreibweisen für gleiche Ressourcen(-cluster) vermieden und Dubletten ausgeschlossen. Zusätzliche Aufwände in der BIA-Auswertung, um Dubletten zu identifizieren und zusam-

menzuführen, können damit vermieden werden. Je zeitkritischem Geschäftsprozess muss festgelegt und dokumentiert werden, welche Ressourcen(-cluster) benötigt werden, um das vorab definierte Notbetriebsniveau zu erreichen. Relevant für die weiteren Schritte in der Notfallplanung der Ressourcen sind die geforderte Wiederanlaufzeit (RTO) und der maximal zulässige Datenverlust (RPO).

RTO

Anhand der MTPD des zeitkritischen Geschäftsprozesses muss die RTO der prozessnotwendigen Ressourcen(-cluster) abgeleitet werden.

Hinweis:

Ähnlich wie die MTPD in den Prozessabhängigkeiten kann auch die RTO individuell abgestimmt werden. Diese ist von folgenden Faktoren abhängig:

- Der zeitlichen Lücke, die sich aus dem Detektions- und Alarmierungsprozess ergibt
- Dem angestrebten Notbetriebsniveau und damit dem Leistungsumfang der Ressource
- Der Art der Prozessunterstützung (Ressource wird benötigt, um den Geschäftsprozess wiederanlaufen, ausführen oder abschließen zu können)

Da in einem Reaktiv-BCMS voraussichtlich noch keine Erfahrungen über die Dauer der Alarmierung vorliegen, kann die RTO näherungsweise mit der Angabe „<“ dokumentiert werden. Die Angabe sollte jedoch in der Weiterentwicklung des BCMS schrittweise konkretisiert werden.

Wenn mehrere Geschäftsprozesse auf dieselbe(n) Ressourcen(-cluster) zurückgreifen, muss die RTO kleiner als die MTPD des zeitkritischsten Geschäftsprozesses im Prozessumfang der BIA gewählt werden (Minimalprinzip). Tabelle 20 greift die Beispiele der Geschäftsprozesse aus Tabelle 17 auf und erweitert diese um die benötigten Ressourcen je Geschäftsprozess. Indem z. B. die Tabelle nach den Ressourcen sortiert wird, wird anhand der mehrfach genannten Ressourcen ersichtlich, wie die kleinste RTO daraus abgeleitet werden kann.

Beispiel (sortiert nach Ressource):

Ressourcen, deren RTO auf Grund des Minimalprinzips ermittelt wurden, sind rot hervorgehoben.

Ressourcen-kategorie	Ressource	RTO	Geschäftsprozess	MTPD
IT	Telefonie	20 Stunden	Incident Management	24 Stunden
IT	Monitoringtool MT	< 3 Tage	Sicherstellung IT-Betrieb	3 Tage
IT	Monitoringtool MT	< 3 Tage	Berechtigungsmanagement	7 Tage
IT	Identity & Access Management Tool IAM	5 Tage	Berechtigungsmanagement	7 Tage
Dienstleistungen	IT-Provider XYZ	8 Stunden	Sicherstellung IT-Betrieb	3 Tage
Dienstleistungen	IT-Provider XYZ	8 Stunden	Berechtigungsmanagement	7 tage
Informationen	Konfigurationsdaten	n/a	Sicherstellung IT-Betrieb	3 Tage

Tabelle 20: Beispiele verschiedener Ressourcenabhängigkeiten von Geschäftsprozesse

RPO

Bei informationsbasierten Ressourcenkategorien, wie im vorliegenden Beispiel IT und Informationen, muss zusätzlich die RPO festgelegt werden. Die RPO stellt in diesem Zusammenhang eine fachliche Anforderung des Prozesseigentümers dar, bis zu welchem Grad er eine Datensicherung voraussetzt, um mit geeigneten Informationen im Notbetrieb arbeiten zu können. Die RPO ist **unabhängig** von der MTPD und muss daher nicht darauf abgestimmt werden. Jedoch sollte analog zur RTO auch die RPO konsolidiert werden, wenn mehrere Geschäftsprozesse auf dieselbe(n) informationsbasierten Ressourcen(-cluster) zurückgreifen (Minimalprinzip). Tabelle 21 greift die Beispiele der Tabelle 17 auf, analog zu Tabelle 20.

Beispiel:

Ressourcen-kategorie	Ressource	Konsolidierte RPO	Geschäftsprozess	RPO
Informationen	Konfigurationsdaten	Transaktionsgenau	Berechtigungsmanagement	Transaktionsgenau
Informationen	Konfigurationsdaten	Transaktionsgenau	Sicherstellung IT-Betrieb	Letzte Tagessicherung

Tabelle 21: Beispiele Informationsbasierter Ressourcenabhängigkeiten von Geschäftsprozessen

Synergiepotenzial:

Die RPO sollte bereits innerhalb des Normalbetriebs z. B. als Datensicherungsintervall definiert worden sein und kann hier zugrunde gelegt werden. Sofern die RPO nicht definiert oder nicht bekannt ist, genügt an dieser Stelle die Information, welcher Datenverlust im Notbetrieb zulässig wäre. Üblicherweise bestehen im IT-Betrieb bereits verschiedene Stufen von Datensicherungsintervallen. Für die Angabe der RPO ist es empfehlenswert, sich auf diese Stufen zu beziehen oder abgestimmt mit dem IT-Betrieb diese Stufen zu erweitern.

Ressourcenbedarf in Abhängigkeit zur Dauer des Notbetriebs

Für bestimmte Ressourcenkategorien wie z. B. Personal und Arbeitsplätze, aber auch Maschinen oder Arbeitsmittel steigt die Anzahl der benötigten Ressourcen mit der Dauer des Ausfalls erfahrungsgemäß an. Dies hat einerseits damit zu tun, das ansteigende Arbeitsvolumen aufzufangen (z. B. durch ein steigendes Notbetriebsniveau) als auch andererseits die weiteren, zeitkritischen Geschäftsprozesse bedienen zu können. Für diese Ressourcenkategorien ist es empfehlenswert, die Anzahl der benötigten Ressourcen über die definierten Zeithorizonte im Notbetrieb hinweg zu erheben.

Bei der Ressource Personal ist es empfehlenswert, zu berücksichtigen, ob sich die Anzahl je Geschäftsprozess aufsummiert oder unterschiedliche zeitkritische Geschäftsprozesse jeweils die gleichen Personen oder Rollen benötigen. In diesem Fall ist es empfehlenswert, die Anzahl kumuliert anstatt pro Geschäftsprozess zu erheben. Dies hat zum Ziel, Ressourcen, die für mehrere Geschäftsprozesse benötigt werden, nicht mehrfach oder als Bruch erfassen zu müssen. Tabelle 22 gibt ein Beispiel für die zeitlich gestaffelte Erhebung anhand des Arbeitsplatz- und Rollenbedarfs der Organisationseinheit wieder.

Beispiel: Benötigte Anzahl Arbeitsplätze oder Personal im Notbetrieb der Organisationseinheit IT-Betrieb

Ressourcen-kategorie	Ressource	Anmerkungen	24 Stunden	3 Tage	7 Tage	14 Tage	30 Tage
Arbeitsplatz	Standard-Arbeitsplatz		2	2	2	4	4
Personal	Teamleiter	arbeiten remote	1	2	2	2	2
Personal	IT-Help Desk-Mitarbeiter		2	2	2	4	4
Personal	Datenbank-Administrator	arbeiten remote	1	2	3	3	3

Tabelle 22: Beispiele für Arbeitsplatz- und Personalabhängigkeiten

Im Beispiel wird angenommen, dass die Organisationseinheit über 2 Teamleiter, 4 Help Desk-Mitarbeiter, 4 System-Administratoren und 3 Datenbank-Administratoren verfügt. Jede dieser Personen verfügt im Normalbetrieb über einen eigenen Arbeitsplatz. Während eines eingeschränkten Notbetriebs werden innerhalb der ersten 24 Stunden zunächst nur 1 Teamleiter, 2 Help Desk-Mitarbeiter und 1 Datenbank-Administrator benötigt, da nur das Incident Management entsprechend zeitkritisch ist. Hierbei werden nur 2 Arbeitsplätze benötigt, damit die Help Desk-Mitarbeiter agieren können. Der Teamleiter und die Administratoren können mobil arbeiten.

4.4.3 Auswertung der BIA

Nachdem die BIA durchgeführt wurde, müssen die Ergebnisse im Rahmen der BIA-Auswertung qualitätssichert und zusammengefasst werden. Um ein einheitlich hohes Qualitätsniveau der BIA-Ergebnisse sicherzustellen, müssen die BIA-Ergebnisse dahingehend überprüft werden, dass diese vollständig, richtig und nachvollziehbar sind. Hierzu ist es empfehlenswert zu überprüfen, ob sämtliche notwendigen Informationen erhoben sowie die Schadensbewertung formal korrekt vorgenommen wurde und die Begründung der Schadensbewertung plausibel erscheint. Zusätzlich ist es hilfreich zu prüfen, ob die RTO der Ressourcen korrekt aus der MTPD der zeitkritischen Prozesse abgeleitet wurde. Falls einzelne Ergebnisse nicht plausibel oder inkorrekt erscheinen, sollte Rücksprache mit den Ansprechpartnern gehalten und die Ergebnisse gemeinsam abgestimmt werden.

Nachdem die Ergebnisse qualitätsgesichert wurden, ist es empfehlenswert, die Einzelergebnisse zu einer Gesamtübersicht der zeitkritischen Geschäftsprozesse und Ressourcen zusammenzufassen. Die BIA-Auswertung schafft damit die notwendigen Voraussetzungen, um mit dem Soll-Ist-Vergleich sowie der Geschäftsfortführungsplanung beginnen zu können.

4.5 Soll-Ist-Vergleich

Als Ergebnis der BIA liegen für alle betrachteten zeitkritischen Ressourcen die RTOs sowie gegebenenfalls die RPO vor. RTO und RPO stellen gewünschte Soll-Werte dar. Die Ressourcenzuständigen müssen im Rahmen des Soll-Ist-Vergleichs die Frage beantworten, ob die RTO tatsächlich erreicht werden kann. Hierzu wird der RTO (geforderte Wiederanlaufzeit) die **Recovery Time Achievable** (**RTA**, deutsch: erreichbare Wiederanlaufzeit), gegenübergestellt und die Zeitwerte miteinander verglichen. Die RTA einer zeitkritischen Ressource bezeichnet den real erreichbaren Zeitraum, von dem Zeitpunkt, an dem die Ressource ausfällt bis zum Zeitpunkt, an dem eine Notfall-Lösung produktiv gesetzt wird. Aus Vereinfachungsgründen wird nachfolgend nur bei Abweichungen im Vorgehen auf die RPO eingegangen. Ansonsten gilt das Vorgehen analog zum RTO Soll-Ist-Vergleich.

Die nachfolgenden Kapitel beschreiben die empfohlene Vorgehensweise, mittels derer der Soll-Ist-Vergleich durchgeführt wird. In Abbildung 29 sind die hierfür erforderlichen Schritte in einer Übersicht dargestellt.

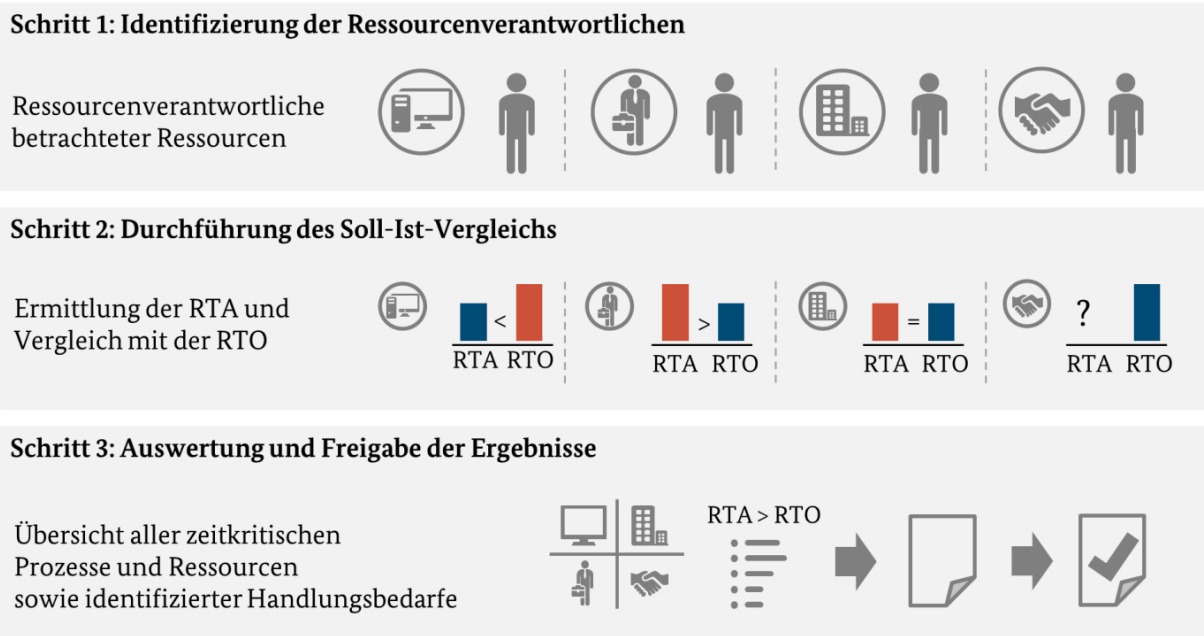

Abbildung 29: BCM-Prozessschritte zum Soll-Ist-Vergleich

4.5.1 Identifizierung der Ressourcenzuständigen

Vor dem Soll-Ist-Vergleich müssen die Ressourcenzuständigen identifiziert werden. Da der BCMB in der Regel über den besten Gesamtüberblick über die BIA-Ergebnisse verfügt, ist es empfehlenswert, dass er diese Aufgabe übernimmt. Hierzu kann er anhand der Ressourcenkategorien vorgehen. Tabelle 23 gibt beispielhaft die typischen Ansprechpartner je Ressourcenkategorie wieder. Falls die Institution abweichende Ressourcenkategorien benannt hat, so müssen diese entsprechend berücksichtigt werden.

Einen direkten Überblick über die Zuständigkeiten einzelner Ressourcen haben die jeweiligen Leiter der Organisationseinheiten, die für die entsprechende Ressourcenkategorie zuständig sind. Die Leiter sollten darüber informiert werden, welche Angaben für den Soll-Ist-Vergleich benötigt werden und welche Relevanz diese Informationen für die weiteren Schritte im BCM haben. Die Leiter können die relevanten Ressourcenzuständigen benennen, um die erforderlichen Informationen einzuholen.

Beispiel:

Ressourcenkategorie	**Geschäftsprozess-** bzw. **Ressourcenzuständige**
IT	Leiter IT
Personal	Leiter Personal
Arbeitsplätze	Leiter Gebäudeverwaltung/Haustechnik
Dienstleistungen	Leiter Einkauf/Provider Management oder dezentrale Provider/Supplier Manager
Informationen	• zentrale physische Daten: Leiter Aktensammelstelle/Archiv • dezentrale physische Daten: Leiter der jeweiligen OE (gemäß BIA) • Bei elektronischen Daten: Leiter IT
Infrastruktur	Leiter Infrastruktur/Werksleiter/Technischer Betriebsleiter
Maschinen/Geräte/ Anlagen/Fahrzeuge	Leiter Infrastruktur/Werksleiter/Technischer Betriebsleiter
Betriebsmittel (Sonstige)	Leiter Infrastruktur/Werksleiter/Technischer Betriebsleiter

Tabelle 23: Ressourcenzuständige (Beispiele)

Für die Sensibilisierung der relevanten Personen kann die *Präsentation zur Erläuterung der BIA* dienen (siehe Kapitel 4.4.1.5 *Vorbereitung der BIA-Hilfsmittel*). Diese kann im Rahmen einer Informationsveranstaltung vorgestellt oder als Begleitmaterial zu einer Informations-E-Mail an die relevanten Personen gesendet werden.

Synergiepotenzial:

Falls bereits ein ISMS nach BSI-Standard 200-2 vorliegt und der Informationsverbund ähnlich zum Geltungsbereich des BCMS festgelegt ist, können die Ressourcenzuständigen anhand der Strukturanalyse ermittelt werden.

4.5.2 Durchführung des Soll-Ist-Vergleichs

Die Ressourcenzuständigen müssen im Rahmen des Soll-Ist-Vergleichs die Frage beantworten, ob die RTO der Ressource durch vorhandene technische und organisatorische Maßnahmen erreicht werden kann.

Hierzu wird der RTO (geforderte Wiederanlaufzeit) die RTA (erreichbare Wiederanlaufzeit) gegenübergestellt und die Zeitwerte miteinander verglichen.

Die RTA kann im Rahmen von Übungen und Tests (siehe Kapitel 4.7 *Üben und Testen*) ermittelt und nachgewiesen werden. Für die Ressourcenkategorie Dienstleistungen muss in den bestehenden Verträgen oder Service Level Agreements geprüft werden, ob Aussagen zur Realisierbarkeit der RTO vorliegen.

Da der PDCA-Lebenszyklus bei einem Reaktiv-BCMS erstmalig durchlaufen wird, kommt es häufig vor, dass noch keine Ergebnisse zu Notfallübungen und -Tests vorliegen. In diesem Fall kann die RTA realistisch geschätzt werden. Falls keine Schätzung möglich ist oder keine technischen und organisatorischen Wiederanlaufmaßnahmen vorliegen, so muss die RTA als unbekannt gekennzeichnet werden.

Der Soll-Ist-Vergleich kann per E-Mail oder über ein Tool abgefragt werden. Auch können Einzelgespräche zwischen dem BCMB und den Ressourcenzuständigen durchgeführt werden. Dies ist insbesondere bei kleinen Institutionen mit wenigen zeitkritischen Ressourcen sinnvoll. Hierzu sollten jeweils mit den vorhandenen Informationen aus der BIA die benötigten Informationen für den Soll-Ist-Vergleich abgefragt werden. Dies sollte anhand eines einheitlichen Schemas abgefragt werden, um eine Auswertung über alle Ressourcen effektiv zu ermöglichen. Tabelle 24 zeigt dies am Beispiel von IT-Ressourcen.

Beispiel:

Ressourcen-kategorie	Ressource	RTO	RTA	Nachweis	RTA ≤ RTO
IT	Standard-IT-Ausstattung	< 3 Tage	2 Tage	Schätzung anhand des Regelprozesses	Ja
IT	Mailservice	< 1 Tag	05:45 h	Funktionstest	Ja
IT	Fileserver	< 1 Tag	unbekannt	nicht vorhanden	unbekannt

Tabelle 24: Beispiel eines Soll-Ist-Vergleichs der RTO anhand der Ressourcenkategorie IT

Für die Ressourcenkategorien, für die eine RPO festgelegt wurde, muss diese mit dem festgelegten Datensicherungszyklus gemäß des IT-Betriebs abgeglichen werden (siehe *Tabelle 25*).

Beispiel:

Ressource	RPO	Datensicherungs-zyklus der IT	Nachweis	Datensicherung ≤ RPO
Kundendaten	Vortag	12 Stunden	Betriebshandbuch	Ja

Tabelle 25: Beispiel eines Soll-Ist-Vergleichs der RPO

4.5.3 Auswertung und Freigabe der Ergebnisse

Es muss eine Übersicht aller Ressourcen, insbesondere jedoch der unzureichend abgesicherten Ressourcen, erstellt und mit der Institutionsleitung abgestimmt werden, damit diese sich der aktuellen Risikosituation bewusst ist. Der Institutionsleitung sollten hierzu folgende Informationen vorgestellt und durch diese bestätigt werden:

- Übersicht über die zeitkritischen Geschäftsprozesse gemäß BIA,

- Übersicht über die zeitkritischen Ressourcen gemäß BIA,
- Übersicht über die unzureichend abgesicherten Ressourcen gemäß Soll-Ist-Vergleich sowie
- Einschätzung möglicher Risiken aus den identifizierten Lücken gemäß Soll-Ist-Vergleich.

Der weitere Handlungsbedarf wird im Reaktiv-BCMS anhand der Geschäftsfortführungsplanung abgeleitet (siehe Kapitel 4.6.2 *Erstellung der GFPs*).

4.6 Geschäftsfortführungsplanung

Innerhalb der Geschäftsfortführungspläne (GFPs) wird dokumentiert, wie die Institution auf der Prozessebene auf eine Geschäftsunterbrechung nach einem Ressourcenausfall reagiert. Die Geschäftsfortführungsplanung muss für alle zeitkritischen Geschäftsprozesse durchgeführt und dokumentiert werden.

Die Geschäftsfortführungsplanung strebt an, konkrete Notfallmaßnahmen zu beschreiben, mit denen zeitkritische Geschäftsprozesse innerhalb der jeweiligen MTPD auf dem in der BIA definierten Notbetriebsniveau wiederaufgenommen oder fortgeführt werden können. Das Reaktiv-BCMS beschränkt sich dabei auf Notfallmaßnahmen, die mit den vorhandenen Mitteln und Ressourcen der Institution möglich sind oder durch kurzfristig umsetzbare Investitionen realisiert werden können. Um die Geschäftsfortführung zu planen, kann die Dokumentenvorlage *Geschäftsfortführungsplan* aus den Hilfsmitteln verwendet werden. Anhand dieser Dokumentenvorlage werden einige der in diesem Kapitel aufgeführten Beispiele und Hinweise dargestellt. Der Detailgrad der beschriebenen Maßnahmen sollte dabei so gewählt sein, dass eine fachkundige dritte Person in der Lage wäre, die Geschäftsfortführung anhand des GFP umzusetzen.

Die nachfolgenden Kapitel beschreiben die empfohlene Vorgehensweise, mittels derer die GFP erstellt werden. In Abbildung 30 sind die hierfür erforderlichen Schritte in einer Übersicht dargestellt.

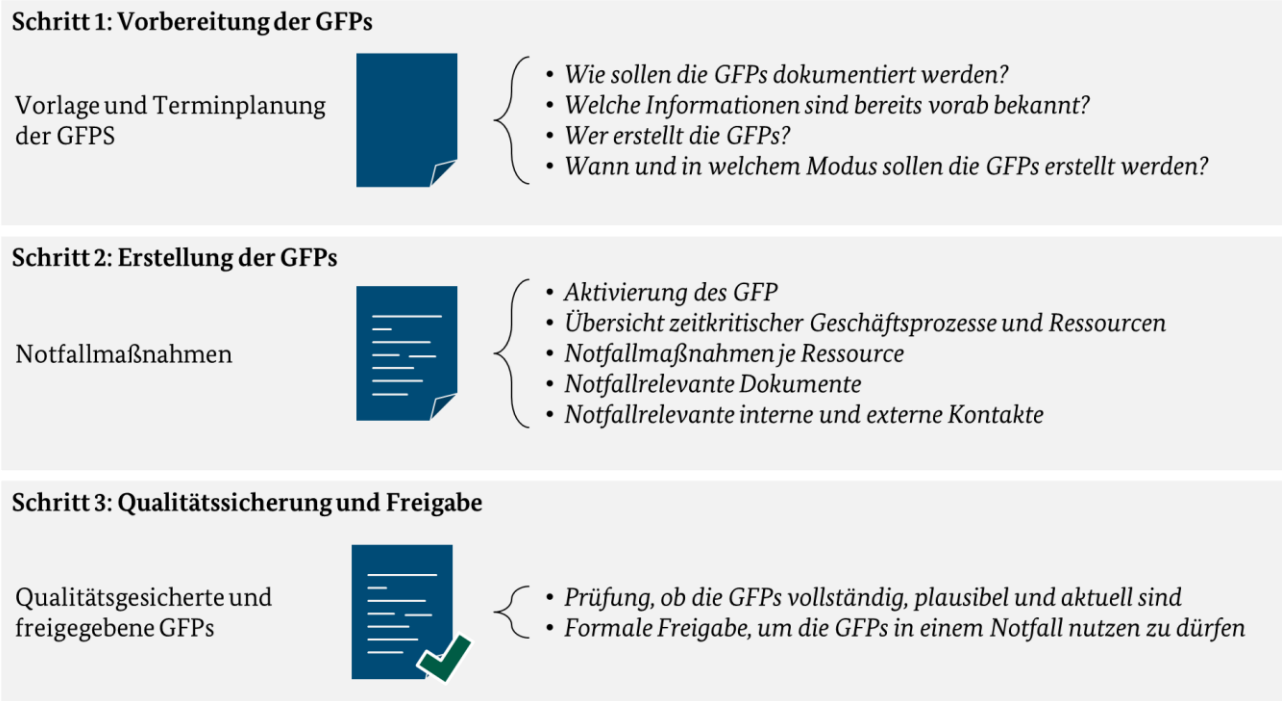

Abbildung 30: BCM-Prozessschritte der Geschäftsfortführungsplanung

Da die Geschäftsfortführungspläne üblicherweise von den Organisationseinheiten selbst erstellt werden, ist es sinnvoll diesen Schritt zentral innerhalb der Notfallvorsorgeorganisation vorzubereiten. Die Geschäftsfortführungsplanung ist abgeschlossen, sobald alle GFPs zentral abgelegt und die Institutionsleitung über den Abschluss der Geschäftsfortführungsplanung informiert wurde.

4.6.1 Vorbereitung der GFPs

Eine effektive Vorbereitung der GFPs ist die Voraussetzung dafür, dass

- die Erstellung der GFPs effizient, vergleichbar und valide durchgeführt werden kann,
- die Teilnehmer optimal auf die Fragestellungen vorbereitet werden, sowie
- im Notfall die Leser die GFPs gut lesen und schnell anwenden können.

Die Erstellung der GFPs sollte daher vorbereitet werden. Es ist empfehlenswert, dass die Vorbereitung durch den BCMB erfolgt, da dieser über das notwendige Fachwissen zum BCM-Prozess verfügt und diesen zeitlich steuert. Er kann vorbereitende Tätigkeiten ganz oder teilweise an weitere Rollen im BCM delegieren, z. B. an lokale BCMB, BCMK oder ein Notfallvorsorgeteam (siehe Kapitel 3.2.2 *Definition der BCM-Aufbauorganisation*). Die Aufgaben in der Vorbereitung der GFPs werden in den nachfolgenden Unterkapiteln näher erläutert. Die Kapitel folgen einer logischen Reihenfolge. Jedoch können sich verschiedene darin beschriebene Aufgaben in der Praxis zeitlich überlagern.

4.6.1.1 Organisatorische Aufteilung der GFPs

Der BCMB muss festlegen, wie die GFPs im Hinblick auf die zugrundeliegende Struktur der Institution aufgeteilt werden sollen. Es gibt viele Möglichkeiten, wie GFPs organisatorisch aufgeteilt werden könnten. So könnte ein GFP je Geschäftsprozess erstellt werden oder für ein bestimmtes Ausfallszenario die jeweils relevanten Ressourcen wiedergeben. Entscheidend für eine schnelle Notfallreaktion ist jedoch, dass

- eine anschauliche Übersicht über die zeitkritischen Geschäftsprozesse und Ressourcen ermöglicht wird sowie
- die Zuständigkeiten der im GFP beschriebenen Notfallmaßnahmen möglichst klar geregelt sind.

Hierbei hat es sich in der Praxis bewährt, einen GFP je Organisationseinheit zu erstellen. Dieses Vorgehen bietet viele Vorteile. Die zuständigen Ansprechpartner, die den GFP erstellen und aktualisieren, können eindeutig der Organisationseinheit zugeordnet werden. Zudem wird eine überschaubare Anzahl an Dokumenten erzeugt und die GFPs spiegeln die vertraute Organisationsstruktur wider. Die GFPs lassen sich so leichter voneinander abgrenzen.

Im Einzelfall kann es sinnvoll sein, von dieser Struktur abzuweichen. Dies ist etwa der Fall, wenn

- Verantwortungs- und Tätigkeitsbereiche nicht klar voneinander abgrenzbar sind, z. B. in einer Matrix-Organisation, oder
- Organisationseinheiten standortübergreifend agieren und auf unterschiedliche Ressourcen zugreifen.

Zusätzlich können länderspezifische Anforderungen und Gegebenheiten unter Umständen dazu führen, dass für gleiche Geschäftsprozesse und Ressourcen im GFP unterschiedliche Notfallmaßnahmen an unterschiedlichen Standorten beschrieben werden müssen.

Hinweis:

Ob die GFPs sinnvoll aufgeteilt und voneinander abgegrenzt wurden, kann mitunter erst im Rahmen der Erstellung der GFPs fundiert bewertet werden. Der BCMB sollte daher die Aufteilung der GFPs im Rahmen der Erstellung der GFPs mit den entsprechenden Ansprechpartnern diskutieren und gegebenenfalls den Geltungsbereich des GFP anpassen bzw. in mehrere GFPs aufteilen.

Alternativ können GFPs auch nach Geschäftsprozessen unterteilt werden, was jedoch zu einer hohen Anzahl an Dokumenten führen kann. Um die Erläuterungen in den folgenden Kapiteln zu vereinfachen, wird davon ausgegangen, dass die GFPs entsprechend der Organisationseinheiten aufgeteilt wurden. Werden die GFPs

in der Institution anderweitig aufgeteilt, so sollten die Inhalte dieses Standards angepasst auf die eigene Vorgehensweise angewendet werden.

4.6.1.2 Erstellung einer GFP-Dokumentenvorlage

Um die Geschäftsfortführung im Notfall zu erleichtern, sollte der BCMB sicherstellen, dass die GFPs einheitlich aufgebaut und nachvollziehbar dokumentiert sind. Hierzu sollte eine GFP-Dokumentenvorlage erstellt werden. Die nachfolgenden Aspekte sollten darin berücksichtigt werden:

Der **Geltungsbereich** beschreibt den organisatorischen und räumlichen Bereich, in welchem die Maßnahmen und Verfahren eines GFP gelten. Die Beschreibung des Geltungsbereichs stellt sicher, dass der GFP sowie die darin beschriebenen Maßnahmen ausschließlich in dem für ihn vorgesehenen Umfeld eingesetzt werden. Es könnte z. B. vorkommen, dass die beschriebenen Maßnahmen nicht in anderen Organisationseinheiten sowie Standorten eingesetzt werden können oder den dort notwendigen Maßnahmen widersprechen.

Die **Zielstellung des GFP** beschreibt, was durch den GFP erreicht werden soll und was explizit nicht durch den GFP forciert wird. Die Beschreibung der Zielstellung stellt sicher, dass der GFP nur zu seinem gedachten Zweck eingesetzt wird und nicht etwa im Rahmen des Normalbetriebs zweckentfremdet oder mit anderen Themen vermischt wird (siehe Aktivierungsprozess).

Der **Aktivierungsprozess** wird in Kapitel 4.6.2.1 *Festlegung organisatorischer Maßnahmen* näher erläutert.

Die **gesonderten Rechte und Pflichten der Mitarbeiter** werden in Kapitel 4.6.2.1 *Festlegung organisatorischer Maßnahmen* näher erläutert.

Die **besonderen Melde- und Berichtspflichten** werden in Kapitel 4.6.2.1 *Festlegung organisatorischer Maßnahmen* näher erläutert.

Innerhalb des GFP werden alle **zeitkritischen Geschäftsprozesse** im Geltungsbereich des GFP sowie deren MTPD dokumentiert. Die Dokumentation hat zum Ziel, dem Stab im Notfall eine Übersicht über die zeitkritischen Geschäftsprozesse im Geltungsbereich sowie deren MTPD zu verschaffen. Die Auflistung schafft Transparenz über die bestehenden zeitkritischen Geschäftsprozesse sowie über die zeitliche Reihenfolge, in welcher diese wieder in einem Notbetrieb anlaufen müssen.

Alle **zeitkritischen Ressourcen** der betrachteten Organisationseinheit sowie die identifizierten RTOs bzw. RTAs sowie RPOs werden innerhalb des GFP dokumentiert. Anhand der aufgelisteten Ressourcen sollen innerhalb des GFP konkrete Notfallmaßnahmen abgeleitet werden (siehe Kapitel 4.6.2 *Erstellung der GFPs*). Die Notfallmaßnahmen zielen darauf ab, die Geschäftsprozesse bei Ausfall der Ressourcen innerhalb der RTO auf dem vorgegebenen Notbetriebsniveau fortzuführen.

Innerhalb des GFP werden sämtliche internen sowie externen **Kontakte** dokumentiert, die im Rahmen der Geschäftsfortführung **relevant** sein könnten. Hierunter fallen etwa Mitarbeiter aus anderen Fachbereichen, interne oder externe Fachexperten sowie innerhalb der Organisationseinheit eingesetzte Dienstleister. Die Dokumentation der relevanten Kontakte ermöglicht einen schnellen Zugriff auf die entsprechenden Stellen sowie eine Unabhängigkeit von anderen, möglicherweise nicht verfügbaren Kontakt-Quellen wie digitalen Telefonbüchern. Sofern die Kontakt-Informationen bereits ausfallsicher an anderer Stelle dokumentiert sind, genügt es, im GFP die Kontakt-Informationen zu referenzieren und im Notfall verfügbar zu machen.

Innerhalb des GFP sollten alle zur Geschäftsfortführung **relevanten Dokumente** sowie ihre jeweiligen Ablageorte notiert werden. Mögliche Dokumente sind etwa Prozessbeschreibungen oder Handlungsanweisungen. Für den Fall eines Notfalls kann durch die Verweise schnell auf die relevante Information in den jeweiligen Dokumenten zugegriffen werden. Voraussetzung ist, dass die für die Notfallbewältigung benötigten Dokumente schnell zu erfassen sind und konkrete Notfallmaßnahmen leicht daraus abgeleitet werden können. Es muss jedoch sichergestellt werden, dass die Ablageorte entsprechend des Schutzbedarfs abgesichert und auch im Notfall zugänglich sind.

Hinweis

Sofern für die Geschäftsfortführung auf Informationen in anderen Dokumenten zurückgegriffen werden soll, ist es empfehlenswert, dass alle im GFP aufgeführten Dokumente am Ende des GFP noch einmal in einer Gesamtliste der benötigten Dokumente namentlich aufgeführt werden. Zusätzlich sollte dann je Dokument der jeweilige Ablageort referenziert werden.

Gegliedert nach Ressourcenkategorien sollten die **Notfallmaßnahmen** unterteilt werden in:

- Maßnahmen, um den Notbetrieb zu erreichen
- Maßnahmen, um den Notbetrieb aufrecht zu erhalten, falls sich dies vom Normalbetrieb unterscheidet
- Maßnahmen, um den Normaltbetrieb aus dem Notbetrieb zu erreichen.
- Weitere Details sind in Kapitel 4.6.2.2 *Entwicklung von Notfallmaßnahmen* beschrieben.

4.6.1.3 Vorausfüllen der GFP

Der BCM-Beauftrage oder weitere Mitglieder der Notfallvorsorgeorganisation sollten die GFP-Erstellung vorbereiten, indem sie die erstellten GFP-Vorlagen mit den bereits bekannten Informationen aus BIA und Soll-Ist-Vergleich vorausfüllen. Dies stellt eine höhere Datenqualität sicher und sorgt dafür, dass sich die Organisationseinheiten auf die wesentlichen Fragestellungen konzentrieren können, nämlich wie der Notbetrieb der Organisationseinheit ausgestaltet sein soll. Zu den bereits bekannten Informationen gehören z. B.:

- der Geltungsbereich des GFP
- die zeitkritischen Geschäftsprozesse in diesem Geltungsbereich
- die MTPD und das Notbetriebsniveau jedes gelisteten Geschäftsprozesses
- die zeitkritischen Ressourcen mit ihrer jeweiligen RTA sowie RPO

Um ursachenbasiert konkrete Notfallmaßnahmen zu beschreiben, bietet es sich in einem GFP an, die relevanten Informationen anhand der Ressourcenkategorien zuzuordnen. Dies erlaubt einen schnellen Zugriff auf die Informationen im Notfall.

4.6.1.4 Organisatorische Planung

Die Geschäftsfortführungsplanung kann weitestgehend analog zum Vorgehen in der BIA organisiert werden (siehe Kapitel 4.4.1.4 *Organisatorische Planung*). Insbesondere, wenn GFPs erstmalig erstellt werden, sollte der BCMB dies im Rahmen von Workshops durchführen. Er kann hierbei die Methodik und die Inhalte des GFP erläutern und den Workshop moderieren.

Es ist empfehlenswert, dass die gleichen Personen wie in den vorangegangenen Schritten zur BIA am Workshop teilnehmen. Dieser Personenkreis verfügt in der Regel über umfangreiches Wissen über die Geschäftsprozesse und die dafür benötigten Ressourcen und kann entsprechend qualitative Aussagen zur Geschäftsfortführung tätigen. Der Teilnehmerkreis bleibt so überschaubar, kann jedoch bei Bedarf durch weitere Prozess- und Ressourcenexperten ergänzt werden.

4.6.2 Erstellung der GFPs

In diesem Kapitel wird beschrieben, wie die Inhalte der GFPs erarbeitet werden.

4.6.2.1 Festlegung organisatorischer Maßnahmen

Die Festlegung organisatorischer Maßnahmen beinhaltet alle übergreifenden Aspekte, die nicht dazu dienen, die Geschäftsfortführung einzelner Geschäftsprozesse zu regeln. Diese werden im Nachfolgenden beschrieben.

In einem ersten Schritt muss die Organisationseinheit beschreiben, wie die relevanten **Mitarbeiter im Falle eines Notfalls alarmiert und informiert** werden, nachdem der GFP durch den Stab formal aktiviert wurde. Die Organisationseinheit kann sich hierzu an den Erläuterungen des Kapitels 4.2.2.3 *Alarmierung der BAO* ausrichten und den festgelegten Alarmierungs- und Eskalationspfad für die Organisationseinheit fortschreiben. Hierzu wird empfohlen, für die Organisationseinheit intern festzulegen,

- welche Personen bzw. Funktionen in Kenntnis gesetzt werden sollen,
- über welche Kommunikationsmittel die Alarmierung im Notfall erfolgen soll sowie
- welche weiteren Schritte sich aus der Alarmierung ergeben.

Zu alarmierende Kontaktpersonen können Mitglieder des Notfallteams, weitere Mitarbeiter, externe Fachexperten oder externe Stellen sein. Die Kontaktlisten können als Anhang zum GFP hinterlegt werden, um personenbezogene oder vertrauliche Kontaktdaten ihrem Schutzbedarf entsprechend ablegen zu können.

Innerhalb des Kapitels 4.2 *Aufbau und Befähigung der BAO* ist beschrieben, nach welchen Kriterien GFPs durch den Stab aktiviert werden. Innerhalb dieses Abschnitts im GFP werden diese Kriterien aufgegriffen und konkretisiert.

Für die Dauer des Notfalls kann es notwendig sein, allen oder einzelnen Mitarbeitern im Geltungsbereich des GFP **besondere Rechte und Pflichten** zuzuteilen. Diese beschreiben etwa, welche gesonderten Zuständigkeiten und (Zugangs-, Zutritts- und Zugriffs-)Rechte Mitarbeitern im Notfall zugeteilt werden. Gesonderte Rechte umfassen auch solche im Rahmen von Freigabeprozessen oder Führungsaufgaben. Die gesonderten Rechte gelten von dem Zeitpunkt an, ab dem der GFP aktiviert wurde bis zu dem Zeitpunkt, an dem der Notfall deeskaliert wird.

Fallen Geschäftsprozesse innerhalb des Geltungsbereichs des GFP aus, können **besondere Melde- und Berichtspflichten an interne und externe Stellen** bestehen. Diese sollten innerhalb des GFP dokumentiert werden, sofern diese von denen des Normalbetriebs abweichen und nur für die Dauer des Notfalls gelten. Die besonderen Melde- und Berichtspflichten richten sich sowohl an interne als auch externe Interessengruppen. Hierunter fallen etwa andere Organisationseinheiten der Institution, Aufsichtsbehörden, Kunden, Dienstleister und Lieferanten, die für die Dauer des Notfalls gesondert informiert werden müssen. Dies kann etwa häufigere Meldungen oder Berichte umfassen oder gesonderte Inhalte der Meldungen. Hierzu ist es empfehlenswert, folgende Informationen zu beschreiben:

- Stelle, an die gemeldet oder berichtet werden soll
- Rolle, die melden oder berichten soll
- Medium, mit dem gemeldet oder berichtet werden soll
- Inhalt, der gemeldet oder berichtet werden soll
- Zeitpunkt bzw. Häufigkeit, zu dem gemeldet oder berichtet werden soll

4.6.2.2 Entwicklung von Notfallmaßnahmen

Innerhalb der GFP-Workshops muss die Organisationseinheit Notfallmaßnahmen entwickeln und dokumentieren. Diese sollten den Wiederanlauf sowie den Notbetrieb ausgefallener Geschäftsprozesse ermöglichen, soweit dies im Reaktiv-BCMS mit bereits vorhandenen oder einfach umsetzbaren BC-Lösungen möglich ist. Einfach BC-Lösungen, die im Rahmen des Reaktiv-BCMS umgesetzt werden, sollten als Maßnahmen im Maßnahmenplan dokumentiert werden und im Rahmen des Reaktiv-BCMS umgesetzt werden. Sie sollten dort entsprechend der Vorlage mit einem Umsetzungsdatum ausgefüllt und innerhalb des Zeitrahmens umgesetzt

werden (siehe Kapitel 4.6.3 *Qualitätssicherung und Freigabe*). Folgende Leitfragen können dabei helfen, die erforderlichen Notfallmaßnahmen zu ermitteln:

- Welche Informationen sollen an wen auf welche Weise weitergegeben werden?
- Welche Notfallmaßnahmen müssen eingeleitet werden, um den gewünschten Zustand zu erreichen (z. B. Notbetriebsniveau)?
- Wie lange würde die Durchführung der Notfallmaßnahmen dauern?
- Welche Voraussetzungen müssten gegeben sein, um die Notfallmaßnahmen durchführen zu können?
- Welche Reaktionen würden von anderen erwartet?

Wenn das Notbetriebsniveau durch die vorhandenen BC-Lösungen und Notfallmaßnahmen nicht erreicht werden kann, sollte dies je Ressource als Verbesserungsbedarf im Maßnahmenplan dokumentiert werden. Dieses Defizit kann dann im Folge-BCMS systematisch behoben werden (siehe Kapitel 4.8 *Weiterentwicklung des BCMS).*

Hinweis:

Die BC-Lösungen und Notfallmaßnahmen sollten geeignet sein, das **definierte Notbetriebsniveau** und die **RTO** zu erreichen. Hierbei handelt es sich um zwei Dimensionen, die innerhalb einer idealen Notfallplanung beide gleichzeitig erfüllt werden sollten.

In der Bandbreite sind hinsichtlich des definierten **Notbetriebsniveaus** zwei Extreme möglich:

- Einerseits kann möglicherweise durch Ausweich- oder Ersatzressourcen dieselbe Funktionalität und Leistungsfähigkeit wie im Normalbetrieb erreicht werden, wie z. B. anhand von Redundanzkonzepten für die IT.
- Andererseits kann möglicherweise das Notbetriebsniveau nicht sichergestellt werden, da ein Reaktiv-BCMS ausschließlich auf bereits vorhandene Ressourcen und Möglichkeiten der Institution aufbaut.

Ähnlich verhält es sich mit der **RTO**. Hier sind in der Bandbreite auch zwei Extreme möglich:

- Einerseits können möglicherweise Ausweich- oder Ersatzressourcen innerhalb der geforderten RTO tatsächlich zur Verfügung gestellt werden.
- Andererseits können aufgrund unzureichender oder fehlender BC-Lösungen möglicherweise Ausweich- oder Ersatzressourcen erst in einem deutlich längeren Zeitraum als die RTO zur Verfügung gestellt werden.

Aus dem Endergebnis des Soll-Ist-Vergleichs lassen sich drei Fälle ableiten, auf die im Nachfolgenden weiter eingegangen wird.

Fall 1 - RTO wird auf Notbetriebsniveau erreicht: Die zugesicherte Wiederanlaufzeit der Ressource ist kürzer oder gleich der geforderten Wiederanlaufzeit (RTA≤RTO). Zusätzlich erreicht die wieder angelaufene Ressource das Notbetriebsniveau.

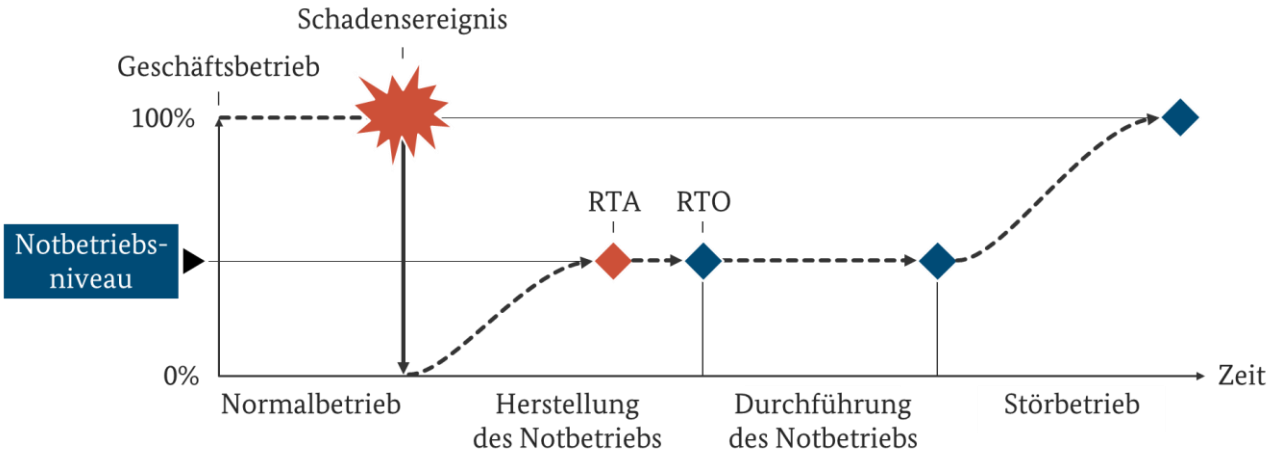

Abbildung 31: Fall 1: RTA≤RTO und das Notbetriebsniveau wird erreicht

Grundsätzlich besteht in diesem Fall kein weiterer Handlungsbedarf seitens der Organisationseinheit, um den Wiederanlauf in den Notbetrieb sicherzustellen. Es muss jedoch dokumentiert werden, dass die vorhandenen Maßnahmen geeignet sind, um die Ressourcen innerhalb der geforderten Zeit zur Verfügung stellen zu können. Falls hierzu weitere Schritte im Notfall durch die Organisationseinheit erforderlich sind, müssen diese im GFP dokumentiert werden. Wird im Notbetrieb eine Ersatzressource bereitgestellt, muss die Organisationseinheit zusätzlich beschreiben, wie diese aus Sicht der Organisationseinheit eingebunden und genutzt werden kann. Sie muss hierzu beschreiben, welche Maßnahmen relevant sind, um den Notbetrieb zu erreichen, aufrechtzuerhalten sowie zurück in den Normalbetrieb zu überführen.

Da infolge der Einschränkungen des Notbetriebs mit Arbeitsrückständen zu rechnen ist, können durch die Organisationseinheit zusätzlich Maßnahmen beschrieben werden, die diese Nacharbeiten identifizieren und behandeln, sodass der Normalbetrieb wieder erreicht werden kann.

Beispiel: Ausfall eines IT-Systems

Im GFP wird durch die Organisationseinheit festgelegt, dass der Wiederanlauf eines ausgefallenen IT-Systems ohne weitere organisatorische Maßnahmen abgewartet wird. Da die RTA kleiner als die RTO ist und keine Einschränkungen der Leistung oder des Umfangs zu erwarten sind, könnte der Geschäftsprozess auch in einem Notbetrieb vollumfänglich ausgeführt werden. Da die RTA jedoch nur geschätzt wurde und ein Funktionstest des IT-Systems erst zu einem späteren Zeitpunkt geplant ist, beruhen die Notfallmaßnahmen der Organisationseinheit auf einer Annahme. Beides wird dokumentiert und die Annahme wird überprüft, sobald die Erkenntnisse aus dem durchgeführten Funktionstest vorliegen.

Beispiel: Ausfall eines Gebäudes

Für einen Gebäudeausfall wird der Organisationseinheit eine gleichwertige Ausweichlokation zur Verfügung gestellt. Für alle Mitarbeiter mit zeitkritischen Aufgaben stehen ausreichend Arbeitsplätze mit den benötigten Arbeitsmaterialien zur Verfügung. Die Organisationseinheit definiert dazu innerhalb ihrer Notfallmaßnahmen, wie sie diese Mitarbeiter an die Ausweichlokation entsendet und dort die Arbeit wiederaufnimmt (Herstellung des Notbetriebs). Dies umfasst etwa Transportmöglichkeiten abzustimmen, notwendige Zutrittsberechtigungen zu erhalten oder die Mitarbeiter auf die vorhandenen Arbeitsplätze zu verteilen. Darüber hinaus legt die Organisationseinheit fest, welche Maßnahmen für die Dauer des Notbetriebs an der Ausweichlokation gelten.

Dies umfasst Regelungen,

- wie mit vertraulichen Dokumenten an der Ausweichlokation umgegangen wird,
- wie Informationen auf Papier, z. B. Postsendungen, nachgesendet werden können sowie
- wie alternative vor Ort befindliche Geräte, Maschinen oder Anlagen eingesetzt werden können.

Abschließend beschreibt die Organisationseinheit, wie sie vom Notbetrieb wieder in den Normalbetrieb zurückkehren kann. Dies umfasst etwa Mitarbeiter wieder auf die regulären Arbeitsplätze zu verteilen, den gesicherten und vertraulichen Transport von im Notbetrieb erstellten Dokumenten zu beauftragen oder temporäre Zutrittsberechtigungen abzugeben.

Fall 2 - RTO wird unter Notbetriebsniveau erreicht: Einen Sonderfall der soeben beschriebenen Option entsteht durch Ressourcen, deren zugesicherte Wiederanlaufzeit kürzer oder gleich der geforderten Wiederanlaufzeit (RTA≤RTO) ist, die aber nicht das gewünschte Notbetriebsniveau des Geschäftsprozesses erreichen. Dies umfasst z. B. Ersatzressourcen, die gegenüber der ausgefallenen Ressource über einen zu stark eingeschränkten Funktions- und Leistungsumfang verfügen.

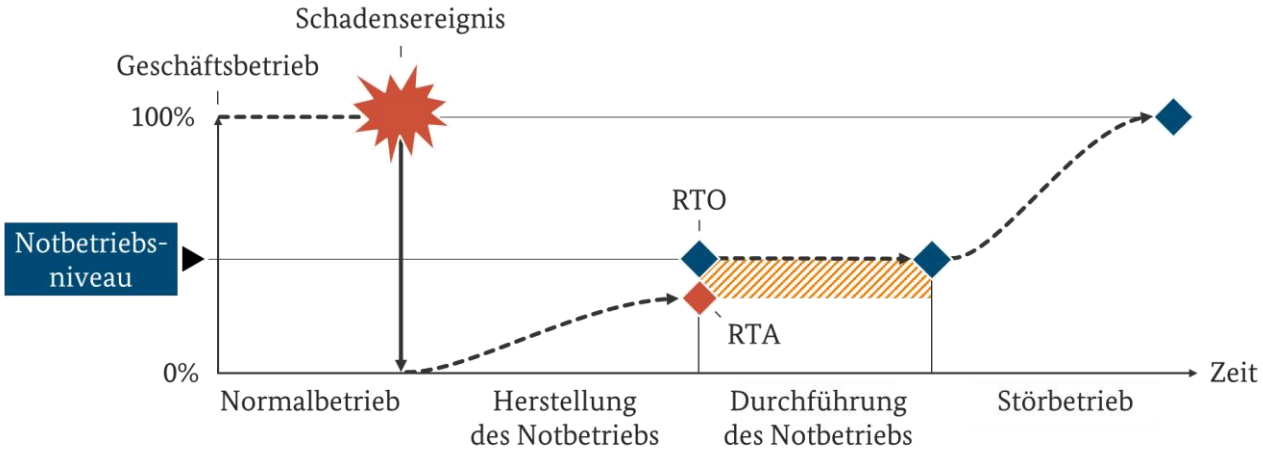

Abbildung 32: Fall 2: RTA≤RTO jedoch wird das Notbetriebsniveau nicht erreicht

Sofern das Notbetriebsniveau durch die wiederangelaufene Ressource nicht vollständig erreicht werden kann, sollte zusätzlich durch die Organisationseinheit beschrieben werden, mit welchen Maßnahmen sie die Lücke zwischen dem Notbetriebsniveau und dem zugesicherten Funktionsumfang der wiederangelaufenen Ressource abdecken kann (siehe Abbildung 32). Sie kann entscheiden, den zugesicherten Funktionsumfang durch Mehrarbeit zu kompensieren oder Tätigkeiten für die Dauer des Notbetriebs zu priorisieren. Darüber hinaus müssen die Ansprechpartner prüfen und dokumentieren, wie mit den daraus resultierenden möglichen Arbeitsrückständen aufgrund des reduzierten Funktionsumfangs verfahren werden soll. Sind keine geeigneten Maßnahmen vorhanden, um das Notbetriebsniveau zu erreichen, könnte die Institution das Notbetriebsniveau anhand der Erkenntnisse an dieser Stelle nochmals hinterfragen. Jedoch muss dann die Information zum Notbetriebsniveau auch in der BIA aktualisiert werden.

Beispiel:

Im Falle eines Gebäudeausfalls wurde der Organisationseinheit zugesichert, innerhalb der RTO eine Ausweichlokation bereitzustellen. In der Ausweichlokation stehen jedoch nicht genügend Arbeitsplätze für alle Mitarbeiter mit zeitkritischen Aufgaben zur Verfügung. Die Organisationseinheit legt zusätzlich zu den Maßnahmen von Fall 1a fest, wie sie das Notbetriebsniveau mit den vorhandenen Arbeitsplätzen herstellen kann. Die Organisationseinheit kann sich etwa dafür entscheiden, die vorhandenen Arbeitsplätze in mehreren

Schichten zu nutzen. Darüber hinaus kann sich die Organisationseinheit dazu entscheiden, bestimmte Tätigkeiten für die Dauer des Notbetriebs auszulassen. Die notwendigen Nacharbeiten werden durch temporäre Mehrarbeit der Mitarbeiter kompensiert.

Fall 3 - RTO wird nicht erreicht: Die zugesicherte Wiederanlaufzeit dauert länger als die geforderte Wiederanlaufzeit (RTA>RTO).

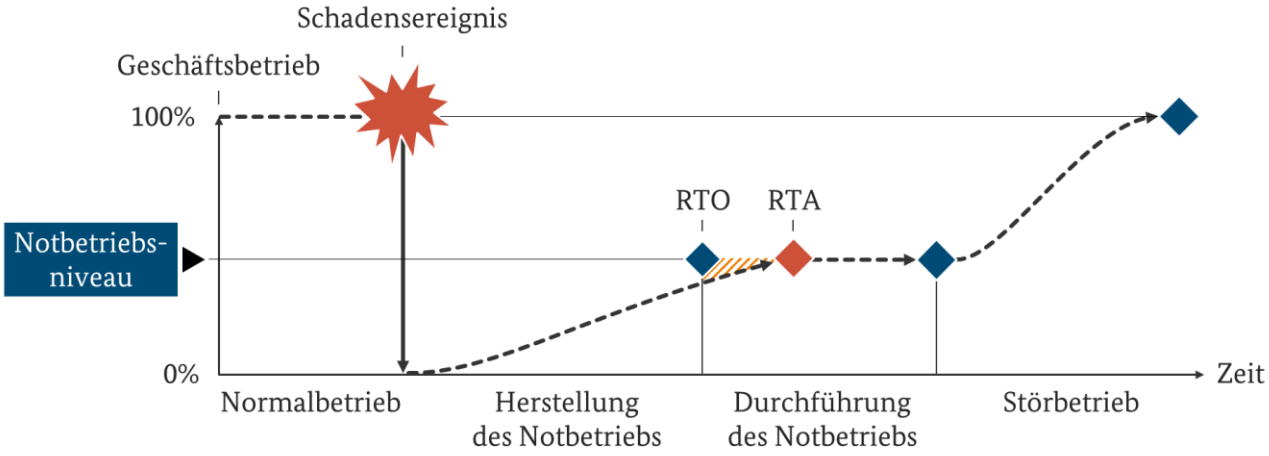

Abbildung 33: Fall 3: RTA>RTO

Zusätzlich zu den Maßnahmen gemäß Fall 1 und 2 muss im Fall 3 die Organisationseinheit festlegen, wie sie die zeitliche Lücke zwischen RTA und RTO überbrücken kann. Eine mögliche Maßnahme ist etwa den Prozess durch alternative Arbeitsschritte durchzuführen.

Beispiel:

Im Falle eines Gebäudeausfalls wurde der Organisationseinheit eine Ausweichlokation zugesichert. Die Wiederanlaufzeit und der Funktionsumfang reichen jedoch nicht aus, um innerhalb der RTO das Notbetriebsniveau sicherzustellen.

Die Organisationseinheit legt daher zusätzlich zu Fall 1 fest, wie sie die zeitliche Lücke bis zur Bereitstellung der Ausweichlokation mit dem zugesicherten Funktionsumfang überbrückt. Sie kann sich beispielsweise dazu entscheiden, bis zur Bereitstellung der Ausweichlokation temporär Tätigkeiten durch einen Dienstleister durchführen zu lassen oder notwendige Tätigkeiten eingeschränkt durch mobiles Arbeiten erlauben. Nachdem die Ausweichlokation bereitgestellt wurde, kann die Organisationseinheit auf die im Beispiel von Fall 1 beschriebenen Maßnahmen zurückgreifen, um das Notbetriebsniveau zu erreichen.

Fallunterscheidung für unterschiedliche schwere Ausfälle

Es kann hilfreich sein, die zeitkritischen Ressourcen gemäß BIA innerhalb eines GFP anhand unterschiedlich schwerer Ausfallszenarien zu betrachten.

Beispiel:

Ein Gebäudeausfall kann den Ausfall eines gesamten Standortes, eines einzelnen Gebäudes oder gar einzelner Gebäudeteile bedeuten.

Je nach Schweregrad des Ereignisses kann es sinnvoll sein, unterschiedliche Notfallmaßnahmen zu treffen. Bei einem gesamten Standortausfall könnte es etwa notwendig sein, sämtliche Tätigkeiten oder eine vorhandene Produktion an eine Ausweichlokation zu verlagern. Fallen hingegen nur einzelne Gebäudeteile aus,

kann die Verlagerung der Arbeitsplätze oder der Produktion innerhalb des Gebäudes oder Standortes ausreichend sein.

Hinweis:

Unter Umständen kann es vorkommen, dass mit den vorhandenen Mitteln sowie den Möglichkeiten des Reaktiv-BCMS keine Notfallmaßnahmen konzipiert werden können, die ausreichen, die zeitliche Lücke zwischen RTA und RTO zu überbrücken oder das Notbetriebsniveau sicherzustellen. Aufgrund der Tragweite eines möglichen Prozessausfalls über die MTPD hinaus muss der Umgang mit den entsprechenden Ressourcen mit der Institutionsleitung als oberste Entscheidungsinstanz abgestimmt werden. Die Institutionsleitung muss entscheiden, ob sie das potenzielle Risiko eines Prozessausfalls über die MTPD hinaus zum gegenwärtigen Zeitpunkt akzeptiert, Ad-hoc-Maßnahmen ergreift oder weitere Notfallmaßnahmen im Rahmen eines Aufbau- oder Standard-BCMS erarbeitet werden sollen.

Schwachstellen und Verbesserungsbedarfe, die innerhalb der Geschäftsfortführungsplanung identifiziert werden sowie getroffene Annahmen und Lücken, die sich aus der Natur des Reaktiv-BCMS ergeben, müssen an den BCMB gemeldet werden. Dieser muss die identifizierten Lücken und Schwachstellen sowie Annahmen und Verbesserungsbedarfe in einem Maßnahmenplan vorhalten (siehe Kapitel *4.8 Weiterentwicklung des BCMS*). Dadurch kann sichergestellt werden, dass diese nicht verlorengehen und so in einem Aufbau- oder Standard-BCMS wieder aufgegriffen und behandelt werden.

4.6.3 Qualitätssicherung und Freigabe

Um sicherzustellen, dass alle Vorgaben zur Geschäftsfortführungsplanung eingehalten wurden, sollten die erstellten GFPs formal qualitätsgesichert werden. Dabei sollten die folgenden Aspekte berücksichtigt werden:

Vollständigkeit: Wurde die GFP-Dokumentenvorlage verwendet und bilden die Inhalte alle vorgegebenen Punkte ab? Wurden alle relevanten Inhalte der BIA innerhalb des GFP erfasst und Notfallmaßnahmen dazu beschrieben? Unvollständige GFPs können dazu führen, dass diese im Notfall nicht oder nur begrenzt einsetzbar sind.

Plausibilität: Sind die beschriebenen Maßnahmen widerspruchsfrei und die getroffenen Annahmen für die Institution realistisch? Sind die Angaben innerhalb des GFP als auch die beschriebenen Abhängigkeiten zu anderen GFP oder WAP/WHP plausibel dargestellt?

Aktualität: Sind die referenzierten Dokumente in der jeweils aktuellen Version hinterlegt? Wurden die relevanten Ansprechpartner auf Basis einer aktuellen Kontaktliste dokumentiert? Veraltete Informationen können dazu führen, dass die beschriebenen Maßnahmen wirkungslos sind oder nicht umgesetzt werden können und der GFP in Gänze nicht oder nur begrenzt einsetzbar ist. Ferner kann durch die Qualitätssicherung der Detailgrad und das sprachliche Niveau der GFPs überprüft und aufeinander abgestimmt werden.

Hinweis:

Die Qualitätssicherung dient zu diesem Zeitpunkt lediglich dazu, sicherzustellen, dass die Vorgaben eingehalten wurden. Ob die in den GFPs beschriebenen Notfallmaßnahmen angemessen, vollständig und wirksam sind, kann erst anhand von Übungen und Tests ermittelt werden (siehe Kapitel 4.7 *Üben und Testen*).

Nachdem die GFPs qualitätsgesichert wurden, müssen diese offiziell freigegeben werden. Dies kann beispielsweise durch die Leitungen der Organisationseinheiten erfolgen. Dieser Schritt signalisiert, dass die Maßnahmen und Verfahren bestätigt wurden und der GFP offiziell in einem Notfall verwendet werden kann.

Die Geschäftsfortführungspläne können sich wesentlich auf die Risiken unzureichend abgesicherter Ressourcen auswirken. Insbesondere die identifizierten Lücken und Schwachstellen aus der Geschäftsfortführungsplanung geben ein realistisches Bild der aktuellen Risikosituation der Institution wieder. Daher sollte der BCMB seine Risikoeinschätzung aus dem Soll-Ist-Vergleich aktualisieren und der Institutionsleitung mitteilen. Zudem ermöglicht diese konkretere Sicht, den Maßnahmenplan entsprechend anzupassen (siehe Kapitel 4.8.2 *Erstellung einer Entscheidungshilfe*).

4.7 Üben und Testen

Wenn die BAO aufgebaut und befähigt wurde, die zeitkritischsten Geschäftsprozesse identifiziert und ein Notfallhandbuch inklusive Geschäftsfortführungspläne erstellt wurden, ist die Institution theoretisch für den Notfall gut gerüstet. Um jedoch sicher zu sein, dass dies auch tatsächlich der Fall ist, müssen die umgesetzten Maßnahmen, die organisatorischen Strukturen und die erstellten Pläne kontinuierlich überprüft werden. Die Bewältigung von Notfällen erfordert von den Beteiligten Höchstleistungen sowie eine schnelle und angemessene Reaktion, um Schäden so weit wie möglich abzuwenden. Unvollständige oder nicht funktionierende Pläne können verheerende Folgen haben und wertvolle Zeit kosten. Regelmäßige Übungen und Tests helfen, Verbesserungsbedarfe im BCM zu identifizieren und die Reaktionsfähigkeit zu erhöhen.

Mit den Übungen und Tests soll Folgendes erreicht werden:

- Alle Informationen, die für die Notfallbewältigung relevant sind, sollten auch fachlich aktuell, plausibel und vollständig sein. Dies gilt insbesondere für das Notfallhandbuch, inklusive der Geschäftsfortführungspläne sowie der Kontaktlisten zur Alarmierung.
- In den Räumlichkeiten, die für die Notfallbewältigung benötigt werden, sollten die IT und alle weiteren Ressourcen einsatzbereit sein.
- Die Abläufe im Notfall sollten wie geplant funktionieren und sowohl angemessen als auch effizient sein.
- Die Mitarbeiter sollten auf den Notfall vorbereitet sein, eigene Erfahrungen sammeln können und in die Lage versetzt werden, im Notfall überlegt zu handeln.

Das Üben und Testen ist mit zeitlichen, technischen und personellen Aufwänden verbunden. Jede Institution muss daher genau abwägen, welche Arten von Übungen und Tests für welchen Zweck sinnvoll sind. Die nachfolgenden Kapitel geben Hilfestellung, welche Übungs- und Testarten sich in welchem Fall anbieten und welche Schritte notwendig sind, um Übungen und Tests zu planen, vorzubereiten, umzusetzen und auszuwerten.

Hinweis:

Eine scharfe Trennung der Begriffe Übung und Test ist nicht immer möglich und sinnvoll. Im ISO-Standard 22398 (siehe [22398]) ist der Begriff Test definiert als eine besondere Art von Übung, bei der ein objektiv gemessenes „Pass or Fail"-Ergebnis (Bestehen oder Nichtbestehen) erwartet und entsprechend als Ziel definiert wird. Bei Übungen sind die Ziele generischer formuliert und dienen üblicherweise dazu, praktische Erfahrungen im Umgang mit den Notfallplänen und Notfallmaßnahmen zu sammeln sowie Korrektur- und Verbesserungsmaßnahmen zu identifizieren. Der BSI-Standard 200-4 folgt der Begriffsdefinition aus den ISO-Standards der 22300-Reihe. Der Begriff Übung wird als Oberbegriff verwendet. Tests stellen eine spezielle Form von Übungen dar. Aus Gründen der besseren Lesbarkeit wird nachfolgend primär von Übungen gesprochen, was Tests einschließt.

Für das Reaktiv-BCMS müssen die in *Tabelle 26* aufgeführten Übungsarten regelmäßig durchgeführt werden.

Übungsart	Inhalt	Beispiel
Stabsübung	Praktisches Üben der Stabsarbeit, um ein vorgegebenes Notfallszenario zu bewältigen. Ziel: die Zusammenarbeit der Mitglieder des Stabs und die Grundelemente der Stabsarbeit üben, z. B. Führungszyklus, Lagebesprechungen, Protokollierung, Visualisierung etc. Wenn für das Szenario bestimmte stabsnahe Unterstützungsrollen benötigt werden, sind diese Teil der Stabsübung.	Stab aktivieren und im Stabsraum zusammenkommen, um anschließend die simulierte Bewältigung eines realitätsnahen Notfallszenarios durch den Stab durchzuführen.
Alarmierungsübung	Aktivieren und Durchlaufen der Alarmierungskette Ziel: Technische Kommunikationsmittel, organisatorische Abläufe sowie vorhandene Dokumentationen zur Alarmierung und Eskalation prüfen.	Auslösen der Alarmierungskette durch einen Anruf bei der zuständigen Meldestelle und systematisches Nachverfolgen der Erreichbarkeits- und Rückrufquote innerhalb eines Zeitfensters.

Tabelle 26: Übungsarten, die im Reaktiv-BCMS durchgeführt werden müssen

Darüber hinaus ist es empfehlenswert, für das Reaktiv-BCMS die in Tabelle 27 aufgeführten Übungsarten regelmäßig durchzuführen.

Übungsart	Inhalt	Beispiel
Planbesprechung („Schreibtischtest“)	Moderierte Besprechung eines Notfallplans. Ziel: Planinhalte hinsichtlich ihrer realistischen Anwendbarkeit prüfen. In der Regel wird dazu fachlich überprüft, ob die Pläne plausibel, vollständig korrekt und aktuell sind. Darüber hinaus kann geprüft werden, ob die untersuchten Pläne untereinander widerspruchsfrei sind.	Ein BCM-relevantes Dokument mit darin vorgesehenen Rolleninhabern durchsprechen, ohne dass Handlungsschritte real ausgeführt werden (GFP, Alarmierungsplan, RZ-Umschaltung, Vertragsklauseln in SLA etc.).
Funktionstest	Reale Ausführung eines Notfallplans Ziel: Einsatzbereitschaft und Funktionsfähigkeit von einzelnen oder mehreren baulichen, technischen oder organisatorischen Maßnahmen bzw. Ressourcen prüfen, die für die Notfallbewältigung benötigt werden.	Test eines Notfallarbeitsplatzes durch einen Mitarbeiter; Test eines IT-Administration-Arbeitsplatzes (Berechtigungen im Notfall etc.); Umschalttest zwischen redundant ausgelegten Systemen; Überprüfen der Notfallausrüstung im Stabsraum, ob diese vorhanden und einsatzbereit ist.

Tabelle 27: Weitere sinnvolle Übungsarten für das Reaktiv-BCMS

Die nachfolgenden Kapitel beschreiben die empfohlene Vorgehensweise, mittels derer Übungen durchgeführt werden. In Abbildung 34 sind die hierfür erforderlichen Schritte in einer Übersicht dargestellt.

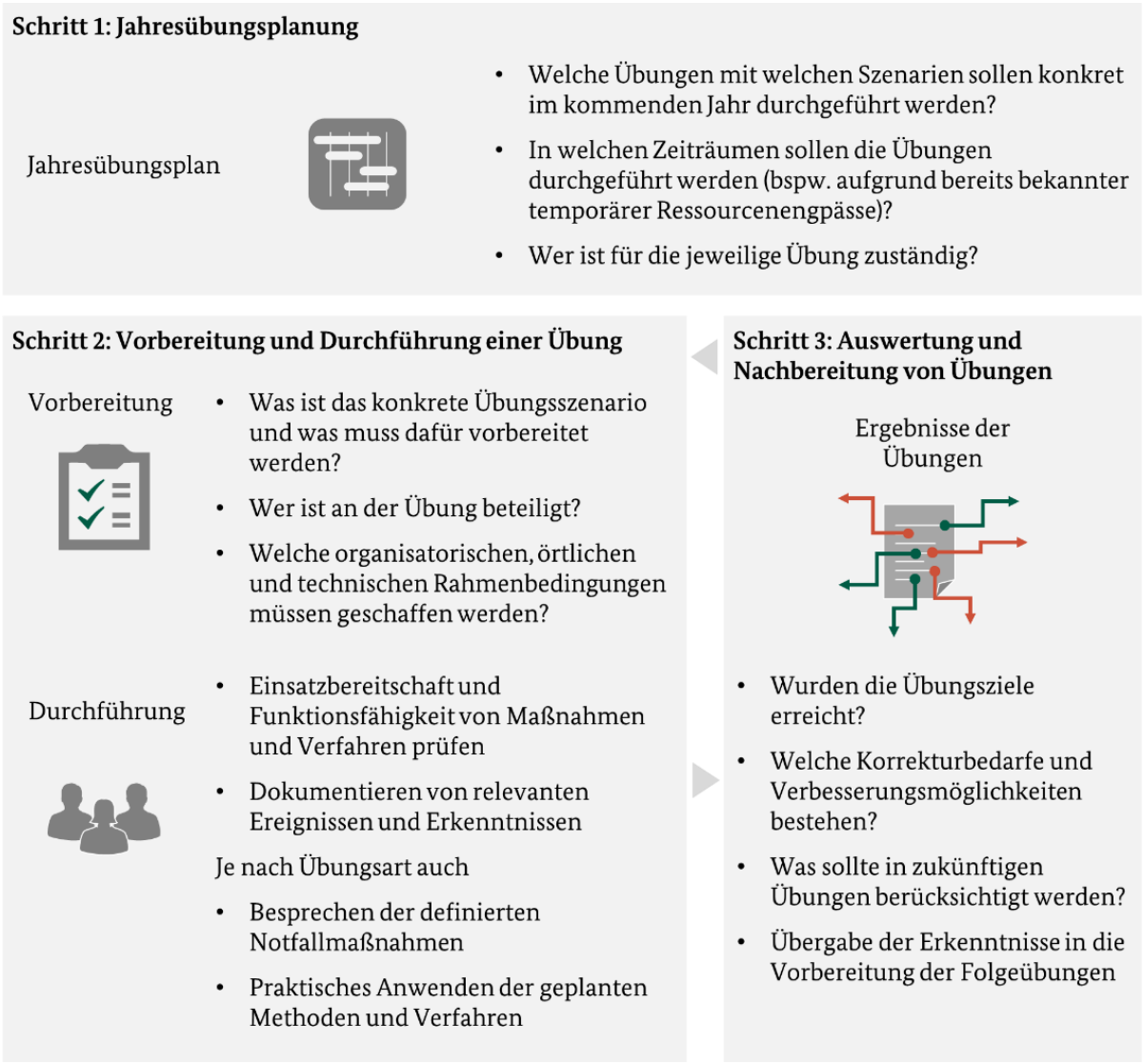

Abbildung 34: BCM-Prozessschritte zu Übungen

Jede einzelne Übung erfordert die allgemeinen Übungs-Prozessschritte Vorbereitung, Durchführung und Nachbereitung. Die wesentlichen Aufgaben der einzelnen Phasen werden in den jeweiligen Unterkapiteln vorgestellt. Um einen für alle beteiligten Personen klaren Rahmen für die Konzeption und Durchführung vorzugeben, sollten jedoch die organisatorischen Eckpunkte für jede Übung in einem **Übungskonzept** zusammenzugefasst werden. Das Übungskonzept beinhaltet folgende Punkte:

- Datum der Übung (gegebenenfalls Konkretisierung der Jahresübungsplanung)
- Standort und Raum, falls relevant (diese müssen eventuell gebucht werden)
- Übungsbeginn (Uhrzeit)
- Übungsende (Uhrzeit)
- Übungsziele (Konkretisieren der Ziele aus der Jahresübungsplanung)
- Teilnehmer innerhalb der Übung

Abweichungen zu dieser Liste sind in den einzelnen Unterkapiteln adressiert.

4.7.1 Jahresübungsplanung

Ziel der Jahresübungsplanung ist es, sicherzustellen, dass die definierten Prozesse, Ressourcen, Verfahren und Abläufe der Notfallbewältigung über mehrere Jahre hinweg vollständig geübt und getestet sowie Korrekturbedarfe und Verbesserungsmöglichkeiten daraus abgeleitet werden können. Als Grundlage der Jahresübungsplanung sollten folgende Aspekte berücksichtigt werden:

- Ergebnisse der BIA
- Ergebnisse des Soll-Ist-Vergleichs
- Geschäftsfortführungsplanung
- Ergebnisse vorheriger Übungen
- Rollen der BAO

Hierbei muss eine Reihe von Einflussfaktoren beachtet werden, unter anderem der Bedarf an zeitlichen und personellen Ressourcen sowie organisatorische Rahmenbedingungen innerhalb der Institution. Daher sollte der BCMB eine zentrale Jahresübungsplanung erstellen und mit der Institutionsleitung abstimmen und durch diese freigeben lassen. Die Jahresübungsplanung sollte einen Zeitraum von mindestens zwölf Monaten umfassen (Jahresübungsplan). Pro Übung sollten mindestens folgende Punkte festgelegt und im Jahresübungsplan dokumentiert werden:

- konkretes Datum oder avisierter Zeitraum der Übung
- Übungsart
- Übungsziel
- zuständige Personen, welche die Übung vorbereiten
- zuständige Personen, welche die Übung durchführen
- avisierte Übende
- Abschätzung der erforderlichen personellen, materiellen und finanziellen Ressourcen
- Abschätzung des zu erwartenden Einflusses der Übung auf den Geschäftsbetrieb.

Das festgelegte **Datum bzw. der geplante Zeitraum** der Übung sollte mit den zuständigen Personen abgestimmt werden, welche die Übung vorbereiten und durchführen. Zusätzlich sollte die Verfügbarkeit aller Übungsteilnehmer berücksichtigt werden. Bei der Terminplanung sollte beachtet werden, dass Stabsübungen und manche Funktionstests eine längere Vorbereitungsphase benötigen, weil z. B. zuvor Übungsunterlagen erstellt und organisatorische oder technische Voraussetzungen geschaffen werden müssen.

Das **Übungsziel** beschreibt konkret, was mit dieser Übung erreicht werden soll. Es sollte sich an der Reife des BCMS sowie dem allgemeinen Übungsziel der Übungsart ausrichten und die Übungserfahrung der Institution berücksichtigen. Übungen sollten so geplant werden, dass sie einerseits herausfordernd für die Übenden sind, andererseits aber auch Erfolgserlebnisse und einen Erkenntnisgewinn für die Teilnehmer bieten. Entsprechend sollten in der Jahresübungsplanung reale Ereignisse aus der Vergangenheit oder realistisch denkbare Schadensereignisse für die Institution berücksichtigt werden. Es reicht für die Jahresübungsplanung aus, das übergeordnete Übungsziel jeder Übung festzulegen. Dieses Übungsziel kann anschließend in der Vorbereitung der einzelnen Übungen konkretisiert und in Teilziele unterteilt werden, anhand derer die Ergebnisse der Übung bewertet werden können.

Es ist empfehlenswert, wenn Übungen aufeinander aufbauen. Eine Planbesprechung für einen GFP kann z. B. eine sinnvolle Vorbereitungsmaßnahme für einen späteren Funktionstest einer Maßnahme aus dem GFP sein und/oder der Kombination daraus.

Beispiel:

In einer Planbesprechung wird überprüft, ob die beschriebenen Aktivitäten, um einen Ausweicharbeitsplatz in Betrieb zu nehmen, schlüssig beschrieben sind. Basierend auf diesen Aktivitäten wird anschließend in einem Funktionstest überprüft, ob der beschriebene Arbeitsplatz auch technisch einsatzfähig ist.

In der Jahresplanung sollte jährlich mindestens eine Stabsübung und eine Alarmierungsübung vorgesehen werden, um die grundlegenden, neu entwickelten Prozesse und Strukturen für die Notfallbewältigung zu überprüfen. Tabelle 28 stellt ein vereinfachtes Beispiel für einen Jahresübungsplan dar.

Beispiel:

Nr.	Übungsart	Datum und Zeitraum	Ziel und Umfang der Übung	Zuständig	Ressourcen
2020-01	Planbesprechung	14.04.2020, 09-11 Uhr	Prüfen des GFP der IT-Abteilung, Szenario Standortausfall	Hr. Meier (IT) (Planung und Durchführung)	2-3 Mitarbeiter IT, ca. 2 h je Teilnehmer
2020-02	Funktionstest	22.09.2020, 3h	Überprüfung der Arbeitsfähigkeit ausgewählter IT-Mitarbeiter an den definierten Notfallarbeitsplätzen	Frau Schmidt (Planung), Hr. Meier (IT) (Durchführung)	2-3 IT-Mitarbeiter, ca. 1 Tag je Teilnehmer
2020-03	Alarmierungs-test	13.11.2020, 08:30 Uhr	Prüfen der Meldewege und Alarmierung der Stabsmitglieder, inkl. Eintreffen im Stabsraum.	BCMB (Planung und Durchführung)	Mitglieder des Stabs, ca. 1 h je Teilnehmer
2020-04	Stabsübung	13.11.2020, 09-11 Uhr	Üben der Abläufe im Stab, Szenario „Brand im RZ“	BCMB (Planung und Durchführung)	Mitglieder des Krisenstabs, Drehbuch und Einlagen, ca. 15 Tage zur Vorbereitung, Durchführung, Nachbereitung und 0,5 Tage je Teilnehmer

Tabelle 28: Beispiel für einen Jahresübungsplan

Hinweis:

Die zuvor erstellten GFPs wurden voraussichtlich auf theoretischer Basis und anhand von Annahmen erstellt. Erst geübte und getestete Pläne lassen jedoch einen Rückschluss auf die tatsächliche Funktionsfähigkeit der GFPs zu. Daher sollten frühzeitig **Planbesprechungen** für GFPs eingeplant werden, auch wenn diese noch nicht im ersten BCMS-Zyklus vollständig umgesetzt werden können.

Eine nicht angekündigte **Stabsübung** (siehe Kapitel 4.7.2 *Stabsübung*) und die **Alarmierungsübung** (siehe Kapitel 4.7.3 *Alarmierungsübung*) können gut miteinander kombiniert werden. In der Alarmmeldung wird den Übenden mitgeteilt, dass sie sich schnellstmöglich oder zu einem bestimmten Zeitpunkt am vorgesehenen Stabsraum einfinden sollen. Anschließend beginnt die eigentliche Stabsübung.

Der BCMB sollte überwachen, dass alle geplanten Übungen und Tests stattfinden. Für ausgefallene, verschobene oder abgebrochene Übungen oder Tests sollte zeitnah ein Ersatztermin gefunden werden. Treten technische oder organisatorische Probleme auf, sollte der BCMB prüfen, ob eine Wiederholung der Übung nach Behebung der Mängel erforderlich ist.

Synergiepotenzial:

Vielfach werden bereits in anderen Managementsystemen Übungen geplant und durchgeführt. So finden aufgrund gesetzlicher Vorgaben regelmäßig Brandschutz- und Räumungsübungen statt, für deren Planung der Brandschutz- oder Arbeitsschutz-Beauftragte zuständig ist. Im Rahmen des ITSCM werden unter anderem Recovery-Tests von IT-Systemen, Schwenktests bei redundanten Rechenzentren sowie Datenwiederherstellungstests durchgeführt. Der BCMB sollte entsprechend seine Jahresübungsplanung mit der Planung der anderen Managementsysteme abstimmen, um Terminkollisionen zu verhindern. Andererseits können bestimmte Übungen bewusst miteinander verbunden werden. So kann eine Räumungsübung sowohl mit einer Alarmierungsübung, einer Planbesprechung oder einem Funktionstest verbunden werden, was den Realitätsgrad für die übenden Personen weiter steigert.

4.7.2 Stabsübung

Eine Stabsübung im BCM behandelt in der Regel Ereignisse, welche die Institution intern betreffen, beispielsweise die ressourcenspezifischen Ausfallszenarien. Das Ziel von Stabsübungen liegt darin, die Zusammenarbeit innerhalb der BAO sowie die Methoden zur Stabsarbeit zu üben und dadurch Routine für einen Ernstfall bei den Stabsmitgliedern herzustellen. Die Stabsübung im BCM wird in einem „geschützten Raum“ durchgeführt, ohne wirklich Einfluss auf den Geschäftsbetrieb zu nehmen. Der Stab muss die Grundelemente der Stabsarbeit praktisch anwenden, um ein vorgegebenes Notfallszenario zu bewältigen. Aufgrund der Komplexität einer Stabsübung, um den reibungslosen Ablauf sicherzustellen, nimmt die Vorbereitung im Verhältnis die meiste Zeit in Anspruch. Folgende Hilfsmittel werden in der Regel innerhalb der Vorbereitung und Durchführung der Stabsübung erstellt:

- Übungskonzept
- Übungsdrehbuch und Einlagen
- Übungsprotokoll

Auf die wesentlichen Hilfsmittel wird im weiteren Verlauf detailliert eingegangen.

Vorbereitung der Stabsübung

Die Vorbereitung wird in der Regel von einem benannten Übungsautor wahrgenommen. Diese Rolle kann durch den BCMB, durch die für die Übung zuständige Person oder weitere beauftragte Personen übernommen werden.

Da Stabsübungen deutlich komplexer sind, sollte im Übungskonzept neben den bereits beschriebenen organisatorischen Eckpunkten die folgenden Punkte festgelegt und dokumentiert werden:

Organisatorische Eckpunkte

Die organisatorischen Eckpunkte für das Übungskonzept wurden bereits beschrieben. Für den Erfolg von Stabsübungen ist insbesondere eine klare Definition der Übungsziele wichtig. Die Übungsziele bei Stabsübungen liegen in der Regel auf einer höheren Abstraktionsebene, als bei anderen Übungen.

Beispiel:

Typische Ziele von Stabsübungen sind:

- die praktische Anwendung und Verinnerlichung der Abläufe und Grundlagen der Stabsarbeit
- das Kennenlernen der beteiligten Personen und Rollen in einer Notfallsituation
- die Überprüfung von Zuständigkeiten, Fähigkeiten und Kenntnissen der BAO
- die Übung von Kommunikations- und Entscheidungsprozessen im Stab
- die aktive Einbindung der Unterstützungsrollen Protokollierung und Visualisierung und die Überprüfung der Zusammenarbeit
- das Training einer einheitlichen und abgestimmten Kommunikation nach innen und außen

Rahmenablauf

Um die Ziele und den zeitlichen Rahmen der Übung besser im Blick zu behalten, sollte der Übungsautor den Rahmenablauf der Stabsübung planen. Hierbei sollten folgende Fragestellungen beantwortet werden:

- Soll die Übung den Teilnehmern vorab angekündigt werden und falls ja, wann und mit welchen Detailinformationen (z. B. Termin, Übungsdauer, Ort etc.)?
- Soll zum Auftakt der Stabsübung eine Alarmierung der Teilnehmer erfolgen, z. B. anhand einer vorgeschalteten Alarmierungsübung?
- Soll direkt im Anschluss an die Stabsübung eine Auswertungsrunde mit allen Beteiligten durchgeführt werden, um ein unmittelbares Feedback zur Übung zu erhalten?

Zusätzliche Zeitbedarfe für die Alarmierung oder Auswertung sollten sinnvollerweise bereits in der Vorbereitung der Übung eingeplant werden. Eine Auswertungsrunde erfolgt idealerweise möglichst direkt im Anschluss an die Stabsübung, um die erste Resonanz der Teilnehmer direkt und ungefiltert aufnehmen zu können. Zudem wird empfohlen, eine zweite Auswertungsrunde mit den Teilnehmern vorzusehen, um ein strukturiertes und konsolidiertes Feedback zu erhalten. Dieser Termin sollte mit etwas zeitlichem Abstand zur Übung stattfinden, damit sich alle Beteiligten darauf vorbereiten können. Die zweite Auswertungsrunde kann auch schriftlich stattfinden, z. B. mit Hilfe eines Fragebogens.

Übungsregeln

Damit im Verlauf der Übung keine Schäden verursacht werden, sollte der Übungsautor die Regeln für die Übung festlegen:

- Welche Abbruchbedingungen führen zu einem vorzeitigen Ende der Übung?
- Gibt es besondere Sicherheitsvorkehrungen, wie z. B. eine bestimmte Kennzeichnung von Dokumenten als Bestandteil der Übung?
- Ist eine Kommunikation durch die Teilnehmer an Personen außerhalb des Übungsraums gestattet und falls ja, an wen und wie?

Abbruchbedingungen für eine Stabsübung sind z. B. der Eintritt eines realen Notfalls, eine deutliche Überschreitung der Übungszeit oder wenn Schlüsselfunktionen die Übung ungeplant verlassen müssen.

Während der Übung sollte die Kommunikation außerhalb des Übungsraums nur in Ausnahmefällen gestattet werden, wenn z. B. eine Auskunft durch einen Fachexperten wichtig für eine bestimmte Entscheidung ist. In jedem Fall muss in der Kommunikation nach außen klar dargestellt werden, dass es sich um eine Anfrage im Kontext einer Übung handelt und nicht um einen echten Notfall. Gerade in einem sehr realistischen Übungsszenario können Teilnehmer dies in der Außenkommunikation schnell vergessen. Daher sollte ein Mitglied

des Übungsteams (z.B. eine Unterstützungskraft) die kommunizierende Person begleiten und dies sicherstellen.

Notfallszenario

Ein wesentlicher Erfolgsfaktor für Stabsübungen ist der Einsatz eines plausiblen und auf die Institution zugeschnittenen Notfallszenarios. Ein Szenario umfasst eine Ausgangssituation und in der Regel eine Abfolge von Ereignissen, auf welche die Teilnehmer reagieren müssen. Das Szenario kann reale oder fiktive realitätsnahe Vorfälle enthalten und liefert die für die Übung relevanten Grundinformationen oder Annahmen.

Das Szenario sollte dafür geeignet sein, die Zielsetzung der Stabsübung zu unterstreichen. Die Übenden sollten die Grundelemente der Stabsarbeit anwenden und sich gegebenenfalls mit den Notfallplänen sowie mit den vorgesehenen Notfallmaßnahmen inhaltlich auseinandersetzen können.

Übungsdrehbuch

Damit die Übungsleitung den Übungsablauf koordinieren und steuern kann, sollte aus der Gesamtheit der Einlagen durch den Übungsautor ein Übungsdrehbuch erstellt werden, das den gedachten Verlauf der Übung detailliert beschreibt. Tabelle 29 zeigt beispielhaft den Aufbau eines Übungsdrehbuchs.

Beispiel:

Nr.	Zeit	Sender	Empfänger	Information bzw. Ereignis	Erwartete Handlung
…	…	…	…	…	…
2	09:15	Leiter RZ	Hr. Lorenz	Löscharbeiten im Rechenzentrum wurden durch die Feuerwehr abgeschlossen.	Funktionsfähigkeit des RZ prüfen und Erstmaßnahmen aus dem GFP initiieren
3	09:22	Mitarbeiter IT	Hr. Meier	Der Ausfall von Anwendung A führt zum Ausfall der zeitkritischen Prozesse X, Y und Z.	Prüfen der konkreten Ausfälle und Ermitteln der Betroffenen
…	…	…	…	…	…

Tabelle 29: Beispiel des Aufbaus eines Übungsdrehbuchs

Einlagen

Sogenannte **Ausgangslagen** beschreiben anhand des Szenarios die Übungsumgebung zur Ausgangssituation. Anhand von **Einlagen** während der Übung können Informationen im Szenario ergänzt, erweitert oder verändert werden, sodass die Teilnehmer dazu animiert werden, zu reagieren und zu handeln.

Beispiel:

Einlagen können z. B. eine Beobachtung, eine eingehende Meldung, ein Pressebericht oder ein weiterer Vorfall zur Lageverschärfung sein.

Je nach hierfür notwendiger Fachexpertise oder anderen Einflussfaktoren kann es erforderlich sein, weitere Personen hinzuzuziehen, die selbst Einlagen entwickeln oder den Übungsautor fachlich beraten.

Hinweis:

Der Übungsautor sollte anhand des Szenarios und der Einlagen sicherstellen, dass jede Funktion im Stab im Verlauf der Stabsübung mindestens eine Aufgabe bearbeiten muss. Gleichzeitig ist es empfehlenswert, wenn keine Funktion so überlastet wird, dass ein „Flaschenhals-Effekt" entsteht.

Übungsrollen

In einem nächsten Schritt muss der Übungsautor die für die Übungsdurchführung relevanten Teilnehmer festlegen und mit konkreten Personen besetzen:

- **Übungsleitung:** Benennen einer Person, welche die Übung insgesamt steuert.
- **Unterstützungskräfte:** Die Übungsleitung sollte abhängig von der Komplexität des Szenarios durch weitere Personen unterstützt werden, insbesondere um Einlagen einzuspielen sowie für den Umgang mit Informationen oder Aufträgen aus dem Stab.
- **Übende:** Alle Personen, die als Mitglieder des Stabs, Unterstützungsfunktionen (Protokollierung und Visualisierung) oder in zusätzlichen Funktionen an der Bewältigung des Übungsszenarios teilnehmen sollen.
- **Übungs-Protokollant:** Eine oder mehrere Personen, die den Verlauf der Übung nachvollziehbar im Übungsprotokoll erfassen. Der Übungs-Protokollant erfüllt nicht die Rolle des Protokollanten des Stabs, der innerhalb des Übungsszenarios mitwirkt und die Aktivitäten und Entscheidungen des Stabs protokolliert.
- **Beobachter (optional):** Eine oder mehrere Personen, welche die Übung neutral „aus der zweiten Reihe" beobachten und hinsichtlich möglicher Verbesserungspotenziale bewerten.

Die genannten Rollen können sich personell überschneiden. Bei sehr einfach gehaltenen Stabsübungen mit wenigen Einlagen kann z. B. die Unterstützungsrolle gleichzeitig auch Beobachter sein. Analog dazu können auch Beobachter dafür eingesetzt werden, das Übungsprotokoll zu erstellen.

Letzte Vorbereitungen

Im letzten Schritt der Vorbereitungsphase sollte dafür gesorgt werden, dass die Übung operativ stattfinden kann. Die hierfür notwendigen Aktivitäten ergeben sich typischerweise aus den vorherigen Schritten.

Beispiel:

- Sicherstellung, dass der Raum am Übungstag verfügbar ist und über die notwendige Ausstattung verfügt
- Versendung von Einladungen an alle Beteiligten (bei angekündigten Übungen)
- Vorbereitung einer Kurzpräsentation zur Einführung in die Besonderheiten einer Übung, wie z. B. die Regeln zur Kommunikation nach außen oder der Appell, das Szenario nicht während der Übung infrage zu stellen
- Prüfung, ob alle Teilnehmer ausreichend geschult sind, um ihre Rolle in der Übung wahrzunehmen
- Vorbereitung der Einlagen, z. B. als Präsentation, als Mails, als Skript zum Vorlesen oder als gedruckte Handouts
- Prüfung der Funktionsfähigkeit von eingesetzter Technik, wie z. B. Beamer, Telefonen etc.
- Prüfung der Aktualität von Notfalldokumentationen, die während der Übung verwendet werden sollen
- Logistische Vorbereitung der Übung, wie z. B. die Verpflegung während der Übung oder die Unterbringung von Teilnehmern
- Durchführung von Briefings für die Übungsrollen

Bis zum Übungstag sollte der Übungsautor immer wiederkehrend prüfen, ob eventuell andere Ereignisse die Durchführung der Übung beeinflussen oder sogar verhindern können, z. B. weil der vorgesehene Raum oder Schlüsselfunktionen aufgrund anderer Termine nicht länger verfügbar sind.

Durchführung der Stabsübung

Auch bei einer guten Vorbereitung können oft nicht alle Eventualitäten vorhergesehen werden. Daher können Übungen auch für die Übungsleitung Herausforderungen mit sich bringen. Die Hauptaufgabe der Übungsleitung ist die Steuerung des Übungsszenarios unter Beachtung der Ziele und der Zeitplanung.

Darüber hinaus koordiniert die Übungsleitung den Übungsablauf. Außerdem sollte die Übungsleitung die Entscheidungshoheit besitzen, von der Zeitplanung abzuweichen oder die Übung abzubrechen. Die Teilnehmer sollten sich während der Übung stets an die geltenden Übungsregeln und -künstlichkeiten halten, ohne jedoch ihren kreativen Handlungsraum zu beschränken. Die Übungsleitung und die unter Umständen vorhandenen Unterstützungsrollen sollten darauf achten, die vorbereiteten Einlagen geeignet in den Übungsverlauf einzuspielen. Die Übungsleitung kann jederzeit entscheiden, dass eine Einlage früher, später oder überhaupt nicht eingespielt wird, wenn sich dies positiv auf den Übungsverlauf auswirkt.

Der Übungs-Protokollant muss den Übungsverlauf und die Ergebnisse dokumentieren.

Beispiele:

- Notizen zum beobachteten Ablauf der Übung
- Hinweise von Teilnehmern als Input für die Übungsauswertung
- Erreichung oder Nicht-Erreichung von Übungszielen
- verwendete Dokumente, Werkzeuge, Ressourcen
- erkannte Korrekturbedarfe oder Verbesserungsmöglichkeiten

Werden Beobachter eingesetzt, sollten diese notieren, was gut funktioniert hat und was noch optimierbar ist. Dabei wird empfohlen, Personen als Beobachter einzusetzen, die viel Wissen zum BCM der Institution besitzen.

Die Protokollanten und Beobachter müssen sich während der Übungsdurchführung neutral verhalten und dürfen nicht in das Geschehen eingreifen. Erst in der Auswertung der Übung sollten die Protokollanten und Beobachter aktiv in die Auswertungsrunde einbezogen werden.

Die Übung muss durch die Übungsleitung offiziell beendet werden. Ein offizielles Ende ist zum einen wichtig, damit alle an der Übung Beteiligten wissen, dass die Übungsregeln nicht mehr gelten, insbesondere die Regelungen zur Außenkommunikation. Zum anderen können Übungen sehr emotional werden und die Teilnehmer können sich stark in das Szenario hineinversetzen. Ein klares Übungsende trägt dazu bei, dass Emotionen abflauen und alle Teilnehmer das durchlebte Szenario abschließen können.

4.7.3 Alarmierungsübung

Die Alarmierungsübung zielt darauf ab, Fehlerquellen und Schwächen in der Alarmierung der BAO zu identifizieren und die Wirksamkeit von Alarmierungsverfahren festzustellen. Eine erfolgreiche Alarmierung ist Grundlage für die weitere Notfallbehandlung und sollte somit schnellstmöglich erfolgen. Ausgehend von einer Information einer Meldestelle wird über die zentrale Entscheidungsinstanz eine Alarmierungsmeldung bzw. die Alarmierungskette ausgelöst und nachverfolgt. Alarmierungsübungen können unterschieden werden in technikorientierte Tests und anwendungsorientierte Übungen.

In technikorientierten Tests wird überprüft, ob die Kommunikationsmittel und -verfahren, die im Notfall eingesetzt werden, funktionsfähig sind. In anwendungsorientierten Übungen werden die organisatorischen

Regelungen wie z. B. die Erreichbarkeit und Verfügbarkeit der relevanten Rolleninhaber, die Stellvertretungen, gegebenenfalls. die Geschwindigkeit der Reaktion und die vorhandene Alarmierungsdokumentation überprüft bzw. eingeübt.

Anwendungsorientierte Alarmierungsübungen setzen voraus, dass ein abgestimmter Alarmierungspfad mit aktuellen Kontaktdaten vorliegt und die zu nutzenden Kommunikationswege und -mittel zwischen den Teilnehmern organisatorisch und technisch festgelegt, dokumentiert, umgesetzt und funktionstüchtig sind.

Vorbereitung der Alarmierungsübung

Der Aufwand einer Alarmierungsübung ist aufgrund der geringen Komplexität deutlich kleiner als der einer Stabsübung. Typischerweise übernimmt der BCMB selbst diese Aufgabe.

Neben den üblichen Einträgen im Übungskonzept, sollte abhängig vom definierten Alarmierungsprozess (siehe Kapitel *4.2.2 Detektion, Alarmierung und Eskalation*) bei anwendungsorientierten Übungen entschieden werden, ob die Erreichbarkeit nur innerhalb oder auch außerhalb der üblichen Dienstzeit getestet werden soll. Falls eine Erreichbarkeit auch außerhalb der Dienstzeit festgelegt wurde, ist es empfehlenswert, Alarmierungsübungen auch vereinzelt zu ungünstigen Zeiten abzuhalten. Beispiele hierfür sind die Mittagspause, kurz nach Feierabend, nachts, am Wochenende oder an Feiertagen.

Die Übungsziele ergeben sich aus der Übungsart und aus dem Alarmierungsprozess. Neben den oben genannten allgemeinen Zielen beinhalten die Übungsziele hier meistens zeitliche Parameter hinsichtlich der Erreichbarkeits- und Rückrufquote der Beteiligten.

Beispiel:

Ziel der Alarmierungsübung: Nach Auslösen der initialen Alarmmeldung dauert es maximal 30 Minuten, bis alle erforderlichen Rolleninhaber der BAO den Alarm positiv quittiert haben.

Notfallszenario

Ein Szenario ist für diese Übungsart nicht unbedingt notwendig. Eine einfache Ausgangslage, die während des Tests kommuniziert wird, ist vollkommen ausreichend.

Beispiel:

Einfache Ausgangslage für eine Alarmierungsübung:

„Übungsalarm! Ausfall von IT-Systemen durch Brand im Serverraum. Übungsalarm!“

Der BCMB sollte in seiner Jahresplanung darauf achten, dass über mehrere Jahre hinweg alle definierten Alarmierungswege getestet werden.

Durchführung der Alarmierungsübung

In der Praxis hat es sich bewährt, die Alarmierungsübung unangekündigt durchzuführen, um möglichst reale Voraussetzungen zu schaffen. Gegebenenfalls können die Teilnehmer aber zuvor informiert werden, dass eine Alarmierungsübung innerhalb eines vorgegebenen Zeitraums stattfinden wird, um deren Kooperationsbereitschaft weiterhin zu erhalten.

4.7.4 Planbesprechung

In Planbesprechungen werden einzelne Pläne der Notfallbewältigung, insbesondere die Geschäftsfortführungspläne, gemeinsam mit den Anwendern auf fachliche Plausibilität der Inhalte und der getroffenen Annahmen überprüft. Ziel der Planbesprechung ist es, die jeweiligen Pläne anhand eines Szenarios theoretisch durchzuspielen, um Korrekturbedarfe und Verbesserungsmöglichkeiten festzustellen.

Um die Planbesprechungen für die Teilnehmer greifbarer zu gestalten, können die Problemstellungen anhand fiktiver Lagen aber auch ohne Lage bzw. Szenario erörtert werden. Die beschriebenen Maßnahmen werden dabei durch die Anwender dahingehend beurteilt, ob diese auch in einer Stresssituation verständlich, und aus fachlicher Sicht plausibel, vollständig und aktuell sind. Planbesprechungen sind vor allem geeignet, um zu sensibilisieren, Abhängigkeiten aufzudecken oder notwendige Voraussetzungen von Maßnahmen zu erkennen bzw. bewusst zu machen.

Vorbereitung einer Planbesprechung

Die Vorbereitung einer Planbesprechung kann der BCMB zwar selbst übernehmen, deutlich sinnvoller ist es jedoch, wenn die Übung durch einen Mitarbeiter aus der Organisationseinheit vorbereitet wird, in dessen Zuständigkeitsbereich der Plan erstellt wurde. Dieser kann besser die Arbeitsbelastung und Terminsituation in der jeweiligen Organisationseinheit einschätzen und so geeignete Zeiträume festlegen, um die Planbesprechung durchzuführen. Zudem sind dem Mitarbeiter geeignete Personen bekannt, die an der Planbesprechung teilnehmen sollen.

Hinweis:

Planbesprechungen können jederzeit auch ohne geeignete organisatorische und technische Grundstrukturen für die BAO durchgeführt werden. Die Pläne werden nur theoretisch innerhalb des jeweils geltenden Bereichs diskutiert und überprüft, jedoch nicht praktisch umgesetzt. Daher ist es empfehlenswert, gleich nach Erstellung eines Plans, diesen in einer Planbesprechung weiter zu plausibilisieren und zu vervollständigen.

Eine Planbesprechung sollte stets angekündigt erfolgen und an einem geeigneten zentralen Ort stattfinden, der mit den erforderlichen Mitteln ausgestattet ist. Die Übungsdauer beträgt typischerweise zwei bis vier Stunden. Diese Details sollten, wie beschrieben, im Übungskonzept dokumentiert werden. Die Übungsziele von Planbesprechungen werden oft „weich“ formuliert.

Beispiel:

- Sensibilisierung und Schaffung eines gemeinsamen Verständnisses aller im Plan involvierten Stellen
- Klärung von Zuständigkeiten bei der Notfallreaktion
- Aufdeckung von internen und externen Abhängigkeiten
- Überprüfung vorhandener Notfallpläne auf Schwachstellen, bevor diese praktisch geübt werden

Ein individuelles, dynamisch aufgebautes Szenario mit weiteren Einlagen, so wie es bei Stabsübungen üblich ist, ist für diese Übungsart nicht notwendig. Ein Szenario, das zu Beginn der Übung als Ausgangslage kommuniziert wird, ist vollkommen ausreichend zur Vermittlung der Problemstellung und des Handlungsbedarfs.

Synergiepotenzial:

Planbesprechungen können eine Plattform bilden, um die Notwendigkeit von Informationsaustausch und Zusammenarbeit aufzuzeigen und den Aufbau von Vertrauensnetzen zu initiieren. Ein Beispiel hierfür ist das Szenario Cyber-Angriff, das gemeinsam mit Vertretern aus der IT-Abteilung und aus der Informationssicherheit im Rahmen einer Planbesprechung geübt werden kann. Hierbei steht das Identifizieren von Zielkonflikten im Fokus, z. B. hinsichtlich der Frage, ob ein IT-Betrieb zugunsten der Informationssicherheit abgeschaltet oder zugunsten des BCM aufrechterhalten werden soll.

Durchführung einer Planbesprechung

Die Planbesprechung hat die Form einer durch die Übungsleitung moderierten Besprechung mit Leitfragen zur konstruktiven Diskussion der folgenden Aspekte:

Vollständigkeit: Sind die Angaben zu den zeitkritischen Geschäftsprozessen, den Abhängigkeiten zu anderen Geschäftsprozessen sowie Ressourcen vollständig? Sind die Notfallmaßnahmen ausführlich genug beschrieben, um einen sachkundigen Dritten in die Lage zu versetzen, die zeitkritischen Geschäftsprozesse in einem Notbetrieb wiederaufzunehmen, die Aufgaben im Notbetrieb zu priorisieren und wieder in den Normalbetrieb zurückzuführen?

Plausibilität: Sind die beschriebenen Maßnahmen widerspruchsfrei und im geforderten Zeitraum (RTO) realistisch umsetzbar? Sind die Angaben innerhalb des GFP sowie die beschriebenen Abhängigkeiten zu anderen GFP oder WAP/WHP plausibel dargestellt?

Aktualität: Sind die Angaben zu den zeitkritischen Geschäftsprozessen, den Abhängigkeiten zu anderen Geschäftsprozessen sowie Ressourcen aktuell? Sind die referenzierten Dokumente in der jeweils aktuellen Version hinterlegt? Wurden die relevanten Ansprechpartner auf Basis einer aktuellen Kontaktliste dokumentiert?

4.7.5 Funktionstest

Funktionstests, auch funktionale Tests genannt, sind in vielen Institutionen bereits fester Bestandteil des Qualitätssicherungsprozesses, z. B. in der Software- oder Systementwicklung. Es existieren unterschiedliche Definitionen zum Begriff Funktionstest. In diesem Standard wird der Begriff weit gefasst und schließt alle Tests mit ein, mit denen funktionale Anforderungen auf systematischem Wege geprüft werden.

In einem Funktionstest werden einzelne oder eine Gesamtheit an Notfallmaßnahmen aus einem oder mehreren Notfallplänen überprüft, ob diese wie vorgesehen funktionieren. Anhand von Funktionstests können die für den Notbetrieb relevanten baulichen, technischen und organisatorischen Aspekte systematisch und, wenn vertretbar, realitätsnah überprüft werden. Außerdem wird überprüft, ob die Inhalte in der Notfalldokumentation verständlich, vollständig und fachlich richtig sind. Zudem kann verifiziert werden, ob die im Notfallplan enthaltenen Zeitvorgaben eingehalten werden können.

Beispiel:

- Ist das Verlagern zum und Arbeiten am Ausweichstandort für eine Auswahl von Mitarbeitern einer Fachabteilung möglich? (Szenario Standortausfall)
- Ist das Erledigen von Geschäftsvorgängen durch einen Mitarbeiter aus einer anderen Abteilung anhand der im Geschäftsfortführungsplan beschriebenen Schritte möglich? (Szenario Personalausfall)
- Ist das temporäre Nutzen eines vorhandenen alternativen Dienstleisters möglich? (Szenario Dienstleisterausfall)
- Ist die Inbetriebnahme von mehreren untereinander abhängigen Ausweichservern und der alternativen Netzverbindungen möglich? (Szenario IT-Ausfall)

- Sind der Anlauf und Betrieb eines Notstromaggregats in der vorgegebenen Zeit, eventuell auch für eine längere Dauer möglich? (Szenario Infrastrukturausfall)

Hinweis:

Funktionstests dienen insbesondere dazu, die RTA bestimmen und nachweisen zu können. Dabei ist es nicht notwendig, bei jedem Test den kompletten Notfallbewältigungsprozess zu simulieren. Aufwand und Kosten einer kompletten Überprüfung sind unter Berücksichtigung des tatsächlichen Notfallrisikos oft nicht angemessen. Stattdessen ist es häufig ausreichend

- sich auf die zeitkritischen Aspekte des Notfallplans zu konzentrieren sowie
- Teilaspekte des Notfallplans in aufeinander aufbauenden Stufen zu testen.

Die Übungsdauer reicht von wenigen Minuten für einen einfachen Funktionstest einzelner Komponenten bis hin zu mehreren Tagen inklusive Herstellen und Rückbau der Testumgebung für einen umfangreicheren Funktionstest.

Vorbereitung eines Funktionstests

Für Funktionstests sollten folgende Eckpunkte im Übungskonzept zusätzlich dokumentiert werden:

- Voraussetzungen (z. B. eine Testumgebung oder vorab durchgeführte Tests einzelner für den Funktionstest notwendiger Basisressourcen)
- Risikoeinschätzung und risikosenkende Maßnahmen

Funktionstests können reale Auswirkungen auf den Geschäftsbetrieb haben und diesen unter Umständen sogar unterbrechen, sowohl geplant als auch unbeabsichtigt. Der Übungsautor sollte eine Risikoeinschätzung zum Funktionstest und zu den damit verbundenen Auswirkungen durchführen und falls erforderlich, risikosenkende Maßnahmen ermitteln. Es wird empfohlen, für Funktionstest mit potenziell möglichen Auswirkungen auf den Geschäftsbetrieb eine Freigabe von der Institutionsleitung einzuholen. Zudem sollten dann auch Maßnahmen vorgesehen werden, die einen Abbruch des Funktionstests und eine schnellstmögliche Wiederherstellung des Ausgangszustands ermöglichen, falls unbeabsichtigte Auswirkungen auftreten.

Im Reaktiv-BCMS sollten Funktionstests immer angekündigt erfolgen. Funktionstests finden in der realen Umgebung oder in einer gesonderten Testumgebung statt. Bei einer Testumgebung handelt es sich idealerweise um ein speziell geschaffenes, möglichst realitätsnahes, aber vom Produktionsbetrieb abgekapseltes Testumfeld. Dies soll verhindern, dass der produktive Betrieb durch die Funktionstests eingeschränkt oder gefährdet wird.

Hinweis:

Die Herstellung und der Rückbau der Testumgebung müssen geplant werden. Die Planung wird am besten von ausgewählten Spezialisten aus Notfallteams durchgeführt. Alle speziell für die Übung geschaffenen Vorkehrungen müssen nach Übungsende rückgängig gemacht werden.

Die Übungsziele von Funktionstests sind in der Regel die praktische Überprüfung reaktiver Maßnahmen hinsichtlich ihrer Funktionsfähigkeit.

Beispiel:

Typische Übungsziele für Funktionstests sind:

- die praktische Überprüfung von technischen Vorkehrungen und organisatorischen Verfahren, die für den Notfall vorgesehen sind

- die praktische Überprüfung vorhandener Notfallpläne in Gänze oder in Teilen in Bezug auf fachliche Korrektheit, Aktualität und Vollständigkeit
- das Training der Mitarbeiter im Umgang mit dem Notfallplan
- die Überprüfung der Einhaltung von Zeitvorgaben, die im Notfallplan enthalten sind

Durchführung eines Funktionstests

Funktionstests finden auf Basis der Ressourcenkategorien statt, die dem Notfallplan zugrunde liegen. Der Ablauf sollte den vorgesehenen Maßnahmen aus dem Notfallplan entsprechen und wird durch die Übungsleitung gesteuert. Bei sehr einfachen Funktionstests, z. B. dem Testen eines Notfall-Laptops, kann die Übungsleitung durch die testende Person selbst wahrgenommen werden. Bei komplexen Funktionstests hingegen, sollte die Übungsleitung durch eine separate Person besetzt sein, welche die Vorgänge koordiniert. Ein Protokollant oder weitere Unterstützungsrollen können den Ablauf sowie die Auswertung unterstützen und die anderen Beteiligten damit entlasten.

Die in dem Funktionstest aufgedeckten Korrekturbedarfe und Verbesserungsmöglichkeiten sollten nachvollziehbar protokolliert werden. Es ist empfehlenswert, anhand einer einheitlichen Protokollvorlage pro getesteter Maßnahme bzw. Ressource zu dokumentieren, ob diese „ohne Befund" funktioniert hat oder ob es Auffälligkeiten bzw. Anmerkungen gab. Die Inhalte des Protokolls sollten prägnant und für sachverständige Dritte verständlich formuliert sein.

Beispiel: Funktionstest Ausweichstandort

Zu testende Ressource	Testaktivität	Ergebnis	Bemerkung	Korrekturmaßnahme
Gebäude	Zugang zum Gebäude über Wachdienst prüfen	**Nicht erfolgreich**	Wachdienst war nicht in seine Aufgaben in einem Notfall eingewiesen.	Schulungsunterlagen und -maßnahmen prüfen
Notfallarbeitsplatz	Vollständigkeit der Ausstattung prüfen	**Erfolgreich**	Alle Materialien des Notfallarbeitsplatzes vorhanden.	
Notfallarbeitsplatz	Anmeldung mit Nutzerkennung prüfen	**Teilweise erfolgreich**	Anmeldung erfolgreich, aber der Notfallarbeitsplatz wurde nicht regelmäßig aktualisiert. Durch eine systemseitige Aktualisierung kommt es zu einer deutlichen Verzögerung.	Aktualisierungs-prozess prüfen
Notfallarbeitsplatz	Notfallrelevante Software prüfen	**Nicht erfolgreich**	E-Mail und Warenwirtschaftssystem verfügbar. Kundenkartei nicht erreichbar.	Kundenkartei für standortübergreifende Zugriffe freischalten

Tabelle 30: Beispiel für den Aufbau eines Testprotokolls

4.7.6 Auswertung und Nachbereitung von Übungen

Die Auswertung und Nachbereitung jeder Übung ist Voraussetzung, um das BCM weiterentwickeln und Korrekturbedarfe und Verbesserungsmöglichkeiten identifizieren zu können. Alle durchgeführten Übungen müssen ausgewertet und nachbereitet werden. In der Auswertung wird zum einen analysiert, ob und wie gut die gesetzten Ziele erreicht wurden.

Zum anderen werden Korrekturbedarfe und Verbesserungsmöglichkeiten abgeleitet. Dies können sowohl dokumentarische oder technische Änderungsbedarfe in den Notfallplänen und -Maßnahmen sein, als auch Anpassungen an der BCM-Aufbauorganisation oder dem BCM-Prozess bzw. der Notfallbewältigungsprozess. Zusätzlich können aus der Übung funktions- bzw. rollenspezifische Verbesserungs- und Unterstützungsbedarfe hervorgehen, z. B. zu den individuellen Aufgaben und Befugnissen einzelner Rollen. Auch Schulungs- oder Trainingsbedarfe für die Rolleninhaber des Stabes zählen dazu.

Sowohl die für die Übung herangezogenen Dokumente, wie die Notfallpläne, als auch in der Übung erstellte Dokumente sollten ausgewertet werden. Erstellte Dokumente sind zum einen Übungsprotokolle und Feedbackbögen der Übungsteilnehmer. Zum anderen geben auch Ergebnisobjekte der Stabsübung, wie Visualisierungen, Protokolle oder fiktive Pressemitteilungen, Auskunft über die Reife des BCM. Alle Übungsergebnisse und identifizierten Korrekturbedarfe und Verbesserungsmöglichkeiten sollten in einem Übungsbericht dokumentiert werden. Der BCMB sollte daraus ableiten, wie ausgereift das BCM der Institution bereits ist.

Hinweis:

Mit der *Darstellung des Übungserfolges* ist hier nicht gemeint, dass beurteilt wird, ob die Teilnehmer immer „richtig“, d. h. wie geplant bzw. aus fachlicher Sicht sinnvoll, gehandelt und entschieden haben. Vielmehr sollte im Rahmen der Auswertung und Nachbereitung dargestellt werden, welcher Lerneffekt erzielt und welche Korrekturbedarfe oder Verbesserungsmöglichkeiten erkannt werden konnten. Eine „fehlerfreie“ Übung ist hingegen kein Erfolgskriterium für eine Übung. Wurden alle Übungsziele erreicht, kann dies als Erfolg angesehen werden. Im Umkehrschluss kann aber auch dann von einer erfolgreichen Übung gesprochen werden, wenn darin Korrekturbedarfe und Verbesserungsmöglichkeiten identifiziert wurden und diese Erkenntnisse genutzt werden, um das BCMS weiter zu verbessern.

Zusätzliche Aspekte zur Auswertung und Nachbereitung einer Stabsübung

Falls im Anschluss an die Stabsübung eine Auswertungsrunde vorgesehen ist, sollte diese zum vorgesehenen Zeitpunkt durch die Übungsleitung oder einen im Vorfeld festgelegten, geeigneten Moderator gestartet werden. Die Teilnehmer sollten ihre persönlichen Eindrücke und die Zielerreichung einschätzen sowie identifizierte Korrekturbedarfe und Verbesserungsmöglichkeiten darstellen. In der Auswertungsrunde können auch Fragebögen genutzt werden. Die Auswertungsrunde sollte protokolliert werden. Daraus sollten Erkenntnisse für die weitere Auswertung abgeleitet werden.

Zusätzliche Aspekte zur Auswertung einer Alarmierungsübung

Die Ergebnisse der Alarmierungsübung müssen protokolliert werden. Wird eine Alarmierungssoftware eingesetzt ist es empfehlenswert, die von der IT-Anwendung erzeugten Protokolle auszuwerten. Die im Übungsverlauf erzeugten Protokolle erlauben es im Anschluss der Übung diese auszuwerten.

Ergebnisvorstellung und Festlegung der Folgeschritte

Das Übungsergebnis sowie die identifizierten Korrekturbedarfe und Verbesserungsmöglichkeiten müssen durch die Übungsleitung an den BCMB kommuniziert werden, damit er diese im Maßnahmenplan aufgreifen kann (siehe Kapitel *4.8 Weiterentwicklung des BCMS*).

4.8 Weiterentwicklung des BCMS

Nachdem alle Schritte des BCM-Prozesses innerhalb des Reaktiv-BCMS durchlaufen wurden, ist die Institution grundsätzlich in der Lage, auf Notfälle zu reagieren und diese mit Hilfe der BAO sowie der Geschäftsfortführungspläne zu bewältigen. Jedoch wurden hierbei wesentliche Schritte zurückgestellt. Infolgedessen ist es sehr wahrscheinlich, dass im BCM der Institution echte Lücken in der Notfallplanung bestehen.

In der Voranalyse wurde der Analysebereich auf die zeitkritischsten Organisationseinheiten begrenzt. Damit besteht für die ausgegrenzten Organisationseinheiten das Risiko, unzureichend im BCM abgesichert zu sein. Zusätzlich basieren die Geschäftsfortführungspläne im Wesentlichen auf den bereits vorhandenen Möglichkeiten. Folgerichtig können auch die im Soll-Ist-Vergleich identifizierten Handlungsbedarfe nur über Anpassungen der Geschäftsabläufe und „Quick-Fixes“ behandelt werden. Auch hier werden wahrscheinlich Lücken im Reaktiv-BCMS bestehen bleiben:

- Es fehlen systematische Business-Continuity Strategien, die den geordneten Wiederanlauf aller zeitkritischen Ressourcen entsprechend der Handlungsbedarfe garantieren.
- Die Wiederanlauffähigkeit zeitkritischer Ressourcen kann nur bedingt überprüft werden, da komplexe Übungs- und Testarten im Reaktiv-BCMS nicht vorgesehen sind.
- Da kein Übungsprogramm definiert wurde, kann die Reife des BCMS nicht anhand komplexer werdender Übungen und Tests gesteigert werden.
- Im Reaktiv-BCMS werden Maßnahmen zur Notfallvorsorge nicht näher betrachtet.

Die genannten Schritte konnten in einem ersten PDCA-Zyklus des Reaktiv-BCMS bewusst zurückgestellt werden, um schnell konkrete Resultate mit Fokus auf die Notfallbewältigung zu erzielen. Jedoch können für die weitere Entwicklung des BCMS die beschriebenen Lücken nicht toleriert werden, da von einem immanenten Risiko eines unzureichend abgesicherten Geschäftsbetriebs ausgegangen werden muss. Daher muss in einem finalen Schritt die Weiterentwicklung des BCMS festgelegt werden. Die nachfolgenden Kapitel beschreiben die empfohlene Vorgehensweise, mittels derer die Weiterentwicklung des BCMS durchgeführt wird. In Abbildung 35 sind die hierfür erforderlichen Schritte in einer Übersicht dargestellt:

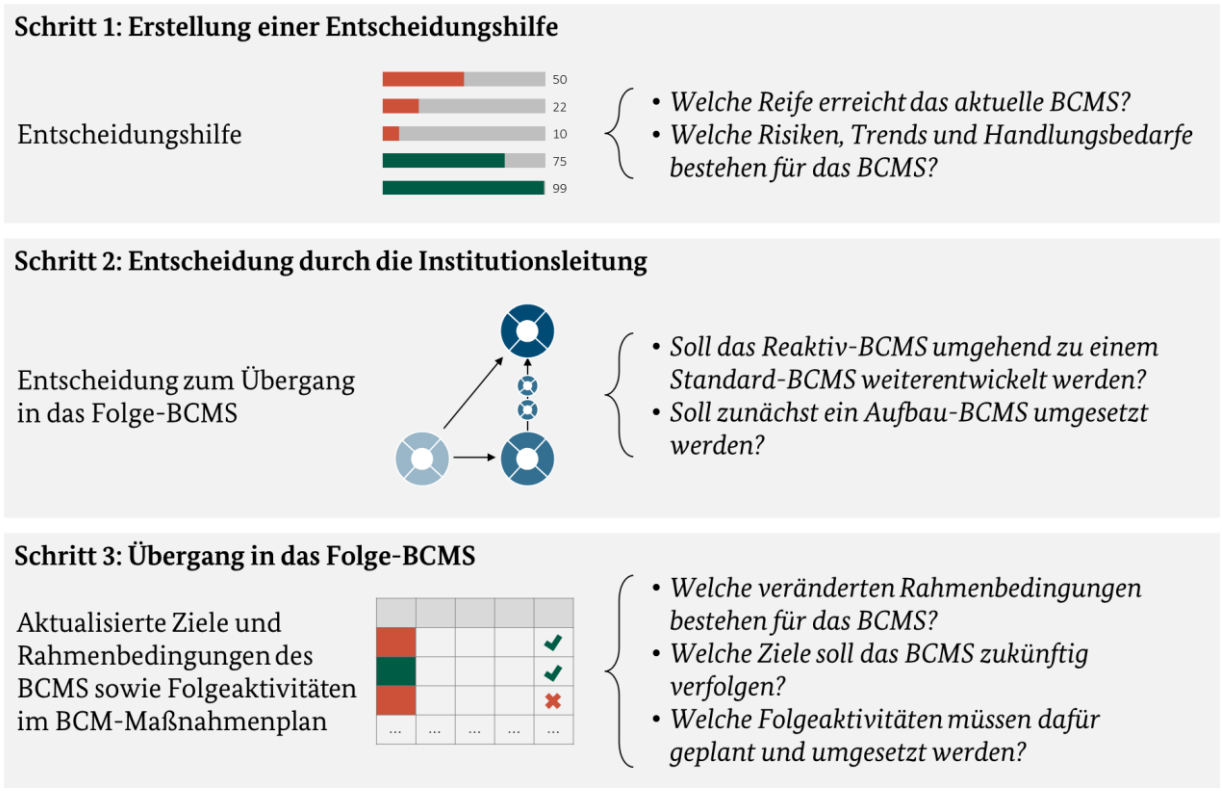

Abbildung 35: BCM-Prozessschritte zur Weiterentwicklung des BCMS

4.8.1 Erstellung einer Entscheidungshilfe

Der BCMB sollte die gewonnenen Erkenntnisse zum BCMS zusammenfassen und der Institutionsleitung als Entscheidungshilfe zur Verfügung stellen. Ziel der Entscheidungshilfe ist es, die wesentlichen Erkenntnisse vorzustellen und die erforderlichen Schritte und Maßnahmen zur Weiterentwicklung des BCMS abzustimmen. Hierbei sollte insbesondere analysiert werden, inwieweit die erreichte Reife die bisherigen Ziele des BCMS abdeckt.

Für einen Bericht an die Institutionsleitung sind die einzelnen Erkenntnisse je BCM-Prozessschritt zu detailliert. Um der Institutionsleitung eine Entscheidungshilfe zu bieten, sollten die vorliegenden Erkenntnisse verdichtet, die Risiken, Trends und Handlungsbedarfe im BCM abgeleitet und eine Option vorgeschlagen werden. Je geringer die Zielerreichung durch den BCMB eingeschätzt wird, desto eher sollte die Weiterentwicklung anhand eines Aufbau-BCMS erfolgen. Tabelle 31 listet mögliche Erkenntnisse auf.

Beispiel:

Erkenntnis	**Quelle**
Fähigkeit der Institution, angemessen auf Notfälle zu reagieren	reale Ereignisse sowie Ergebnisse der Stabsübung(en)
Effektivität und Angemessenheit der Methoden und Verfahren zur Identifikation von zeitkritischen Geschäftsprozessen und Ressourcen	identifizierte Korrekturbedarfe und Verbesserungsmöglichkeiten aus der Voranalyse und BIA
Abdeckungsgrad ausreichend abgesicherter Ressourcen gemäß RTA vs. RTO	Soll-Ist-Vergleich
Effektivität und Angemessenheit der Geschäftsfortführungsplanung	identifizierte Korrekturbedarfe und Verbesserungsmöglichkeiten aus der Geschäftsfortführungsplanung sowie aus Planbesprechungen und Funktionstests
Abdeckungsgrad der zeitkritischen Organisationseinheiten bzw. GPs im Geltungsbereich des BCMS	Übersicht, welche zeitkritischen Organisationseinheiten bereits einen GFP dokumentiert und getestet haben und in welchem Grad diese GFPs geeignet sind die MTPDs einzuhalten.
Fähigkeiten und Kenntnisse der BCM-Rolleninhaber und Grad der BCM-Kultur in der Institution	identifizierte Korrekturbedarfe und Verbesserungsmöglichkeiten aus durchgeführten Schulungen, Sensibilisierungsmaßnahmen sowie Rückmeldungen der Rolleninhaber in Stabsübungen
Im Rahmen des Reaktiv-BCMS identifizierte Korrekturbedarfe und Verbesserungsmöglichkeiten	Maßnahmenliste

Tabelle 31: Übersicht möglicher Kriterien zur Einschätzung der Reife des BCMS (Beispiele)

4.8.2 Entscheidung durch die Institutionsleitung

Anhand der Entscheidungshilfe sollte die Institutionsleitung den weiteren Handlungsbedarf ermitteln und entscheiden, wie das BCMS weiterentwickelt werden soll. Hierzu bieten sich zwei verschiedene Optionen an:

Option 1: Erstellung einer Roadmap für ein Aufbau-BCMS sieht vor, dass alle BCM-Prozesses-Schritte eines Standard-BCMS durchlaufen werden.

Wegen des weiterhin eingeschränkten Analysebereichs besteht bei einem Wechsel zu einem Aufbau-BCMS weiterhin das Risiko der nicht untersuchten und daher nicht abgesicherten Bereiche. Die Roadmap für ein Aufbau-BCMS muss daher einerseits einen Zeitplan aufzeigen, aus dem hervorgeht, bis wann ein Standard-BCMS erreicht werden soll. Zum anderen müssen die mittelfristigen Etappen dokumentiert werden, um sichtbar zu machen, wie der Analysebereich der BIA schrittweise an den Geltungsbereich des BCMS herangeführt wird. Anhand regelmäßiger Managementberichte sollte die Roadmap jeweils auf die aktuellen Gegebenheiten angepasst werden.

Option 2: Erstellung einer Roadmap für ein Standard-BCMS sieht vor, dass alle Teilschritte des BCM-Prozesses eines Standard-BCMS durchlaufen werden und der gesamte BCMS-Geltungsbereich untersucht und bedarfsgerecht abgesichert wird. Eine zeitliche Vorgabe der Roadmap entfällt damit, da sich diese an der Geschwindigkeit des BCM-Lebenszyklus orientiert.

Mit dem Übergang von einem Reaktiv-BCMS zu einem Standard-BCMS steigen sowohl die methodischen Anforderungen als auch die Anzahl der zu berücksichtigenden Organisationseinheiten und damit der Geschäftsprozesse. Zusätzlich hat die Institution weniger Zeit, Erfahrungen mit den zusätzlichen Methoden und Verfahren zu sammeln, als bei einem Umweg über ein Aufbau-BCMS. Daher kann es sinnvoll sein, sich dieses Expertenwissen zum Aufbau eines Standard-BCMS extern zu beschaffen, z. B. durch einen Erfahrungsaustausch in Arbeitsgremien.

4.8.3 Verfolgung der BCM-Maßnahmenliste

Wenn ein Reaktiv-BCMS in ein Aufbau- oder Standard-BCMS übergeht, besteht die Besonderheit, dass bereits identifizierte Korrekturbedarfe- und Verbesserungsmöglichkeiten darin aufgegriffen werden müssen. Zum einen umfasst dies Korrekturbedarfe und Verbesserungsmöglichkeiten, die im Reaktiv-BCMS noch nicht behandelt werden konnten. Diese sollten im Rahmen der Risikoanalyse aufgegriffen und anhand konkreter BC-Strategien und -Lösungen behandelt werden (siehe Kapitel 6.7 *BCM-Risikoanalyse*). Zum anderen müssen bereits eingeleitete Korrektur- und Verbesserungsmaßnahmen weiterhin im Folge-BCMS nachverfolgt werden.

Um sicherzustellen, dass identifizierte Korrekturbedarfe und Verbesserungsmöglichkeiten nicht vergessen werden und die entsprechenden Maßnahmen umgesetzt sowie nachverfolgt werden können, sollte der BCMB bereits mit der Initiierung des Reaktiv-BCMS einen Maßnahmenplan erstellen und nachverfolgen. Die folgende Tabelle zeigt beispielhaft eine mögliche Struktur eines Maßnahmenplans anhand einer identifizierten, fiktiven Abweichung und seiner Korrekturmaßnahme.

Beispiel:

Eindeutige Kennung der Maßnahme	**BCM-Korrektur-0001a**	**BCM-Korrektur-0001b**
Korrekturbedarf oder Verbesserungsbedarf	Im Rahmen der durchgeführten Übungen und Tests wurde festgestellt, dass die Geschäftsfortführungspläne der Organisationseinheiten Bürgerbüro und IT-Help Desk weder vollständig noch aktuell waren. So fehlten zeitkritische Ressourcen aus dem Soll-Ist-Vergleich und es wurde auf nicht länger bestehende Dokumente verwiesen.	Siehe BCM-Korrektur-0001a Mitarbeiter sind nicht in die Bearbeitung von Geschäftsfortführungsplänen eingewiesen worden.

Eindeutige Kennung der Maßnahme	**BCM-Korrektur-0001a**	**BCM-Korrektur-0001b**
Ursache	Grund für die BCM-Korrektur-0001a ist, dass die zuständigen Mitarbeiter nicht in die Bearbeitung von Geschäftsfortführungsplänen eingewiesen worden sind.	Ursache hierfür ist, dass Mitarbeiter sich nicht im Schulungs- und Sensibilisierungsplan befanden. Grund hierfür ist, dass diese dem BCMB nicht als neue Mitarbeiter gemeldet wurden. Mit der Organisationseinheit Personal wurde bislang kein Meldeprozess definiert für den Fall, dass Mitarbeiter die Organisationseinheit wechseln oder die Institution verlassen.
Vorgesehene Korrektur- oder Verbesserungsmaßnahme	Zur kurzfristigen Behandlung der Abweichung werden die Geschäftsfortführungspläne gemeinsam mit den BCMK aktualisiert und im Rahmen einer Planbesprechung erneut geübt. (Maßnahmen zur langfristigen Behandlung siehe BCM-Korrektur-0001b)	Um die Abweichung langfristig abzustellen, soll der Prozess für Mitarbeiterwechsel und Benennung von BCM-Rollenträgern gemeinsam mit der Organisationseinheit Personal überarbeitet und entsprechende Kontrollmechanismen entwickelt werden.
Zuständige Stelle(n)	BCMB, BCMK	Organisationseinheit Personal
Festgelegte Priorität	**Hoch** – ~~Mittel~~ – ~~Gering~~	~~Hoch~~ – **Mittel** – ~~Gering~~
Geplanter Fertigstellungstermin	16.08.2020 (Heute + 2 Wochen)	31.12.2020
Notwendige Ressourcen	Verfügbarkeit der zuständigen BCMK und der zuständigen Mitarbeiter	Verfügbarkeit der Mitarbeiter der Organisationseinheit Personal
Umsetzungsstatus	~~Offen~~ – ~~in Umsetzung~~ – **abgeschlossen** – ~~abgeschlossen und Wirksamkeit geprüft~~	**Offen** – ~~in Umsetzung~~ – ~~abgeschlossen~~ – ~~abgeschlossen und Wirksamkeit geprüft~~
Umsetzungsdetails	01.08.: Maßnahme freigegeben durch BCMB 14.08.: GFP wurden aktualisiert.	01.08.: Maßnahme freigegeben durch BCMB

Tabelle 32: Struktur des Maßnahmenplans am Beispiel einer fiktiven Abweichung

Anhand des Maßnahmenplans sollten die Maßnahmen nicht nur geplant und priorisiert, sondern auch deren Fortschritt überwacht werden. Zudem erleichtert der Maßnahmenplan es dem BCMB den Gesamtüberblick zu behalten und die Korrektur- und Verbesserungsmaßnahmen steuern zu können. Der Maßnahmenplan schafft damit die idealen Voraussetzungen, um die geeignete Stufe des Folge-BCMS auszuwählen, die Ziele und Prioritäten im BCM zu konkretisieren und den Ressourcenbedarf des BCMS neu darauf auszurichten.

4.8.4 Übergang in das Folge-BCMS

Für einen geregelten Übergang vom Reaktiv-BCMS in ein Folge-BCMS müssen die nachfolgenden Aspekte behandelt werden:

Aktualisierung der Ziele und Rahmenbedingungen des BCMS

Sobald die Institutionsleitung sich für ein Folge-BCMS entschieden hat, müssen die Ziele und Rahmenbedingungen des BCMS innerhalb der nächsten Initiierung angepasst werden. Auf jeden Fall sollte sichergestellt werden, dass die notwendige BCM-Kultur geschaffen wird. Dies bedeutet, dass alle am Aufbau des BCMS beteiligten Personen sowie die Institution als Ganzes willens und kompetent sein sollten, die Aufgabe zu meistern, das BCMS kontinuierlich weiterzuentwickeln. Dies kann anhand eines Schulungs- und Sensibilisierungsprogramms des BCMS sichergestellt werden.

Anwendungshinweise bei der Überführung des Reaktiv-BCMS in ein Folge-BCMS

Das Reaktiv-BCMS ist so aufgebaut, dass dieses nahtlos in ein Aufbau- oder Standard-BCMS weiterentwickelt werden kann. Daher wiederholen sich in den Kapiteln zum Aufbau- und Standard-BCMS eine Reihe an Aspekten. Diese sind jedoch oft erweitert und sollten daher gelesen werden. Neben den hinzukommenden Kapiteln (siehe Abbildung 37), sind die größten Erweiterungen hier zusammengefasst:

- Der Aufbau und die Befähigung der BAO beinhaltet detaillierte Anforderungen an eine Geschäftsordnung des Stabes (siehe Kapitel 6.4.4 *Definition der Geschäftsordnung des Stabs*).
- Innerhalb der BIA werden zusätzlich Prozessabhängigkeiten sowie Single Point of Failures identifiziert (siehe Kapitel 6.5.2.2 *Identifizierung der Prozessabhängigkeiten* sowie 6.5.2.4 *Identifizierung vorhandener Single Point of Failure*).
- Innerhalb der Geschäftsfortführungsplanung werden die festgelegten Business Continuity Strategien und Lösungen sowie die Ergebnisse der BCM-Risikoanalyse berücksichtigt (siehe Kapitel 6.9.2.2 *Entwicklung von Notfallmaßnahmen*).
- Übungen und Tests werden mit umfangreicheren Übungsarten konkreter geplant, gesteuert und ausgewertet (siehe insbesondere Kapitel 6.11.1 *Festlegung der Rahmenbedingungen zum Üben* sowie 6.11.3 *Vorbereitung und Durchführung einer Übung)*.
- Die Weiterentwicklung des BCMS geht in eine kontinuierliche Verbesserung des BCMS über und wird dazu um einige Aspekte, wie z. B. eine regelmäßige Überprüfung des BCMS durch die Institutionsleitung, erweitert (siehe Kapitel 6.13 *Korrektur und Verbesserung des BCMS*).

Zahlreiche einzelne Anforderungen in den BCM-Prozessschritten weichen ebenfalls von denen im Reaktiv-BCMS ab. Die Anforderungen an das Standard-BCMS können dem Anforderungskatalog entnommen werden (siehe Kapitel 8 *Anhang A: Anforderungskatalog*).

5 Aufbau-BCMS

Das Aufbau-BCMS bildet einen Mittelweg zwischen dem Reaktiv BCMS und dem Standard-BCMS, indem es die vollständige Methodik des Standard-BCMS mit den Einschränkungen des Prozessumfangs des Reaktiv-BCMS verbindet. Das Aufbau-BCMS wird nicht durch separate Unterkapitel je BCMS-Prozessschritt vorgestellt. Die Beschreibungen zu den einzelnen Prozessschritten können den Kapiteln zum Standard-BCMS entnommen werden. Die zusätzlichen Beschreibungen zur Voranalyse können dem Reaktiv-BCMS entnommen werden. Das vorliegende Kapitel stellt nur eine grundlegende Übersicht über den prozessualen Ablauf dar und visualisiert in Abbildung 36, wie die einzelnen Prozessschritte ineinandergreifen.

Plan-Phase

Für den Erfolg des Aufbau-BCMS ist es entscheidend, in der Plan-Phase die Anforderungen an das BCMS genau zu **analysieren** und das BCMS auf die berechtigten Bedürfnisse und Anforderungen von relevanten Interessengruppen auszurichten. Damit die jeweilige Zielgruppe innerhalb der Institution zur richtigen Zeit auf die relevanten Informationen zugreifen kann, ist es wichtig, die **Dokumentation** näher festzulegen. In der **Leitlinie** dokumentiert die Institutionsleitung ihre Selbstverpflichtung und legt die Rahmenbedingungen für das BCMS (z. B. Ressourcenausstattung) fest.

Do-Phase

Der **Aufbau und die Befähigung der BAO** beinhaltet alle Aspekte, um eine funktionierende BAO zu etablieren, die auch im Not- und Krisenfall erreichbar und handlungsfähig ist. Die Institution kann so auf Schadensereignisse reagieren, unabhängig davon, ob bereits Notfallpläne für die Fortführung von Geschäftsprozessen vorliegen.

Alle weiteren Prozessschritte in der DO-Phase dienen der angemessenen Absicherung der zeitkritischen Geschäftsprozesse. In der **Voranalyse** wird der Untersuchungsbereich vorgefiltert, der in den nachfolgenden Prozessschritten näher untersucht und angemessen abgesichert werden soll. Die **Business Impact Analyse** untersucht näher, was innerhalb des Untersuchungsbereichs abgesichert werden soll. Dazu analysiert die Institution, welche der Geschäftsprozesse im Untersuchungsbereich zeitkritisch sind, wie lange diese ausfallen dürfen und welche Ressourcen sie im Notbetrieb benötigen. Im **Soll-Ist-Vergleich** wird festgestellt, ob diese Ressourcen schon ausreichend abgesichert sind. In der **BCM-Risikoanalyse** wird untersucht und entschieden, gegen welche Gefährdungen die identifizierten zeitkritischen Geschäftsprozesse und die dazu benötigten Ressourcen mit **Business Continuity-Strategien und -Lösungen** abgesichert werden sollen. Dazu werden geeignete BC-Strategien und –Lösungen festgelegt und umgesetzt. Darauf aufbauend dokumentieren die **Geschäftsfortführungspläne** (auf Ebene der Geschäftsprozesse) und **Wiederanlaufpläne** (auf Ebene der Ressourcen) die Handlungsschritte, die im Notfall durchgeführt werden müssen, damit die zeitkritischen Geschäftsprozesse innerhalb der geforderten Zeit fortgeführt werden können. Die **Wiederherstellungspläne** dokumentieren dagegen, welche Handlungsschritte nötig sind, um die Ressourcen wieder für den Normalbetrieb bereitzustellen.

Check-Phase

Anhand von **Übungen und Tests** wird überprüft, ob die beschriebenen Strukturen, Notfallpläne und insbesondere die reaktiven Maßnahmen, nicht nur theoretisch, sondern auch praktisch wirksam sind. Weiterhin wird in **Leistungsüberprüfungen** untersucht, ob das BCMS den gesetzten Anforderungen und Zielen entspricht.

Act-Phase

Im Rahmen der Act-Phase des BCMS werden die identifizierten Korrekturbedarfe und Verbesserungsmöglichkeiten in konkrete Maßnahmen überführt, umgesetzt und auch weiter nachverfolgt.

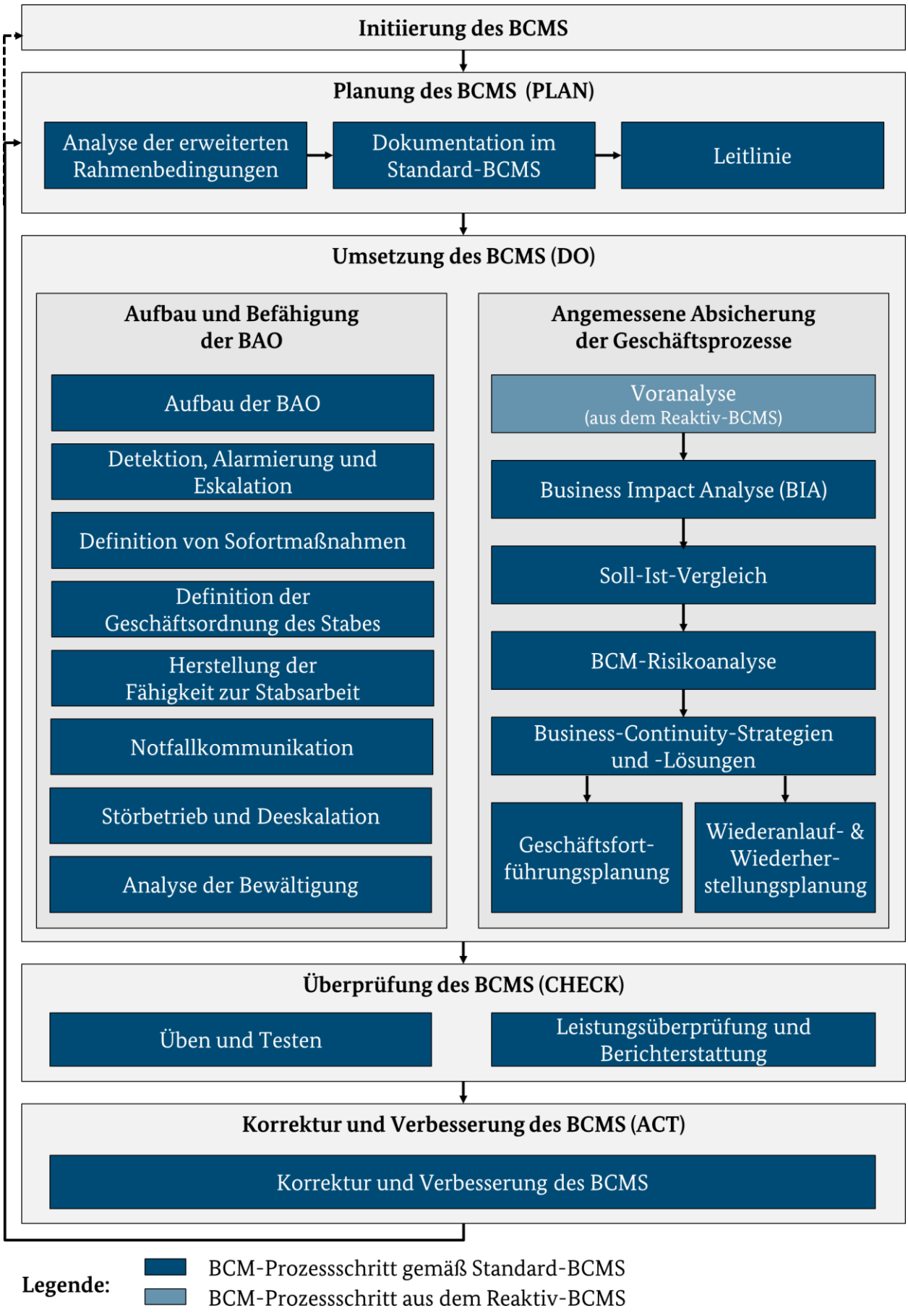

Abbildung 36: BCM-Prozess des Aufbau-BCMS

Hinweis:

Im Rahmen des Reaktiv-BCMS wurde empfohlen, zunächst die BAO aufzubauen und zu befähigen. Im Rahmen des Aufbau-BCMS kann frei entschieden werden, ob die BAO **vor**, **gleichzeitig mit** oder **nach** der angemessenen Absicherung der Geschäftsprozesse aufgebaut und befähigt wird. Hierbei bestehen unterschiedliche Vorteile, die Im Kapitel zum Standard-BCMS beschrieben werden (siehe Kapitel 6 *Standard-BCMS*).

6 Standard-BCMS

Das Standard-BCMS beinhaltet alle Schritte, um ein vollständiges, angemessenes und interessengruppengerechtes BCMS zu etablieren. Werden alle Schritte des Standard-BCMS umgesetzt, ist das daraus entstandene BCMS zur Norm ISO 22301 kompatibel. Das vorliegende Kapitel stellt nur eine grundlegende Übersicht über den prozessualen Ablauf dar und visualisiert in Abbildung 37, wie die einzelnen Prozessschritte ineinandergreifen.

Plan-Phase

Für den Erfolg des Standard-BCMS ist es entscheidend, in der Plan-Phase die Anforderungen an das BCMS genau zu **analysieren** und das BCMS auf die berechtigten Bedürfnisse und Anforderungen von relevanten Interessengruppen auszurichten. Damit die jeweilige Zielgruppe innerhalb der Institution zur richtigen Zeit auf die relevanten Informationen zugreifen kann, ist es wichtig, die **Dokumentation** näherfestzulegen. In der **Leitlinie** dokumentiert die Institutionsleitung ihre Selbstverpflichtung und legt die Rahmenbedingungen für das BCMS (z. B. Ressourcenausstattung) fest.

Do-Phase

Der **Aufbau und die Befähigung der BAO** beinhaltet alle Aspekte, um eine funktionierende BAO zu etablieren, die auch im Not- und Krisenfall erreichbar und handlungsfähig ist. Die Institution kann so auf Schadensereignisse reagieren, unabhängig davon, ob bereits Notfallpläne für die Fortführung von Geschäftsprozessen vorliegen.

Alle weiteren Prozessschritte in der DO-Phase dienen der angemessenen Absicherung der zeitkritischen Geschäftsprozesse. Die **Business Impact Analyse** untersucht näher, was innerhalb des Untersuchungsbereichs abgesichert werden soll. Dazu analysiert die Institution, welche der Geschäftsprozesse im Untersuchungsbereich zeitkritisch sind, wie lange diese ausfallen dürfen und welche Ressourcen sie im Notbetrieb benötigen. Im **Soll-Ist-Vergleich** wird festgestellt, ob diese Ressourcen schon ausreichend abgesichert sind. In der **BCM-Risikoanalyse** wird untersucht und entschieden, gegen welche Gefährdungen die identifizierten zeitkritischen Geschäftsprozesse und die dazu benötigten Ressourcen mit **Business Continuity-Strategien und -Lösungen** abgesichert werden sollen. Dazu werden geeignete BC-Strategien und –Lösungen festgelegt und umgesetzt. Darauf aufbauend dokumentieren die **Geschäftsfortführungspläne** (auf Ebene der Geschäftsprozesse) und **Wiederanlaufpläne** (auf Ebene der Ressourcen) die Handlungsschritte, die im Notfall durchgeführt werden müssen, damit die zeitkritischen Geschäftsprozesse innerhalb der geforderten Zeit fortgeführt werden können. Die **Wiederherstellungspläne** dokumentieren dagegen, welche Handlungsschritte nötig sind, um die Ressourcen wieder für den Normalbetrieb bereitzustellen.

Check-Phase

Anhand von **Übungen und Tests** wird überprüft, ob die beschriebenen Strukturen, Notfallpläne und insbesondere die reaktiven Maßnahmen, nicht nur theoretisch, sondern auch praktisch wirksam sind. Weiterhin wird in **Leistungsüberprüfungen** untersucht, ob das BCMS den gesetzten Anforderungen und Zielen entspricht.

Act-Phase

Im Rahmen der Act-Phase des BCMS werden die identifizierten Korrekturbedarfe und Verbesserungsmöglichkeiten in konkrete Maßnahmen überführt, umgesetzt und auch weiter nachverfolgt.

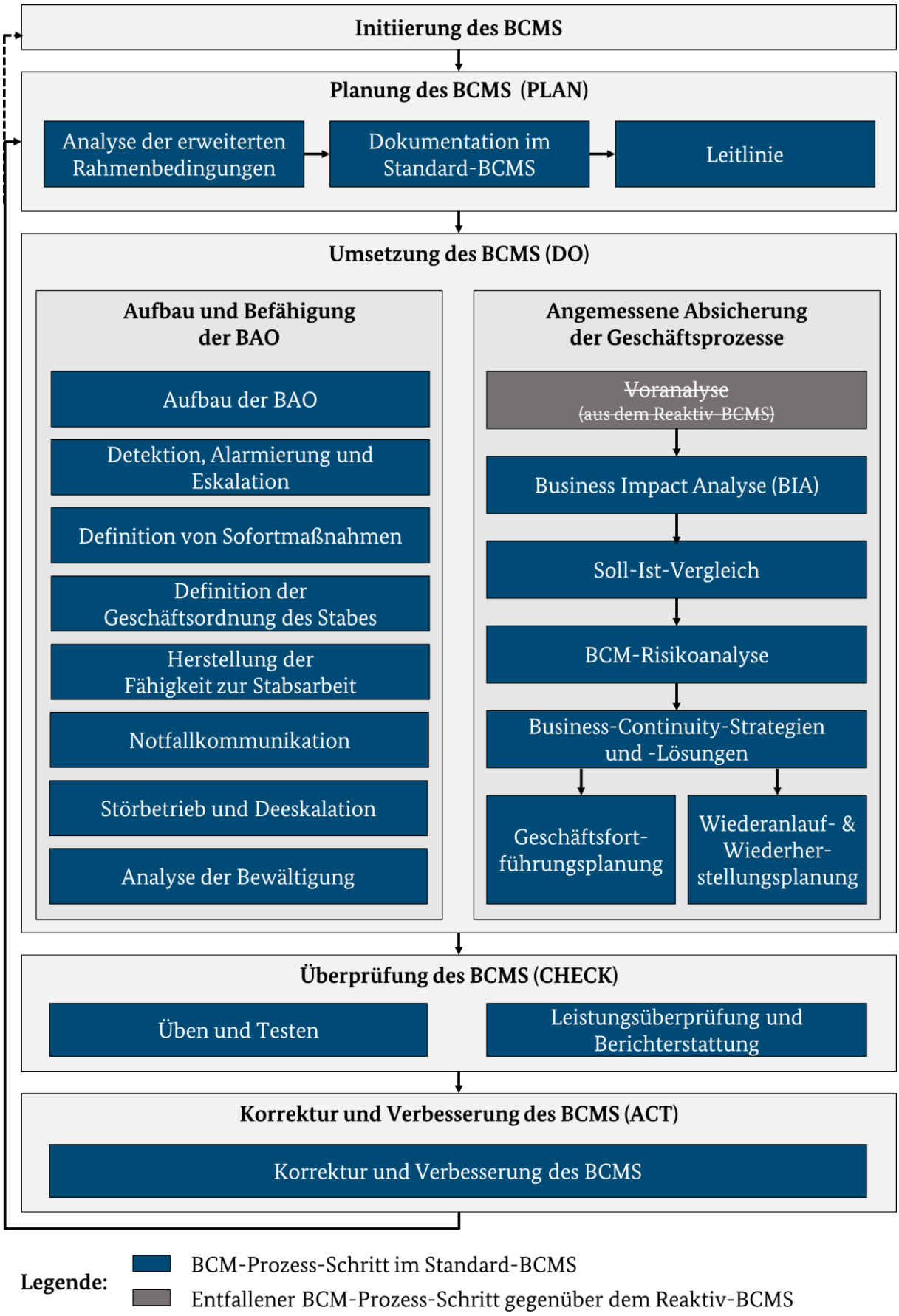

Abbildung 37: BCM-Prozess des Standard-BCMS

Hinweis:

Im Rahmen des Reaktiv-BCMS wurde empfohlen, zunächst die BAO aufzubauen und zu befähigen. Im Rahmen des Standard-BCMS kann frei entschieden werden, ob die BAO **vor**, **gleichzeitig mit** oder **nach** der angemessenen Absicherung der Geschäftsprozesse aufgebaut und befähigt wird. Hierbei bestehen unterschiedliche Vorteile, die folgend erläutert werden:

Wird die BAO **vor der angemessenen Absicherung der Geschäftsprozesse aufgebaut und befähigt**, ermöglicht dies schneller eine allgemeine Reaktionsfähigkeit in einem Notfall.

Wird die BAO **gleichzeitig mit der angemessenen Absicherung der Geschäftsprozesse** aufgebaut und befähigt, ermöglicht dies ebenfalls eine schnelle allgemeine Reaktionsfähigkeit, während gleichzeitig eine allgemein schnellere Gesamtentwicklung des BCMS möglich ist. Dieses Vorgehen erfordert jedoch, dass das BCMS mit ausreichenden Ressourcen ausgestattet wurde, um beide Aspekte parallel bearbeiten zu können.

Wird die BAO **nach der angemessenen Absicherung der Geschäftsprozesse** aufgebaut und befähigt, können die in der Analysephase erhobenen Informationen dazu beitragen, die BAO sowie die begleitenden Maßnahmen gezielter auf die konkreten Anforderungen an die Notfallplanung auszurichten. Dies bedeutet jedoch auch, dass erst zu einem späteren Zeitpunkt eine allgemeine Reaktionsfähigkeit in einem Notfall vorhanden ist.

Zur Übersicht zeigt Abbildung 38, welche Aspekte der Notfallbewältigung jeweils vorbereitet werden.

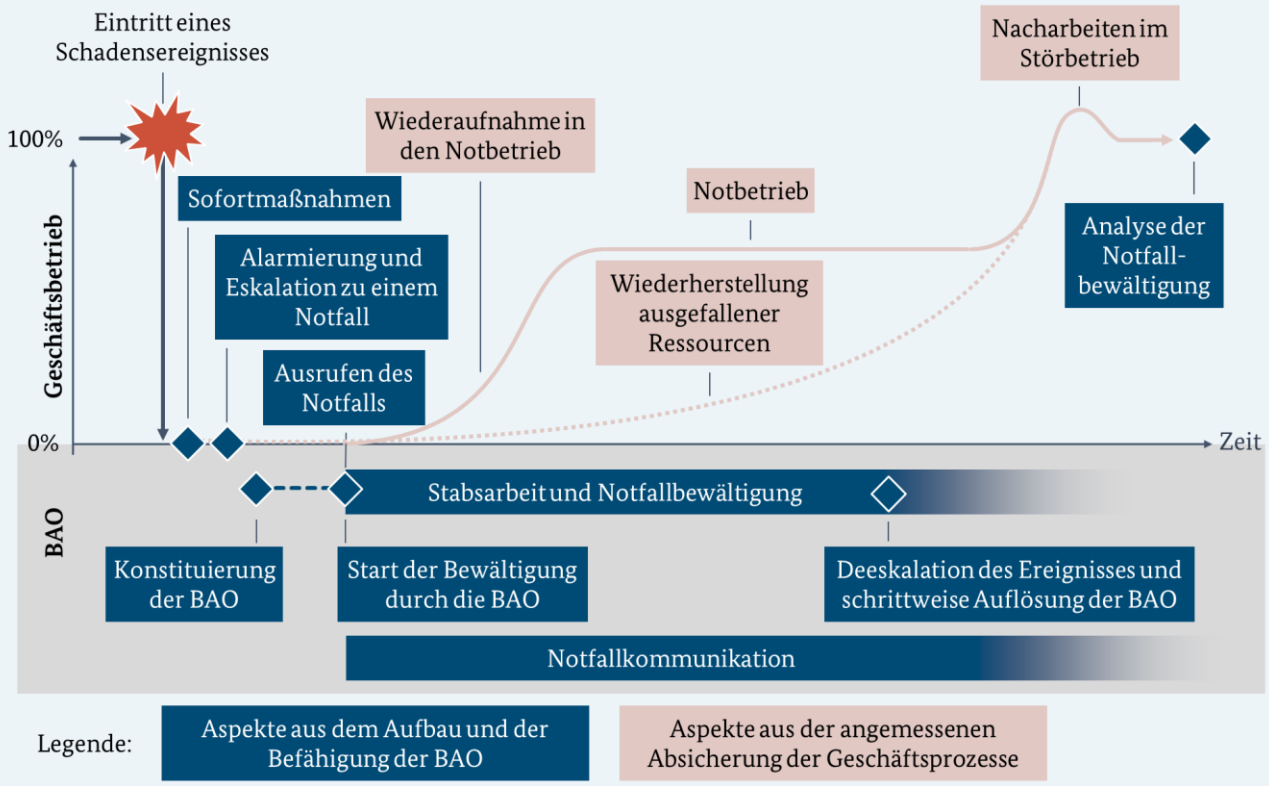

Abbildung 38: Vorbereitung der Notfallbewältigung

6.1 Analyse der erweiterten Rahmenbedingungen

Als erweiterte Rahmenbedingungen werden sämtliche internen und externen Anforderungen an die Institution sowie interne und externe Faktoren mit Bezug auf die Institution bezeichnet, die auch ihr BCMS beeinflussen können. Diese erweiterten Rahmenbedingungen werden im ISO-Standard 22301 auch als „Kontext der Organisation“ bezeichnet. Die nachfolgenden Kapitel beschreiben die empfohlene Vorgehensweise, mittels derer die erweiterten Rahmenbedingungen strukturiert identifiziert werden können. In Abbildung 39 sind die hierfür erforderlichen Schritte in einer Übersicht dargestellt.

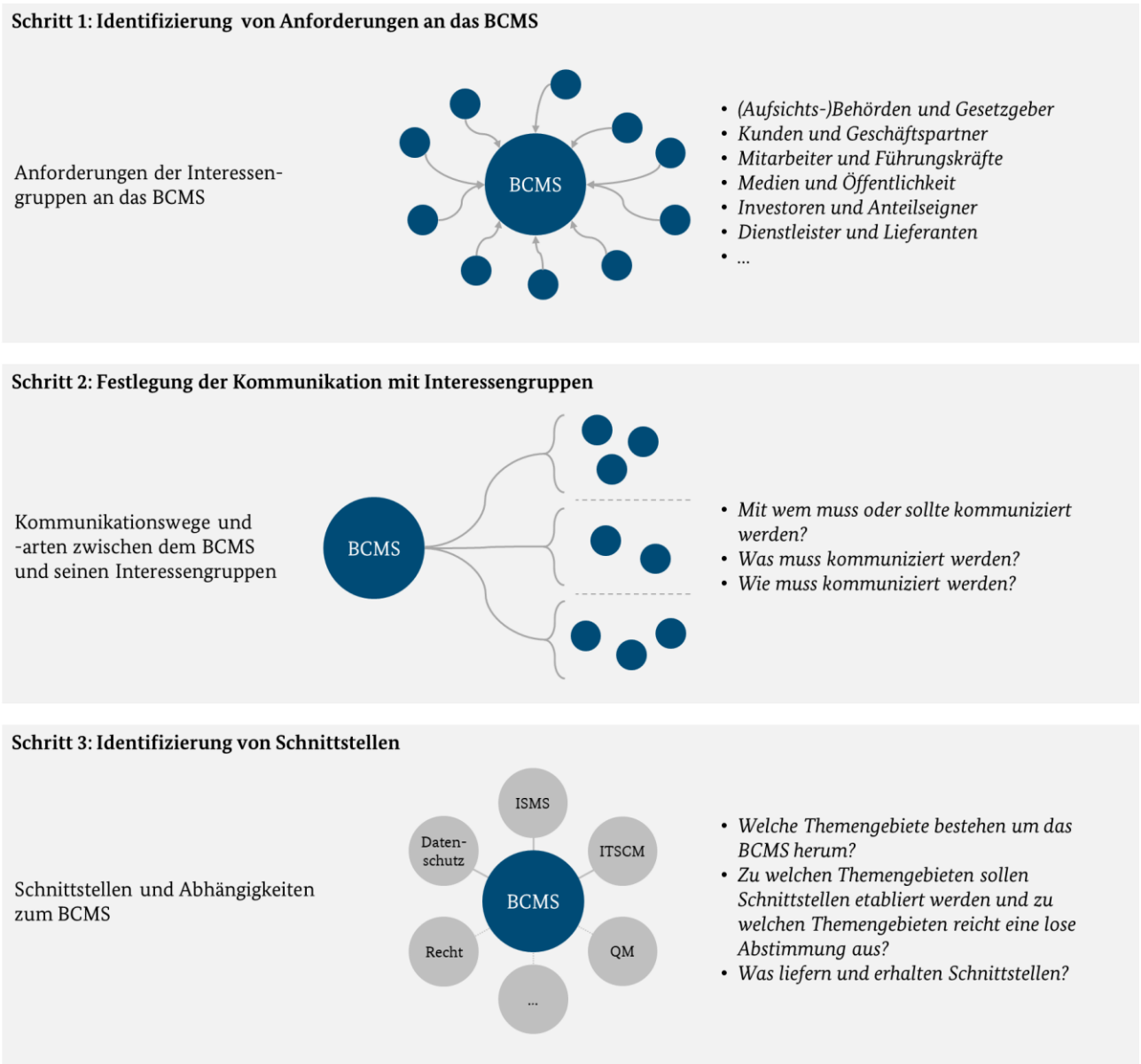

Abbildung 39: Erweiterte Rahmenbedingungen ermitteln

Synergiepotenzial:

Liegt bereits ein ISMS nach BSI-Standard 200-2 oder ISO-Standard 27001 vor, so kann geprüft werden, inwieweit die Interessengruppenanalyse für das BCM übernommen und weitergenutzt werden kann.

6.1.1 Identifizierung von Anforderungen an das BCMS

Für die weitere Planung des BCMS müssen die relevanten Interessengruppen im BCMS ermittelt werden, da diese die Rahmenbedingungen und Ziele des BCMS beeinflussen können. Einige Interessengruppen haben ausschließlich Informationsansprüche. Andere Interessengruppen, wie z. B. Kunden oder Aufsichtsbehörden, haben klare Erwartungen an das BCMS oder stellen spezifische Anforderungen. Damit diese Ansprüche und Erwartungen angemessen berücksichtigt werden können, müssen die Interessengruppen sowie deren Anforderungen ermittelt werden. Grundsätzlich kann zwischen internen und externen Interessengruppen unterschieden werden.

Als interne Interessengruppen werden beispielsweise die Institutionsleitung, der Betriebsrat, Mitarbeiter, Beauftragte anderer Managementsysteme (z. B. Informationssicherheitsbeauftragter) oder die vom BCM betroffenen Organisationseinheiten angesehen. Mutter- und Tochtergesellschaften, die sich aus Konzernstrukturen ergeben, werden in der Praxis ebenfalls den internen Interessengruppen zugeordnet.

Zu externen Interessengruppen zählen beispielsweise Anteilseigner, Fachaufsichten, Investoren, Kunden, Lieferanten, Geschäftspartner, Medien aber auch Versicherungen, Behörden, Branchenverbände, der Gesetzgeber oder die Öffentlichkeit.

Bedeutsam sind insbesondere diejenigen Interessengruppen,

- die rechtlichen und regulatorischen Anforderungen an die Institution stellen,
- auf deren Kooperation die Institution angewiesen ist,
- die einen hohen Einfluss auf das öffentliche Meinungsbild der eigenen Organisation haben sowie diejenigen,
- welche die Geschäftstätigkeit der Institution einschränken oder verbessern können.

Die Abbildung 40 zeigt Beispiele für verschiedene Interessengruppen.

Beispiel:

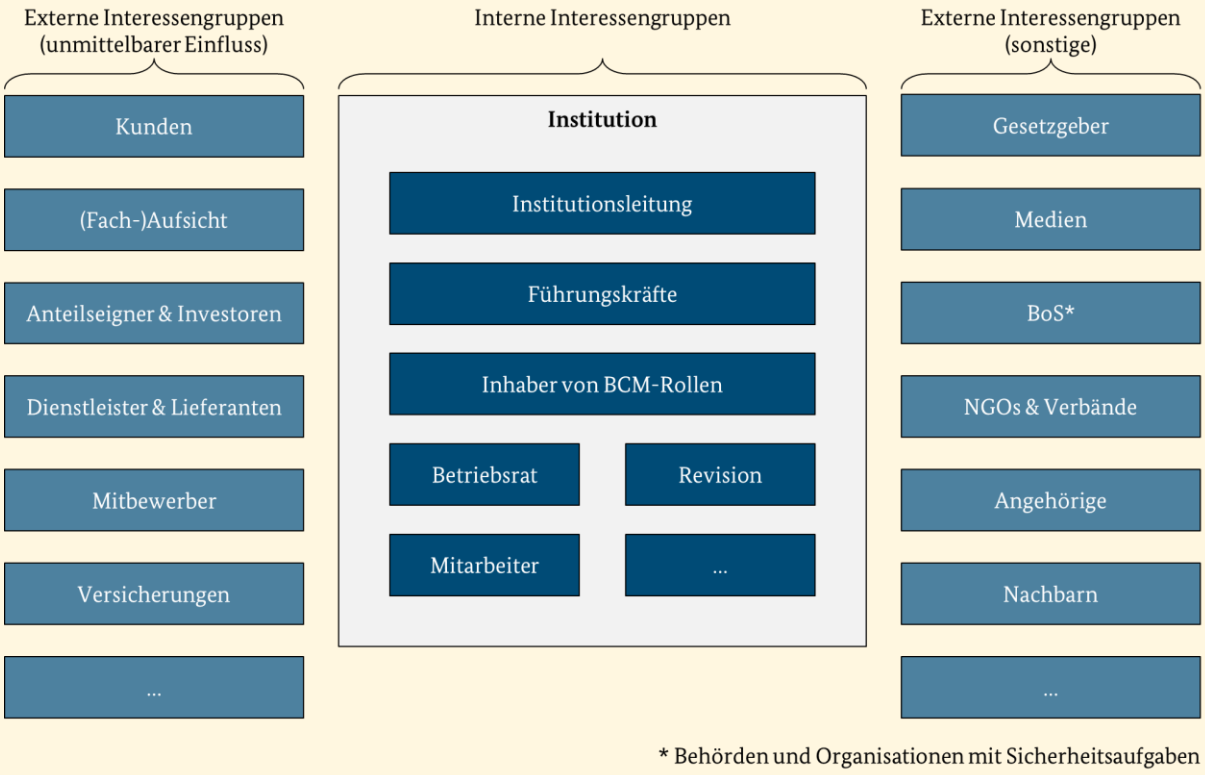

Abbildung 40: Beispiele für Interessengruppen

Die für das BCMS relevanten Interessengruppen und die Arten der Interessen können mittels einer *Interessengruppen-Analyse (engl.: Stakeholder Analysis)* ermittelt werden. Dabei handelt es sich um eine tabellarische Übersicht aller Interessengruppen, in der diese kategorisiert und hinsichtlich ihrer Erwartungen oder Anforderungen analysiert werden.

Eine wesentliche Quelle für die *Interessengruppen-Analyse* sind alle Informationen zu internen und externen Gründen für ein BCM, die im Prozess zur Initiierung des BCMS (siehe Kapitel 3.1.1.1 *Motivation für den Aufbau eines BCMS)* erhoben wurden. Zu diesen Gründen zählen z. B. die relevanten Gesetze und Verordnungen. Insbesondere für regulatorische, aber auch für alle anderen Anforderungen sollte dokumentiert werden, wo die notwendigen Informationen zu finden sind, wie etwa in einschlägigen Gesetzestexten, Rundschreiben von Aufsichtsbehörden etc. Während der Analyse ist es empfehlenswert, nicht nur die verbindlichen und formal vorliegenden Anforderungen zu ermitteln, sondern auch die implizit vorhandenen informellen Erwartungen.

Beispiel:

Eine formale Anforderung für eine Bank ergibt sich z. B. aus dem Rundschreiben 09/2017 (BA) - Mindestanforderungen an das Risikomanagement – MaRisk, AT 7.3: „Für Notfälle in zeitkritischen Aktivitäten und Prozessen ist Vorsorge zu treffen (Notfallkonzept)."

Eine formale Anforderung für einen Industriebetrieb ergibt sich z. B. aus der vertraglichen Anforderung einer Versicherung, geeignete Maßnahmen zu definieren, um Schäden fristgerecht zu melden.

Eine informelle Erwartung von Kunden an eine Institution ist z. B. die unterbrechungsfreie telefonische Erreichbarkeit innerhalb der normalen Geschäftszeiten, obwohl dies weder gesetzlich gefordert noch vertraglich vereinbart ist.

Die Steuerungs- und Kommunikationsaufwände, um mit Interessengruppen adressatengerecht zu kommunizieren, können von Gruppe zu Gruppe unterschiedlich sein. Erfahrungsgemäß steigen diese mit dem Grad, mit dem Interessengruppen auf das BCMS Einfluss nehmen. Daher ist es für die weitere Planung des BCMS empfehlenswert, den Grad der Einflussnahme pro Interessengruppe einzuschätzen, z. B. anhand der Kategorien niedrig, mittel und hoch. Interessengruppen mit hohem Einfluss sollten von der Institution besondere Aufmerksamkeit erhalten, während diejenigen mit niedrigem Einfluss nur im geringen Umfang berücksichtigt werden müssen.

Tabelle 33 und Tabelle 34 zeigen ein vereinfachtes Beispiel für eine Interessengruppen-Analyse. Der Grad der Einflussnahme der betrachteten Interessengruppen ist nicht repräsentativ. Sofern die nachstehende Vorgehensweise genutzt wird, muss die Institution den Grad der Einflussnahme selbstständig festlegen.

Beispiel:

Interne Interessengruppe	Erwartungen und Anforderungen	Grad der Einflussnahme
Institutionsleitung	• Schutz der Reputation • stabiler Geschäftsbetrieb • wirtschaftliche Planungssicherheit • Transparenz • Rechtskonformität (gesetzlich, regulatorisch, vertraglich) • Haftungsvermeidung • Vermeidung von Kosten durch Ausfälle oder Sanktionen • Wettbewerbsvorteil	Hoch
Führungskräfte	• Verminderung von Risiken • Erfüllung von geschäftlichen Anforderungen • Transparenz	Mittel

Interne Interessengruppe	Erwartungen und Anforderungen	Grad der Einflussnahme
Inhaber von BCM-Rollen	• Ausreichende Ressourcenausstattung (um das BCMS betreiben zu können) • Angemessenheit, Effektivität und Effizienz der Methoden des BCMS	Hoch
Revision	• Angemessenheit, Effektivität und Nachvollziehbarkeit des BCMS sowie der getroffenen Maßnahmen	Hoch
Mitarbeiter	• Absicherung des Arbeitgebers (wirtschaftlich, Reputation) • Sicherheit der eigenen Handlungen • Relevanz oder Bedeutung im Notfall	Mittel
Betriebsrat	• Schutz bzw. Durchsetzen von Mitarbeiter-Interessen bei personalrelevanten Entscheidungen • Sicherstellung und Aufrechterhaltung der Arbeitsplätze in und nach einem Notfall bzw. einer Krise	Hoch

Tabelle 33: Beispiele interner Interessengruppen

Externe Interessengruppe	Erwartungen und Anforderungen	Grad der Einflussnahme
Kunden	• Erfüllung von Verträgen bzw. Service Level Agreements • Sicherstellung der eigenen Arbeitsfähigkeit und Aufgabenerfüllung • Generierung eines eigenen Wettbewerbsvorteils • Sicherstellung der eigenen Konformität zu Richtlinien, Vorgaben sowie rechtlichen und regulatorischen Anforderung en	Mittel
Angehörige der Mitarbeiter	• Wirtschaftliche Absicherung • Schutz vor Gefahr für Leib und Leben der Mitarbeiter	Mittel
Behörden und Organisationen mit Sicherheitsaufgaben	• Sicherstellung von Gefahrenabwehr und von Hilfeleistungen • Aufrechterhaltung der öffentlichen Sicherheit und Ordnung	Hoch
Öffentlichkeit/Medien	• Interesse an sensationellen Meldungen • Berichterstattung über Meinungen, Missstände und menschliche Schicksale	Mittel
Versicherungen	• Risikominderung eines Schadensfalls • Nachweisbarkeit im Schadensfall	Mittel
Dienstleister und Lieferanten	• Vereinbarte Leistungsabnahme und Vergütung	Niedrig

Tabelle 34: Beispiele externer Interessengruppen

Hierzu ist es empfehlenswert, jeweils diejenigen Ansprechpartner einzubeziehen, die als Vertreter oder Kontakt einer Interessengruppe aussagefähig zu den Erwartungen und Anforderungen sind. Dies sind üblicherweise Ansprechpartner aus den OEs Kommunikation, Recht, Vertrieb, Dienstleistersteuerung, Betriebsrat oder Revision oder vergleichbaren.

Die Interessengruppen sowie deren Anforderungen und Erwartungen sollten möglichst immer aktuell gehalten werden, z. B. indem ein regelmäßiger Aktualisierungszyklus festgelegt wird. Sollten im weiteren Verlauf zur Planung und Umsetzung des BCMS weitere Interessengruppen oder Anforderungen bekannt werden oder sich grundsätzlich ändern, dann sollte die Tabelle überprüft und aktualisiert werden.

6.1.2 Festlegung der Kommunikation mit Interessengruppen

Der Umgang mit den Interessengruppen erfordert eine adressatengerechte Kommunikation. Nicht immer bestehen jedoch direkte Beziehungen vom BCM zu einer bestimmten Interessengruppe, wie z. B. zu den Anteilseignern eines Unternehmens oder zur Öffentlichkeit. Aus diesem Grund sollte anhand der identifizierten Interessengruppen abgeleitet werden, welchen Informationsanspruch diese besitzen. Zudem sollte in Bezug auf das BCM festgelegt werden,

- ob Kommunikation stattfinden soll oder darf,
- wer kommuniziert,
- welche Informationen weitergegeben werden,
- über welches Medium kommuniziert wird und
- wie häufig und zu welchen Zeitpunkten kommuniziert wird.

Beispiel:

Eine betrachtete Institution kommuniziert im Normalbetrieb Themen des BCM auf folgenden Wegen:

- Mitarbeiter werden im Rhythmus von zwei Monaten auf der Intranet-Seite über Neuigkeiten zum BCM informiert. Zudem erhalten sie Informationen direkt von Führungskräften sowie im Rahmen von Schulungen und Awareness-Maßnahmen.
- Ausgewählte Führungskräfte sind aktiv in Gremien eingebunden, in denen auch BCM-Themen besprochen werden. Darüber hinaus erhalten sie einen Quartalsbericht zu den Aktivitäten des BCM sowie zu aktuellen Risiken, Vorfällen und Trends.
- Die Institutionsleitung wird in einem BCM-Jahresbericht über den Status informiert.
- Kunden erhalten initial die Information, dass ein BCMS implementiert ist. Weitere Informationen erfolgen nur im Rahmen eines eingetretenen Notfalls.

Die Kommunikation mit Interessengruppen in einem Notfall wird in Kapitel 6.4.6.3 *Externe Kommunikation* näher beschrieben.

6.1.3 Identifizierung von Schnittstellen

Wie schon in Kapitel 1.2 *Zielsetzung* und Kapitel 2.4 *Abgrenzung und Synergien* angedeutet, kann das BCMS nicht als isoliertes, unabhängiges Managementsystem betrachtet werden. Vielmehr bestehen wechselseitige Abhängigkeiten zu angrenzenden Themenfeldern und Organisationseinheiten. Werden die Schnittstellen frühzeitig identifiziert, können die Qualität der Arbeitsergebnisse verbessert und doppelte Arbeiten vermieden werden. Weiterhin kann so Fehlern, wie z. B. inkonsistenten oder widersprüchlichen Aussagen, vorgebeugt werden.

Die Schnittstellen und Abhängigkeiten des BCM sind für jede Institution sehr individuell ausgeprägt. Der BSI-Standard 200-4 setzt daher keine konkreten Schnittstellen voraus, sondern stellt in diesem Kapitel allgemeine Beispiele für typische Schnittstellen vor, die in vielen Institutionen vorzufinden sind. Ergänzend dazu finden sich in den nachfolgenden Kapiteln weitere Hinweise auf mögliche Schnittstellen und Synergiepotenziale.

Das Beispiel in Abbildung 41 zeigt eine Auswahl an typischen Schnittstellen im Überblick.

Beispiel:

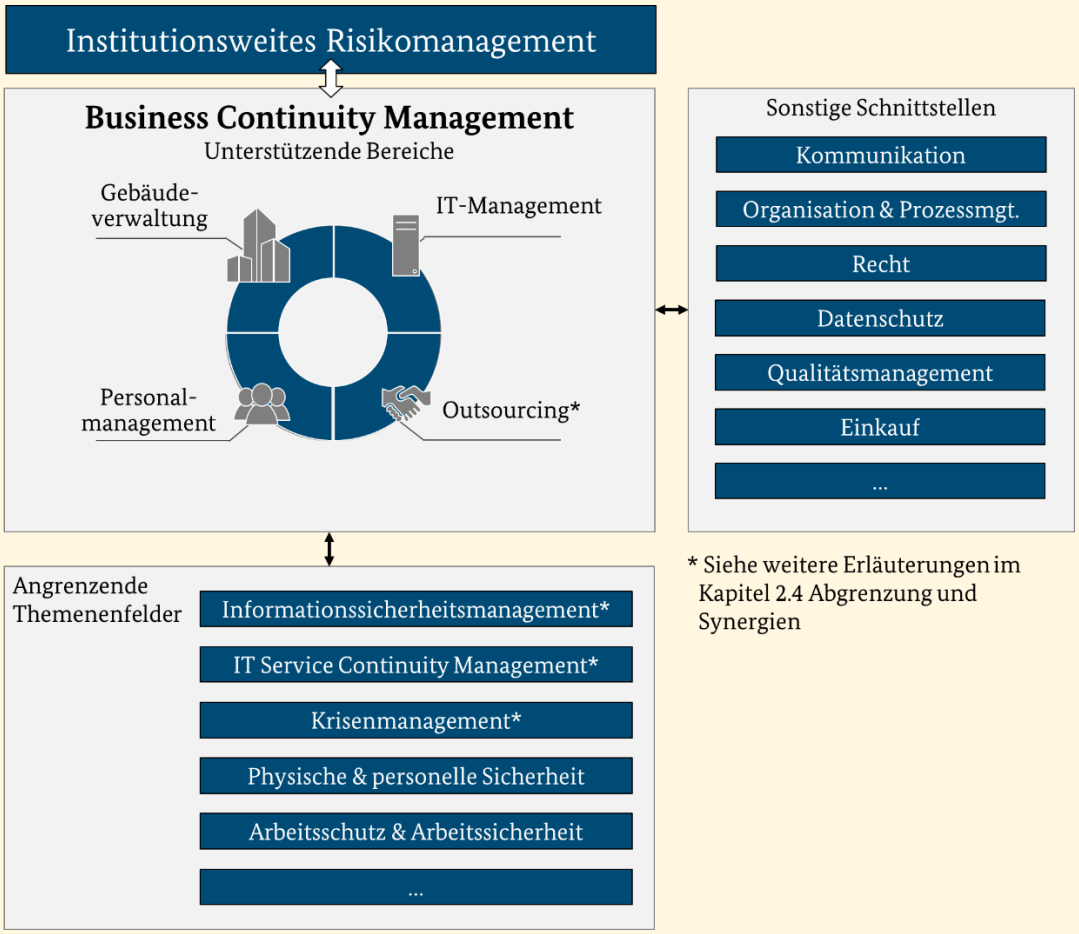

Abbildung 41: Übersicht über mögliche Schnittstellen eines BCMS

Alle für das BCMS relevanten Schnittstellen müssen ermittelt und dokumentiert werden. Als Ausgangsbasis können die Ergebnisse der *Interessengruppen-Analyse,* sowie die Hinweise aus Kapitel 2.4 *Abgrenzung und Synergien* verwendet werden. Für jede Schnittstelle des BCMS sollte festgelegt werden, welche gegenseitigen Informationen oder Leistungen ausgetauscht und welche der angewendeten Methoden und Verfahren aufeinander abgestimmt werden. Zudem sollten die Art und die Häufigkeit eines Austauschs sowie die abzustimmenden Aspekte festgelegt und dokumentiert werden. In der Praxis hat es sich bewährt, die Schnittstellen in Form von gemeinsamen Gremientreffen zu gestalten und sich so abzustimmen.

Hinweis:

Im Hinblick auf die erwarteten Aufwände und den Nutzen sollte abgewogen werden, in welcher Intensität eine Schnittstelle genutzt wird. Möglicherweise ist eines der Themenfelder aufgrund fehlender Ressourcen oder Kapazitäten nicht zu einer Zusammenarbeit bereit oder die Schnittstelle weist noch nicht den erforderlichen Reifegrad auf. Dann kann es auch von Vorteil für den Fortschritt im BCMS sein, wenn diese Schnittstelle zunächst nicht bedient wird.

Im Folgenden werden einige Beispiele für wechselseitige Abhängigkeiten und die damit zusammenhängenden Informationsaustausche bzw. die zu erbringenden Leistungen dargestellt. Die Abhängigkeiten in Bezug auf das Informationssicherheitsmanagement, ITSCM, Krisenmanagement und Outsourcing bzw. Lieferketten wurden bereits in Kapitel 2.4 *Abgrenzung und Synergien* ausführlich beschrieben. Diese werden daher an dieser Stelle nicht erneut wiederholt.

Risikomanagement

Mit dem Risikomanagement sollten vor allem die Vorgehensweisen zur Erhebung, Auswertung und Behandlung von Risiken abgestimmt werden. So können etwa die im Risikomanagement definierten Parameter (z. B. Risikokategorien, Akzeptanzkriterien) als Grundlage dienen, die zeitkritischen Geschäftsprozesse im Rahmen der Business Impact Analyse zu identifizieren.

Sowohl die Methode als auch die Parameter, wie die Risikokategorien und Akzeptanzkriterien des Risikomanagements sowie gegebenenfalls bereits vorhandene Ergebnisse können im Rahmen der BCM-Risikoanalyse verwendet werden. Darüber hinaus ist es möglich, die BCM-Risikoanalyse als Teil des Risikomanagements durchzuführen. Umgekehrt unterstützt das BCM das Risikomanagement, sobald risikomindernde Maßnahmen zur Notfallvorsorge und Notfallbewältigung entwickelt und umgesetzt werden.

Gebäudemanagement

Die Mitarbeiter des Gebäudemanagements unterstützen das BCM z. B. bei der Bewertung und Ausgestaltung von Maßnahmen zur physischen Sicherheit sowie zur Verfügbarkeit der Gebäude und Infrastruktur. Zudem setzt das Gebäudemanagement die definierten Maßnahmen um.

Im Notfall können Gebäudenotfallteams die unter Umständen erforderliche Räumung von Gebäuden durchführen. Auch können Sie den Wiederanlauf und den Notbetrieb unterstützen, indem sie etwa Ausweichstandorte und -arbeitsplätze vorbereiten.

Personalmanagement

Das BCM hat Auswirkungen auf jeden Mitarbeiter. Die Personalabteilung sollte bei allen Entscheidungen und Maßnahmen im Kontext BCM involviert werden, die wesentlichen Einfluss auf die Rechte und Pflichten der Mitarbeiter haben. Das Personalmanagement kann bei der Planung von Schulungen und Awareness-Maßnahmen unterstützen, damit das BCM ein Teil der „Kultur“ der Institution wird.

Organisation und Prozessmanagement

Die Organisationsabteilung ist zum einen dafür zuständig, dass Richtlinien und Anweisungen einheitlich gestaltet und gepflegt werden. Dies betrifft auch die Dokumentation des BCMS. Zum anderen werden dort in der Regel die Geschäftsprozesse der Institution modelliert und aktualisiert. Diese Informationen über die Geschäftsprozesse werden in der Regel vom BCM in der BIA als Bewertungsgrundlage genutzt.

Kommunikation und Öffentlichkeitsarbeit

Die Kommunikationsabteilung dient als Sprachrohr zu allen internen und externen Interessengruppen. Insbesondere in einem Notfall oder einer Krise ist die interne und externe Kommunikation von zentraler Bedeutung. Die Mitarbeiter müssen in einer Notfallsituation informiert und geführt werden. Zugleich müssen die externen Interessengruppen betreut werden, um nachhaltige Reputationsschäden zu verhindern. Daher ist eine enge Zusammenarbeit mit der Kommunikationsabteilung von großer Bedeutung für das BCM. Für die Kommunikation im Normalbetrieb ist es hilfreich, sich der Methoden der OE Kommunikation und Öffentlichkeitsarbeit zu bedienen.

Recht

Die Rechtsabteilung bearbeitet alle rechtlichen Fragestellungen der Institution. Dies beinhaltet alle wesentlichen gesetzlichen und regulatorischen Anforderungen an das BCM der Institution. Der Umgang mit diesen Anforderungen sollte zwischen BCM und Rechtsabteilung abgestimmt und regelmäßig aktualisiert werden.

Datenschutz

Der Datenschutz regelt, wie personenbezogene Daten in einer Institution erhoben, gespeichert, verarbeitet und weitergegeben werden dürfen. Die Anforderungen des Datenschutzes müssen auch im Notbetrieb eingehalten werden. Die Abstimmung im Notfall ist daher bedeutsam.

BCMS und Datenschutz können auch zusammenarbeiten, um gemeinsam technisch-organisatorische Maßnahmen des Datenschutzes zu definieren, umzusetzen und zu prüfen. Zusätzlich können weitere Synergien geschaffen werden, indem Ressourcen oder Anforderungen an Ressourcen gemeinsam erhoben und gepflegt werden.

Qualitätsmanagement

Das Qualitätsmanagement entwickelt Anforderungen, um die Effektivität und Effizienz der Geschäftsprozesse einer Institution systematisch zu verbessern. Hierunter fallen somit auch die Prozesse des BCMS.

Das Qualitätsmanagement erstellt häufig Vorgaben für die einzelnen Themenfelder oder stellt Hilfsmittel für diese bereit. Vorgaben des Qualitätsmanagements z. B. an die Dokumentation, die Leistungsüberprüfung oder die Korrektur und Verbesserung, sollten vom BCM berücksichtigt werden.

Auch gibt es im Qualitätsmanagement häufig dokumentierte Geschäftsprozesse oder Ressourcenlisten, auf die das BCMS im Rahmen der Business Impact Analyse zurückgreifen kann.

Einkauf und Outsourcing

Der Einkauf ist dafür zuständig, die Institution mit notwendigen Gütern und Dienstleistungen zu versorgen. Werden in diesem Rahmen Dienstleister eingebunden (Outsourcing bzw. Lieferkette), sollten neben den betriebswirtschaftlichen Aspekten ergänzende Anforderungen des BCM an den Einkaufsprozess gestellt werden. (siehe Kapitel 7 *BCM im Rahmen des Outsourcings und von Lieferketten*).

6.2 Dokumentation im Standard-BCMS

Eine angemessene Dokumentation ermöglicht es, getroffene Entscheidungen nachzuvollziehen, Handlungen zu wiederholen sowie Managementsysteme zu überprüfen und zu zertifizieren (siehe Kapitel 3.2.3 *Dokumentation*). Zusätzlich können Korrekturbedarfe und Verbesserungsmöglichkeiten besser nachverfolgt werden. Im BCMS stellt die Dokumentation ferner sicher, dass den berechtigten Interessengruppen der Zugang zu relevanten Informationen möglich ist. Um diesen Ansprüchen gerecht zu werden, bedarf es im Standard-BCMS einer Dokumentenlenkung. Die Dokumentenlenkung beinhaltet Vorgaben, wie die Dokumente gestaltet, überarbeitet und freigegeben werden, sodass die enthaltenen Informationen verfügbar, aktuell und in angemessener Qualität vorliegen.

Synergiepotential:

Die Dokumentenlenkung ist üblicherweise als Bestandteil des Qualitätsmanagementsystems definiert. Sofern ein Qualitätsmanagementsystem z. B. nach ISO 9001 betrieben wird, können die Vorgaben aus diesem Standard mit den institutionsspezifisch geltenden Anforderungen abgestimmt werden. Alternativ kann auf die Regelungen zur Dokumentenlenkung gemäß BSI-Standard 200-2 zurückgegriffen werden.

Die Abbildung 42 gibt einen Überblick über die Dokumentation im Standard-BCMS.

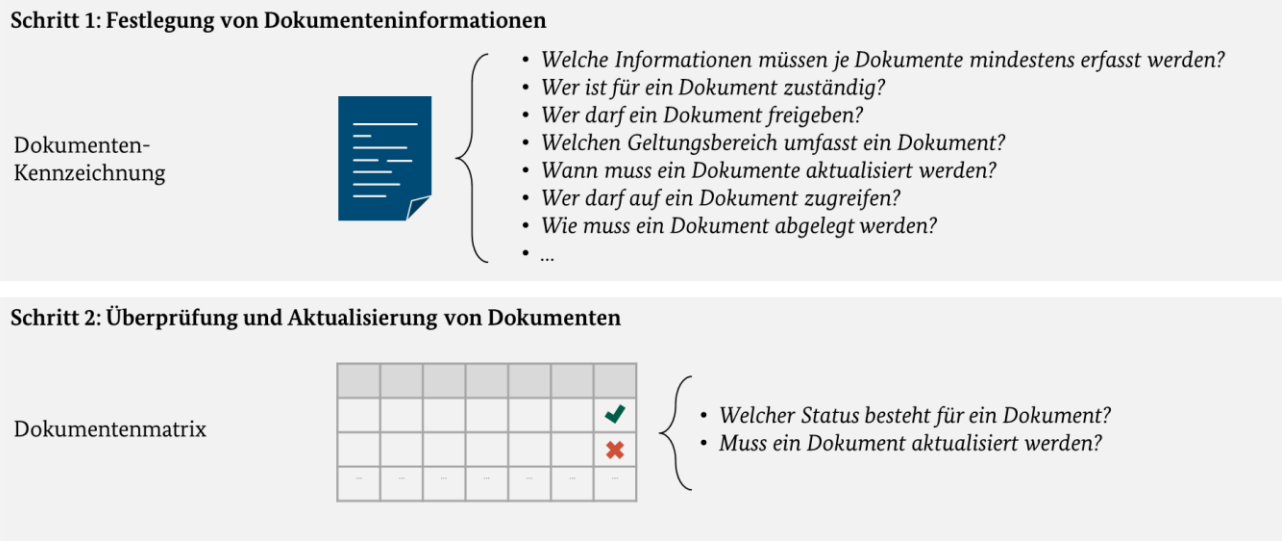

Abbildung 42: BCM-Prozessschritte zur Dokumentation im Standard-BCMS

6.2.1 Festlegung von Dokumenteninformationen

Die verschiedenen Inhalte und Vorgaben an die Dokumentation des BCMS werden oft auf verschiedene Einzeldokumente verteilt, um Informationen gezielt steuern, aufbereiten und hierarchisch einordnen zu können. Vorgaben aus übergeordneten Dokumenten müssen dann bindenden Charakter für untergeordnete Dokumente besitzen. Im Gegenzug müssen die konkretisierenden Inhalte der untergeordneten Dokumente konform zu den übergeordneten Vorgaben aufgebaut werden.

Die Anzahl und jeweilige Ausprägung der Dokumente ist abhängig von der Größe und Komplexität der Institution, den zu berücksichtigenden Interessengruppen sowie institutionsspezifischen Vorgaben. Die Dokumentenpyramide aus Kapitel 3.2.3 *Dokumentation* sowie die darin beschriebenen Klammerdokumente Notfallvorsorgekonzept und Notfallhandbuch können hierfür zur Orientierung genutzt werden.

Um Dokumente gezielt zuordnen und nachhalten zu können, sollten diese zudem eindeutig gekennzeichnet werden. Eindeutig gekennzeichnete Dokumente geben den Lesern zudem einen schnellen Überblick darüber, was in den Dokumenten geregelt wird, wie mit den Dokumenten umgegangen werden muss und wer zuständig für den Inhalt der Dokumente ist. Die wesentlichen Inhalte, die für jedes Dokument berücksichtigt werden sollten, werden im folgenden Beispiel veranschaulicht und im Anschluss näher erläutert.

Hinweis

Jedes Dokument muss hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität angemessen geschützt werden. Hierzu sollte in jedem Dokument selbst der Schutzbedarf dokumentiert werden (siehe Kapitel 3.2.3 *Dokumentation*). Insbesondere innerhalb der reaktiven Notfalldokumentation werden oftmals interne oder vertrauliche Informationen dokumentiert. Für diese Dokumente sollte die Zielgruppe auf wenige bestimmte Personen begrenzt werden.

Weitere Informationen zur Klassifizierung von Informationen können dem BSI-Standard 200-2, Kapitel 5.1 entnommen werden.

Beispiel:

Kennzeichnung	Erläuterung
Titel	BCM-Leitlinie
Dokumentenart	Leitlinie
Version	1.0
Autor	Frauke Musterfrau (BCMB)
Freigabedatum und -person	31.07. durch Erika Mustermann (Institutionsleitung)
Datum der nächsten geplanten Überarbeitung	31.07. (jährliche Überprüfung)
Geltungsbereich des Dokuments	Gesamter BCM-Geltungsbereich
Klassifizierung	Intern
Zielgruppe	Mitarbeiter im Geltungsbereich sowie Externe mit begründetem Interesse
Ablage	https://intranet.institution.de/BCM/Leitlinie
Aufbewahrungszeitraum	10 Jahre (interne Anforderung)
Änderungshistorie	05.06.: Erster Entwurf, 07.07.: Anpassung der Ziele

Tabelle 35: Beispielkennzeichnung eines Dokuments

Dokumente sollten mindestens mit nachfolgenden Eigenschaften gekennzeichnet werden:

- Titel
- Eindeutige Versionsnummer
- Dokumentenart (siehe hierzu auch Abbildung 13)
- Autor
- Freigabedatum und –Person
- Datum der nächsten geplanten Überarbeitung (für Dokumente, die regelmäßig aktualisiert werden)
- Geltungsbereich des Dokuments (sofern für die Dokumentenart erforderlich)
- Klassifizierung
- Zielgruppe
- Ablage
- Aufbewahrungszeitraum (falls erforderlich)
- Änderungshistorie

Darüber hinaus kann es sinnvoll sein, die Funktion des Autors oder der zuständigen Person zu dokumentieren.

6.2.2 Überprüfung und Aktualisierung von Dokumenten

Es muss sichergestellt werden, dass die Dokumente des BCMS die geforderten Dokumenteigenschaften umfassen sowie aktuell und den jeweiligen Zielgruppen zugänglich sind. Auch muss überprüft werden, dass die Informationen in untergeordneten Dokumenten den Regelungen übergeordneter Dokumente nicht widersprechen. Daher müssen die Überprüfung und Aktualisierung von Dokumenten zentral gesteuert werden.

Daher sollte für zentrale Dokumente des BCM der BCMB selbst zuständig sein. Er betreut etwa die übergreifenden Aspekte des Notfallvorsorgekonzepts, wie z. B. das Übungshandbuch sowie Anweisungen. Im Notfallhandbuch umfassen die zentralen Aspekte beispielsweise die Alarmierung und Eskalation. Der BCMB ist erfahrungsgemäß am besten mit den zentralen BCM-Prozessen vertraut und sollte daher die dort dokumentierten Inhalte steuern. Für dezentrale Dokumente und Inhalte, wie beispielsweise Geschäftsfortführungs-, Wiederanlauf- und Wiederherstellungspläne ist es empfehlenswert, dass der BCMB die Aufgaben und Zuständigkeiten an die BCMK oder den jeweiligen Zuständigen überträgt. Diese verfügen in der Regel über das detaillierte Fachwissen, das für diese Dokumente relevant ist. Sofern weitere Autoren oder zuständige Personen erforderlich sind, werden diese in den jeweiligen Kapiteln dieses Standards definiert.

Im Rahmen der stetigen Leistungsüberprüfung muss festgestellt werden, ob die Dokumente entsprechend ihres Aktualisierungszyklus von den jeweiligen Zuständigen geprüft und, wenn notwendig, aktualisiert wurden (siehe Kapitel 6.12 *Leistungsüberprüfung und Berichterstattung*). Insbesondere muss überprüft werden, ob veraltete Dokumente durch neue Versionen an allen Ablageorten ersetzt wurden. So wird sichergestellt, dass veraltete Versionen nicht weiter genutzt werden, sondern ausschließlich die jeweils aktuellste Fassung.

Hinweis:

Für den überwiegenden Teil der Dokumente hat sich eine Überprüfung nach jedem durchlaufenen Zyklus des BCM-Prozesses bewährt. Für reaktive Dokumente empfiehlt es sich unter Umständen, kürzere Überprüfungszyklen festzulegen. Dies gilt insbesondere für solche Dokumente, in denen Angaben zu Personen, Kontaktinformationen oder sich schnell ändernden Verfahren enthalten sind. Weiterhin können geänderte Rahmenbedingungen, Geschäftsziele, Aufgaben oder Strategien der Institution dazu führen, dass Dokumente abweichend vom Aktualisierungszyklus überprüft werden müssen.

Es muss sichergestellt werden, dass relevante Änderungen identifiziert und die betroffenen Dokumente zeitnah aktualisiert werden. Hierzu kann etwa mit den jeweiligen Ansprechpartnern ein Meldeprozess etabliert werden.

Beispiel:

Der BCMB hat mit der Rechtsverwaltung vereinbart, dass er informiert wird, wenn sich gesetzliche oder regulatorische Anforderungen ändern, denen die Institution unterliegt. Bei entsprechenden Änderungen kann der BCMB dann die Ziele und Ausrichtung des BCMS überprüfen und korrigieren, sofern dies erforderlich ist.

Um eine bessere Übersicht der Dokumente zu erhalten und diese leichter steuern zu können, kann der BCMB eine Dokumentenmatrix erstellen. Die Dokumentenmatrix ist eine Übersicht, in der die einzelnen Dokumente mit den notwendigen Informationen der Dokumentenlenkung aufgeführt werden.

Tabelle 36 zeigt beispielhaft auf, wie eine Dokumentenmatrix aufgebaut werden kann. Die dargestellten Informationen zur Dokumentenlenkung werden typischerweise auch in Dokumentenmanagementsystemen angewendet (siehe Kapitel Hilfsmittel *Tools*).

Beispiel:

Dokument	Klassifizierung	Erstellt durch	Freigabe durch	Version	Aktualisiert am
Leitlinie	Intern	BCMB	Institutionsleitung	5.0	31.07.2020
GFP (OE Einkauf)	Vertraulich	BCMK OE Einkauf	Leiter OE Einkauf)	3.2	30.10.2020
WAP (E-Mail Server)	Vertraulich	Ressourcenverantwortlicher Serverbetrieb	Leiter IT	4.0	19.11.2020

Tabelle 36: Beispiel einer Dokumentenmatrix

6.3 Leitlinie

Die Leitlinie bildet den verbindlichen Rahmen und Auftrag zum Aufbau und Betrieb des BCMS. Sie ist das ranghöchste Dokument im gesamten BCMS und führt auf strategischer Ebene die Ziele des BCMS auf. Durch die Leitlinie fixiert die Institutionsleitung ihre Selbstverpflichtung zur Einführung des BCMS und betont damit den Stellenwert des BCM innerhalb der Institution. Die Leitlinie kann anhand der Dokumentenvorlage *Leitlinie* aus den Hilfsmitteln erstellt werden. Diese beinhaltet bereits mögliche Textbausteine als Vorschläge.

Synergiepotenzial

Sofern bereits Managementsysteme, wie beispielsweise ein ISMS nach BSI-Standard 200-2, mittels einer Leitlinie in der Organisation fixiert wurden, kann der Aufbau dieser Leitlinien als Vorlage genutzt werden.

6.3.1 Erstellung der Leitlinie

Die Leitlinie hat drei wesentliche Funktionen:

1. Sie dient als dokumentierte Absichtserklärung der Institutionsleitung, ein BCMS aufbauen, betreiben und kontinuierlich verbessern zu wollen.
2. Sie dient dazu, die wesentlichen Rahmenbedingungen festzulegen, unter denen ein BCMS etabliert und betrieben werden soll.
3. Sie dient als verbindlicher Auftrag an alle Mitarbeiter daran mitzuwirken, das BCMS zu etablieren, aufzubauen und kontinuierlich weiterzuentwickeln und somit die Institution gegenüber Schadensereignissen selbst und deren Auswirkungen resilienter zu machen.

Hinweis:

Je detaillierter die Leitlinie auf konkrete Inhalte des BCMS eingeht, desto höher wird der Pflege- und Aktualisierungsaufwand. So müssten bereits kleine Veränderungen im weiteren Aufbau des BCMS in der Leitlinie angepasst werden. Um die Leitlinie konsistent zu halten, ist es daher empfehlenswert, einen geringen Detaillierungsgrad zu wählen und lediglich „Leitplanken“ zu beschreiben, innerhalb derer das BCMS aufgebaut und betrieben werden kann.

Aufgrund ihres Stellenwertes im BCM sowie ihrer weitreichenden Wahrnehmung in der Institution ist die Leitlinie auch eine Sensibilisierungsmaßnahme zur Schaffung einer BCM-Kultur in der Institution. Die Leitlinie sollte zu diesem Zweck leicht verständlich und präzise formuliert sowie übersichtlich gestaltet werden.

In der Leitlinie müssen mindestens die folgenden Inhalte und Entscheidungen aus der Initiierung des BCMS beschrieben werden (siehe Kapitel 3.1 *Initiierung des BCMS durch die Institutionsleitung*):

- Motivation für den Aufbau des BCMS (siehe Kapitel 3.1.1.1 *Motivation für den Aufbau eines BCMS*)
- Abzusichernder Zeitraum durch ein BCM (siehe Kapitel 3.1.1.2 *Abzusichernder Zeitraum durch ein BCM*)
- Geltungsbereich des BCMS (siehe Kapitel 3.1.2 *Geltungsbereich*)
- Übernahme der Gesamtverantwortung der Institutionsleitung (siehe Kapitel 3.1.4 *Übernahme der Verantwortung durch die Leitungsebene*)
- institutionsspezifische Definition des Begriffs BCM und der Eskalationsstufen Störung, Notfall und Krise (siehe Kapitel 3.2.1 *Definition und Abgrenzung*)
- zentrale Rollen im BCMS (ohne Besetzung) (siehe Kapitel 3.2.2 *Definition der BCM-Aufbauorganisation*),
- Ressourcenbereitstellung (siehe Kapitel 3.2.4 *Ressourcenplanung*)
- rechtliche und regulatorische Anforderungen und relevante Anforderungen von identifizieren Interessengruppen (siehe Kapitel 6.1.1 *Identifizierung von Anforderungen an das BCMS*).

6.3.2 Veröffentlichung und Aktualisierung der Leitlinie

Die Institutionsleitung muss die Leitlinie inhaltlich prüfen, freigeben und gegenüber allen Mitarbeitern bekannt geben. Um ein Bewusstsein für das BCM bei den Mitarbeitern zu schaffen und eine BCM-Kultur in der gesamten Institution zu etablieren, ist es wichtig, dass alle Mitarbeiter die Leitlinie kennen. Daher sollten auch neue Mitarbeiter auf die Leitlinie hingewiesen werden.

Darüber hinaus sollte die Institution prüfen, ob neben den Mitarbeitern auch weitere Gruppen die Leitlinie zur Kenntnis nehmen sollen, wie z. B. Kunden, zeitkritische Dienstleister oder anderweitige Geschäftspartner.

Falls sich wesentliche Rahmenbedingungen, Geschäftsziele, Aufgaben und Strategien der Institution verändern, muss die Leitlinie anlassbezogen aktualisiert werden. Dafür müssen die wesentlichen Änderungen identifiziert, die Auswirkungen der Änderung für das BCMS bewertet und die Leitlinie entsprechend angepasst werden. Im Anschluss sollte die Leitlinie durch die Institutionsleitung erneut freigegeben werden.

6.4 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 nachfolgend beschriebenen Maßnahmen plant und umsetzt.

Hinweis:

Grundsätzlich werden Institutionen in die Lage versetzt, alle Arten von Notfällen oder Krisen zumindest rudimentär zu bewältigen, wenn sie die Inhalte dieses Kapitels umsetzen. Wenn die Bewältigungsorganisation aufgebaut ist, 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 hilfreich.

Falls die Bewältigungsorganisation zuerst aufgebaut wird und die Geschäftsprozesse noch nicht angemessen abgesichert wurden, sind bei einem Schadensereignis Ad-hoc-Lösungen erforderlich. Entsprechend der De-

finition 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.

Die in Abbildung 37 aufgezeigten Aspekte zum Aufbau und zur Befähigung der BAO werden in den folgenden Unterkapiteln aufgegriffen. Diese überlagern sich zeitlich oder stehen in Wechselwirkung zueinander. In der Praxis bildet z. B. häufig oft der Aufbau der BAO sowie die Geschäftsordnung des Stabes die Grundlage für die Schulungen, Trainings und Übungen. Erkenntnisse aus durchgeführten Schulungen und Trainings führen wiederum zu Anpassungen der BAO, der Geschäftsordnung oder anderen Aspekten der Stabsarbeit.

Zudem stellen die beschriebenen Aspekte nur einen von vielen möglichen Pfaden dar. Einige weitere mögliche Umsetzungsformen und Aspekte der Bewältigung können dem Hilfsmittel *Weiterführende Aspekte zur Bewältigung* entnommen werden.

Alle beschriebenen Maßnahmen sollten spezifisch auf die Institution angepasst werden und in einem Notfallhandbuch (siehe Kapitel 3.2.3 *Dokumentation*) dokumentiert werden. Das Notfallhandbuch kann anhand der Dokumentenvorlage *Notfallhandbuch* aus den Hilfsmitteln erstellt werden.

Hinweis:

In der Regel gibt die Institutionsleitung im Not- und Krisenfall bestimmte Entscheidungs- und Handlungsvollmachten an die BAO ab, wie in den nachfolgenden Kapiteln erläutert wird. Daher ist es von besonderer Bedeutung, dass sie in der Vorbereitung in allen Punkten eingebunden ist und die beschlossenen Regelungen und Maßnahmen freigibt.

6.4.1 Aufbau der BAO

In einer Allgemeinen Aufbauorganisation (AAO) sind Abstimmungswege häufig komplex, wodurch kurzfristige Entscheidungen in Notfällen und Krisen oftmals nicht zeitgerecht getroffen werden können. Eine zielgerichtete und rasche Bewältigung erfordert daher eine besondere Aufbauorganisation (BAO).

Beispiel:

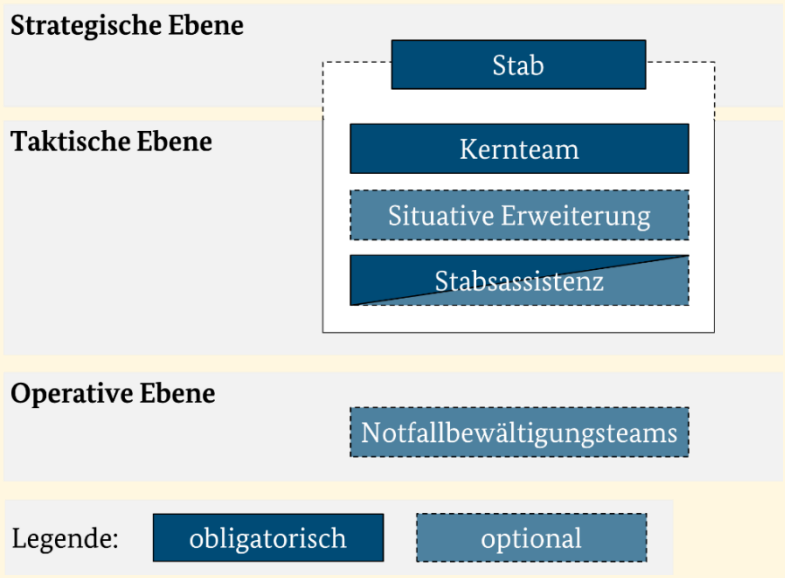

Abbildung 43: Beispiel verschiedener Rollen in einer BAO

Abbildung 45 erläutert ein Beispiel verschiedener Rollen einer BAO in den drei Ebenen strategisch, taktisch und operativ, wie sie im Rahmen dieses Standards definiert sind:

- Die **Strategische Ebene** legt die Ziele und Prioritäten in der Bewältigung fest.
- Die **Taktische Ebene** analysiert die Lage, beschließt dahingehend Maßnahmen und überwacht, ob diese umgesetzt wurden und wirksam sind.
- Die **Operative Ebene** setzt die beschlossenen Maßnahmen um und meldet den Erfolg oder die Wirkung der umgesetzten Maßnahmen an die taktische Ebene.

Hinweis:

In anderen Standards, z. B. zur öffentlichen Gefahrenabwehr, haben die Ebenen eine andere Bedeutung. Daher sollte im Zusammenspiel mit anderen Stäben stets geprüft werden, wie diese Begriffe belegt sind, falls sie benutzt werden.

Die BAO hat zum Ziel, komplexe Notfall- und Krisensituationen koordiniert zu bearbeiten und dabei alle relevanten Schnittstellen geeignet zu bedienen. Üblicherweise wird die BAO durch einen Stab geleitet, der komplexe Situationen beurteilen und geeignete Maßnahmen ableiten kann. Dieser agiert außerhalb der in der Alltagsorganisation etablierten Organisationsform, z. B. Linien- oder Matrixorganisation. Dadurch kann sichergestellt werden, dass komplexe und damit langwierige Entscheidungs- und Abstimmungswege vermieden werden, wie sie in der Praxis häufig in der AAO vorkommen. Der Stab hat dabei innerhalb eines vorher festgelegten Rahmens Entscheidungsgewalt (siehe Kapitel 6.4.4 *Definition der Geschäftsordnung des Stabs*).

Analog zur Definition der BCM-Aufbauorganisation (siehe Kapitel 3.2.2 *Definition der BCM-Aufbauorganisation*) müssen die Aufgaben, Rechte und Pflichten für alle Rollen der BAO im Vorfeld festgelegt werden. Für jede definierte Rolle der BAO kann der BCMB eine Besetzung vorschlagen. Für jedes Stabsmitglied muss mindestens ein Stellvertreter vorgesehen werden, da der Stab ad hoc und bei Bedarf über einen längeren Zeitraum handlungsfähig sein muss.

6.4.1.1 Aufbau des Stabs

Die Institution sollte in der BAO einen Stab als zentrales Führungsgremium der Bewältigung definieren. Der Stab lenkt, koordiniert und unterstützt die Bewältigung. Ferner sollte er an die relevanten Parteien zum Fortschritt der Notfallbewältigung kommunizieren

Hinweis:

Verschiedene Notfall- oder Krisenstabsmodelle werden in dem Hilfsmittel *Weiterführende Aspekte zur Bewältigung* erläutert. Um der Institution offenzulassen, mit welchem Gremium sie die Bewältigung sicherstellt, wird nachfolgend bewusst nur vom Stab gesprochen. Das Kapitel fokussiert entsprechend, welche Kriterien ein Stab grundsätzlich erfüllen soll.

Die Zuständigkeit für strategische Entscheidungen verbleibt auch in Notfällen bei der Institutionsleitung. Der Stab unterstützt die Institutionsleitung, indem er Lösungen entwickelt und alle Tätigkeiten hierzu koordiniert. Ziel des Stabes ist es,

- zu gewährleisten, dass zeitkritische Geschäftstätigkeiten schnellstmöglich wiederaufgenommen werden,
- weitere Auswirkungen des Schadensereignisses von der Institution abzuwenden sowie
- eine effektive und effiziente Zusammenarbeit sowie Kommunikation zwischen allen betroffenen Organisationseinheiten, der Institutionsleitung sowie Einsatzkräften, Behörden, Medien und anderen Parteien zu gewährleisten.

In diesem Zusammenhang sollte die Institutionsleitung dem Stab Entscheidungsbefugnisse übertragen. Ferner ist es empfehlenswert, dem Stab zusätzlich Finanzbefugnisse zu erteilen. Der Stab kann daher je nach Ausprägung auf der strategisch-taktischen oder nur auf der taktischen Ebene agieren.

Es ist empfehlenswert, dass der BCMB einen ersten Vorschlag für die allgemeinen Aufgaben des Stabes erstellt. Dieser sollte in der Geschäftsordnung konkretisiert werden (siehe Kapitel 6.4.4 *Definition der Geschäftsordnung des Stabs)*. Der Vorschlag kann sich an folgender Liste orientieren:

- Lage feststellen, beurteilen und fortschreiben
- einzuleitende Maßnahmen abstimmen und darüber entscheiden
- Arbeitsaufträge an unterstützende Einheiten, z. B. Notfallbewältigungsteams, erteilen (Aufgabenmanagement)
- umgesetzte Maßnahmen auf deren Wirksamkeit überprüfen und, falls erforderlich, korrigierende Maßnahmen einleiten
- interne und externe Notfallkommunikation sowie Öffentlichkeitsarbeit (z. B. Pressestelle) steuern
- an die Institutionsleitung oder andere Zuständige eskalieren, falls die Situation die Grenzen der eigenen Zuständigkeit übersteigt

Es gibt verschiedene Möglichkeiten, wie sich Stäbe personell und funktionell zusammensetzen können. Um die in den folgenden Kapiteln aufgeführten Aufgaben der Stabsarbeit sinnvoll Personen zuordnen zu können, sollte der Stab mindestens aus einem **Kernteam** bestehen. Das Kernteam besteht jeweils aus verschiedenen Rollen, die bestimmte Aufgaben und Zuständigkeiten in der Stabsarbeit innehaben. Das Kernteam sollte lageabhängig weitere Rollen als **situative Erweiterung** hinzuziehen. Um den Stab zu unterstützen, sollte zusätzlich eine **Stabsassistenz** vorgesehen werden.

Beispiel:

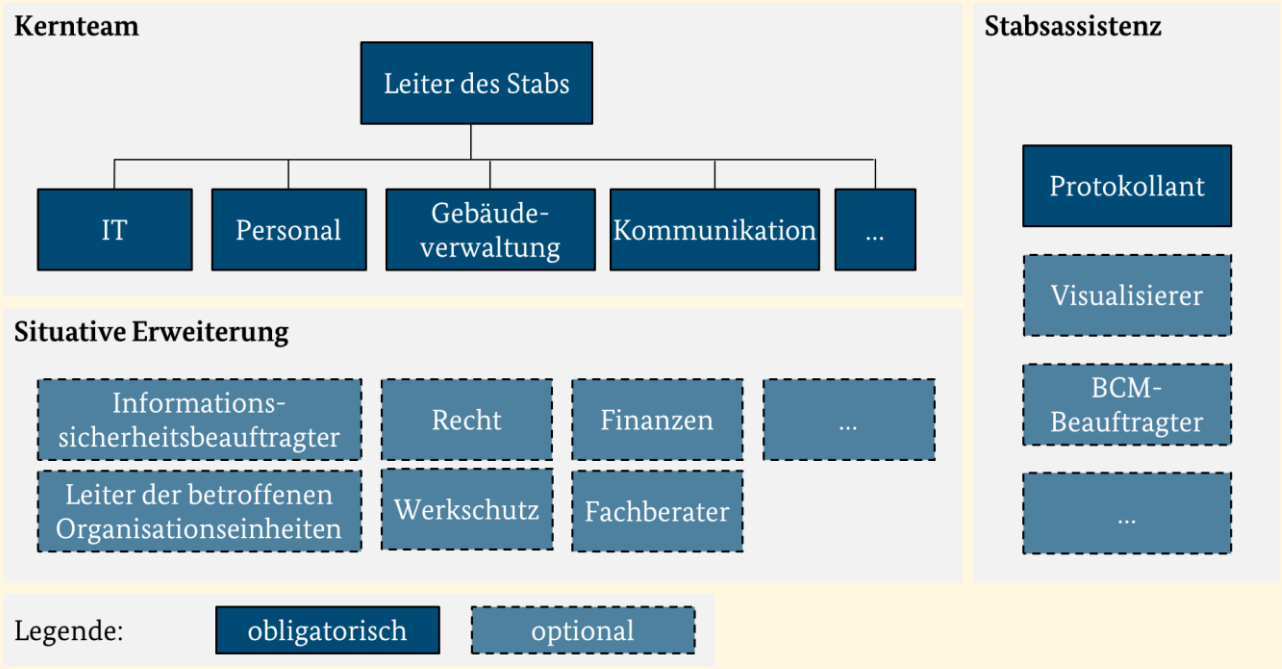

Abbildung 44: Beispiele verschiedener Rollen in einem Stab

Hinweis:

Der Informationsaustausch und damit die Entscheidungsfähigkeit des Stabes sollten nicht durch zu viele Mitglieder ausgebremst werden. Daher sollten die Rollen der situativen Erweiterung bzw. bei Bedarf auch des Kernteams jeweils nur solange im Stab verbleiben, wie es erforderlich ist, um die Lage zu beurteilen oder Maßnahmen abzuleiten.

Die Institution sollte eine grafische Übersicht des Stabsaufbaus erstellen. Abbildung 44 zeigt beispielhaft den Aufbau eines Stabes, bestehend aus Kernteam, situativer Erweiterung und Stabsassistenz. Der Aufbau entspricht den Empfehlungen des Standard-BCMS und wird nachfolgend erläutert. Wie eingangs dargestellt, sind die Stabsstrukturen je nach Institution sehr unterschiedlich. Daher sollte das Beispiel institutionsspezifisch angepasst werden.

6.4.1.2 Aufbau des Kernteams

Der Stab sollte aus einem Kernteam bestehen, dessen Mitglieder Schlüsselpositionen für Entscheidungen in Not- oder Krisenfall abdecken und lageunabhängig für die Bewältigung alarmiert werden. Das Kernteam sollte, neben einem Leiter des Stabes, Mitglieder zu folgenden Themen beinhalten:

- IT
- Personal
- Gebäudeverwaltung
- Kommunikation

Der **Leiter des Stabes** koordiniert die Aktivitäten aller Stabsmitglieder in der Bewältigung. Er trifft grundsätzlich die Entscheidungen im Stab. Für den Leiter des Stabes muss neben den Aufgaben und Zuständigkeiten zusätzlich die Verantwortung im Not- und Krisenfall definiert werden, sobald er bei Ausrufung des Not- oder Krisenfalls über die AAO hinausgehende Entscheidungsbefugnisse oder finanzielle Spielräume erhält. Die Entscheidungsbefugnis kann der Leiter an das Kernteam delegieren. Daraufhin kann jede Rolle im Kernteam nach außen in Vertretung bzw. im Auftrag des Leiters Weisungen geben. Für den Leiter des Stabes sollten mehrere Stellvertreter benannt werden, um sicherstellen zu können, dass diese zentrale Rolle für die Bewältigung besetzt ist.

Die Rollen **IT**, **Personal** und **Gebäudeverwaltung** repräsentieren die Vertreter der Organisationseinheiten, die über die jeweilige Fach- und Sachkenntnis der Ressourcen verfügen. Diese Rollen können in der Notfallbewältigung geeignete technische, bauliche oder organisatorische Maßnahmen ableiten. Ferner bilden diese Rollen die jeweiligen Schnittstellen zu den Einheiten, welche die Maßnahmen umsetzen. Es ist empfehlenswert, die Rollen im Kernteam dem Schwerpunkt der Institution anzupassen.

Beispiel:

Eine Institution, deren IT-Betrieb vollständig ausgelagert wurde (Outsourcing), bindet die Zuständigen, die die Dienstleister steuern, als eigene Rolle im Kernteam ein. Ein Produktionsunternehmen bindet wiederum die Produktionssteuerung als eigene Rolle im Kernteam ein.

Die Rolle Kommunikation ist zuständig für die Informationssammlung sowie adressatengerechte Informationsaufbereitung und -verteilung nach innen und außen. Der Notfallkommunikation kommt eine sehr hohe Bedeutung für den Erfolg der Notfallbewältigung zu (siehe Kapitel 6.4.6 *Notfallkommunikation*).

6.4.1.3 Aufbau der situativen Erweiterung

Zum erweiterten Stab zählen Rollen, die durch ihre Expertise und Ressourcen zur Bewältigung beitragen können. Der Personenkreis beschränkt sich dabei normalerweise auf die eigene Institution. Folgende Rollen sind unter anderem typisch bei der situativen Erweiterung:

- Informationssicherheitsbeauftragter (ISB)
- Leiter der betroffenen Organisationseinheiten
- Recht
- Werkschutz
- Arbeitssicherheit und Brandschutz
- Finanzen
- interne und externe Fachberater

Es können auch Personen aus der AAO in den Stab beordert werden, um besondere Meldepflichten gegenüber Regulatoren wahrzunehmen.

Zudem können externe Mitglieder in den Stab aufgenommen werden, beispielsweise Dienstleister und Berater. In diesem Fall sollten unter anderem die Punkte Vertraulichkeit von Informationen sowie Handlungs- und Entscheidungsbefugnisse explizit geregelt werden.

6.4.1.4 Aufbau der Stabsassistenz

Der Stab sollte durch eine Stabsassistenz ergänzt werden. Die Rollen der Stabsassistenz entlasten den Stab von organisatorischen Aufgaben und schaffen damit den Freiraum zur Handlungs- und Entscheidungsfähigkeit des Stabes.

Hinweis:

Je nach Arbeitsweise im Stab und den individuellen Fähigkeiten der agierenden Personen kann es möglich sein, verschiedene Rollen durch eine Person wahrnehmen zu lassen. So kann beispielsweise in der Praxis die Rolle des Visualisierers sowie des Aufgabenkoordinators sinnvoll miteinander verbunden werden, wenn die jeweiligen Arbeitsphasen zeitlich auseinanderliegen.

Die Stabsassistenz muss mindestens aus der Rolle **Protokollant** bestehen. Der Protokollant führt die Nachweise über die Schadensbewältigung zusammen und unterstützt damit den Stab, die getroffenen Entscheidungen und Ereignisse nachzuhalten. Das erstellte Protokoll dient dazu, die Institution rechtlich abzusichern, Entscheidungen zu dokumentieren und unmittelbar identifizierte Verbesserungsbedarfe in der Bewältigung nachzuhalten. Weiterführende Informationen zur Protokollierung sind im Kapitel 6.4.4.4 *Protokollierung* beschrieben.

Es ist empfehlenswert, den Stab durch die Rolle **Visualisierung** zu unterstützen. Die Rolle Visualisierung dient dazu, das Ereignis in einem Schaubild, auch Lagebild genannt, darzustellen (siehe Kapitel 6.4.5.2 *Lagebeobachtung und -visualisierung)* und so Lageveränderungen sowie die Maßnahmenumsetzung zu verfolgen. Dies fördert das Lageverständnis des Stabes und trägt zu einer effizienteren Bewältigung bei.

Um ein strukturiertes Aufgabenmanagement gewährleisten zu können, ist es empfehlenswert, hierfür eine eigene Rolle **Aufgabenkoordinator** zu schaffen. Der Aufgabenkoordinator sammelt die verschiedenen Aufträge aus dem Stab. Dies entlastet andere Rollen des Stabes in komplexen Notfallsituationen.

Der **BCMB** ist eine Rolle in der präventiven BCM-Organisation. Es ist aber empfehlenswert, diesen auch in der BAO einzubinden. Dies hat den Vorteil, dass das Wissen über die zeitkritischen Geschäftsprozesse und

Ressourcen sowie die Notfalldokumentation dem Stab jederzeit direkt zur Verfügung steht und falls erforderlich erfragt werden kann. Abbildung x zeigt ein mögliches Beispiel, in dem der BCMB der Stabsassistenz zugeordnet ist.

6.4.1.5 Aufbau von Notfallbewältigungsteams

Zur operativen Bewältigung eines Notfalls sollten Notfallbewältigungsteams aufgebaut werden.

Hinweis:

Die Größe der Teams richtet sich an der Komplexität und der Personalausstattung der Institution aus. Gerade in kleinen Institutionen kann es daher möglich sein, dass statt eines Teams nur ein einzelner Mitarbeiter für bestimmte Aktivitäten der Notfallbewältigung zuständig ist. Nachfolgend wird jedoch zur besseren Verständlichkeit nur von Teams gesprochen.

Die Notfallbewältigungsteams erhalten ihre Arbeitsaufträge aus dem Stab und setzen die darin beschriebenen technischen, baulichen oder organisatorischen Maßnahmen zur Notfallbewältigung um. Im Vorfeld festgelegte Notfallbewältigungsteams haben gegenüber ad hoc zusammengestellten Teams drei Vorteile:

- Sie können anhand von Trainings und Übungen auf verschiedene Notfallszenarien vorbereitet werden.
- Sie können im Notfall aufgrund des Trainingseffekts in der Regel schneller und zielgerichteter agieren.
- Die Kommunikationswege zwischen Stab und Notfallbewältigungsteams können im Vorfeld festgelegt und erprobt werden.

Die Leiter der Notfallbewältigungsteams sollten während der Notfallbewältigung dem Stab in regelmäßigen Abständen berichten. Dazu sollte jeder Leiter die Informationen vor Ort sammeln und an den Stab weiterleiten. Darüber hinaus sollten die Leiter koordinieren und kontrollieren, ob die vom Stab angeordneten Maßnahmen vor Ort umgesetzt werden und wirksam sind. In der Praxis haben sich die folgenden Notfallbewältigungsteams bewährt:

- IT
- Personal
- Gebäudeverwaltung
- Notfallkommunikation

Es ist empfehlenswert, diese institutionsspezifisch durch weitere Notfallbewältigungsteams zu ergänzen. Zum Beispiel können Notfallteams in den zeitkritischsten Organisationseinheiten etabliert werden, die das Kerngeschäft repräsentieren.

6.4.1.6 Personelle Besetzung der BAO

Der festgelegte Aufbau der BAO sowie die Rollenbesetzung müssen von der Institutionsleitung freigegeben werden. Um der Institutionsleitung einen Gesamtüberblick über die BAO zu ermöglichen, sollte diese schematisch beschrieben werden. Hierzu kann ein Schaubild, wie in Abbildung 44 dargestellt, erstellt werden. Anhand von Rollenkarten können zusätzlich die jeweiligen Aufgaben und Zuständigkeiten jeder Rolle im Detail vorgestellt werden.

Anhand des festgelegten Aufbaus des Stabes muss sichergestellt werden, dass jede Rolle mit einem geeigneten Hauptzuständigen sowie einem Stellvertreter besetzt wird. Unter anderem durch Schulungen kann sichergestellt werden, dass die Rolleninhaber fachlich geeignet sind (siehe Kapitel 6.4.5.1 *Schulung der BAO*). Gleichzeitig sollte geklärt werden, ob die Personen mental in der Lage sind, in besonderen Stresssituationen zu arbeiten (siehe hierzu auch das Hilfsmittel *Weiterführende Aspekte zur Bewältigung*).

Die Rollenbesetzung sollte nach der Freigabe durch die Institutionsleitung in der Geschäftsordnung des Stabes dokumentiert werden. In der Geschäftsordnung sollte neben der Stabsform und den darin enthaltenen Rollen die Besetzung des Stabes namentlich benannt werden. Ferner sollte neben den Aufgaben und Zuständigkeiten jeder Rolle die Entscheidungs- und Weisungsbefugnisse konkretisiert werden.

Beispiel:

Herr Mustermann wird als Leiter des Krisenstabes benannt. Er verfügt über das Recht, über einen Notfall final zu entscheiden und den Stab zusammenzurufen. Er ist dafür zuständig, den beteiligten Personen im Stab klare Aufgaben zuzuteilen. […] Der Leiter des Stabes trägt die Leitungs- und Entscheidungskompetenz, zieht jedoch die Empfehlungen und Einschätzungen der Stabsmitglieder in seine Überlegungen mit ein. Während die BAO gilt, ist Herr Mustermann von seinen Aufgaben und Pflichten der AAO entbunden.

6.4.2 Detektion, Alarmierung und Eskalation

Je schneller ein Schadensereignis richtig eingestuft und behandelt wird, desto eher werden Folgeschäden eingedämmt und eine weitere Eskalation des Ereignisses verhindert. Wenn ein Notfall eintritt, ist es daher wichtig, dass dieser möglichst schnell erkannt und an die Entscheider gemeldet wird. Daher sollte vorab festgelegt werden, wie die Meldung von Schadensereignissen mit Notfallpotenzial erfolgt. Hierzu sollte die Art der Meldung näher definiert werden. So kann eine Meldung entweder der Information oder der Alarmierung dienen.

Die **Information** (Zustand bzw. Störung) dient ausschließlich dazu, den Sachverhalt eines Ereignisses zu übermitteln. Die Information wird in der Praxis z. B. genutzt, wenn der Leiter des Stabes über eine Störung informiert wird, die potenziell zu einem Notfall eskalieren kann. Dies erfordert von Seiten des Leiters des Stabes keine direkte Handlung, da die Störungsbeseitigung in der AAO durchgeführt wird. Durch eine transparente und frühzeitige Kommunikation ist der Leiter des Stabes für den Fall informiert, dass die Störung dennoch eskaliert und kann bei Bedarf eine schnellere und qualifiziertere Bewertung durchführen.

Die **Alarmierung** führt immer zu einer Handlung von ausgewählten Mitarbeitern in der BAO, die über das weitere Vorgehen entscheiden dürfen.

Die Detektion von Ereignissen kann bereits in anderen Prozessen der Institution geregelt sein, z. B. im IT Incident Management, in der Störungsbehandlung der Gebäudeverwaltung, in Entstörungsdiensten von Dienstleistern oder in der Sicherheitsvorfallbehandlung. Es sollte geprüft werden, ob entsprechende Prozesse zur Behandlung von Störungen und Sicherheitsvorfällen in der Institution bereits vorhanden sind. In diesem Fall ist es empfehlenswert, diese unterschiedlichen Prozesse aufeinander abzustimmen. Hierbei sollte sichergestellt werden, dass Schadensereignisse und Störungen mit Notfallpotenzial an eine zentrale Entscheidungsinstanz gemeldet werden und Reaktionszeiten aufeinander abgestimmt sind. Zusätzlich sollte die Kommunikations- und Alarmierungstechnik redundant ausgelegt sein. Es sollten außerdem Kommunikationskanäle zur Verfügung stehen, die unabhängig von der IT der Institution funktionieren.

Allerdings kann ein Notfall auch durch Ereignisse ausgelöst werden, die weder aus einer Störung heraus eskalieren noch als Sicherheitsvorfall eingestuft werden. Für solche Ereignisse ist kein Prozess zur Alarmierung und Eskalation vorhanden. Ein Beispiel ist ein krankheitsbedingter, massiver Personalausfall in einer Organisationseinheit, der zu nicht tolerierbaren Auswirkungen auf den Geschäftsbetrieb führt. Auch für diese Ereignisse sollten Kriterien festgelegt werden, was durch wen an eine Meldestelle gemeldet werden sollte. Die Abbildung 45 stellt verkürzt mögliche Alarmierungspfade dar. Die einzelnen Aktivitäten werden in den nachfolgenden Kapiteln näher beschrieben

Beispiel:

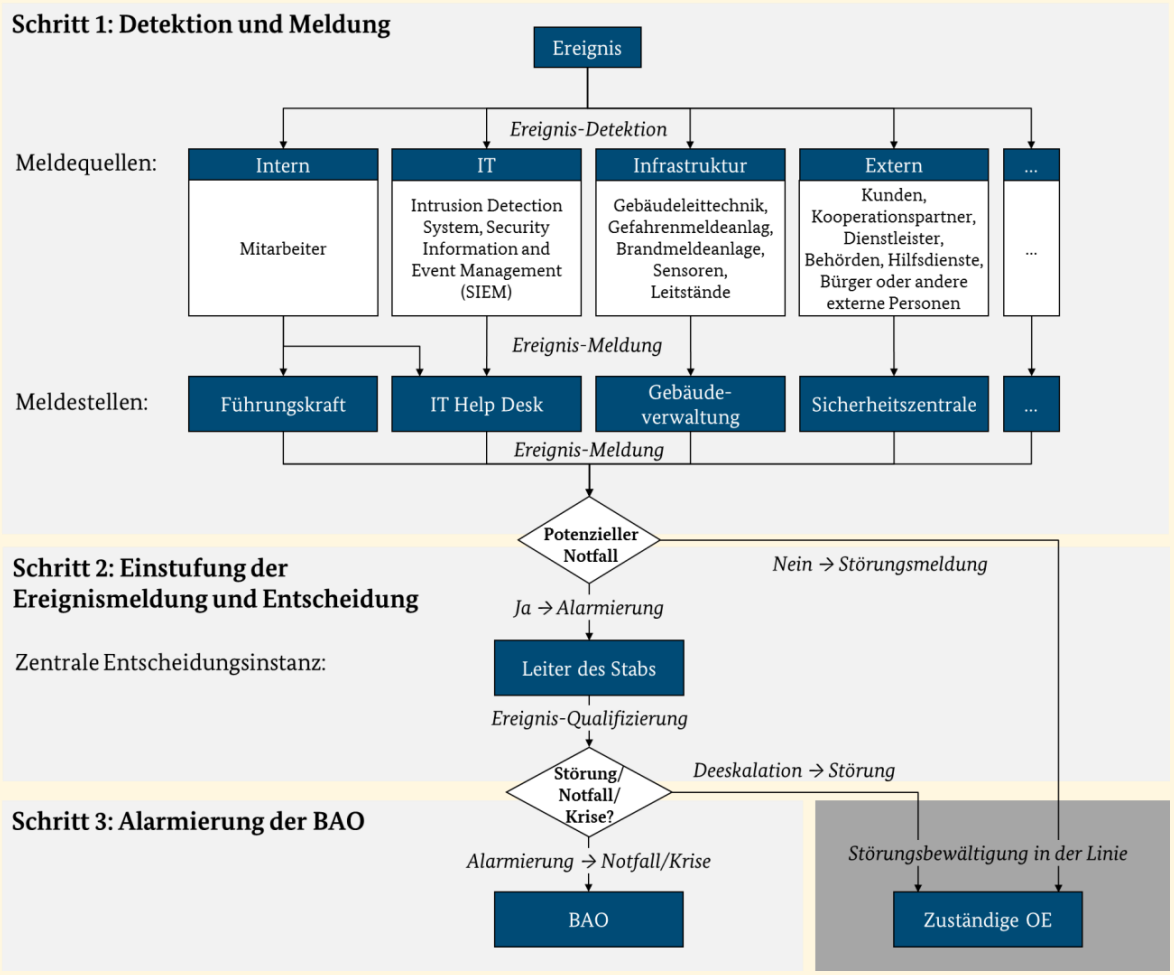

Abbildung 45: Beispiel eines Eskalations- und Alarmierungspfads

6.4.2.1 Detektion und Meldung

Die Detektion eines Schadensereignisses und die anschließende Weitergabe der Meldung können durch verschiedene interne und externe Personen oder technische Systeme erfolgen. Diese werden im Folgenden als Meldequellen bezeichnet.

Beispiel:

Typische Beispiele für Meldequellen sind

- interne Mitarbeiter,
- das IT-Monitoring der IT-Infrastrukturen (z. B. zur Überwachung der Verfügbarkeit der IT-Systeme oder zur Überwachung auf IT-Sicherheitsvorfälle durch Intrusion Detection Systeme (IDS) oder Security Information and Event Management (SIEM)),
- das technische Monitoring der Infrastruktur (z. B. Gebäudeleittechnik, Gefahrenmeldeanlage für Brandschutz, Einbruchschutz etc.), Sensoren zur Überwachung der grundlegenden Versorgung (Strom, Wasser, Klimatisierung etc.) oder durch Leitstände der Produktion zur Betriebs- bzw. Werkssteuerung) sowie
- externe Personen (z. B. Kunden, Kooperationspartner, Dienstleister, Behörden, Hilfsdienste, Bürger etc.).

Die relevanten Meldequellen der Institution müssen identifiziert werden. Zudem muss sichergestellt werden, dass Meldungen an die zuständigen Meldestellen gelangen und nicht verloren gehen. Entsprechend müssen die identifizierten Meldequellen sowie zuständigen Meldestellen im Notfallhandbuch dokumentiert werden.

Dabei kann entweder genau eine Meldestelle für jegliche Meldungen festgelegt werden oder es werden individuelle Stellen entsprechend des Ereignistyps bestimmt. Letzteres hat den Vorteil, dass jede Ereignismeldung direkt diejenige spezialisierte Meldestelle erreicht, die durch ihre Fachkunde entscheidungs- bzw. aussagefähig sind. Ein weiterer Vorteil ist, dass durch mehrere individuelle Stellen die Last einer Vielzahl von Meldungen auf die einzelnen Meldestellen verteilt wird. Ein Meldeweg über mehrere Meldestellen ist beispielhaft in Abbildung 45 am Anfang des Kapitels dargestellt.

Beispiel:

In vielen Institutionen sind bereits mehrere zuständige Stellen etabliert, die Ereignismeldungen entgegennehmen, bearbeiten und erste Maßnahmen zum Eindämmen von Schäden einleiten. Folgende Meldestellen sind häufig vorhanden:

- Technische Alarme der Gefahrenmeldeanlage oder Elementarschäden laufen meist bei einer Sicherheitsleitstelle oder einem Sicherheitsdienst auf.
- Personalausfälle oder Störungen bei Dienstleistern werden über die Linienorganisation an die jeweils zuständigen Führungskräfte gemeldet.
- Ausfälle von IT-Anwendungen werden häufig an einen zentralen Service Desk bzw. First-Level-Support gemeldet
- Oft nehmen auch der Empfang, die Telefonzentrale oder die Kundenhotline Meldungen über Schadensereignisse mit Notfallpotenzial entgegen.

Die identifizierten und festgelegten Meldewege müssen mit den beteiligten, organisatorischen Schnittstellen abgestimmt werden, sodass diese bei Schadensereignissen mit Notfallpotenzial mit den definierten Wegen vertraut sind. Ferner sollte durch Schulungen und Sensibilisierung für alle Mitarbeiter und möglicherweise Externe sichergestellt werden, dass der Alarmierungs- und Eskalationsprozess bekannt ist und korrekt angewendet wird. Die im Notfallhandbuch dokumentierten Meldeverfahren sollten den gelebten Prozessen entsprechen.

Um Ereignisse anhand möglichst vollständiger Informationen einschätzen zu können, sollte jede Meldestelle die Meldungen in einem einheitlichen Format erfassen. Meldungen sollten kurzgefasst sein und effizient die nötige Information beinhalten. Dabei sollten die Tatsachen von Vermutungen voneinander getrennt werden. Mindestens folgende Angaben sollten aufgenommen werden:

- Zeitpunkt und Ort des Ereignisses
- meldende Person oder Stelle
- eventuell betroffene Personen, Bereiche oder Prozesse
- mögliche Ursache oder Auslöser
- bereits ergriffene Sofortmaßnahmen
- die aktuellen Auswirkungen

Unter Berücksichtigung der Rahmenbedingungen sowie der Risikobereitschaft der Institution muss definiert und dokumentiert werden, wie die Meldestellen sowohl während als auch außerhalb der üblichen Geschäftszeiten erreicht werden können. So können z. B. Rufbereitschaften festgelegt werden. In der Praxis sind Vorgaben seitens des Arbeitsschutzes sowie vorhandene Regelungen der Institution zur Arbeitszeit und Erreichbarkeit zu beachten. Daher sollten die Regelungen zur Erreichbarkeit mit den relevanten Stellen abgestimmt werden, z. B. mit der Institutionsleitung, der Personalabteilung und dem Betriebs- bzw. Personalrat. Falls nur

eine eingeschränkte Erreichbarkeit einzelner Meldestellen realisiert werden kann, muss dies ebenfalls im Notfallhandbuch dokumentiert sein. Zudem sollte dann eine Risikoübernahme durch die Institutionsleitung herbeigeführt werden.

Hinweis:

Einige Institutionen unterliegen gesetzlichen oder regulatorischen Anforderungen, die vorschreiben, dass bestimmte Schadensereignisse innerhalb von wenigen Stunden an ausgewählte Interessengruppen (z. B. die zuständige Aufsichtsbehörde) gemeldet werden müssen. Wenn solche kurzfristigen Meldepflichten erfüllt werden müssen, muss für die Institution sichergestellt werden, dass die Meldepflicht z. B. durch Rufbereitschaftsregelungen oder eine durchgängige Besetzung eingehalten wird.

Jede Meldestelle muss befähigt werden, bei einem Schadensereignis initial einschätzen zu können, ob ein Ereignis mit Notfallpotenzial vorliegt. Dies kann im Rahmen eines gemeinsamen Termins erfolgen, in dem der aktuelle Stand erklärt und gemeinsam Kriterien zur Ersteinschätzung gefunden werden. Klare und für alle Beteiligten verständliche Kriterien sind von hoher Bedeutung, da die Ersteinschätzung möglichst schnell erfolgen muss und die weiteren Abläufe der Notfallbewältigung so früh wie möglich eingeleitet werden sollen. Dieser Zeitfaktor hängt sehr stark mit den definierten Erreichbarkeiten der Meldestellen zusammen. Wenn eine Meldestelle z. B. nur von 8 bis 17 Uhr erreichbar ist, kann ein Schadensereignis mit Notfallpotenzial um 17:30 Uhr mitunter erst am Folgetag festgestellt und weitergemeldet werden. Durch wen die Ersteinschätzung vorgenommen wird, sollte sich an den bereits etablierten Meldestellen und Meldewegen orientieren. Die Kriterien, um ein Ereignis einschätzen zu können, sollten auch durch Personen mit nur geringen fachlichen oder technischen Kenntnissen angewendet werden können. Die Ersteinschätzung sollte deshalb nach einem einfachen Schema erfolgen, z. B. per Ja-Nein-Antwort auf allgemein verständliche Fragen. In den folgenden Tabellen (Tabelle 39 bis Tabelle 37) ist jeweils ein generisches Beispiel für die Ersteinschätzung eines Schadensereignisses für die häufigsten vier Ressourcenkategorien dargestellt. Für jede Institution und Meldestelle müssen diese Fragen individuell konkretisiert werden. Hierbei kann darauf hingewiesen werden, dass die Information zur Bewertung auch von den Meldestellen in einem Schadensereignis erfragt werden kann, wenn sie nicht offensichtlich ist.

Meldestelle: Gebäudemanagement/Sicherheitszentrale/Sicherheitsdienstleister/Leitstand

Leitfragen für Schadensereignisse mit Notfallpotenzial – Gebäude/Infrastruktur	Ja/Nein
• Ist/war die Räumung eines Gebäudes notwendig, z. B. aufgrund eines Brandes oder eines Sicherheitsvorfalls? • Kann oder darf mindestens ein Gebäudeteil (gesamte Etage, Brandabschnitt, Trakt etc.) zeitweise nicht genutzt werden, z. B. aufgrund eines Gebäudeschadens oder eines Defekts einzelner Infrastrukturkomponenten (Brandschutzeinrichtungen, Sanitäranlagen etc.)? • Ist die Versorgung mit Strom, Wasser oder Klimatisierung ausgefallen und eine ausreichend schnelle Wiederherstellung nicht absehbar? • Ist eine Produktionsmaschine oder -anlage ausgefallen und eine ausreichend schnelle Reparatur oder ein Ersatz nicht absehbar? • Ist die Sicherheit der Mitarbeiter am Standort aufgrund eines Ereignisses (z. B. Unwetterwarnung, politische Demonstration oder Schadensereignis im Umfeld) möglicherweise gefährdet?	

Sobald mindestens eine Frage mit JA beantwortet werden kann, bitte
umgehend an den Leiter des Stabes melden: Telefon 1234567890

Tabelle 37: Beispiel einer Ersteinschätzung eines Schadensereignisses am bzw. im Gebäude

Beispiel: Meldestelle: IT-Help Desk (1st/2nd Level Support)

Leitfragen für Schadensereignisse mit Notfallpotenzial - IT	Ja/Nein
• Ist das betroffene IT-System oder die betroffene Anwendung wesentlicher Bestandteil der Sicherheitsinfrastruktur (Viren-Management, Firewall etc.)? Für nähere Details siehe IT-Servicekatalog oder IT-Anwendungsliste. • Hat der Ausfall des betroffenen IT-Systems oder der betroffenen Anwendung Auswirkungen auf einen großen Nutzerkreis oder den wesentlichen Geschäftsbetrieb der Institution? • Besteht ein dringender Verdacht auf vorsätzliche Daten- oder Systemmanipulationen (Datenabfluss), unerlaubte Ausübung von Rechten oder eines gezielten Angriffs (physisch oder virtuell) auf IT-Komponenten? • Ist zu erwarten, dass die Auswirkungen des Ereignisses einen Zeitraum > X Stunden übersteigen werden? (Gegebenenfalls die Information im 2nd Level Support erfragen.) • Hat der Ausfall des betroffenen IT-Systems oder der betroffenen IT-Anwendung Auswirkungen auf externe Interessengruppen, wie z. B. Kunden, Medien, Aufsichtsbehörden? Gegebenenfalls die Information beim Anwender erfragen.	

Sobald mindestens eine Frage mit JA beantwortet werden kann, bitte umgehend an den Leiter des Stabes melden: Telefon 1234567890

Tabelle 38: Beispiel einer Ersteinschätzung eines Schadensereignisses in der IT

Meldestelle: Führungskraft Personal

Leitfragen für Schadensereignisse mit Notfallpotenzial - Personal	Ja/Nein
• Sind in Ihrem Zuständigkeitsbereich in Summe so viele Mitarbeiter nicht arbeitsfähig, dass Sie möglicherweise den Geschäftsbetrieb nicht mehr aufrechterhalten können? • Ist durch die Abwesenheit von Mitarbeitern mit bestimmten Berechtigungen der normale Geschäftsbetrieb eventuell nicht mehr möglich?	

Sobald mindestens eine Frage mit JA beantwortet werden kann, bitte umgehend an den Leiter des Stabes melden: Telefon 1234567890

Tabelle 39: Beispiel einer Ersteinschätzung eines Schadensereignisses beim Personal

Meldestelle: Provider Management bzw. Dienstleistersteuerung

Leitfragen für Schadensereignisse mit Notfallpotenzial - Dienstleister	Ja/Nein
• Liegt beim Dienstleister oder dessen Subunternehmen ein nicht geplanter Ausfall bzw. Notfall vor oder ist dieser absehbar? • Hat der Dienstleister den Vertrag einseitig gekündigt und mit sofortiger Wirkung seine Leistung eingestellt?	

Sobald mindestens eine Frage mit JA beantwortet werden kann, bitte umgehend an den Leiter des Stabes melden: Telefon 1234567890

Tabelle 40: Beispiel einer Ersteinschätzung eines Schadensereignisses beim Dienstleister

Wenn es sich um ein Schadensereignis mit Notfallpotenzial handelt, muss die zuständige Stelle unverzüglich eine vordefinierte zentrale Entscheidungsinstanz alarmieren. Hierbei müssen

- alle bekannten Details zum Schadensereignis,
- die bisher bekannten Auswirkungen sowie
- bereits eingeleitete Maßnahmen zur Bewältigung des Ereignisses

übermittelt werden.

Sollte die Meldestelle bei der Ersteinschätzung unsicher sein, gilt der Grundsatz „Lieber zu viel melden, als zu wenig". Dementsprechend sollte die zentrale Entscheidungsinstanz von der Meldestelle informiert werden. Eventuelle Fehlmeldungen können im Nachgang untersucht und der Prozess *Alarmierung und Eskalation* entsprechend angepasst werden, z. B. indem die Kriterien anhand der gewonnenen Erkenntnisse geschärft werden.

Um eine möglichst verzugslose Alarmierung sicherzustellen, muss festgelegt werden, wie Alarmmeldungen übermittelt werden sollen, z. B. per Telefon, Alarm-SMS mit Lesebestätigung oder Alarmierungstool. Es wird empfohlen, Kommunikationsmittel einzusetzen, die den direkten, verzugslosen Dialog erlauben und damit zusätzlich sicherstellen, dass Informationen aufgenommen und verstanden wurden.

Für den Fall, dass die Kommunikations- und Alarmierungstechnik vom Schadensereignis selbst betroffen ist, müssen alternative Techniken vorgesehen werden. Es sollten außerdem Kommunikationskanäle zur Verfügung stehen, die unabhängig von der IT der Institution funktionieren.

Hinweis:

Asynchrone Kommunikationsmittel sind für den Alarmierungs- und Meldeprozess weniger geeignet, da der Absender nicht wissen kann, ob und wann der Empfänger die Information erhält. So erzeugen z. B. Alarmmeldungen über E-Mail häufig nicht genügend Aufmerksamkeit für Schadensereignisse und gehen in der Menge von anderen E-Mails unter. Besser geeignet sind z. B. manuelle oder automatisierte Anrufe auf Mobiltelefonen oder Alarm-Apps.

6.4.2.2 Einstufung der Ereignismeldung und Entscheidung

Die Einstufung und Entscheidung, ob es sich bei dem Schadensereignis um eine Störung, einen Notfall oder eine Krise handelt, muss durch eine **zentrale Entscheidungsinstanz** getroffen werden. Eine zentrale Entscheidungsinstanz verhindert, im Gegensatz zu dezentralen Entscheidungsinstanzen, zeitaufwändige Abstimmungen oder unklare Entscheidungsbefugnisse und ermöglicht so eine schnelle Entscheidungsfindung. Dies ist von hoher Bedeutung, da die Entscheidung über das Ereignis weitreichende Auswirkungen auf das weitere Geschehen der Bewältigung hat. Stellt sich heraus, dass ein Schadensereignis als Störung bewertet wurde, es sich aber um einen Notfall handelt, ist wahrscheinlich wertvolle Zeit verloren gegangen. Deshalb muss die zentrale Entscheidungsinstanz geschult, erfahren und befugt sein.

Geschult bedeutet hier, dass die zentrale Entscheidungsinstanz über die hierzu erforderliche Sachkenntnis verfügen muss, z. B. um die Begriffe Störung, Notfall und Krise unterscheiden zu können (siehe Kapitel 3.2.5 *Schulung*). Zudem muss die zentrale Entscheidungsinstanz den Alarmierungsprozess kennen. Das Verständnis der Entscheidungsinstanz kann darüber hinaus erhöht werden, indem sie reale, praktische Erfahrungen bei Übungen und Tests sammeln kann. Wenn außerdem die Entscheidungskriterien verbessert werden, begünstigt dies eine korrekte Einschätzung von Schadensereignissen. So werden Fehleinschätzungen kontinuierlicher Verbesserung des BCMS gesenkt.

Die Entscheidungsinstanz muss auch erfahren sein und einen guten Überblick über die Institution haben, damit sie die Auswirkungen einschätzen kann. In den meisten Fällen liegen zu einem Schadensereignis nur eingeschränkte Informationen vor. Auch dann sollte die Entscheidungsinstanz entscheidungsfreudig sein.

Als letzter Punkt muss die Entscheidungsinstanz entsprechend befugt sein, eigenständig die Ereignismeldung einzustufen und eine Entscheidung zu fällen. Dies verkürzt die Zeitspanne, die bis zum Beginn der Bewältigung verstreicht.

Hinweis:

Aufgrund ihrer Aufgaben, Fähigkeiten und Erfahrungen sind in der Praxis häufig der Leiter des Stabs oder der BCMB geeignete Rollen, um die Ereignismeldung qualifizieren zu können.

Um die Entscheidung zu vereinfachen und sie transparent zu machen, sollte der zentralen Entscheidungsinstanz eine Checkliste mit Kriterien zur Verfügung gestellt werden. Auf deren Basis kann eine nachvollziehbare und dokumentierte Entscheidung zur Einstufung des Ereignisses getroffen werden. Um Kriterien für einen Notfall (siehe Kapitel 3.2.1 *Definition und Abgrenzung*) ableiten zu können, können zunächst folgende Punkte als Grundlage herangezogen werden:

Beispiel:

- Fall 1: Der normale Geschäftsbetrieb der Institution oder einzelne Teile davon sind unterbrochen.
- Fall 2: Ein Ausfall des Geschäftsbetriebs steht unmittelbar bevor bzw. ist absehbar und folgende Kriterien treffen zu:
    - Mindestens ein zeitkritischer Geschäftsprozess ist betroffen.
    - Die Bewältigung erfordert eine BAO, z. B. für kurze Entscheidungswege und schnellen Zugriff auf Spezialisten.

Wenn zu einem späteren Zeitpunkt durch die Institution konkreter festgelegt wird, wie der Stab final über einen Notfall oder Krise entscheidet, dann können die Kriterien bereits in der ersten Einstufung des Schadensereignisses hinzugezogen werden.

Das Ergebnis der Ersteinschätzung kann zwei Ausgänge haben:

- Das Ereignis wird als **Störung** eingestuft. (Dann muss das Ereignis als Störung gemeldet und durch die entsprechende Fachabteilung innerhalb der AAO behoben werden. Da ein Schadensereignis jederzeit durch Lageveränderungen eskalieren kann, sollte sich die Entscheidungsinstanz über den Verlauf der Störungsbeseitigung durch die zuständige Fachabteilung informieren lassen.)
- Das Ereignis wird als **Notfall** oder **Krise** eingestuft. (Dann muss die Entscheidungsinstanz die BAO unverzüglich alarmieren. So wird sichergestellt, dass die Lage möglichst schnell beurteilt und das Schadensereignis anhand von Sofort- und Notfallmaßnahmen bewältigt werden kann.)

In jedem Fall muss die zentrale Entscheidungsinstanz die getroffene Entscheidung mit den notwendigen Details dokumentieren, wie z. B. Zeitpunkt und Auswirkung des Ereignisses, Begründung der Entscheidung und Beteiligte an der Entscheidung.

In der Konstituierung der BAO muss diese Entscheidung durch den Stab anhand weiterer Kriterien überprüft und bestätigt bzw. deeskaliert werden (siehe Kapitel 6.4.7 *Störbetrieb und Deeskalation*).

6.4.2.3 Alarmierung der BAO

Um sicherzustellen, dass die BAO unverzüglich alarmiert werden kann, müssen die hierfür notwendigen organisatorischen und technischen Voraussetzungen geschaffen und dokumentiert werden. Ein zentraler Punkt, der hierfür gemeinsam mit den Rolleninhabern und der Institutionsleitung abgestimmt werden muss, ist die **Erreichbarkeit der BAO** innerhalb und außerhalb der üblichen Geschäftszeiten. Analog zu dem be-

schriebenen Vorgehen für die zentrale(n) Meldestelle(n) sollten Rufbereitschaften der BAO eingerichtet werden. Für Zeiten, in denen eine Erreichbarkeit der BAO nicht garantiert ist, sollten Risikoübernahmen durch die Institutionsleitung herbeigeführt werden.

Die Benachrichtigung der Rolleninhaber der BAO sollte kurz und präzise sein. Diskussionen und längere Ausführungen zur Lage müssen bei der Alarmierung vermieden werden. Zum einen können zu viele Informationen den Einzelnen verwirren. Zum anderen wird die Alarmierung unnötig verzögert. Detaillierte Informationen werden in der ersten Lagebesprechung für alle Anwesenden gemeinsam vorgestellt und besprochen. Organisatorisch sollte festgelegt werden,

- wie die BAO innerhalb und außerhalb der üblichen Geschäftszeiten erreicht wird,
- welche Personen durch die zentrale Entscheidungsinstanz alarmiert werden,
- welche weiteren Personen durch die zuerst alarmierten Personen alarmiert werden,
- welche Kommunikationskanäle hierzu eingesetzt werden sowie
- welche Informationen vermittelt werden.

In der Nachricht sollte klar erkennbar sein, welche nächsten Schritte der Alarmierte unternehmen muss, beispielsweise sich im Stabsraum oder einer virtuellen Arbeitsumgebung (z. B. Telefonkonferenz) einzufinden. Der Alarmierte muss dem Aufruf zeitnah folgen. Leben im Haushalt des Alarmierten weitere Personen, die den Anruf entgegennehmen könnten, so sollten diese für den Umgang mit empfangenen Alarmmeldungen sensibilisiert werden.

Je nach Größe der BAO kann es zeitaufwändig sein, alle Rolleninhaber einzeln persönlich zu benachrichtigen, z. B. via manuellem Telefonanruf. Zur Unterstützung der Alarmierung kann es sinnvoll sein, eine Alarmierungssoftware oder eine Alarm-App einzusetzen (siehe Hilfsmittel *Tools).* Diese IT-Anwendungen ermöglichen es, auf Knopfdruck die zur Bewältigung erforderlichen Personen zu benachrichtigen. Sofern eine Alarmierungssoftware eingesetzt wird, muss diese auch im Notfall oder in der Krise verfügbar sein.

Beispiel:

Neben der Alarmauslösung bieten die IT-Anwendungen oft wichtige Zusatzfunktionen, wie z. B.:

- eine Alarmnachverfolgung
- eine automatische Benachrichtigung der Stellvertreter bei Nicht-Erreichbarkeit
- die Möglichkeit, dass die Alarmierten dem Leiter des Stabes den erwarteten Zeitpunkt des Eintreffens im Stabsraum mitteilen können, falls dies der nächste Schritt ist

Der vollständig definierte Eskalations- und Alarmierungsprozess sollte visualisiert und im Notfallhandbuch dokumentiert werden. Dafür kann z. B. die Abbildung 45 vom Beginn des Kapitels angepasst werden. Diese ist auch in den Hilfsmitteln zum BSI-Standard 200-4 hinterlegt.

Dokumentierte Vorgaben und begleitenden Maßnahmen stellen sicher, dass die definierten Meldewege, wie vorgesehen, eingehalten werden. Als begleitende Maßnahme ist unter anderem empfehlenswert, dass Meldestellen und Kommunikationswege organisationsweit bekannt gegeben werden. Dazu können z. B. Aushänge oder andere Informationsmaterialen genutzt werden. Die Notfallkarte in den Hilfsmitteln stellt ein mögliches Beispiel dafür dar. Des Weiteren sollten Schulungen und Sensibilisierungsmaßnahmen für die Mitarbeiter geplant und veranlasst werden, um eine schnelle Alarmierung und Eskalation zu gewährleisten.

6.4.3 Definition von Sofortmaßnahmen

Mit Sofortmaßnahmen sind Maßnahmen gemeint, die keinen zeitlichen Aufschub dulden und möglichst unmittelbar nach Eintritt eines Schadensereignisses eingeleitet werden müssen, um den Schutz von Leib und Leben von Personen sicherzustellen sowie weitere Schäden abzuwenden. Zu Sofortmaßnahmen zählen z. B.

die Räumung des Gefahrenbereichs, die aus Sicherheitsgründen erforderliche Abschaltung der Stromversorgung oder die vorgeschriebene Sofortmeldung an einen Regulator.

In einem Notfall gilt der Grundsatz, dass der Schutz von Leib und Leben vor dem Schutz von Sachwerten und Gütern steht. Entsprechend muss sichergestellt sein, dass entsprechende Anweisungen und konkrete Aufgaben festgelegt werden. Es muss klar sein, wer welche Sofortmaßnahmen durchführen darf oder muss. Insbesondere sollte die Institution Sofortmaßnahmen für Notfallszenarien festlegen, bei denen „Gefahr im Verzug" besteht.

Beispiel:

- Maßnahmen zur Ersten Hilfe
- Maßnahmen zur Rettung und Bergung von Verletzten
- Maßnahmen zur Räumung von Gebäuden und Betriebsstätten
- Handlungsanweisungen für spezielle, wahrscheinliche Schadensereignisse, wie z. B.
    - Brand
    - Wassereinbruch
    - Ausfall der Strom-, Wasser oder Gas-Versorgung
    - Gefahr durch einen Sicherheitsvorfall, z. B. herrenloser Koffer im Gebäude
    - Großereignis im unmittelbaren Umfeld, z. B. Demonstrationen

Je nach Branche der Institution kann davon ausgegangen werden, dass es weitere spezielle Schadensereignisse gibt, für die Sofortmaßnahmen festgelegt werden müssen.

Synergiepotenzial:

Häufig existieren bereits gesetzliche Vorgaben für die oben genannten Punkte, die durch die jeweiligen Berufsgenossenschaften konkretisiert werden. Somit sollten entsprechende Anweisungen für Sofortmaßnahmen bereits in der Institution vorhanden sein, z. B. seitens der Fachkraft für Arbeitssicherheit. Die entsprechenden organisatorischen Maßnahmen können in geeigneter Form in die Ablauforganisation der Notfallbewältigung integriert werden. Entsprechend sollten die im Notfallhandbuch dokumentierten Sofortmaßnahmen zum Schutz von Leib und Leben mit der Fachkraft für Arbeitssicherheit abgestimmt werden. Im Notfallhandbuch sollte auf vorhandene Regelungen und Rollen verwiesen werden, z. B. die Aufgaben und Zuständigkeiten der Ersthelfer, Betriebssanitäter, Brandhelfer, Evakuierungshelfer oder Einsatzteams sowie entsprechende Aushänge in den Gebäuden. Die Sofortmaßnahmen sollten in Form von Checklisten dokumentiert werden. Dies ermöglicht auch unter Zeitdruck eine strukturierte Vorgehensweise.

Hinweis:

Häufig wird unter Sofortmaßnahmen die Evakuierung des Gebäudes verstanden, beispielsweise bei einem Brand. BCM-relevante Sofortmaßnahmen greifen jedoch in der Regel erst ab dem Zeitpunkt, wenn die Mitarbeiter das Gebäude nach einem Brand verlassen haben und beim Sammelpunkt eingetroffen sind. Deswegen sollten die vorhandenen Regelungen und Sofortmaßnahmen dahingehen geprüft werden, welche Inhalte aus anderen Themenfeldern in das BCM einbezogen und dokumentiert werden sollten.

Beispiel:

Hellgrau hinterlegte Zeilen stellen übliche Sofortmaßnahmen der AAO dar, während weiß hinterlegte Zeilen Sofortmaßnahmen des BCM wiedergeben.

Nr.	Aktivität	Zuständig
1	Meldung des Schadensereignisses an Gebäudemanagement (Erstmeldung)	Feststellende Person
2	Fehlersuche und Schadensbegrenzung	Mitarbeiter Gebäudemanagement
3	Rufen eines Wartungs- bzw. Reparaturdienstes,	Mitarbeiter Gebäudemanagement
4	Ermitteln der konkreten Auswirkungen bzw. betroffenen Gebäude(teile)	Mitarbeiter Gebäudemanagement
5	Aktuellen Arbeitsstand der zeitkritischen Geschäftsprozesse prüfen und Aufgaben priorisieren	Führungskräfte der betroffenen OEs
6	Mobile Arbeitsfähigkeit gewährleisten Mitarbeiter des Notfallteams sollen Laptops mitnehmen (Sicherheit geht jedoch vor!) Schlüsselpersonen mit Token ausstatten	Betroffene OE bzw. Führungskräfte
7	Zuständige Meldestelle informieren	Mitarbeiter Gebäudemanagement

Tabelle 41: Beispiel für Sofortmaßnahmen bei einem Gebäudeausfall

Nach Eskalation zu einem Notfall:

Nr.	Aktivität	Zuständig
8	Ausweichstandorte aktivieren und arbeitsfähig machen	Notfallteam Gebäude
9	Sofortigen Umzug auf Ausweichstandorte anordnen	Betroffene OE bzw. Führungskräfte

Tabelle 42: Beispiel für Sofortmaßnahmen bei einem Gebäudeausfall

6.4.4 Definition der Geschäftsordnung des Stabs

Die Arbeitsweise im Stab unterscheidet sich deutlich von der gewohnten Zusammenarbeit im Normalbetrieb aufgrund der deutlich größeren Herausforderungen im Notfall, z. B. hoher Entscheidungs- und Handlungsdruck, gestörte Kommunikationswege, unvollständige oder widersprüchliche Informationen etc.

Eine unklare Rollen- und Aufgabenverteilung im Stab, unklare Mitsprache- und Entscheidungsrechte oder eine unstrukturierte Kommunikation zwischen den Mitgliedern können die Stabsarbeit stark beeinträchtigen. Um dies zu vermeiden, müssen die Regeln für die Stabsarbeit schon in der Notfallvorsorge erarbeitet, abgestimmt und festgelegt werden. Zudem müssen die Rechte und Pflichten der BAO klar und ohne Interpretationsspielraum festgelegt werden, insbesondere dann, wenn sich diese von der normalen Aufbauorganisation unterscheiden.

Mit einer sogenannten **Geschäftsordnung des Stabes** schafft die Institution einen gesicherten Handlungs- und Rechtsrahmen für die Mitglieder des Stabes. Die Geschäftsordnung sollte die Antworten auf die folgenden Fragestellungen dokumentieren:

- Wie setzt sich der Stab personell zusammen (**Personelle Besetzung der BAO**)?
- Wie erfolgt der Übergang von einer AAO in die BAO und wieder zurück (**Konstituierung und Auflösung der BAO**)?
- Wie arbeitet der Stab in einem Not- oder Krisenfall (Zusammenarbeitsmodell)?
- Welche Arbeitsbedingungen werden für die Stabsarbeit geschaffen (Arbeitsbedingungen)?
- Wie werden Entscheidungen und Maßnahmen dokumentiert (Protokollierung)?
- Welche rechtlichen oder finanziellen Rahmenbedingungen gelten für den Stab (Compliance)?
- Wie werden die Vorgaben verbindlich eingehalten (**Verhaltenskodex**)?

Die Geschäftsordnung stellt sicher, dass alle Maßnahmen der BAO, die Verfahren und Verhaltensregeln sowie die Rechte und Pflichten der Rollen präzise festgelegt werden. Der Stab kann dadurch im Notfall seine Arbeit direkt aufnehmen und ist unmittelbar handlungsfähig. Hierbei ist es empfehlenswert, dass der BCMB aufgrund seiner Sachkenntnis einen Vorschlag für die Geschäftsordnung erstellt. Gleichzeitig ist es jedoch auch empfehlenswert, die Leitungsebene und die Stabsmitglieder möglichst frühzeitig mit einzubinden, damit die Geschäftsordnung von allen Beteiligten akzeptiert wird. Die Geschäftsordnung des Stabes kann ein Teil des Notfallhandbuchs sein oder als eigenständiges Dokument behandelt werden.

6.4.4.1 Konstituierung und Auflösung der BAO

Die Konstituierung und Auflösung der BAO markiert den jeweiligen Übergang vom Normal- in den Notbetrieb bzw. vom Not- und Störbetrieb in den Normalbetrieb. Die Konstituierung der BAO schließt sich dem Alarmierungs- und Eskalationsprozess unmittelbar an (siehe Kapitel 6.4.2 *Detektion, Alarmierung und Eskalation*).

In der Geschäftsordnung des Stabes sollte daher auf Basis des Alarmierungsprozesses konkreter geregelt werden, welche Einzelschritte in der Startphase der Bewältigung erforderlich sind, damit die Stabsarbeit im Notfall zeitnah aufgenommen werden kann. Insbesondere sollten Kriterien festgelegt werden, die der Stab nutzt, um final über einen Notfall zu entscheiden.

Beispiel:

- Das Leben und die Gesundheit von Personen ist durch das Ereignis selbst gefährdet.
- Das Leben und die Gesundheit von Personen ist durch die Geschäftsunterbrechung gefährdet.
- Das Ansehen der Institution in der Öffentlichkeit ist gefährdet.
- Der zu erwartende finanzielle Schaden des Ereignisses ist wahrscheinlich hoch, unter Umständen sogar existenzbedrohend (siehe Kapitel 3.1.4 Selbstverpflichtung der Institutionsleitung).
- Es wurde ein bedeutsamer Verstoß gegen Gesetze, Vorschriften oder Verträge festgestellt, der zu Meldepflichten an Dritte oder zu rechtlichen Konsequenzen führen kann.

Die meisten dieser Kriterien können in der Regel anhand der Ergebnisse der BIA beantwortet werden. Liegen noch keine Ergebnisse der BIA vor, dann müssen die genannten Kriterien ad hoc durch den Stab überprüft werden.

Die Institution sollte im Vorhinein Abläufe festlegen, sowohl um einen Notfall auszurufen als auch um ein Ereignis zu deeskalieren. Im Falle eines Schadensereignisses können dann diese Abläufe unmittelbar eingeleitet werden, nachdem der Stab entschieden hat, ob es sich um einen Notfall, eine Krise oder eine Störung handelt. Zudem ist es empfehlenswert, nachfolgende Schritte zu klären:

- Wie erfolgt eine Prüfung der Vollständigkeit, Handlungs- und Entscheidungsfähigkeit des Stabes?
- Wie erfolgt eine erste Lagebesprechung? (z. B. Vorstellung anwesender Personen in Rollen, die vom Normalbetrieb abweichen, oder Regelungen zur Redezeit je Teilnehmer)
- Wie wird über die erforderlichen Mitglieder im Kernteam bzw. hinsichtlich einer situativen Erweiterung des Stabes entschieden?
- Wie wird die finale Entscheidung, ob es sich um einen Notfall handelt, dokumentiert und in der Institution kommuniziert?
- Wer entscheidet, wann die Wiederanlauf- und Geschäftsfortführungspläne (siehe Kapitel 6.9 *Geschäftsfortführungsplanung*) aktiviert werden?
- Unter welchen Voraussetzungen wird die Stabsarbeit beendet und die BAO schrittweise aufgelöst?

Beispiel:

Checkliste zum Konstituieren des Stabes:

- Wie werden die Stabsmitglieder alarmiert?
- Wie wird die Anfahrt und der Zugang zum Stabsraum sichergestellt?
- Wie wird der Ablageort der Ausstattung des Stabsraums dokumentiert, eventuell inklusive Hinweisen zum Zugang?
- Wo und wie wird der Aufbau der Ausstattung des Stabsraums dokumentiert?
- Welche Rollen sind für den Aufbau der Ausstattung des Stabsraums zuständig?
- Wie erfolgt die erste Lagebesprechung durch den Stab?

Checkliste zum Auflösen der BAO:

- Anhand welcher Kriterien entscheidet es sich, wann die letzte Lagebesprechung durchgeführt wird?
- Wann beendet jede Rolle offiziell ihre Mitarbeit in der BAO?
- Wurden alle notwendigen Beschlüsse für den Störbetrieb getroffen?
- Ist die Maßnahmenverfolgung (auch für Aufgaben im Störbetrieb) vollständig dokumentiert bzw. durch wen wird diese in der AAO fortgeführt?
- Ist das Protokoll der Stabsarbeit vollständig, vertraulich und wiederauffindbar abgelegt?
- Wann und durch wen erfolgt der Rückbau des Stabsraums?

6.4.4.2 Festlegung eines Zusammenarbeitsmodells

Damit die Mitglieder des Stabes im Vorfeld die Stabsarbeit schulen und üben sowie im Ernstfall unmittelbar beginnen können, sollte bereits in der Notfallvorsorge ein Weg zur strukturierten Entscheidungsfindung (**Führungszyklus)** definiert werden. Im Themenbereich Unternehmensführung bzw. in der klassischen Führungslehre existieren verschiedene Arten von Führungszyklen und Führungsvorgängen, wovon einige in dem Hilfsmittel *Weiterführende Aspekte zur Bewältigung* beschrieben werden. In der Geschäftsordnung des Stabes sollte dokumentiert werden, welcher Führungszyklus in der BAO der Institution eingesetzt wird. Ferner ist es empfehlenswert, konkret zu definieren, inwieweit bestehende Hierarchiestufen der AAO auch in der Stabsarbeit gelten oder bewusst für die Stabsarbeit außer Kraft gesetzt werden.

6.4.4.3 Festlegung der Arbeitsbedingungen

Die Stabsarbeit erfolgt unter Stress und ist physisch wie psychisch belastend. Zudem endet die Stabsarbeit oft nicht zum Ende eines regulären Arbeitstages. Daher sollten die Möglichkeiten eines Schichtbetriebs für den Stab geprüft, organisatorisch geregelt und in der Geschäftsordnung des Stabes dokumentiert werden. Hierbei müssen die institutionsspezifischen Arbeitszeit- und Überstundenregelungen daraufhin geprüft werden, inwieweit diese im Notfall abweichen oder speziell dafür gesondert geregelt werden können. Abweichende Regelungen für den Notfall müssen vorab mit den relevanten Stellen, wie z. B. der Rechtsabteilung, Personal-bzw. Betriebsrat sowie der Institutionsleitung abgestimmt werden.

In der Stabsarbeit sollten der Wechsel zwischen vorgegebenen Phasen sowie die Taktung von Besprechungen geklärt sein. Diese Aspekte werden unter dem **Führungsrhythmus** zusammengefasst und haben wesentlichen Einfluss auf die Arbeitsbedingungen im Stab. Je nach Situation werden die Arbeitsbedingungen vom Normalbetrieb abweichen, z. B. hinsichtlich der Schichtlänge, Schichtwechsel oder des Bedarfs an Mehrarbeit. Hierzu ist es empfehlenswert die institutionsspezifischen Möglichkeiten und Grenzen vorab zu identifizieren, abzustimmen und im Führungsrhythmus zu berücksichtigen.

Beispiel: Aussagen zu den Arbeitsbedingungen in der Geschäftsordnung

Jedes Mitglied des Krisenstabs hat einen benannten ersten Vertreter, der nach Ende der Schicht oder im Verhinderungsfall dessen Funktion übernimmt. Ist der erste Vertreter verhindert, kann der Leiter des Krisenstabs oder dessen Vertreter eine Person aus der entsprechenden Organisationeinheit in den Krisenstab berufen. Diese Entscheidung muss schriftlich dokumentiert werden.

Die Übergabephase zwischen zwei Schichten erfolgt zu definierten Zeiten, ist kurz und überschaubar zu halten und soll 15 bis 20 Minuten nicht überschreiten. In dieser Zeit sind alle notwendigen und wichtigen Informationen auszutauschen. Dies beinhaltet eine Übersicht über die aktuelle Lage, die getroffenen Entscheidungen und die durchgeführten, eingeleiteten und ausstehenden Maßnahmen.

Die Arbeitsphasen des Stabes orientieren sich an der Kern-Arbeitszeit, sodass ein Wechsel des Personals innerhalb der üblichen Arbeitszeiten ohne Mehrarbeit erfolgen kann. Wenn aufgrund eines länger anhaltenden Notfalls absehbar wird, dass der Stab über die Zehn-Stunden-Arbeitsgrenze hinaus besetzt sein muss, muss geprüft werden, wie viele und welche Mitarbeiter in der darauffolgenden Schicht benötigt werden.

6.4.4.4 Protokollierung

Mit der Protokollierung werden zwei unterschiedliche Zielsetzungen verfolgt: Zum einen dient das Protokoll als Nachweis bei einer möglichen späteren Revision oder Ermittlung zu den Entscheidungen im Stab. Zum anderen ist das Protokoll die Basis für eine Auswertung im Nachgang, um Lücken und Verbesserungspotenziale für das BCMS und die Ereignisbewältigung identifizieren zu können (siehe Kapitel 6.4.8 *Analyse der Bewältigung*). Die formalen Anforderungen an die Dokumentation der Bewältigung, insbesondere an die Protokollierung im Stab sollten in der Geschäftsordnung des Stabes dokumentiert werden.

Beispiel:

Grundsätzlich müssen alle wesentlichen durchgeführten Aktivitäten und Entscheidungen des Stabes protokolliert werden. Die Arbeit im Stab muss dabei so dokumentiert werden, dass im Nachhinein nachvollzogen werden kann, auf welcher Grundlage jede Entscheidung im Stab getroffen wurde und welche Stabsmitglieder an der Entscheidung beteiligt waren. Die Protokollierung kann in elektronischer Form oder in Papierform anhand der zur Verfügung gestellten Protokollvorlage erfolgen.

6.4.4.5 Festlegung besonderer Befugnisse

Die Entscheidungen des Stabes können sich je nach Situation sowohl intern auf die gesamte Institution als auch extern auf Interessengruppen auswirken. Damit die Mitglieder des Stabes die Möglichkeiten und Grenzen ihres Handlungsspielraums kennen, sollte in der Geschäftsordnung geregelt werden, inwieweit Weisungen in die Institution gegeben werden dürfen oder über Geldmittel verfügt werden darf.

Beispiel:

Der Stab darf für den Zeitraum der Bewältigung fachliche Weisungen an alle Organisationseinheiten geben, sofern diese Anweisungen der Gefahrenabwehr, der Verhinderung, Vermeidung oder Reduzierung von (weiteren) Schäden sowie der Rückkehr in den Normalbetrieb dienen. […]

Im Notfall kann der Leiter des Krisenstabs für die Bewältigung notwendige Zahlungen bis zu einer Gesamthöhe von 500.000 € eigenständig veranlassen, wenn dadurch ein höherer Schaden abgewendet werden kann. Darüber hinaus ist die Zustimmung der Institutionsleitung notwendig. […]

Die Haftung der Mitglieder des Stabes ist in Ausübung ihrer Tätigkeit auf Vorsatz und grobe Fahrlässigkeit beschränkt.

Mitglieder des Stabes werden für mögliche Fehlentscheidungen auf Grund der Stabsarbeit in der AAO nicht personalrechtlich belangt.

Hinweis:

In wirtschaftsorientierten Institutionen ist eine Haftungsausschlusserklärung gegenüber dem Leiter des Stabes dringend anzuraten. Davon müssen vorsätzliche Handlungen gegen gesetzliche und institutionsinterne Regularien ausgeschlossen werden.

6.4.4.6 Erstellung eines Verhaltenskodex

Auch wenn die Geschäftsordnung des Stabes die Rahmenbedingungen festlegt und dokumentiert, ist damit nicht sichergestellt, dass in der üblichen Hektik der Bewältigung diese „Spielregeln“ auch eingehalten werden. Zu diesem Zweck sollten die elementarsten Regeln in einem **Verhaltenskodex** zusammengefasst und den Mitgliedern des Stabes während der Stabsarbeit zugänglich gemacht werden (z. B als Aushang).

Der Verhaltenskodex für den Stab fasst die wichtigsten Aspekte der Geschäftsordnung übersichtlich zusammen. Damit unterstützt der Verhaltenskodex den Stab dabei, die vereinbarten Verfahren und Verhaltensregeln während der Stabsarbeit einzuhalten. Im Nachfolgenden wird ein einfaches Beispiel für einen Verhaltenskodex dargestellt. Dies muss von jeder Institution an die eigenen Bedürfnisse und Anforderungen angepasst werden.

Auf Grund der Bedeutung des Verhaltenskodexes für die Zusammenarbeit während eines Notfalls bzw. einer Krise ist es empfehlenswert, diesen im Notfallhandbuch zu dokumentieren. So kann bei unklaren Situationen in der Stabsarbeit jederzeit darauf zugegriffen werden, um sich die getroffenen Vereinbarungen in Erinnerung zu rufen.

Beispiel:

1. Der Stab richtet seine Arbeitsweise anhand der vorliegenden Notfallplanung aus. Liegen keine Notfallpläne vor oder greifen diese nicht, wird die Arbeitsweise am Führungszyklus FOR-DEC ausgerichtet.
2. Der Stab hat Arbeits- und Besprechungsphasen (Lagebesprechungen). Diese müssen eindeutig festgelegt und allen Stabsmitgliedern kommuniziert werden.
3. **Lagebesprechungen**
   - dauern nie länger als 30 Minuten,

- brauchen immer einen Moderator (der nicht gleichzeitig den Stab leitet),
- dürfen ihren Fokus nicht durch Einzeldiskussion zu Spezialthemen verlieren (diese Diskussionen können im Nachgang geklärt werden),
- müssen immer eindeutig beendet werden sowie
- müssen immer zeitlich klar terminiert und angesagt werden.

4. Jedes Stabsmitglied hat das gleiche Mitsprache-Recht. Es gilt für alle eine **maximale Redezeit** von 3 Minuten.
5. Es muss immer ein **Protokoll** geführt werden, aus welchem die Meldungen bzw. Ereignisse und Beschlüsse des Stabes mit den notwendigen Angaben zu Ort, Zeit und Status nachvollziehbar dokumentiert werden. Im Protokoll muss zudem erfasst werden, wer wann anwesend war.
6. Fakten müssen von Gerüchten getrennt und Informationen immer verifiziert werden. In komplexen Lagen sollte dazu ein **Informationsmanagement** aufgebaut werden.
7. Die **Visualisierung** sollte regelmäßig genutzt und aktualisiert werden.
8. Aufgaben müssen klar benannt, terminiert und delegiert werden (Zielstellung, Aufgabenstellung, Zuständigkeiten, Umsetzungsfrist bzw. Wiedervorlage). Darüber hinaus werden sie im **Aufgabenmanagement** festgehalten.
9. Damit allen anwesenden Personen bewusst ist, wer welche Rolle oder Funktion in der BAO einnimmt, muss sich jeder in der ersten Lagebesprechung mit Namen und Rolle bzw. Funktion vorstellen. Dies wird wiederholt, wenn neue Mitglieder hinzustoßen.

6.4.5 Herstellung der Fähigkeit zur Stabsarbeit

Für eine funktionierende Bewältigung ist es wichtig, dass die in den vorherigen Schritten geschaffenen organisatorischen Voraussetzungen durch die BAO-Rolleninhaber verstanden und verinnerlicht werden. Daher müssen die Stabsmitglieder hinsichtlich der geschaffenen BAO-Strukturen und ihrer Aufgaben für den Notfall **geschult** werden. Die Stabsmitglieder müssen nicht nur theoretisches Wissen erwerben, sondern möglichst auch eigene Erfahrungen in geschützter Umgebung sammeln, wie Stabsarbeit in der Praxis funktioniert. Dies kann am besten über Trainings und Übungen erreicht werden.

Zudem sollte geregelt werden, wie die **Lagebeobachtung und -visualisierung** im Stab erfolgt. Über diese wird sichergestellt, dass alle Mitglieder des Stabes einen Überblick zur aktuellen Situation erhalten und den jeweiligen Sachstand kennen oder nachverfolgen können.

Um die getroffenen Entscheidungen und Maßnahmen zum jederzeitigen Nachlesen sowie für eine spätere Analyse der Bewältigung (siehe Kapitel 6.4.8 *Analyse der Bewältigung*) dokumentieren zu können, müssen Vorgaben zur **Protokollierung** getroffen werden. Außerdem muss festgelegt werden, in welchem **Raum** und mit **welcher Ausstattung** die Stabsarbeit stattfindet, damit diese Infrastruktur im Notfall verfügbar und einsatzbereit ist.

Die nachfolgenden Kapitel beschreiben die wesentlichen Schritte zur

- Schulung der BAO,
- Festlegung der Vorgaben an die Protokollierung,
- Festlegung eines Stabsraums,
- Ausstattung des Stabsraums sowie
- Freigabe durch die Institutionsleitung.

Weitere Informationen, wie diese Grundlagen praktisch umgesetzt werden können, sind in dem Hilfsmittel *Weiterführende Aspekte zur Bewältigung* beschrieben.

6.4.5.1 Schulung der BAO

Alle Stabsmitglieder, einschließlich der Stellvertreter, müssen für ihre Aufgaben und Zuständigkeiten im Notfall befähigt werden. Der Schulungsbedarf ist maßgeblich davon abhängig, durch welche Personen die jeweiligen Rollen der BAO besetzt werden (siehe Kapitel 6.4.1.6 *Personelle Besetzung der BAO*).

Insbesondere bei unerfahrenen Personen, die ihre Rolle erst verinnerlichen müssen, sollten zunächst die theoretischen Grundlagen der Notfallbewältigung geschult werden. Die **Grundlagenschulung** sollte folgende Aspekte beinhalten:

- In welchen Phasen läuft eine Notfallbewältigung ab?
- Warum gibt es eine BAO?
- Wie interagieren die verschiedenen Rollen in der BAO miteinander?
- Welche Rollen übernehmen die zu schulenden Personen darin?

Wenn Personen erfahren sind oder die Grundsätze der Notfallbewältigung und der Besonderheiten einer BAO kennen, ist es empfehlenswert, die **Methoden und Regeln der Stabsarbeit** für die Institution zu entwickeln, bevor die Stabsmitglieder darin geschult und trainiert werden. So wird sichergestellt, dass die Stabsmitglieder genau die Methoden und Abläufe verinnerlichen, die auch in der Institution angewendet werden sollen.

Weiter ist es empfehlenswert, verschiedene Schulungen für Stabsmitglieder anzubieten, die sich am jeweiligen Erfahrungsstand orientieren, z. B.:

- Schulung zu den institutionsspezifischen Aspekten der Notfallbewältigung und Stabsarbeit für neue Stabsmitglieder
- rollenspezifische, praktische Trainings für einzelne Rollen innerhalb des Stabes (z. B. Visualisier, Protokollanten)

Das **praktische Training zur Stabsarbeit** kombiniert inhaltliche und methodische Aspekte der Stabsarbeit. Ziel des Trainings ist es, dass die Rolleninhaber ihre individuellen Aufgaben verstehen und die für ihre Aufgaben festgelegten Methoden und das Notfallhandbuch sicher anwenden können. Im Training werden die rollenspezifischen Aufgaben detaillierter erläutert und im Rahmen kurzer Trainingsszenarien durch die Teilnehmer praktisch angewendet. Entsprechend sollte das Training durch einen erfahrenen Trainer für Stabsarbeit moderiert und geleitet werden.

Hinweis:

Gerade, wenn sich das BCMS noch im Aufbau befindet, liegen häufig noch nicht ausreichend eigene Erfahrungen und Kenntnisse vor, um Schulungen, Trainings und Übungen selbstständig vorzubereiten und durchzuführen. In diesem Fall empfiehlt es sich, externe Fachexperten einzubeziehen oder Seminarangebote zu nutzen.

Mögliche weiterführende Schulungen und praktische Trainings, unter anderem zur Protokollierung, zur Visualisierung, zum Aufgabenmanagement sowie zur „Führung im Notfall“, sollten nach Bedarf zusätzlich eingeplant werden.

Im Anschluss an diese Schulungen sollte eine Stabsübung durchgeführt werden, um das erlangte Wissen zu vertiefen und praktische Erfahrungen aufzubauen. Die hierzu erforderlichen Schritte sind im Kapitel 6.11.3.2 *Stabsübung* beschrieben.

In der weiteren Entwicklung des BCMS können sich einzelne Aspekte zur Stabsarbeit verändern bzw. weiter konkretisieren. Daher sollten die Schulungsinhalte für die Stabsmitglieder regelmäßig geprüft und angepasst werden.

Für die weiteren Mitglieder der BAO, wie z. B. die Notfallbewältigungsteams, sollten ebenfalls regelmäßig spezifische Schulungen und Awareness-Veranstaltungen durchgeführt werden (siehe Kapitel 3.2.5 *Schulung sowie 3.2.6 Sensibilisierung*). In der Schulung sollten nicht nur allgemein das BCM der Institution, sondern auch die Abläufe im Notfall erläutert werden. Darüber hinaus sollten die Aufgaben im Rahmen der BAO erörtert werden. Ergänzend dazu sollten alle Mitglieder der BAO mindestens ein Mal in drei Jahren an einer Übung teilnehmen, in der sie ihre jeweiligen Aufgaben im Notfall trainieren können (siehe Kapitel 6.11 *Üben und Testen*).

6.4.5.2 Lagebeobachtung und -visualisierung

Notfälle und Krisen sind dadurch gekennzeichnet, dass sich die aktuelle Lage laufend verändert. Hierbei gibt es erwünschte Lageänderungen, z. B. aufgrund eingeleiteter Notfallmaßnahmen sowie unerwünschte Lageänderungen, z. B. aufgrund einer Eskalation des Ereignisses infolge nicht wirksamer Gegenmaßnahmen.

Lageänderungen können darüber hinaus aus neu gewonnenen Erkenntnissen heraus entstehen, z. B. weil Ursachen des Ereignisses ermittelt wurden. Lageänderungen können auch zu neuen Herausforderungen in der Bewältigung führen, z. B. weil das Ereignis extern bemerkt wurde.

Mithilfe der Lagebeobachtung werden diese Veränderungen der Lage schnell erfasst, sodass darauf reagiert werden kann, z. B. indem angepasste oder neue Notfallmaßnahmen abgeleitet und umgesetzt werden.

Für eine effektive **Lagebeobachtung** sollten die folgenden Punkte vorab festgelegt werden:

- zuständige Rollen in der Lagebeobachtung
- Schwerpunkte der Lagebeobachtung, z. B.
  - bisher umgesetzte Sofortmaßnahmen
  - bekannte Fakten zum Ereignis
  - jegliche, bisher ergriffene Maßnahmen und deren Wirksamkeit
- Mögliche Quellen der Lagebeobachtung, z. B.
  - Informationen der Stabsmitglieder oder Notfallbewältigungsteams
  - Medienmonitoring (siehe Kapitel 5.11.6.3 Externe Kommunikation)

Die **Lagevisualisierung** hat das Ziel, eine einheitliche und schnelle Übersicht über die Lage zu geben und den Stab bei Lagebesprechungen sowie bei der Schichtübergabe zu unterstützen. Grundsätzlich gilt: Je mehr in der Stabsarbeit visualisiert wird, desto besser ist das gemeinsame Lagebild des Stabes. Folgende Elemente zur Lagevisualisierung sollten vorab geplant werden:

- Wie wird visualisiert (Medium und Detailgrad)
- fortlaufendes Lagebild (z. B. eingehende Meldungen, grafische Übersichten zum Schadensereignis, Zeitstrahl)
- Übersicht aller Aufgaben mit Status und Priorisierung (Aufgabenmanagement)
- Besetzung des Stabes (z. B. mit Schichtplan)
- Übersicht zur internen und externen **Notfallkommunikation**

Abbildung 46 veranschaulicht exemplarisch die Visualisierung eines fortlaufenden Lagebildes anhand eines Zeitstrahls.

Beispiel:

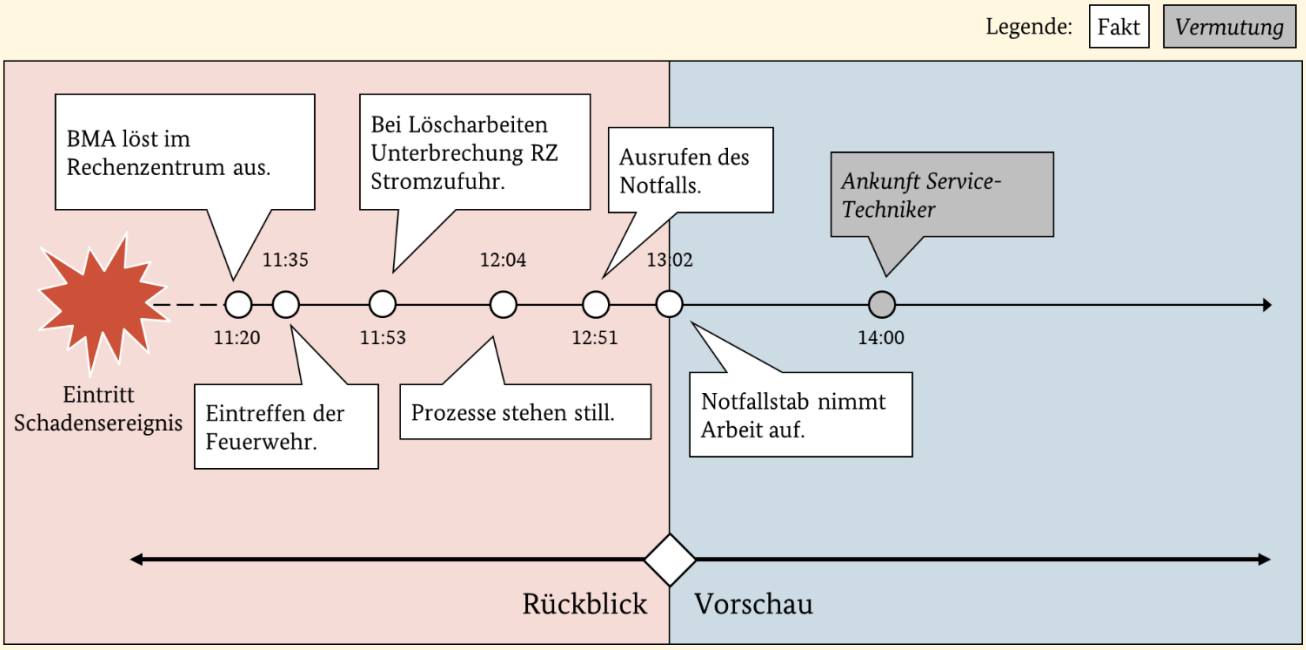

Abbildung 46: Beispiel eines Zeitstrahl zur Visualisierung von Ereignissen

Es sollten bevorzugt gesicherte Informationen visualisiert werden. Vermutungen und Annahmen müssen als solche kenntlich gemacht werden. Falls die Rolle Visualisierer eingesetzt wird, sollte diese für die Elemente zur Lagevisualisierung ausführlich geschult werden. Dabei sollte auch gemeinsam mit dem Leiter des Stabes besprochen werden, wie mit dem Stab und der Protokollierung zusammengearbeitet werden soll. Wird keine separate Rolle Visualisierer eingesetzt, sollten alle Mitglieder des Kernteams mit den Grundsätzen der Lagevisualisierung vertraut gemacht werden.

6.4.5.3 Festlegung eines Stabsraums

Eskaliert ein Ereignis zu einem Notfall werden die Mitglieder des Stabes umgehend informiert und treffen sich an einem zuvor festgelegten Ort, dem Stabsraum. Der Stabsraum dient dem Stab als Arbeitsumgebung, an die besondere Anforderungen gestellt werden die im Nachfolgenden näher erläutert werden

Hinweis:

Je nach dem Bedarf und den baulichen Möglichkeiten der Institution kann es sich bei einem Stabsraum um genau einen Raum handeln oder verschiedene Bereiche umfassen. Verschiedene Bereiche bieten sich an, um die Arbeits-, Ruhe- und Besprechungsphasen örtlich voneinander zu trennen. Nachfolgend wird nur von Stabsraum gesprochen, ohne die Anzahl an Bereichen konkret festzulegen.

Erreichbarkeit und Zutritt

Da Zeit in einem Notfall von essenzieller Bedeutung ist, ist es wichtig, dass der Stabsraum von allen Mitgliedern des Stabes in einem angemessenen Zeitraum erreichbar und auch außerhalb der üblichen Arbeitszeiten jederzeit für diese zugänglich ist. Hierzu muss geprüft werden, welche Zutrittsregelungen bestehen oder benötigt werden. Die Stabsmitglieder sowie ihre Stellvertreter müssen mit den entsprechenden Zutrittsmitteln und -rechten für alle notwendigen Räumlichkeiten ausgestattet sein. Da eine Lageänderung im Notfall jederzeit zu einer situativen Erweiterung des Stabes führen kann, sollten die Zutrittsregelungen für neue Mitglieder des Stabes zeitnah erweitert werden können. Anhand von Begehungen oder Stabsübungen sollte überprüft werden, ob der Stabsraum für alle Mitglieder jederzeit zugänglich ist, damit es im Notfall nicht zu unnötigen Verzögerungen kommt.

Verfügbarkeit

Eine Grundanforderung an den Stabsraum ist, dass dieser im Notfall verfügbar ist. Dies kann dadurch erreicht werden, dass ein Raum als dedizierter Stabsraum festgelegt wird und damit allein für diesen Zweck zur Verfügung steht. Aufgrund mangelnder räumlicher Ressourcen und fehlender finanzieller Mittel kann ein Stabsraum häufig jedoch nicht dauerhaft für diesen Zweck allein vorgehalten werden, sondern wird als Besprechungsraum oder Ähnliches im Tagesbetrieb genutzt. In diesem Fall muss durch entsprechende organisatorische Regelungen sichergestellt werden, dass in einem Notfall der Einsatz als Stabsraum immer Vorrang hat und anderweitig geplante Einsatzzwecke, wie Besprechungen oder Veranstaltungen, gegebenenfalls verdrängt werden. Außerdem sollte verhindert werden, dass der Raum bei Zweitnutzung zu stark verändert oder wichtige Ausstattung entfernt wird.

Ein weiterer Aspekt der Verfügbarkeit ist das Szenario, dass der Stabsraum vom Schadensereignis selbst betroffen ist und damit nicht wie vorgesehen genutzt werden kann. Aus diesem Grund sollte ein alternativer Raum an einem Ausweichstandort definiert werden. Dies kann z. B. ein ähnlicher Raum in einem Gebäude mit ausreichendem Abstand sein, aber auch ein Konferenzcenter, ein Hotelbesprechungsraum etc. Der Ausweichstandort sollte möglichst vergleichbare Gegebenheiten bieten wie der Haupt-Stabsraum. Zudem ist es empfehlenswert, dass ein Stabsraum gegen Ausfälle der Grundversorgung (z. B. Strom, Wasser, Wärme) abgesichert wird, z. B. durch eine eigene Notstromversorgung.

Liegen keine geeigneten alternativen Räume vor oder erlaubt die Lage keine physische Zusammenkunft der Stabsmitglieder, kann eine Sekundärlösung auch aus einer virtuellen Arbeitsumgebung bestehen, die z. B. über ein Webkonferenz- oder ein Krisenmanagement-Tool bereitgestellt wird. Hierbei müssen die Anforderungen an die Informationssicherheit, d. h. die Verfügbarkeit, Vertraulichkeit und Integrität der Informationen, in der Planung mitberücksichtigt werden.

Größe und Aufteilung

Die Größe des Stabsraums sollte nicht zu knapp bemessen sein, da keine genaue Vorhersage über die Anzahl der Stabsmitglieder gemacht werden kann, die für ein bestimmtes Notfallereignis hinzugezogen werden. Es ist empfehlenswert, dass der Raum über ausreichend Arbeitsplätze, über Bereiche für Visualisierungstechnik und über abgetrennte Besprechungszonen verfügt.

Einhaltung von Sicherheitsanforderungen

Für alle definierten Stabsräume muss sichergestellt werden, dass die geltenden Sicherheitsanforderungen der Institution eingehalten werden. Ein Beispiel hierfür betrifft den Umgang mit vertraulichen Informationen. Die Sicherheitsanforderungen müssen sowohl bei der Planung als auch im späteren Betrieb der Stabsräume eingehalten werden.

6.4.5.4 Ausstattung des Stabsraums

Neben den räumlichen Anforderungen an den Stabsraum ist es im Notfall entscheidend, dass dieser mit allen erforderlichen Materialien und der erforderlichen Technik ausgestattet ist, damit der Stab schnell arbeitsfähig ist. Daher muss der Ausstattungsbedarf für den Stabsraum vorab ermittelt, durch die Institutionsleitung freigegeben (siehe Kapitel 6.4.5.5 *Freigabe durch die Institutionsleitung*) sowie durch die zuständigen Organisationseinheiten beschafft werden. Die Ausstattung sollte regelmäßig auf ihre Vollständigkeit, Aktualität und Funktionsfähigkeit hin überprüft werden. Dies gilt insbesondere, wenn der Stabsraum im Normalbetrieb anderweitig genutzt wird. Die notwendige Ausstattung für die Notfallbewältigung lässt sich in die folgenden Kategorien unterteilen:

- Kommunikationsausstattung
- Visualisierungsausstattung
- Battleboxen mit BCM-Equipment und -Dokumentation (siehe Hilfsmittel *Weiterführende Aspekte zur Bewältigung*)

Kommunikationsausstattung

Der Raum, in dem der Stab sich bespricht, sollte weitgehend frei von Kommunikationsausstattung gehalten werden. Zum einen handelt es sich um einen Raum, der im Schwerpunkt für die Besprechungsphasen des Stabes genutzt wird, in denen keine ständige Kommunikation nach außen notwendig ist. Zum anderen stört jede Kommunikation, egal ob Telefongespräche oder die Bearbeitung von E-Mails, die konzentrierte Arbeitsumgebung. Es ist jedoch empfehlenswert, ein zentrales Konferenztelefon („Telefonspinne“) als Grundausstattung im Stabsraum vorzuhalten. Hiermit können Mitglieder des Stabes oder Fachexperten, die nicht vor Ort sind, telefonisch zu den Besprechungen hinzugezogen werden. Zudem ist es hilfreich ein Notfall-Laptop vorzuhalten, welches autark funktioniert und auf dem unter anderem die BCM-Dokumentation hinterlegt ist. Je nach eingesetzter Methodik zur Dokumentation und Visualisierung kann es erforderlich sein, weitere Laptops oder PC-Arbeitsplätze vorzusehen.

Im Gegensatz zu der stark reduzierten Kommunikationsausstattung des Stabsraums sollte ein zusätzlicher Raum in der Nähe dauerhaft mit allen etablierten Kommunikationskanälen ausgestattet sein. Dieser sollte entsprechend vorbereitet werden. Dazu zählen:

- Telefonie (mehrere Leitungen, unter Umständen auch Videotelefonie)
- E-Mail (z. B. durch vorbereitete Funktionspostfächer für einzelne Rollen)
- Fax
- Funk, Satellitentelefonie oder kryptografische Kommunikationsinfrastruktur

Dieser Raum sollte ebenfalls die räumlichen Anforderungen an die Verfügbarkeit und Sicherheit erfüllen, wie der Stabsraum selbst. Falls ein zweiter Raum aus wirtschaftlichen oder anderen Gründen nicht bereitgestellt werden kann, kann auch der Stabsraum entsprechend ausgestattet werden. In diesem Fall sollte in der Stabsarbeit strikt zwischen Besprechungsphasen ohne Außenkommunikation und Arbeitsphasen, in denen die Kommunikation aus dem Stab heraus erfolgt, unterschieden werden. Eingehende Meldungen und Anrufe während einer Besprechungsphase sollten entsprechend durch die Stabsassistenz angenommen werden.

Hinweis:

Bei der Planung muss unbedingt auf Ausfallsicherheit und Redundanz der Ausstattung geachtet werden, damit die Notfallbewältigung nicht durch den Ausfall eines Kommunikationsmittels zusammenbricht. Dies kann z. B. neben dem normalen Telefon ein Notfallhandy oder ein Laptop mit SIM-Karte sein.

Visualisierungsausstattung

Im Stabsraum sollten ausreichende und geeignete Materialien zur Visualisierung der Lage, also für das *Lagebild*, vorgehalten werden. Neben ortsfesten Materialien, wie Beamern, digitalen Tafeln, Monitoren und Whiteboards sollte auch folgende Ausstattung im Vorfeld beschafft werden:

- Moderationskoffer mit Visualisierungsflächen (z. B. Flipcharts)
- Vorlagen, um unter anderem folgende Inhalte darzustellen (nicht abschließende Aufzählung)
  - Stand der Visualisierung (Datum, Uhrzeit)
  - nächste Sitzung (Datum, Uhrzeit, Gäste)
  - Kartenmaterial (Gebietskarte, Werkgelände etc.)
  - Aufgabenliste (Was? Durch wen? Bis wann?)
  - Zeitstrahl (bisherige Ereignisse und Prognose im fortlaufenden Lagebild)
  - Schadensübersicht und -schwerpunkte (Wo? Wann? Was und wer?)
  - Besetzung der BAO (falls erforderlich mit Schichtplan)
  - Kommunikationsübersicht (Was? Wer? Wann? Mit wem?)

Battlebox

Im Rahmen der Stabsarbeit greifen die verschiedenen Rollen auf unterschiedliche Pläne, Checklisten und Hilfsmittel zurück, insbesondere auf das Notfallhandbuch. Sämtliche für den Notfall relevante BCM-Dokumentation sollte daher einerseits im Stabsraum und andererseits zentral zugänglich vorgehalten werden. So bleibt sie auch verfügbar, z. B. bei physischer Zerstörung des Stabsraums, der Dokumentation an sich oder des Notfall-Laptops. Diese doppelte Vorhaltung kann z. B. durch weitere physische oder digitale Kopien erfolgen. Hierbei muss auf Aktualität und die Anforderungen der Informationssicherheit und des Datenschutzes geachtet werden. So müssen papierhafte Dokumente bei jeder Aktualisierung der Dokumentation neu ausgedruckt und an den Ablageorten ausgetauscht werden. Andererseits sind sie auch ohne Vorhandensein von Strom oder IT verfügbar und einsetzbar. Elektronische Informationen haben wiederum den Vorteil, dass sie schneller aktualisiert bzw. ausgetauscht werden können. Ergänzend zur oben genannten BCM-Dokumentation kann es hilfreich sein, eine Checkliste im Stabsraum zu hinterlegen, die erläutert, wie die Materialien und Technik in Betrieb genommen und genutzt werden. Zusätzlich dazu können die Checklisten im Anhang des Notfallhandbuchs hinterlegt werden, damit im Bedarfsfall eine Kopie verfügbar ist.

Beispiel:

Die Checkliste „Einrichtung des Stabsraums“ kann im Detail beschreiben, welche Tätigkeiten erforderlich sind und wer dafür zuständig ist.

Mögliche Tätigkeiten können sein:

- Raum aufschließen und lüften
- Visualisierungsflächen vorbereiten, wie z. B. Maßnahmenverfolgung oder Ereigniszeitstrahl
- Tische und Stühle U-förmig in Richtung Visualisierungsflächen aufstellen
- Namenskarten entsprechend des Sitzplans aufstellen
- BCM-Dokumentation sortiert nach den Rollen im Raum verteilen
- Telefonkonferenzschaltung bereitstellen
- Kommunikationsmittel und Technik auf Einsatzfähigkeit testen
- Verpflegung und Getränke bereitstellen

6.4.5.5 Freigabe durch die Institutionsleitung

Die erarbeiteten, abgestimmten und dokumentierten Aspekte zur Stabsarbeit sowie die zur Alarmierung und Eskalation (siehe Kapitel 6.4.2 *Detektion, Alarmierung und Eskalation*) sollten der Institutionsleitung vorgestellt und durch diese freigegeben werden. Dies stellt sicher, dass die Institutionsleitung Einfluss auf diese wichtigen Aspekte der Notfallbewältigung nehmen und die erforderlichen personellen und finanziellen Ressourcen freigeben kann. Insbesondere die zentrale Entscheidungsinstanz im Alarmierungsprozess muss durch die Institutionsleitung freigegeben werden, da sie Handlungs- und Entscheidungsbefugnisse auf den Stab übertragen kann, die im Normalbetrieb der Institutionsleitung vorbehalten sind.

6.4.6 Notfallkommunikation

Wie die Institution im Notfall wahrgenommen wird und ob Vertrauen in die Notfallbewältigung gesetzt wird, hängt im Wesentlichen auch davon ab, wie gut die Notfallkommunikation gelingt. Daher muss die Notfallkommunikation im Vorfeld gut vorbereitet und geplant werden. Dabei ist es wichtig, dass in der Institution präventiv überlegt wird, wann Meldungen an die Mitarbeiter und an externe Interessengruppen erforderlich sind, um Reputationsschäden zu vermeiden. Zudem sollte in der externen Notfallkommunikation das Kommunikationsgeschehen überwacht und analysiert (**Medienmonitoring**) sowie gesteuert werden. Die eigenen für extern bestimmten Informationen sollten darauf abgestimmt sein.

Geschäftspartner müssen beispielsweise über Stornierungen informiert werden oder Kunden über Zeitverzögerungen bei der Lieferung bestellter Waren. Auch die Kommunikation zu Polizei, Feuerwehr und Rettungsdiensten gehört dazu, sofern die Art des Notfalls deren Einsatz verlangt.

6.4.6.1 Allgemeine Regelungen zur Kommunikation

Aus den zuvor genannten Gründen ist die Notfallkommunikation einer der zentralen Erfolgsfaktoren in der Notfallbewältigung. Sowohl die interne als auch externe Kommunikation bedarf einer systematischen Vorbereitung. Für die Rolle Kommunikation sollten im Vorhinein verbindliche Regeln für folgende Aufgaben definiert werden:

- interne Kommunikation (Was dürfen oder müssen die Mitarbeiter wann erfahren?)
- externe Kommunikation durch Mitarbeiter (Was dürfen die Mitarbeiter wann und wie gegenüber der Presse und in sozialen Medien äußern und was nicht?)
- externe Kommunikation durch Rolle Kommunikation (Was soll die Rolle Kommunikation wann und wie gegenüber der Presse und in sozialen Medien bekannt geben?)
- Regelungen für den Kontakt mit Polizei und anderen Behörden sowie Hilfsorganisationen
- Meldepflichten der Institution, die sich aus einem Notfall ergeben
- Regelungen zum Medienmonitoring

Um im Notfall alle Interessengruppen auf geeignetem Weg und innerhalb einer angemessenen Zeit zu erreichen, müssen die Möglichkeiten zur Kommunikation bekannt und die Kommunikationstechnik einsatzbereit sein. Dies umfasst:

- Ausfallsicherheit der Kommunikationsmittel (z. B. Notstrom)
- Redundanz der Kommunikationsmittel (z. B. Ersatz-TK-Anlage)
- Schutz der vertraulichen Kommunikation
- Eingrenzung und Aktualität der Nutzungsberechtigungen

Ferner sollten die anzuwendenden Kommunikationskanäle (z. B. Telefon, E-Mail, Chat, Webseiten, Fax) und Medienformate (z. B. Pressemitteilung, Pressekonferenz, Stellungnahme auf der Webseite oder über soziale Medien) vorab festgelegt werden. Sofern innerhalb der Institution mehr als eine Person für die Notfallkommunikation zuständig ist, müssen die jeweiligen Aufgaben und Zuständigkeiten innerhalb des Notfallkommunikationsteams festgelegt und dokumentiert werden, damit diese Arbeit effektiv koordiniert werden kann.

6.4.6.2 Interne Kommunikation

Eine kontinuierliche interne Notfallkommunikation ist entscheidend, um während eines Notfalls die Unsicherheit unter den Mitarbeitern so weit wie möglich zu minimieren. Eine sachliche interne Notfallkommunikation erhöht das allgemeine Vertrauen in die Institutionsleitung und die BAO, dass diese die Situation kontrollieren können. Wenn die Mitarbeiter frühzeitig und angemessen in die Notfallbewältigung einbezogen werden, steigt deren Bereitschaft, erforderliche Maßnahmen umzusetzen und mit Informationen sorgsam umzugehen.

Es ist oft nicht notwendig, dass die Mitarbeiter jedes Detail des Notfallereignisses kennen. Falls eine Information jedoch die persönliche Situation oder die persönliche Sicherheit betrifft, sollte diese in jedem Fall kommuniziert werden. Zudem sollten relevante Informationen im Zusammenhang mit dem Status der Notfallbewältigung insbesondere für diejenigen Mitarbeiter bereitgestellt werden, die in Kontakt mit externen Interessengruppen stehen, z. B. mit Kunden, Behörden oder Dienstleistern.

Hinweis:

In der Praxis hat es sich bewährt, dass alle Mitarbeiter zeitlich mindestens dieselben Informationen erhalten wie die allgemeine Öffentlichkeit. Das bedeutet, dass die Informationen aus der externen Notfallkommunikation zeitgleich oder früher intern kommuniziert werden sollten. Somit wird vermieden, dass Mitarbeiter erst durch Medien über das Notfallereignis selbst oder über Neuigkeiten in dessen Zusammenhang erfahren und sich dadurch vernachlässigt fühlen. Außerdem wird Gerüchten und Mutmaßungen vorgebeugt. Gleichzeitig gilt: Informationen, die auf keinen Fall nach außen kommuniziert werden dürfen, sollten in der Regel auch nicht intern an alle Mitarbeiter kommuniziert werden.

6.4.6.3 Externe Kommunikation

In jedes Notfallszenario sind diverse Interessengruppen direkt oder indirekt involviert. Die Institution muss sämtliche Interessengruppen berücksichtigen. Typische Beispiele hierfür sind Journalisten, Medien, Kunden, Dienstleister, Aufsichtsbehörden, Polizei und Angehörige von Mitarbeitern.

Die externe Kommunikation hat die Aufgabe, alle relevanten externen Interessengruppen adressatengerecht und unter Beachtung der Grundsätze für die Notfall- und Krisenkommunikation zu informieren. Oberstes Ziel ist es, die Kommunikation zu kontrollieren, um Reputationsschäden zu minimieren.

Im Vergleich zur internen Kommunikation erfordert die externe Kommunikation eine intensive Analyse der relevanten Interessengruppen und eine Planung der jeweiligen Kommunikationsstrategie sowie die Erstellung eines Kommunikationskonzeptes. Detailliertere Informationen dazu können im Hilfsmittel *Weiterführende Aspekte zur Bewältigung* nachgeschlagen werden.

Tabelle 43 zeigt ein vereinfachtes Beispiel für ein wichtiges Element des Kommunikationskonzeptes: Die adressatenspezifische Information der relevanten Interessengruppen (siehe auch Kapitel 6.1.1 *Identifizierung von Anforderungen an das BCMS*).

Beispiel:

Priorität	Interessengruppe	Kommunikationsbedarf im Notfall	Kommunikationswege	Zuständig
1	Kunden	Bei direkter Betroffenheit	Website Telefon	Kundenservice
2	Öffentlichkeit und Medien	Individuelle Strategie zur Notfallkommunikation ist abhängig vom jeweiligen Schadensszenario und dem Interesse der Öffentlichkeit	Pressemitteilung Website Soziale Medien Interview/Gespräch Pressekonferenz	Pressesprecher, Leiter Kommunikation
3	Versicherungen	Versicherter Schadensfall	Telefon Mail bzw. Brief	Leiter Recht
4	Dienstleister und Lieferanten	Bei direkter Betroffenheit	Telefon Mail	Leiter Kommunikation

Tabelle 43: Externe Kommunikation mit Interessengruppen

Für die externe Notfallkommunikation bieten sich z. B. folgende Kanäle an, sofern verfügbar:

- E-Mail
- Telefon
- Notfall-Hotline
- Website der Institution mit Informationen über den Notfall und FAQs
- alternative Notfall-Website („Dark Site“)
- Public Relations Agentur
- Soziale Medien
- persönliches Interview
- Fernseh- oder Radio-Interview
- Pressemitteilung
- Pressekonferenz

Für mögliche Presseanfragen sollte eine Person sowie ein Stellvertreter als Notfallsprecher namentlich benannt und innerhalb der Institution sowie extern veröffentlicht werden. Dies stellt eine einheitliche und offizielle externe Kommunikation sicher.

Die externe Notfallkommunikation begrenzt sich nicht auf die einseitige Kommunikation der Institution mit Dritten sowie der Öffentlichkeit, sondern sollte auch die Kommunikation Dritter untereinander betrachten. Dies betrifft vor allem die Medienberichterstattung. Notfälle, die durch die Medien aufgegriffen werden, können eine kritische Berichterstattung nach sich ziehen, die sich schnell verbreiten kann und durch Diskussionen in sozialen Medien weiter verschärft wird.

Im Notfall sollten Medien daher zum Schutz der Reputation der Institution stetig beobachtet werden Relevante Meldungen über die Institution in Bezug auf das Ereignis können dann zeitnah ausgewertet werden. Nur so kann die Institution bei Bedarf frühzeitig kommunikative Gegenmaßnahmen einleiten.

6.4.7 Störbetrieb und Deeskalation

Ist das Schadensereignis überwunden, sollte der Stab den Notfall offiziell für beendet erklären und diese Entscheidung innerhalb der Institution kommunizieren. Hierzu können die gleichen Kommunikationskanäle verwendet werden wie beim Ausrufen des Notfalls. Dies stellt sicher, dass allen Beteiligten und Betroffenen bewusst ist, dass nun wieder die regulären Prozesse im Normalbetrieb greifen.

Störbetrieb

Abhängig von der Art und dem Ausmaß des Schadensereignisses kann es sein, dass zwar die Ursachen und Auswirkungen des Ereignisses vollständig unter Kontrolle gebracht wurden, aber noch kein Normalzustand für die zeitkritischen Prozesse erreicht ist. Die Institution befindet sich übergangsweise im sogenannten Störbetrieb, der dadurch gekennzeichnet ist, dass die Wiederherstellungsmaßnahmen oder Nacharbeiten noch nicht abgeschlossen sind, sodass noch nicht von einem Normalbetrieb gesprochen werden kann.

Beispiel:

Ein Gebäude kann je nach Schadensszenario teilweise, z. B. etagenweise, wiederhergestellt werden. Der Normalbetrieb kann darüber schrittweise erreicht werden. In dieser Zeit befindet sich jedoch die Institution im Störbetrieb, bis das ganze Gebäude wiederhergestellt ist.

Ein IT-System muss inklusive der Daten vollständig wiederhergestellt sein, bevor der Normalbetrieb erreicht werden kann. Innerhalb des Notbetriebs wurde auf einem Ersatzsystem gearbeitet. Eine notwendige Maßnahme innerhalb des Störbetriebs ist es, die Daten vom Ersatzsystem auf das wiederhergestellte Hauptsystem einzuspielen.

Hierzu kann eine Checkliste mit konkreten Prüfpunkten oder zu treffenden Entscheidungen für die Rückführung in den Normalbetrieb entwickelt werden. Neben den direkt ersichtlichen Aspekten, wie z. B. der Reihenfolge der wieder in den Normalbetrieb zu versetzenden Geschäftsprozesse, sollten auch die durch den Notbetrieb entstandenen Folgen betrachtet werden.

Beispiel: Checkliste zur Rückführung in den Normalbetrieb

- Wie und wann wird die BAO aufgelöst und in die normale AAO überführt?
- Welche Arbeitsrückstände sind institutionsweit entstanden und wie können diese am besten abgearbeitet werden?
- Durch wen erfolgt die interne und externe Kommunikation für die Dauer des Störbetriebs?
- Wie, durch wen und in welchen zeitlichen Intervallen werden die Mitarbeiter über den Fortschritt der Rückführung in den Normalbetrieb informiert?
- An wen sollen die Organisationseinheiten in dieser Zeit ihre Erkenntnisse und Fortschritte melden? Gemeldet werden sollten z. B.:
  - Schäden oder Verluste durch den Notbetrieb
  - der aktuelle Stand der Arbeitsrückstände
  - die erwartete Dauer im Störbetrieb bis zur Rückkehr in den Normalbetrieb

In den Geschäftsfortführungsplänen wird näher festgelegt, mit welchen Arbeitsrückständen auf Grund des individuell festgelegten Notbetriebs zu rechnen ist. Welche Optionen genutzt werden können, um diese abzuarbeiten, sollte daher individuell in den Geschäftsfortführungsplänen geregelt werden (siehe Kapitel 6.9.2 *Erstellung der GFPs*).

Deeskalation und Auflösen der BAO

Üblicherweise erreichen in der Praxis die betroffenen Organisationseinheiten den Normalbetrieb schrittweise. Auch die BAO kann schrittweise aufgelöst werden, wenn es die jeweiligen Umstände erforderlich machen. Auch wenn der Notfall nicht mehr akut gegeben ist, können Teile der BAO die AAO für eine gewisse Zeit weiterhin unterstützen. Jedoch sollte zu einem spezifischen Zeitpunkt an alle Interessengruppen kommuniziert werden, wenn der Notfall für beendet erklärt wird. Dieser Zeitpunkt wird als Deeskalation des Ereignisses definiert. Ab diesem Zeitpunkt gelten wieder die üblichen Zuständigkeiten der AAO.

Für die Deeskalation sollten geeignete Kriterien und Zuständigkeiten definiert werden. Bei der Ausgestaltung der Kriterien bieten die Anforderungen der Eskalation Orientierung (siehe Kapitel 6.4.2 *Detektion, Alarmierung und Eskalation*). Folgende Fragen können hilfreich sein, um die Kriterien für die Deeskalation festzulegen:

- Sind sämtliche Ereignisse bewältigt, die eine BAO benötigen?
- Können die restlichen Probleme vollständig durch die AAO gelöst werden?
- Kann eine erneute Verschärfung der Lage bei einer schrittweisen Überführung in den Normalbetrieb ausgeschlossen werden?
- Kann die interne und externe Kommunikation wieder vollständig durch die AAO erfolgen?

6.4.8 Analyse der Bewältigung

Nachdem die Institution einen Notfall oder eine Krise bewältigt hat, ist die Analyse der Bewältigung ein weiterer wichtiger Schritt. Nur so kann die Institution aus Notfällen und Krisen lernen. Durch eine strukturierte Analyse kann ermittelt werden, was gut funktioniert hat und an welchen Stellen Optimierungsbedarf besteht. Anschließend kann aus den Ergebnissen der Analyse abgeleitet werden, was noch präventiv getan werden sollte, damit die Notfallbewältigung und somit auch die Resilienz der Institution weiter verbessert werden können.

Durch entsprechende Vorgaben sollte sichergestellt werden, dass im Nachgang jedes Notfalls und jeder Krise untersucht wird, inwieweit Korrekturbedarfe und Verbesserungsmöglichkeiten für das BCMS abgeleitet werden können. Es ist empfehlenswert, dass der BCMB die Notfallbewältigung zentral analysiert, z. B. in Form von Workshops mit den Beteiligten. Es ist empfehlenswert, eine Analyse zeitnah zum Notfallereignis sowie mit einigem zeitlichen Abstand dazu durchzuführen. Weitere Informationen dazu können dem Kapitel Hilfsmittel *Weiterführende Informationen zur Bewältigung* entnommen werden. Die Workshops können anhand eines vorab festgelegten Frageschemas aufgebaut sein.

Beispiel:

Fragenkatalog – Analyse der Bewältigung

- Wie kam es zu dem Ereignis?
- Welche Auswirkungen hatte das Ereignis?
- Wie schnell und wie effektiv erfolgte die Reaktion auf das Ereignis?
- Welche Elemente der Aufbau- und Ablauforganisation der BAO haben gut funktioniert und welche weniger gut?
- Gab es Unterschiede zur geplanten Notfallbewältigung?
- Waren alle zeitkritischen Geschäftsprozesse und Ressourcen bekannt?
- Welche Notfallmaßnahmen wurden ergriffen bzw. neu eingeführt?
- Wie gut haben die vorbereiteten Notfallpläne funktioniert?
- Wurden Notfallpläne neu erstellt oder angepasst?
- Wie gut hat die interne Notfallkommunikation funktioniert? (z. B. Kooperationsbereitschaft der Mitarbeiter, Einhaltung der Schweigepflichten)
- Wie gut hat die externe Notfallkommunikation funktioniert? (z. B. Effektivität des Medienmonitoring, Einflussmöglichkeiten auf die externe Wahrnehmung?)

Ferner sollte durch entsprechende Vorgaben sichergestellt werden, dass die Ergebnisse der Analyse dokumentiert und an die Institutionsleitung berichtet werden. Falls bei der Analyse konkrete Mängel und Verbesserungsmöglichkeiten identifiziert werden, können zeitnah entsprechende Korrektur- und Verbesserungsmaßnahmen initiiert werden. Die Verbesserungsbedarfe des BCMS sollten in den Maßnahmenplan des BCM aufgenommen werden, um das BCMS weiterzuentwickeln (siehe Kapitel 6.13 *Korrektur und Verbesserung des BCMS*).

Hinweis:

Es geht in der Mängel-Analyse nicht darum, mögliche Fehlentscheidungen oder Leistungen einzelner Personen zu bewerten. Wenn jedoch eine Fehlentscheidung getroffen wurde, sollte diese analysiert werden, z. B. wie es dazu kam bzw. warum die Person so entschieden hat. Möglicherweise fehlten Informationen im Lagebild oder die Entscheidung wurde vorschnell getroffen, die Methoden der Stabsarbeit wurden nicht angewendet, oder es gab andere „psychologische“ Gründe.

6.5 Business Impact Analyse

Während der Initiierung des BCM wurde durch die Institutionsleitung entschieden, welcher Geltungsbereich und welcher Zeitraum durch das BCM abgesichert werden sollen (siehe Kapitel 3.1.2 *Geltungsbereich sowie* 3.1.1.2 *Abzusichernder Zeitraum durch ein BCM*).

In der BIA wird untersucht, welche Geschäftsprozesse innerhalb des Geltungsbereichs zeitkritisch sind und ab wann deren Ausfälle nicht tolerierbare Auswirkungen haben. Dies bestimmt, ob und ab wann für diese Geschäftsprozesse ein Notbetrieb zur Verfügung stehen sollte. Zusätzlich werden für zeitkritische Geschäftsprozesse die Prozessabhängigkeiten, die Ressourcen für den Notbetrieb sowie die Wiederanlaufzeiten ermittelt.

Die BIA erfolgt stets bezogen auf die **Auswirkungen** eines Geschäftsprozessausfalls, nicht auf die Ursachen. Ob ein Geschäftsprozess aufgrund der Nichtverfügbarkeit des Gebäudes durch Feuer, Hochwasser, Stromausfall oder aufgrund der Nichtverfügbarkeit einer für den Geschäftsprozess zwingend benötigten IT-Anwendung ausfällt, spielt daher für die Schadensbewertung keine Rolle. Innerhalb der BIA muss vom Totalausfall des Geschäftsprozesses ausgegangen und in dessen Folge die zu erwartenden Schäden bewerten werden.

In einer BIA wird nicht nur bewertet, welche Auswirkungen ein Ausfall eines Geschäftsprozesses für die Institution hat, sondern auch wie sich der Schaden zeitlich entwickelt. Das Ergebnis der BIA legt fest, welche Geschäftsprozesse und Ressourcen zeitkritisch sind und daher in den nachfolgenden Schritten des BCM berücksichtigt werden müssen. Falls die BAO schon aufgebaut wurde, helfen diese Informationen der BAO zudem,

- die zeitkritischen Geschäftsprozesse und Ressourcen in einem Notfall zu priorisieren,
- früh zu erkennen, ob ein Schadensereignis eskaliert werden muss sowie
- den Geschäftsbetrieb aufrechtzuerhalten.

In der BIA werden die Kenngrößen erhoben, die für die weitere Notfallplanung benötigt werden. Abbildung 47 verdeutlicht den Zusammenhang dieser Kenngrößen anhand einer verkürzten Darstellung der Notfallbewältigung. Diese besteht hier nur aus den Phasen Normalbetrieb, Wiederanlauf einer zeitkritischen Ressource und Notbetrieb eines zeitkritischen Geschäftsprozesses.

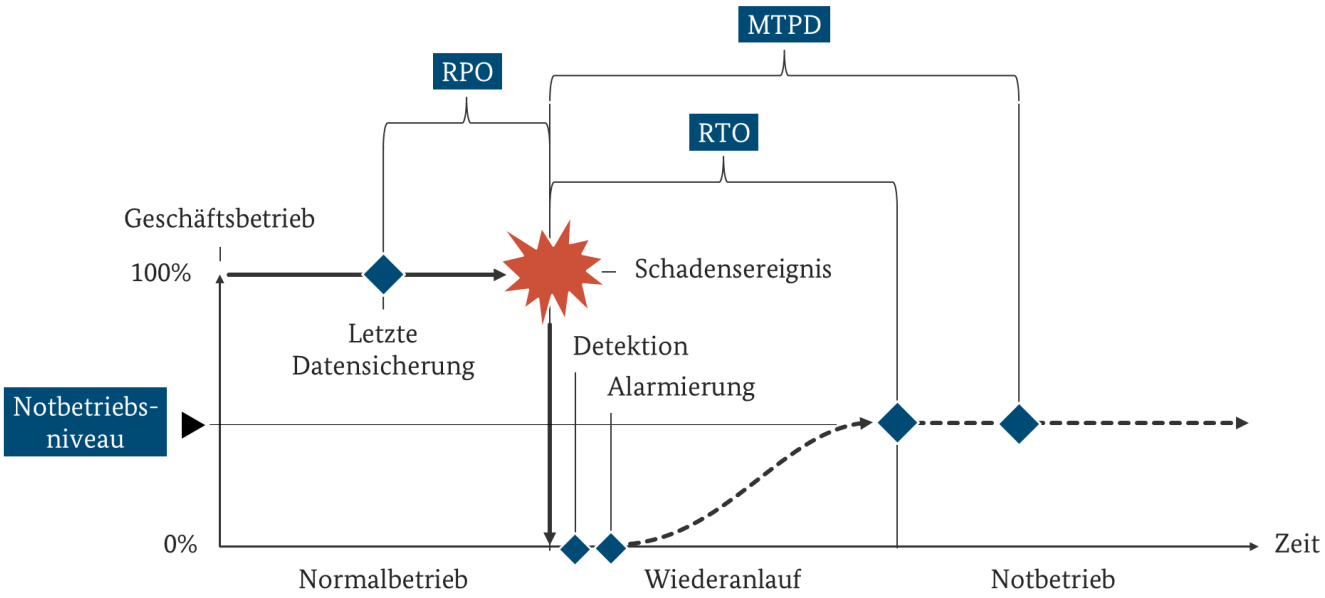

Abbildung 47: Erläuterung der Kenngrößen MTPD, RTO, RPO sowie Notbetriebsniveau

1. Die **Maximum tolerable Period of Disruption** (**MTPD**, deutsch: Maximal tolerierbare Ausfallzeit, MTA) legt fest, wie lange ein Geschäftsprozess maximal ausfallen darf, bevor nicht tolerierbare Auswirkungen für die Institution auftreten. Sie wird anhand einer Schadensbewertung je Geschäftsprozess ermittelt.
2. Die **Recovery Time Objective (RTO,** deutsch: Geforderte Wiederanlaufzeit, WAZ) wird aus der MTPD abgeleitet und den Ressourcen zugeordnet, die relevant sind für die Aufrechterhaltung der zeitkritischen Geschäftsprozesse. Die RTO einer zeitkritischen Ressource umfasst den Zeitraum vom Zeitpunkt des Ausfalls der Ressource bis zum Zeitpunkt der geforderten Inbetriebnahme der Notfall-Lösung, z. B. durch Schwenk auf eine Ausweich- oder Ersatzressource oder durch Zurücksetzen eines IT-Systems auf den letzten gesicherten Zustand. Die RTO der Ressource muss zwingend kürzer sein als die MTPD des relevanten Geschäftsprozesses, um zwischen Eintritt eines Schadensereignisses und der Detektion sowie Alarmierung bis hin zum Einleiten der Maßnahme zum Wiederanlauf über ausreichend zeitlichen Puffer zu verfügen.
3. Der **Recovery Point Objective** (**RPO**, deutsch: Maximal zulässige Datenverlust) legt fest, wie alt verfügbare Daten maximal sein dürfen, um im Notbetrieb sinnvoll damit arbeiten zu können. Diese Kenngröße dient auch dazu, die minimal notwendigen Datensicherungszyklen daraus abzuleiten.
4. Das **Notbetriebsniveau** definiert, wie leistungsfähig der Notbetrieb sein soll, um einen sinnvollen Geschäftsbetrieb gewährleisten zu können. Das Notbetriebsniveau wird je Geschäftsprozess individuell festgelegt. Hierzu kann die Leistungsfähigkeit des Notbetriebs z. B. prozentual angegeben werden oder alternativ Aktivitäten priorisiert werden. In der Abbildung 47 wird das Notbetriebsniveau nur schematisch dargestellt.

Die Vorgehensweise zur BIA sollte in einer schriftlichen Anweisung dokumentiert sein, um nachvollziehbare Ergebnisse mit einer angemessenen Qualität zu erhalten. Hierzu kann auf die erläuternden Texte aus diesem Kapitel zurückgegriffen werden. Die schriftliche Anweisung kann z. B. in das Notfallvorsorgekonzept integriert sein. Die Vorgehensweise sollte darin anhand der definierten Rollen und Hilfsmittel institutionsspezifisch beschrieben werden. Um eine BIA durchzuführen, kann die Dokumentenvorlage *BIA-Auswertungsbogen* aus den Hilfsmitteln verwendet werden.

Die nachfolgenden Kapitel beschreiben die empfohlene Vorgehensweise, mittels derer die BIA vorbereitet, durchgeführt und ausgewertet werden kann. In Abbildung 48 sind die hierfür erforderlichen Schritte in einer Übersicht dargestellt.

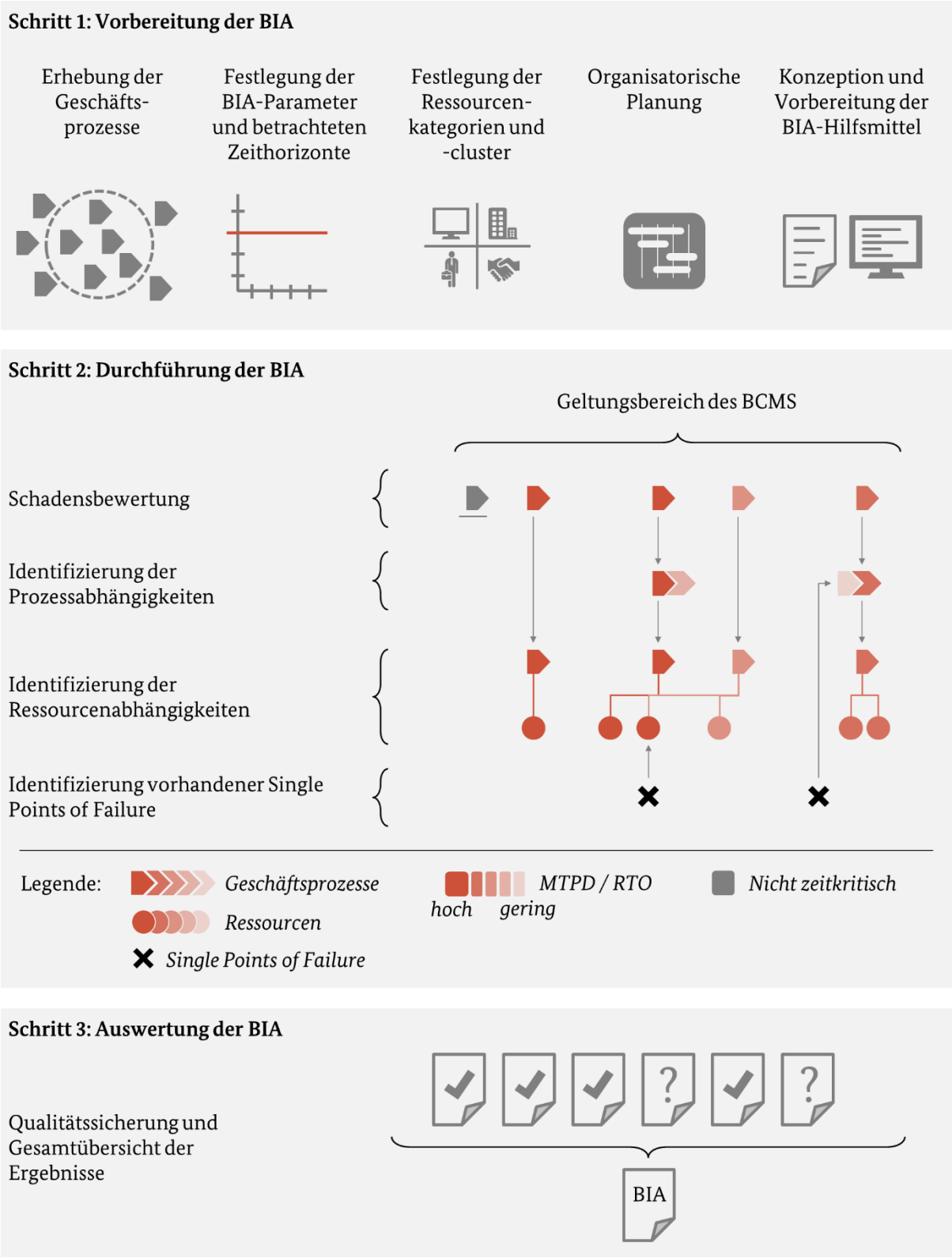

Abbildung 48: BCM-Prozessschritte der Business Impact Analyse

6.5.1 Vorbereitung der BIA

Der BCMB sollte die Methodik der BIA festlegen und die BIA organisatorisch vorbereiten. Dies ist sinnvoll, da er über das notwendige Fachwissen verfügt und den BCM-Prozess zeitlich steuert. Er kann vorbereitende Tätigkeiten ganz oder teilweise an weitere Rollen im BCM delegieren. Die Aufgaben in der Vorbereitung der BIA werden in den nachfolgenden Unterkapiteln näher erläutert. Die Kapitel folgen einer logischen Reihenfolge, jedoch können sich verschiedene darin beschriebene Aufgaben in der Praxis zeitlich überlagern.

6.5.1.1 Erhebung der Geschäftsprozesse

Für den aktuellen Prozessumfang müssen alle Geschäftsprozesse identifiziert werden, die innerhalb der BIA bewertet werden sollen. Institutionen können hierzu möglicherweise auf vorhandene Übersichten über ihre Geschäftsprozesse zurückgreifen. Diese Übersichten sollten daraufhin überprüft werden, dass sie vollständig den Geltungsbereich des BCMS abdecken und aktuell sind.

Solche Übersichten werden häufig in einem Prozessmanagement erstellt oder durch Querschnittsfunktionen wie zentrale Dienste, Betriebsorganisation oder Vorstandsstab. In einer vollständigen „Prozesslandkarte" sind nicht nur sämtliche Prozesse der Institution dokumentiert, sondern häufig auch die zuständigen Personen sowie die Abhängigkeiten der Prozesse untereinander. Die Informationen über vor- und nachgelagerte Geschäftsprozesse werden zu einem späteren Zeitpunkt in der BIA benötigt, um feststellen zu können, ob ausgefallene Geschäftsprozesse einen Einfluss auf weitere abhängige Geschäftsprozesse haben. Zudem wird ersichtlich, ob zeitkritische Geschäftsprozesse andere Prozesse zum Wiederanlauf benötigen. Somit kann auch die Wiederanlaufreihenfolge bestimmt werden.

Hinweis:

Da sowohl Aufbau- und Standard-BCMS in diesem Kapitel abgebildet werden, wird in diesem Zusammenhang vom Prozessumfang gesprochen (siehe Kapitel *2.6 BCMS Stufenmodell*). Für ein Standard-BCMS entspricht der Prozessumfang dem Geltungsbereich des BCMS. Im Aufbau-BCMS kann der Prozessumfang anhand der Voranalyse festgelegt werden.

Liegt keine aktuelle Übersicht der Geschäftsprozesse und ihrer Abhängigkeiten vor, so muss diese im Rahmen der BIA erhoben oder aktualisiert werden. Hierzu können Geschäftsverteilungspläne, Aufgabenbeschreibungen oder andere organisationsbeschreibende Dokumente der Institution zu Hilfe genommen werden. Zudem ist es empfehlenswert, die BIA anhand derjenigen Organisationseinheiten auszurichten, die für den Prozessumfang relevant sind. So kann auf Ansprechpartner zurückgegriffen werden.

Während in einer Prozesslandkarte häufig eine sehr große Anzahl an Informationen vorliegt, werden im Rahmen der BIA nur die Prozessbezeichnung sowie die zuständige Organisationseinheit benötigt. Eine kurze Beschreibung der Aktivitäten oder Ergebnisse des Geschäftsprozesseses kann für die Schadensbewertung hilfreich sein.

Synergiepotenzial:

Liegt ein ISMS nach BSI-Standard 200-2 oder nach ISO-Standard 27001 vor, können die dort identifizierten Geschäftsprozesse als Grundlage verwendet werden.

Das Verfahrensverzeichnis für den Datenschutz kann möglicherweise ebenfalls als Grundlage genutzt werden. Es fasst alle Geschäftsprozesse zusammen, in denen personenbezogene Daten verarbeitet werden.

Wird auf vorhandene Prozessübersichten zurückgegriffen, sollten diese hinsichtlich des Prozessumfangs des BCMS auf Vollständigkeit überprüft werden.

Je nach Größe und Komplexität der Institution kann es unterschiedliche Detailebenen der Geschäftsprozesse geben. Bevor die BIA durchgeführt wird, sollte festgelegt werden, auf welcher Abstraktionsebene der Geschäftsprozesse die BIA durchgeführt werden soll. Dies dient einerseits dazu, die BIA zeitlich exakter planen zu können, indem die Anzahl der zu untersuchenden Geschäftsprozesse eingegrenzt wird (Je tiefer die Detailebene, desto größer ist die Anzahl an Geschäftsprozessen). Zum anderen kann darüber gesteuert werden, wie detailliert die Schadensbewertung erfolgen soll.

Als Vorgabe für den Detailgrad der zu berücksichtigenden Geschäftsprozesse sollte ein Mittelweg zwischen zu starker Zusammenfassung von Geschäftsprozessen und einer zu detaillierten Betrachtung gefunden werden. Eine zu starke Bündelung von Geschäftsprozessen führt zu einer mangelnden Aussagekraft hinsichtlich

der zeitkritischen Aktivitäten innerhalb des Geschäftsprozesses. Eine zu detaillierte Betrachtung führt zu einer nicht zu bewältigenden Anzahl zu betrachtender Geschäftsprozesse. Ein wesentliches Merkmal dieses Mittelweges liegt darin, dass die Planung des Notbetriebs und Erstellung von geeigneten Geschäftsfortführungsplänen mit den Ergebnissen der BIA erreicht werden sollen.

Eine Schadensbewertung der in Abbildung 49 dargestellten Prozessebene 3 stellt beispielsweise einen guten Kompromiss hinsichtlich des aussagekräftigen Detailgrads und der Menge an Geschäftsprozessen dar. Die beschriebenen Geschäftsprozesse sind als Beispiele zu verstehen und decken nur einen kleinen Teil der üblichen Geschäftsprozesse innerhalb einer Institution ab.

Beispiel:

Prozessebene 1	Prozessebene 2	Prozessebene 3	...
Personalmanagement	Personalbeschaffung	Personalrekrutierung	...
		Einstellungsverfahren	...
		...	...
	Personalbetreuung	Personalservice	...
		Personalentwicklung	...
		Personalaustritt	...
		...	...
IT	IT-Steuerung	IT-Strategie	...
		IT-Ressourcenmanagement	...
		...	...
	IT-Betrieb	Sicherstellung IT-Betrieb	...
		Berechtigungsmanagement	...
		Incident Management	...
		Problem Management	...
		...	...
	IT-Anwendungsentwicklung	Softwareauswahl	...
		Softwaretest	...
		...	...

Abbildung 49: Beispiele hierarchisch angeordneter Geschäftsprozesse

Die BIA sollte alle Hierarchie-Ebenen der Organisationseinheiten berücksichtigen, nicht nur die unterste Ebene. Nur so kann sichergestellt werden, dass anhand der jeweiligen Ansprechpartner eine Aussage zu allen Geschäftsprozessen möglich wird.

Beispiel:

Die Geschäftsprozesse *IT-Strategie* und *IT-Ressourcenmanagement* werden durch die IT-Abteilung verantwortet. Der Unterstützungsprozess *IT Incident Management* wird hingegen durch ein untergeordnetes Referat verantwortet. Um alle Geschäftsprozesse in der BIA zu berücksichtigen, ist es empfehlenswert, die BIA sowohl mit einem Ansprechpartner der Abteilung als auch mit einem Ansprechpartner aus dem Referat durchzuführen oder diese beiden Ansprechpartner gemeinsam in einem Termin zu befragen.

6.5.1.2 Festlegung der BIA-Parameter und betrachteten Zeithorizonte

Ziel der BIA ist es, einheitlich festzustellen, ob ein Geschäftsprozess zeitkritisch ist und wie lange dieser ausfallen darf, bevor nicht mehr tolerierbare Schäden entstehen. Hierfür wird in der BIA betrachtet, welche

Schäden durch den ausgefallenen Geschäftsprozess über einen definierten Zeitverlauf entstehen. Dafür müssen sogenannte Zeithorizonte festgelegt werden. Die BIA stellt zur Schadensbewertung die folgende Leitfrage:

> **Wenn ein Geschäftsprozess ausfällt, mit welchem Schadenspotenzial ist im jeweiligen Zeithorizont zu rechnen?**

Um die Schadensbewertung und die anschließende Auswertung zu vereinheitlichen und zu erleichtern, sollten für die Zeithorizonte und Schadenspotenziale eindeutige Skalenwerte definiert werden, anhand derer eine Bewertung erfolgen kann. Dies gestattet es, dass alle Geschäftsprozesse nach einem einheitlichen Schema bewertet werden und subjektives Empfinden das Ergebnis nicht zu sehr beeinflusst. Zudem muss ein Untragbarkeitsniveau festgelegt werden, um festzustellen, zu welchem Zeitpunkt ein Ausfall eines Geschäftsprozesses aufgrund der Höhe seines Schadenspotenzials nicht länger akzeptiert werden kann.

Die nachfolgende Abbildung 50 stellt beispielhaft die **Schadensbewertung** für einen Geschäftsprozess grafisch dar und fasst die relevanten BIA-Parameter zusammen:

Beispiel:

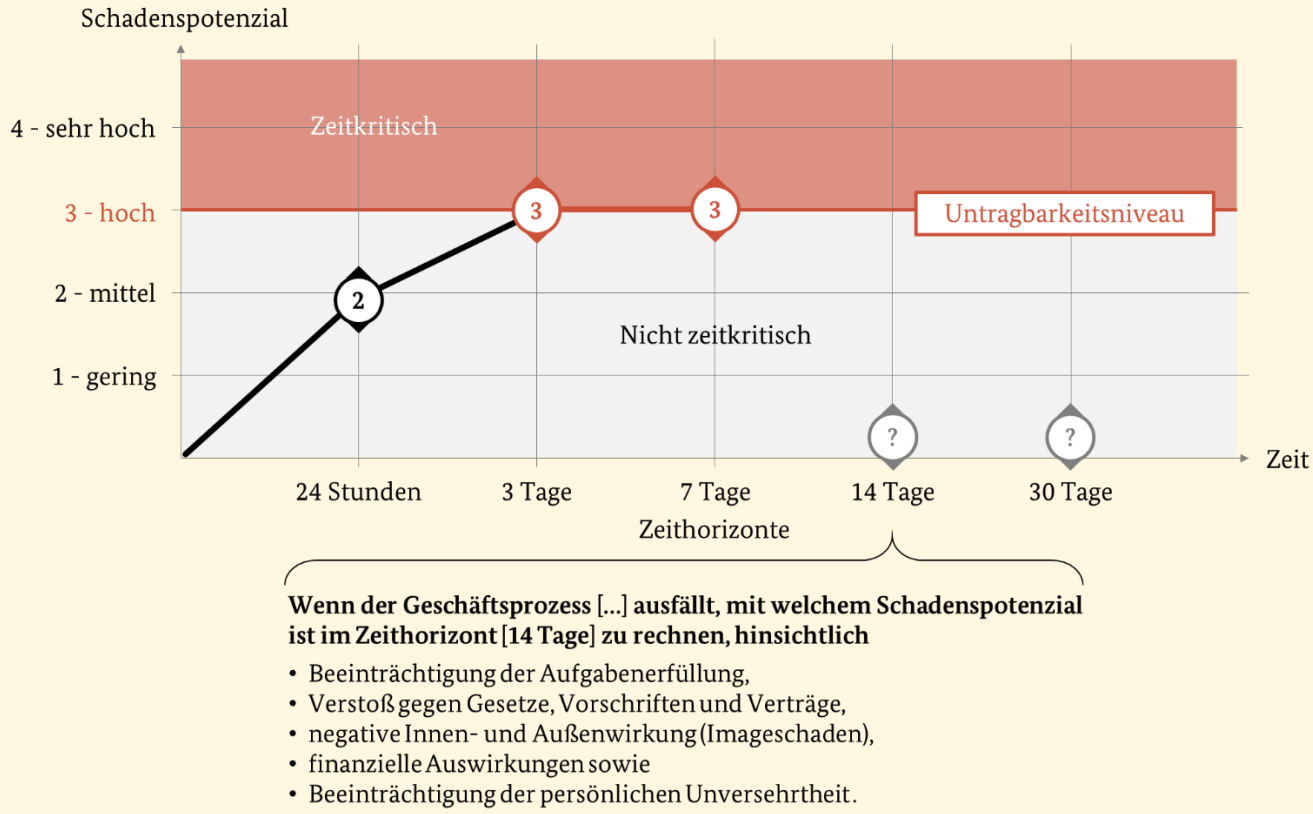

Abbildung 50: Beispiel einer Schadensbewertung je Zeithorizont

Die **Zeithorizonte** (im Beispiel-Diagramm auf der Zeit-Achse aufgetragen) legen den jeweiligen Zeitpunkt fest, zu dem ein Schaden bewertet wird. Die Zeitpunkte x (24 Stunden, 3 Tage, 7 Tage etc.) markieren je einen Zeitraum von 0 bis x und sind zu verstehen als „*Der Geschäftsprozess ist ausgefallen bis zum Zeitpunkt x*“.

- Das **Schadenspotenzial** (im Beispiel-Diagramm als Kreis auf dem Koordinatensystem dargestellt) lässt sich aus den Schadensszenarien und Schadenskategorien ableiten.
- Die **Schadensszenarien** (im Beispiel unter dem Diagramm dargestellt) beschreiben die Szenarien, in denen ein Schaden entstehen könnte.

Die **Schadenskategorien** (im Beispiel-Diagramm auf der Schadenspotenzial-Achse aufgetragen) klassifizieren den Schaden, der je Schadensszenario entstehen kann.

Das **Untragbarkeitsniveau** wird im Beispiel-Diagramm als horizontale rote Linie dargestellt. Oberhalb der Schadensstufe 3 (hoch) erzeugt der Ausfall des Geschäftsprozesses Schäden, die durch die Institution nicht toleriert werden, d. h. der Prozess wird zeitkritisch.

Der Verlauf des Graphen, d. h. der dickeren, schwarzen Linie im Beispiel-Diagramm, zeigt die Entwicklung des Schadenspotenzials über die Zeit. Der Graph verdeutlicht, wann ein Geschäftsprozess zeitkritisch wird und ob das Schadenspotenzial über den Zeitverlauf stagniert oder mit längerer Ausfallzeit weiter ansteigt.

Definition von Zeithorizonten

Sowohl die Anzahl als auch die genaue Unterteilung der Zeithorizonte müssen sich an den Gegebenheiten der Institution ausrichten. Deswegen sollten Zeithorizonte festgelegt werden, zu denen sich typischerweise der Schadensverlauf in der Institution wesentlich verändert.

Hinweis:

Die Wahl der Zeithorizonte wird unter anderem beeinflusst durch:

- die Zyklen, in denen Produkte hergestellt oder Services bereitgestellt werden
- die Erwartungshaltung von Interessengruppen
- interne Vorgaben und Geschäftsziele
- branchenübliche Standards
- gesetzliche Vorgaben
- den Risikoappetit der Institution

Entsprechend können z. B. dynamische Branchen, wie der Onlinehandel, sehr kurze Zeithorizonte wählen, während Institutionen mit sehr langen Produktions- oder Bearbeitungszeiten eher längere Zeithorizonte bevorzugen.

In der Praxis hat sich eine Einteilung in fünf bis acht Zeithorizonte bewährt. Der längste zu betrachtende Zeithorizont sollte am Zeitraum ausgerichtet sein, der in der Initiierung des BCMS (siehe Kapitel 3.1.1.2 *Abzusichernder Zeitraum durch ein BCM*) festgelegt wurde.

Beispiel:

Die Beispiele erläutern, wie die Zeithorizonte anhand branchen- oder institutionsspezifischer Vorgaben sowie besonderer Termine und Ereignisse abgeleitet werden können.

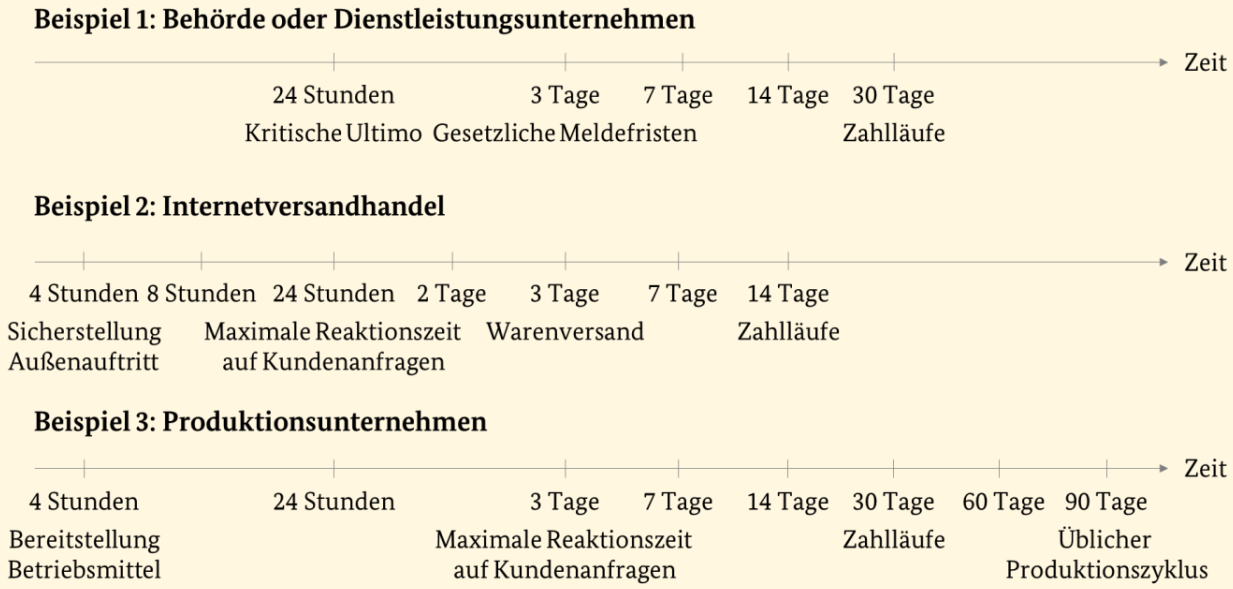

Abbildung 51: Beispiel für Zeithorizonte

Schadensszenarien

Um die Schäden besser einschätzen zu können, werden die potenziellen Auswirkungen von Ausfällen anhand von Schadensszenarien untersucht. Die Schadensszenarien sollten sich an den Rahmenbedingungen der Institution ausrichten und sowohl direkte als auch indirekte Schäden berücksichtigen. Direkte Schäden umfassen beispielsweise entgangene Gewinne sowie unmittelbare Auswirkungen auf Leib und Leben oder die persönliche Unversehrtheit von Menschen. Indirekte Schäden berücksichtigten z. B. Verluste durch entgangene Aufträge, Verlust an Marktanteil, Imageschäden oder negative Auswirkungen auf Dritte. Innerhalb der BIA sollten die folgenden Schadensszenarien berücksichtigt werden:

- Beeinträchtigung der Aufgabenerfüllung
- Verstoß gegen Gesetze, Vorschriften und Verträge
- negative Innen- und Außenwirkung (Imageschaden)
- finanzielle Auswirkungen
- Beeinträchtigung der persönlichen Unversehrtheit

Hinweis:

Auch Behörden können durch einen Ausfall des Geschäftsbetriebs von finanziellen Auswirkungen betroffen sein. Neben Strafzahlungen aufgrund nicht eingehaltener Fristen gehören hierzu Ausgaben für nicht einsatzfähige Ressourcen und Personal oder entgangene Beiträge, Forderungen oder Steuern. Im Regelfall sollten diese finanziellen Schäden für Behörden keine existenzbedrohenden oder nicht tolerierbaren Auswirkungen haben. Um mögliche Ausnahmefälle zu identifizieren, wird empfohlen, die finanziellen Auswirkungen in der Schadensbewertung dennoch mit zu berücksichtigen und unter Umständen als nicht relevant zu markieren.

Schadenskategorien

Die festgelegten Schadensszenarien erlauben noch keine Schadensbewertung, da hierbei für den Anwender nicht klar ersichtlich ist, wonach er den potenziellen Schaden bewerten soll. Zu diesem Zweck muss für alle Schadensszenarien das Schadenspotenzial anhand verschiedener Schadenskategorien definiert werden. Die Anzahl an Schadenskategorien muss für alle Schadensszenarien einheitlich definiert werden. Üblicherweise wird mit drei bis fünf Schadenskategorien gearbeitet.

Für die fortfolgenden Beispiele werden die Schadenskategorien 1 - gering bis 4 – sehr hoch zugrunde gelegt. Tabelle 44 erläutert beispielhaft, wie die Schadenskategorien je Schadensszenario konkretisiert werden können. Die Definitionen sollten individuell für die Institution angepasst werden. Die angepasste Tabelle 44 kann gleichzeitig als Hilfsmittel eingesetzt werden, um bei der Durchführung der BIA die Schadensbewertung zu unterstützen.

Es bietet sich an, wie in der Tabelle 44 aufgezeigt, die Schadensbewertungen gesammelt je Schadenskategorie aufzuführen und nicht jeweils für nur ein Schadensszenario. Das Schadenspotenzial wird bewertet, indem vom schlimmsten anzunehmenden Fall (*worst case*) ausgegangen wird. Für jede Schadenskategorie können also alle jeweils schlimmsten Bewertungen pro Szenario zusammengefasst werden (siehe Kapitel 6.5.2.1 *Schadensbewertung).*

Beispiel:

Schadens-kategorie	Erläuterung je Schadensszenario
1 - Gering	**Allgemeine Beschreibung:** Ausfall hat geringe, kaum spürbare Auswirkungen. • **Beeinträchtigung der Aufgabenerfüllung:** Der Geschäftsbetrieb wird unwesentlich beeinträchtigt. • **Verstoß gegen Gesetze, Vorschriften und Verträge:** Es wird nur in einem geringen Maß gegen interne Vorgaben und Anweisungen verstoßen. Verstöße führen zu keinen Konsequenzen. • **Negative Innen- und Außenwirkung (Imageschaden):** In Einzelfällen ist eine geringe, nicht nachhaltige Ansehensbeeinträchtigung zu erwarten. • **Finanzielle Auswirkungen:** Der finanzielle Schaden ist für die Institution unerheblich. • **Beeinträchtigung der persönlichen Unversehrtheit:** Eine Beeinträchtigung ist ausgeschlossen.
2 - Mittel	**Allgemeine Beschreibung:** Ausfall hat spürbare Auswirkungen. • **Beeinträchtigung der Aufgabenerfüllung:** Der Ausfall hat spürbare Auswirkungen auf den Geschäftsbetrieb. Mit Arbeitsrückständen ist zu rechnen. • **Verstoß gegen Gesetze, Vorschriften und Verträge:** Es wird ausschließlich gegen interne Vorgaben und Anweisungen verstoßen. • **Negative Innen- und Außenwirkung (Imageschaden):** Eine geringe Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten. • **Finanzielle Auswirkungen:** Der finanzielle Schaden ist für die Institution tolerabel. • **Beeinträchtigung der persönlichen Unversehrtheit:** Eine Beeinträchtigung ist unwahrscheinlich.
3 - Hoch	**Allgemeine Beschreibung:** Ausfall hat nicht tolerierbare Auswirkungen.

	• **Beeinträchtigung der Aufgabenerfüllung:** Der Geschäftsbetrieb ist massiv eingeschränkt. Arbeitsrückstände sind nur mit erhöhtem Arbeitsaufwand zu kompensieren. • **Verstoß gegen Gesetze, Vorschriften und Verträge:** Es wird gegen Gesetze verstoßen. Verstöße führen zu erheblichen Konsequenzen, z. B. hohe Bußgelder. Vertragsverletzungen führen zu hohen Konventionalstrafen oder Konsequenzen. • **Negative Innen- und Außenwirkung (Imageschaden):** Eine erhebliche, nachhaltige Ansehens- oder Vertrauensbeeinträchtigung ist intern und extern zu erwarten. • **Finanzielle Auswirkungen:** Der finanzielle Schaden ist für die Institution erheblich und nachhaltig spürbar. • **Beeinträchtigung der persönlichen Unversehrtheit:** Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden.
4 - Sehr hoch	**Allgemeine Beschreibung:** Ausfall führt zu existentiell bedrohlichen Auswirkungen. • **Beeinträchtigung der Aufgabenerfüllung:** Der Ausfall hat fundamentale und langfristige Auswirkungen auf den Geschäftsbetrieb. Arbeitsrückstände können nicht mehr aufgeholt werden. • **Verstoß gegen Gesetze, Vorschriften und Verträge:** Es wird im hohen Maß gegen Gesetze verstoßen. Verstöße haben strafrechtliche Konsequenzen. Vertragsverletzungen führen zu ruinösen Konventionalstrafen oder Konsequenzen. • **Negative Innen- und Außenwirkung (Imageschaden):** Eine fundamentale, nachhaltige, in der breiten Öffentlichkeit vorhandene Ansehens- oder Vertrauensbeeinträchtigung, bis hin zu existenzgefährdender Art, ist zu erwarten. • **Finanzielle Auswirkungen:** Der finanzielle Schaden hat existenzbedrohende Ausmaße. • **Beeinträchtigung der persönlichen Unversehrtheit:** Es besteht akut Gefahr für Leib und Leben oder gravierende Beeinträchtigungen der persönlichen Unversehrtheit.

Tabelle 44: Beispiele von Schadenskategorien und Erläuterung je Schadensszenario

Neben harten Faktoren wie Liquidität können auch Vorgaben der Institutionsleitung oder Anforderungen aus dem Risikomanagement Basis für die Ausprägung der Schadenskategorien sein. So können z. B. anhand konkreter Euro-Werte, die im Risikomanagement definiert werden und sich am jeweils aktuellen Umsatzziel oder Haushaltsbudget orientieren, die Schadenskategorien zu finanziellen Auswirkungen voneinander abgegrenzt werden.

Synergiepotenzial:

Sofern bereits ein ISMS nach BSI-Standard 200-2 vorliegt, können die in der Schutzbedarfsfeststellung definierten Schadensszenarien und Schadenskategorien als Grundlage genutzt werden. Dies fördert die Vergleichbarkeit von Ergebnissen zwischen dem BCMS und ISMS.

Ferner können die in vorhandenen Risikoanalysen genutzten Parameter zum Schadenspotenzial auch für die BIA herangezogen werden.

Untragbarkeitsniveau

Das Untragbarkeitsniveau definiert, ab welcher Schadenskategorie die Auswirkungen eines Ausfalls durch die Institution nicht länger toleriert werden (siehe Abbildung 50). Die Entscheidung darüber, ab welcher Höhe Schäden nicht länger toleriert werden, sollte aufgrund der Tragweite für die weitere Notfallplanung die

Institutionsleitung treffen. Anhand des festgelegten Untragbarkeitsniveaus kann in der BIA identifiziert werden, zu welchem Zeitpunkt die erwarteten Schäden so hoch werden, dass diese nicht länger akzeptiert werden. Dies ist dann die MTPD des Geschäftsprozesses.

6.5.1.3 Festlegung der Ressourcenkategorien und -cluster

Innerhalb der BIA müssen die Ressourcenabhängigkeiten der zeitkritischen Geschäftsprozesse (die in Kapitel 6.5.2.1 *Schadensbewertung* identifiziert werden) erhoben werden, da der Ausfall eines Geschäftsprozesses üblicherweise auf den Ausfall einer notwendigen Ressource zurückgeführt werden kann. Alle für den Notbetrieb eines zeitkritischen Geschäftsprozesses erforderlichen Ressourcen werden nachfolgend vereinfacht als **zeitkritische Ressourcen** bezeichnet. Hierzu muss vorbereitend festgelegt werden, welche Ressourcenkategorien in der Institution relevant sind. Darauf aufbauend müssen die Ressourcen der jeweiligen Kategorie ermittelt werden. Einheitliche Namen und damit einheitlich definierte Ressourcenkategorien stellen sicher, dass die benötigten Ressourcen einheitlich erhoben werden können. Dann können auch die Informationen zu RTO und RPO den Ressourcen richtig zugeordnet und so nach der BIA unmittelbar mit dem Soll-Ist-Vergleich begonnen werden (siehe Kapitel 6.6 *Soll-Ist-Vergleich).*

Ressourcenkategorien

Grundsätzlich benötigt eine Institution für ihren Geschäftsbetrieb Strom, Wasserversorgung, Klimatechnik etc. Es ist jedoch nicht zweckmäßig diese Ressourcen für jeden Geschäftsprozess einzeln zu erheben, da diese für die Aufrechterhaltung des gesamten Geschäftsbetriebs vorausgesetzt werden. Diesen Ressourcen kann der kleinste, zeitkritische Zeithorizont zugeordnet werden, der für die Institution vorgegeben wird.

Werden darüber hinaus spezifische Ressourcen für einen Geschäftsprozess benötigt, so müssen diese in der BIA ermittelt werden. Die Ressourcen können in verschiedene Ressourcenkategorien unterteilt werden. Es müssen mindestens die folgenden in Tabelle 45 beschriebenen Ressourcenkategorien berücksichtigt werden:

- IT
- Personal
- Infrastruktur
- Dienstleistungen

Für das produzierende Gewerbe sollten zusätzlich die folgenden in Tabelle 45 beschriebenen Ressourcenkategorien verwendet werden:

- Maschinen/Geräte/Anlagen/Fahrzeuge
- Betriebsmittel (Sonstige)

Die Institution sollte die Anzahl und Beschreibung der Ressourcenkategorien auf ihre Bedürfnisse anpassen.

Beispiel:

Ressourcenkategorie	Beschreibung
IT	IT umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen.

Ressourcenkategorie	Beschreibung
Personal	Um Geschäftsprozesse durchführen zu können werden Mitarbeiter benötigt, die Entscheidungen treffen, Aufgaben ausführen, Maschinen bedienen oder sonstige Arbeitsschritte durchführen. Die Mitarbeiter verfügen hierzu über spezielle Fähigkeiten und Kenntnisse. Die jeweiligen Aufgaben und Pflichten werden in Form von Rollen und Funktionen definiert. Ferner sind an Rollen Berechtigungen für Zugang, Zutritt und Zugriff sowie Stellvertreterregelungen geknüpft.
Dienstleistungen	Unter dem Begriff Dienstleistungen werden alle intern und extern bezogenen Leistungen zusammengefasst, die einen Input liefern oder benötigte Ressourcen für einen Geschäftsprozess bereitstellen.
Informationen	Für gewöhnlich werden aus Endanwendersicht Anwendungen inklusive der darin gespeicherten oder verarbeiteten Daten (siehe Ressourcenkategorie IT) betrachtet. In der Praxis können aber auch Daten in elektronischer Form vorliegen, die keiner Anwendung zugeordnet werden. Hierzu gehören z. B. gespeicherte Daten auf mobilen Datenträgern, in Dateisystemen oder Cloudlösungen. Neben elektronischen Daten können auch papierhafte Dokumente der Ressourcenkategorie Informationen zugeordnet werden. Achtung: Informationen die in den Köpfen der Mitarbeiter gespeichert sind werden der Kategorie Personal zugeordnet.
Infrastruktur	Zur Infrastruktur zählen z. B. Gelände, Grundstücke, Gebäude inklusive Lager, Produktionshallen, Parkgaragen, Aktenarchive, Server- oder Büroräume sowie Strom-, Gas-, Wasser oder Fernwärmeversorgung sowie und (TV-, Internet-, Telefon-Verbindung), die für einen oder mehrere Geschäftsprozesse benötigt werden.
Maschinen/ Geräte/ Anlagen/ Fahrzeuge	Insbesondere im produzierenden Gewerbe stellen Maschinen, Geräte und Anlagen eine wesentliche Komponente in Geschäftsprozessen dar. Unter Fahrzeuge fallen Transport- und Verkehrsmittel (PKW, LKW, Zug, Flugzeug, Schiff etc.). Auch spezielle Bürogeräte können unter dieser Kategorie zusammengefasst werden.
Betriebsmittel (Sonstige)	Unter Betriebsmittel sind alle weiteren Ressourcen zu verstehen, die in keiner vorherigen Ressourcenkategorie erfasst wurden. Dies kann auch Rohstoffe für eine Produktion oder Kleinmaterial (z. B. Büromaterial, Büroausstattung, Zugangstoken etc.) umfassen.

Tabelle 45: Beispiele verschiedener Ressourcenkategorien

Ressourcencluster

Innerhalb bestimmter Ressourcenkategorien, wie z. B. der IT, können mitunter sehr viele einzelne Ressourcen vorhanden sein, die in der BIA berücksichtigt werden müssen. Wenn alle Ressourcen einzeln erfasst werden, besteht jedoch die Gefahr, dass diese aufgrund der Menge und der Komplexität nicht handhabbar sind. Ressourcen sollten deshalb sinnvoll zu Clustern zusammengefasst werden. Das gängigste Beispiel für ein Cluster ist der Arbeitsplatz.

Ein **Arbeitsplatz** fasst alle Arbeitsmittel und Geräte zusammen, die für eine spezifische Aufgabenstellung innerhalb eines Geschäftsprozesses benötigt werden. Hierbei kann allgemein zwischen einem Standardar-

beitsplatz und Spezialarbeitsplätzen unterschieden werden. Ein Arbeitsplatz kann Teil einer größeren Infrastruktur sein und wiederum aus einer Menge an Maschinen, Geräten, Anlagen oder Betriebsmitteln zusammengesetzt sein.

Beispiel:

Ein **Standardarbeitsplatz** wird definiert als ein Schreibtisch mit Bürostuhl und PC sowie ein Telefon. Der Standard-Arbeitsplatz wird mit den Medien Strom und Internet versorgt. Auf dem PC sind die gängigen Anwendungen der Institution installiert, z. B. Mail und Textverarbeitung. Weitere Ausstattung muss rollen- oder funktionsspezifisch definiert werden.

In einer Bank wird ein **Handelsarbeitsplatz** definiert, der zusätzlich zu einem Standard-Arbeitsplatz mit mehreren großformatigen Monitoren, einer speziellen Tastatur und einem Kartenlesegerät ausgestattet sowie an eine Telefonanlage mit Sprachaufzeichnung angeschlossen ist. Auf dem PC sind neben Standardprogrammen spezielle Bankanwendungen installiert, für die spezifische Berechtigungen erforderlich sind.

In einem Logistikbetrieb wird abweichend zu einem Standard-Arbeitsplatz ein **Kommissionierarbeitsplatz** definiert, der aus einem Arbeitstisch, einem PC mit Zugang zum Lieferketten- und Lagerverwaltungssystem (Supply Chain und Warehouse Management), einem Touchpad zur Dateneingabe, einem Label-Drucker sowie Handscanner, Verpackungsmaterial und Transportboxen besteht.

Synergiepotenzial:

Liegt ein ISMS nach BSI-Standard 200-2 vor, können Informationen aus der Strukturanalyse für die Bezeichnung verschiedener Ressourcen übernommen werden. Allerdings kann die Gruppenbildung gemäß BSI-Standard 200-2 voraussichtlich nicht für die Ressourcencluster im BCM angewendet werden, da diese einem abweichenden Zweck dienen.

Ist der IT-Betrieb nach ITIL ausgerichtet, kann der Bedarf an IT anhand des IT-Servicekatalogs ermittelt werden.

Auf Grund von Datenschutzvorgaben werden kontinuierlich die IT-Anwendungen ermittelt, die personenbezogene Daten verarbeiten. Diese Ergebnisse können ebenfalls als Grundlage für eine IT-Anwendungsliste dienen.

Über die Gebäudeverwaltung können häufig Arbeitsplatz-Definitionen sowie Raumlisten übernommen werden.

Im produzierenden Gewerbe liegen meist Maschinen- und Geräte-Inventarlisten vor, die für die Ressourcenkategorie Maschinen/Geräte/Anlagen/Fahrzeuge herangezogen werden können.

6.5.1.4 Organisatorische Planung

Vor Beginn der BIA sollte festgelegt werden, wie die Informationen zur BIA erhoben werden sollen. Hierzu bieten sich verschiedene Formate an, z. B.:

- Selbstauskunft durch den Prozess-Eigentümer anhand eines papierbasierten, elektronischen oder toolgestützten Fragebogens
- Einzel-Interviews mit verschiedenen Personen (z. B. Leitern der Organisationseinheiten, Prozesseigentümer oder sonstigen Prozessexperten, die Auskunft geben können)
- Workshops, mit mehreren Personen

Wird die BIA zum ersten Mal durchgeführt, sollte überprüft werden, ob sie anhand von Workshops durchgeführt werden soll. Der Workshop bietet verschiedene Vorteile gegenüber Formaten, in denen die Ansprechpartner die Informationen selbstständig erheben:

- Im Workshop kann näher erläutert werden, welche Auswirkung die BIA auf spätere Folgeschritte im BCM hat, beispielsweise auf die Geschäftsfortführungsplanung.
- Es ist hilfreich darauf hinzuweisen, dass die BIA nicht der Organisationsoptimierung dient und anhand der Ergebnisse weder Umstrukturierungen, Arbeitsplatzverdichtung oder ähnliches abgeleitet werden können, da die Fragestellungen sich auf einen temporären Notbetrieb beziehen.
- Es ist hilfreich darauf hinzuweisen, dass die Frage, ob ein Geschäftsprozess zeitkritisch ist, nicht damit gleichzusetzen ist, ob dieser für die Organisationseinheit wichtig ist.

Darüber hinaus bestehen weitere Vorteile eines Workshops:

- Der Workshop lässt Raum für Fragen und gestattet mögliche Unsicherheiten und Bedenken der Teilnehmer auszuräumen.
- Es kann sichergestellt werden, dass die Ergebnisse anhand der Dokumentenvorlage BIA einheitlich erhoben werden.
- Fehlerhafte oder fehlende Angaben in der Dokumentenvorlage BIA können bereits im Workshop vermieden werden, sodass Nacharbeiten geringer ausfallen.

Es ist empfehlenswert, dass ein BIA-Workshop durch eine BCM-sachkundige Person moderiert und darin die BIA-Methodik erläutert wird. Weiter nehmen am BIA-Workshop die jeweiligen Prozess-Eigentümer (die für den Geschäftsprozess zuständig sind) sowie eventuell weitere Prozess-Experten (die den Geschäftsprozess im Detail kennen) teil. Die Anzahl der BIA-Workshops kann sich an der Anzahl zu berücksichtigender Geschäftsprozesse ausrichten.

Wurde die BIA bereits häufiger durchgeführt oder sind die Ansprechpartner mit der BIA-Methodik vertraut, können die Ansprechpartner die BIA auch selbstständig durchführen. Der BCMB oder die BCMK können in diesem Fall für Rückfragen zur Verfügung stehen. Es ist in diesem Fall empfehlenswert, dass der BCMB oder BCMK die BIA zwecks Qualitätssicherung auswertet (siehe Kapitel 6.5.3 *Auswertung*).

Unabhängig vom gewählten Format sollten bei der Terminplanung etwaige Spannungsfelder aufgrund von Ressourcenengpässen oder besonderen Terminen und Ereignissen (z. B. Endjahresgeschäft) in der Terminfestlegung berücksichtigt werden. Zudem sollten Pufferzeiten für etwaige Nacharbeiten, Rückfragen oder Abstimmungsrunden berücksichtigt werden.

Es ist empfehlenswert, den maximal erwünschten Gesamtzeitraum der BIA inklusive Nachbereitung und Auswertung festzulegen. Dadurch können die personellen und zeitlichen Ressourcen darauf ausgerichtet werden (siehe Kapitel 3.2.4 *Ressourcenplanung).*

6.5.1.5 Vorbereitung der BIA-Hilfsmittel

Es muss sichergestellt werden, dass die Ergebnisse des BIA-Durchlaufs einheitlich und nachvollziehbar dokumentiert werden. Hierzu sollten Hilfsmittel vorbereitet werden, die den Ansprechpartnern die Schadensbewertung vereinfachen.

Präsentation zur Erläuterung der BIA

Mit der Präsentation zur Erläuterung der BIA können die Ansprechpartner thematisch auf die Schadensbewertung vorbereitet werden. Dazu ist es empfehlenswert, das Ziel der BIA und die Vorgehensweise zur Schadensbewertung vorzustellen (siehe Abbildung 50). Zudem ist es hilfreich zu erläutern, welche Auswirkungen

die Antworten auf die Folgeschritte im BCM-Prozess haben, unter anderem auf die Geschäftsfortführungsplanung. Um die BIA-Methodik vorzustellen, kann die *Präsentationsvorlage Voranalyse/BIA* aus den Hilfsmitteln verwendet werden.

Liste der Geschäftsprozesse

Als Ergebnis der Identifizierung der Geschäftsprozesse (siehe Kapitel 6.5.1.1 *Erhebung der Geschäftsprozesse*) liegt eine Liste aller Geschäftsprozesse innerhalb des jeweiligen Prozessumfangs vor. Da alle Geschäftsprozesse anhand dieser Liste in der BIA untersucht werden müssen, kann daraus der zu erwartende Umfang der BIA abgeleitet werden. Dies vereinfacht die organisatorische Planung.

Hilfsmittel zur Erhebung und Auswertung der BIA

Um die Informationen einheitlich und vollständig zu erheben, sollte ein Hilfsmittel zur Erhebung und Auswertung der BIA genutzt werden. Dies kann eine Dokumentenvorlage oder ein Software-Tool sein.

Hinweis:

Der Einsatz geeigneter Software-Tools kann die Tätigkeiten der an der BIA beteiligten Personen erheblich erleichtern. Einige Softwareprodukte geben dabei eigene Methoden und Vorgehensmodelle zur Business Impact Analyse vor, an denen sich die Benutzer orientieren können. Entsprechende Frage- und Auswertungsschemata sind vorgegeben und können ohne größere Aufwände sofort umgesetzt und genutzt werden, da sich diese üblicherweise an den etablierten BCM-Standards orientieren. Anhand von Pflichtfeldern und Prüffunktionen kann die Datenqualität sichergestellt werden. Bei der Auswahl eines Software-Tools sollte neben dem Preis und den Leistungsmerkmalen, darauf geachtet werden, dass die Größe und die Art der eigenen Institution unterstützt wird. Weitere Information zum Tooleinsatz können dem Hilfsmittel *Tools* entnommen werden.

Es ist empfehlenswert, die Vorlage oder das Tool mit den bereits bekannten Daten zu Geschäftsprozessen und möglichen Ressourcen(-clustern) im Vorfeld zu befüllen. Hierzu kann auf bereits bestehende Dokumentationen oder Datenbanken zurückgegriffen werden. Eine vorgegebene Auswahl möglicher Geschäftsprozesse und Ressourcen(-cluster) erleichtert es den Ansprechpartnern, die BIA durchzuführen und Fehleingaben zu vermeiden. Ferner müssen die Daten in der Auswertung nicht mehr auf Dubletten oder Schreibfehler untersucht werden. Die Dokumentenvorlage *BIA-Auswertungsbogen* aus den Hilfsmitteln zeigt eine Variante auf, wie eine BIA einheitlich und vollständig erhoben werden kann.

Synergiepotenzial:

Sofern bereits ein ISMS nach BSI-Standard 200-2 besteht, könnten für die Schutzbedarfsfeststellung (SBF) bereits Hilfsmittel erstellt worden sein, die für die BIA adaptiert werden können. Werden in der BIA und SBF dieselben Schadensszenarien und -kategorien verwendet, können die Analysen kombiniert erhoben werden. Dies bietet sich insbesondere bei Einsatz eines Software-Tools an. Der Vorteil besteht darin, dass Abweichungen zwischen der Verfügbarkeit und Kontinuität leichter identifiziert werden können.

Ferner können aus der Strukturanalyse mögliche Zuordnungen zwischen Geschäftsprozessen und Ressourcen übernommen werden. Diese sollten jedoch anschließend in der Durchführung der BIA auf ihre Relevanz für den Notbetrieb überprüft werden.

Übersicht zu Schadenskategorien und Schadensszenarien

Um eine vergleichbare Schadensbewertung zu erhalten, sollten die Ansprechpartner die Schadensszenarien und Ausprägungen je Schadenskategorie kennen. Wie in Tabelle 44 dargestellt, sollten den Ansprechpartnern ein entsprechendes Hilfsmittel schriftlich zur Verfügung gestellt werden, z. B. in Form einer BIA-Anweisung oder einer Präsentation.

6.5.2 Durchführung der BIA

Sind die notwendigen Vorbereitungen abgeschlossen, kann mit der BIA begonnen werden. Abhängig von der organisatorischen Planung erfolgt die BIA-Durchführung entweder in Form von Workshops oder eigenständig durch die zuständigen Ansprechpartner. Die Durchführung der BIA unterteilt sich in die nachfolgenden zwei Teilprozessschritte **Schadensbewertung**, **Identifizierung der Prozessabhängigkeiten** und **Identifizierung der Ressourcenabhängigkeiten**.

6.5.2.1 Schadensbewertung

Die Schadensbewertung umfasst die im Nachfolgenden vorgestellten Teilprozessschritte.

Festlegung des Schadenspotenzials

Durch die Ansprechpartner muss das Schadenspotenzial ihrer Geschäftsprozesse für alle definierten Zeithorizonte bewertet werden. Hierzu kann auf die Leitfrage der BIA zurückgegriffen werden, die z. B. in der Workshop-Präsentation oder in der BIA-Anweisung dokumentiert wurde (siehe Kapitel 6.5.1.5 *Vorbereitung der BIA-Hilfsmittel*).

Tabelle 46 zeigt beispielhaft eine Schadensbewertung für einen Geschäftsprozess anhand der verschiedenen Schadensszenarien. Hierzu werden die BIA-Parameter zugrunde gelegt, die in der Vorbereitung der BIA im Kapitel 6.5.1.2 *Festlegung der BIA-Parameter und betrachteten Zeithorizonte* erläutert wurden.

Die Einzelbewertungen je Schadensszenario müssen nicht gesondert dokumentiert werden, um im folgenden Schritt die MTPD festlegen zu können. Um den Dokumentationsaufwand zu reduzieren, kann das Schadenspotenzial anhand des schlimmsten, anzunehmenden Falls (engl.: *worst case*) dokumentiert werden. Entsprechend muss nur das Schadensszenario mit dem jeweils höchsten Schadenspotenzial in einem Zeithorizont dokumentiert werden. Hierzu wurde in der Vorbereitung der BIA auch das Hilfsmittel *Übersicht zu Schadensszenarien und Schadenskategorien* so aufgebaut, dass diese die worst case-Betrachtung erleichtert (siehe Tabelle 44). Tabelle 47 greift das Beispiel von Tabelle 46 *a*uf, reduziert jedoch die Schadensbewertung auf eine worst case-Sicht, die alle Schadensszenarien beinhaltet. Neben dem Vorteil, dass die Schadensbewertung beschleunigt wird, ermöglicht diese Sicht einen Gesamtüberblick über die Geschäftsprozesse und deren Schadensbewertung.

Hinweis:

Mitunter kann es ein ausgefallener Geschäftsprozess zu bestimmten Ereignissen und Terminen zu höheren Schäden als gewöhnlich führen. Dies kann etwa im Rahmen des Endjahresgeschäftes, Rechnungsabschlüssen oder vergleichbarem der Fall sein. Um diesen Umstand in der weiteren Notfallplanung zu berücksichtigen, können die Geschäftsprozesse grundsätzlich unter der Prämisse bewertet werden, dass diese am ungünstigsten Zeitpunkt (engl.: worst case) im Jahr ausfallen. Grundsätzlich ist es auch möglich, die Zeiträume getrennt zu betrachten und in der weiteren Notfallplanung auch getrennt zu behandeln. Erfahrungsgemäß führt dies jedoch zu einer hohen Komplexität und damit verbunden höheren Gesamtaufwänden. Es ist empfehlenswert, den ungünstigsten Zeitpunkt oder Zeitraum zu dokumentieren, der für die Bewertung zu Grunde gelegt wurde. Dadurch kann die BAO im Not- oder Krisenfall den Wiederanlauf der zeitkritischen Geschäftsprozesse konkreter anhand der jeweiligen Situation priorisieren.

Beispiel: Schadensbewertung des Geschäftsprozesses „Sicherstellung IT-Betrieb“ anhand verschiedener Schadensszenarien

Leitfrage: Wenn der Geschäftsprozess **Sicherstellung IT-Betrieb** ausfällt, mit welchem Schadenspotenzial *[1-gering, 2-mittel, 3-hoch, 4-sehr hoch]* ist bei einem Ausfall bis zu *[24 Stunden, 3 Tage, 7 Tage, 14 Tage, 30 Tage]* zu rechnen?

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

Tabelle 46: Beispiel einer Schadensbewertung anhand der verschiedenen Schadensszenarien

Wenn der nachfolgend aufgeführte Geschäftsprozess ausfällt, mit welchem Schadenspotenzial [1-gering, 2-mittel, 3-hoch, 4-sehr hoch] ist bei einem Ausfall bis zu … zu rechnen?

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

Tabelle 47: Beispielhafte Schadensbewertung nach dem worst case-Prinzip

In der Schadensbewertung muss berücksichtigt werden, dass ein einmal eingetretener Schaden nur gleichbleiben oder weiter steigen, nicht jedoch im Laufe der Zeit wieder abnehmen kann. Tabelle 48 zeigt hierzu beispielhaft ein korrektes (Geschäftsprozess RICHTIG) und fehlerhaftes Ergebnis (Geschäftsprozess FALSCH). Die fehlerhafte Angabe ist rot hervorgehoben.

Beispiel:

Geschäftsprozess	24 Stunden	3 Tage	7 Tage	14 Tage	30 Tage
Geschäftsprozess RICHTIG	2 - mittel	3 - hoch	3 - hoch	4 - sehr hoch	4 - sehr hoch
Geschäftsprozess FALSCH	2 - mittel	2 - mittel	3 - hoch	3 - hoch	2 - mittel

Tabelle 48: Beispiel einer korrekten und fehlerhaften Schadensbewertung

Festlegung der MTPD

Um die MTPD eines Geschäftsprozesses zu bestimmen, muss der kleinste Zeithorizont gewählt werden, bei dem das Untragbarkeitsniveau erreicht wird. Tabelle 49 zeigt einige Beispiele, wie die MTPD anhand des Schadenspotenzials festgelegt wird. Die relevanten Zeithorizonte, zu denen das Untragbarkeitsniveau erreicht wird, sind rot eingefärbt. Der daraus jeweils kleinste Zeithorizont liefert die MTPD (rot umrandet). Für die nachfolgenden Beispiele wird die Schadenskategorie 3 – Hoch als Untragbarkeitsniveau zugrunde gelegt.

Das erste Beispiel in Tabelle 49 (Geschäftsprozess Sicherstellung IT-Betrieb) greift das Geschäftsprozess-Beispiel aus der Abbildung 49 und Tabelle 47 auf.

Beispiel:

Leitfrage: Wenn der Geschäftsprozess ausfällt, mit welchem Schadenspotenzial [1 - gering, 2 - mittel, 3 - hoch, 4 - sehr hoch] ist bei einem Ausfall bis zu … zu rechnen?

Geschäftsprozess	24 Stunden	3 Tage	7 Tage	14 Tage	30 Tage	MTPD
Sicherstellung IT-Betrieb	2-mittel	3 - hoch	4 – sehr hoch	4 – sehr hoch	4 - sehr hoch	3 Tage
Berechtigungsmanagement	1 - gering	2 - mittel	3 - hoch	3 - hoch	3 - hoch	7 Tage
Incident Management	3 - hoch	3 - hoch	3 - hoch	4 - sehr hoch	4 - sehr hoch	24 Stunden
Problem Management	1 - gering	1 - gering	1 - gering	1 - gering	1 - gering	Keine

Tabelle 49: Beispiele für die Festlegung der MTPD (Erreichen des Untragbarkeitsniveaus 3-hoch rot hervorgehoben)

Hinweis:

In der Praxis wird das Schadenspotenzial durch die Prozesseigentümer bzw. Prozessexperten häufig zunächst anhand der direkten Auswirkungen auf den Geschäftsprozess bewertet. Jedoch können aus vorherigen BCMS-Zyklen Erkenntnisse aus den Prozessabhängigkeiten vorliegen, die in der Schadensbewertung berücksichtigt werden sollten (siehe Kapitel 6.5.2.3 *Identifizierung der Ressourcenabhängigkeiten)*. Diese Erkenntnisse sollten sich auch in der nachfolgenden Begründung der Schadensbewertung wiederfinden.

Begründung der Schadensbewertung

Die Schadensbewertung muss je Geschäftsprozess begründet und dokumentiert werden. Dies hat zwei wesentliche Gründe:

- Wenn die BIA in einem neuen BCMS-Zyklus aktualisiert wird, kann auf die bestehenden Informationen zurückgegriffen werden. Damit die Schadensbewertung auch zu einem späteren Zeitpunkt nachvollziehbar ist, sollte diese begründet werden.
- Regulatoren setzen eine Begründung voraus, um auch als außenstehende Dritte die Schadensbewertung dahingehend überprüfen zu können, ob diese plausibel ist.

Die Schadensszenarien, die maßgeblich in der Schadensbewertung zur MTPD beigetragen haben, sollten in der Begründung benannt werden. Wird die BIA aktualisiert, kann so besser überprüft werden, ob die für die Schadensbewertung getroffenen Annahmen noch aktuell sind oder angepasst werden müssen. Tabelle 50 greift das Beispiel aus Tabelle 49 auf und erweitert dieses um die Begründung der Schadensbewertung. Aus Platzgründen wird die Schadensbewertung ausgeblendet.

Beispiel:

Geschäftsprozess	~	MTPD	Begründung des Schadenspotenzials
Sicherstellung IT-Betrieb	~	3 Tage	Bei Ausfall des Prozesses ist kein IT-Monitoring und keine Wartung der Systeme möglich. Zudem können keine IT-Arbeitsplätze bereitgestellt oder defekte Geräte ausgetauscht werden. Ein kurzfristiger Ausfall des Prozesses bis 24 h führt zu Arbeitsrückständen, wird jedoch nur intern bemerkt. Fällt der Prozess bis zu 3 Tage aus ist mit nicht tolerierbarer Beeinträchtigung der Aufgabenerfüllung in der gesamten Institution zu rechnen, da kein reibungsloser IT-Betrieb garantiert werden kann. Nicht eingespielte Patches bergen zudem ein zunehmendes Sicherheitsrisiko. Ab 7 Tagen ist zusätzlich sowohl mit internem Ansehensverlust als auch mit einer erheblichen negativen Außenwahrnehmung zu rechnen.
Berechtigungsmanagement	~	24 Stunden	Bei Ausfall des Prozesses können bestehende Berechtigungen nicht angepasst oder neue Berechtigungen gesetzt werden. Zudem können die vorhandenen Regeln nicht überwacht werden. Dies wäre im Normalbetrieb bis zu 3 Tage tolerierbar. Da jedoch im Notfall für zeitkritische Geschäftsprozesse Berechtigungen zeitnah konfiguriert werden müssen, wird das Berechtigungsmanagement durch das Incident Management und IT-Notfallmanagement zeitkritischer bewertet (Prozessabhängigkeit).

Tabelle 50: Beispielhafte Begründung einer Schadensbewertung

Für nicht zeitkritische Geschäftsprozesse entfallen die nachfolgenden Schritte, da diese im Rahmen des BCM nicht weiter betrachtet werden.

Festlegung des Notbetriebsniveaus

Um im folgenden Schritt die für einen Notbetrieb zwingend erforderlichen Prozess- und Ressourcenabhängigkeiten ermitteln zu können, muss vorab festgelegt werden, welches Notbetriebsniveau in einem zeitkritischen Geschäftsprozess erreicht werden soll.Hierzu genügt eine stichpunktartige Beschreibung, welche Aktivitäten des Geschäftsprozesses innerhalb des Notbetriebs aufrechterhalten werden sollen bzw. welche Aktivitäten zurückgestellt werden können (Priorisierung). Je nach Aufgaben- bzw. Geschäftszweck ist auch eine prozentuale Angabe des Notbetriebsniveaus möglich, z. B. im produzierenden Gewerbe.

Tabelle 51 greift das Beispiel aus Tabelle 50 auf und erweitert dieses um das Notbetriebsniveau zu den einzelnen Prozessen. Aus Platzgründen wird die Schadensbewertung und Begründung des Schadenspotentials ausgeblendet.

Beispiel:

Geschäftsprozess	~	Notbetriebsniveau
Sicherstellung IT-Betrieb	~	Der Fokus liegt auf dem IT-Monitoring sowie Patchen von Systemen. Wartungsarbeiten, die nicht der Sicherheit oder Stabilität des IT-Betriebs dienen, werden zurückgestellt. Anfragen von Organisationseinheiten zum Austausch fehlerhafter Geräte oder dem Bereitstellen neuer Geräte werden nach Dringlichkeit bearbeitet und unter Umständen zurückgestellt.
Incident Management	~	Der Fokus liegt auf der Bearbeitung von Major Incident-Tickets. Wenn der Notbetrieb nur wenige Tage andauert, können bei 50% Arbeitsvolumen die entstehenden Arbeitsrückstände leicht kompensiert werden. Da mit jedem weiteren Tag auf Notbetriebsniveau jedoch Tickets unbearbeitet bleiben, muss das Notbetriebsniveau schrittweise auf 80% Arbeitsvolumen gesteigert werden.

Tabelle 51: Beispiel eines dokumentierten Notbetriebsniveaus

Zudem kann es hilfreich sein, nicht nur den Zielzustand des Notbetriebsniveaus zu beschreiben, sondern auch mögliche kurz- und langfristige Ziele, z. B. was soll in den ersten Stunden, Tagen oder bis Zeitraum x im Notbetrieb erreicht werden? Wenn das Notbetriebsniveau über einen zeitlichen Verlauf betrachtet wird, kann die Information dabei helfen den Ressourcenbedarf im Notbetrieb zeitlich differenziert zu erheben.

Die Schadensbewertung ist abgeschlossen, wenn

- die Geschäftsprozesse im Prozessumfang hinsichtlich ihres Schadenspotenzials bewertet,
- die MTPD je zeitkritischem Geschäftsprozess festgelegt und begründet sowie
- für zeitkritische Geschäftsprozesse das erforderliche Notbetriebsniveau definiert wurde.

6.5.2.2 Identifizierung der Prozessabhängigkeiten

In der Schadensbewertung wurden die Geschäftsprozesse der Institution weitestgehend isoliert betrachtet. In der Praxis bestehen jedoch verschiedene Abhängigkeiten zwischen den Geschäftsprozessen (Prozessketten), z. B. durch vor- oder nachgelagerte, aufeinander aufbauende Tätigkeiten.

Beispiel:

Informationsbasierte Abhängigkeiten: Die Geschäftsprozesse erhalten oder liefern Informationen an andere Geschäftsprozesse, wie z. B. die Kommunikation des 1st-Level-Supports mit dem 2nd-Level-Support.

Güterbasierte Abhängigkeiten: Die Geschäftsprozesse erhalten oder liefern Güter an andere Geschäftsprozesse. Häufig läuft dies zeitlich oder kausal bedingt in einer festen Reihenfolge ab, z. B. bei aufeinander aufbauenden Produktionsschritten oder in Logistikprozessen.

Tätigkeitsbasierte Abhängigkeiten: Die Geschäftsprozesse dienen dazu, Aufträge von anderen Geschäftsprozessen zu erledigen, wie z. B. den postalischen Versand von Briefen an Kunden durch die Poststelle im Auftrag der Kundenbetreuer.

Geschäftsprozesse können nicht nur ausfallen, weil Ressourcen ausgefallen sind, sondern auch, weil benötigte Geschäftsprozesse nicht verfügbar sind. Für alle zeitkritischen Geschäftsprozesse muss daher ermittelt werden, ob für einen Notbetrieb eine unverzichtbare Abhängigkeit zu anderen Geschäftsprozessen besteht.

Unverzichtbar bedeutet hierbei, dass benötigte Geschäftsprozesse den Notbetrieb verhindern oder stark beeinträchtigen, wenn die Wiederanlaufzeiten der abhängigen und benötigten Geschäftsprozesse nicht aufeinander abgestimmt sind. Sofern im Rahmen der Erhebung der Geschäftsprozesse bereits Prozessabhängigkeiten erfasst wurden, können diese als Grundlage zum weiteren Vorgehen verwendet werden.

Grundsätzlich kann zwischen zwei Abhängigkeitsgraden unterschieden werden:

1. Es besteht keine Prozessabhängigkeit im Notfall.
2. Es besteht eine Prozessabhängigkeit und die Wiederanlaufzeiten der Geschäftsprozesse müssen zeitlich aufeinander abgestimmt werden. Die MTPD der benötigten Geschäftsprozesse müssen so gewählt werden, dass die MTPD des abhängigen Geschäftsprozesses jeweils gewährleistet wird. Die MTPD des benötigten Geschäftsprozesses muss darüber bestimmt werden, ob er nur wiederangelaufen oder bereits abgeschlossen sein muss, bevor der abhängige Geschäftsprozess startet. Ob die MTPD des benötigten Geschäftsprozesses kleiner, gleich oder größer sein darf als die MTPD des abhängigen Geschäftsprozesses, muss im Einzelfall abgestimmt werden.

Wurden abhängige Geschäftsprozesse identifiziert, sollte mit dem Ansprechpartner des abhängigen Geschäftsprozesses abgestimmt werden, welche MTPD der benötigte Geschäftsprozess erhält. Dieser Prozess wird damit automatisch auch zeitkritisch. Abhängigkeiten zwischen Geschäftsprozessen sollten individuell eingeschätzt werden, da diese von den individuellen Anforderungen an den Notbetrieb eines Geschäftsprozesses sowie vom Grad der Abhängigkeit beeinflusst werden.

Hinweis:

Über diesen BCM-Prozessschritt wird iterativ in jedem BIA-Zyklus eine weitere Stufe der Prozessabhängigkeiten erfasst. So können über mehrere Zyklen zeitkritische Prozessketten identifiziert werden. Bei der Abstimmung der MTPD sollte daher darauf geachtet werden, dass die MTPD eines abhängigen Geschäftsprozesses sich nicht automatisch auf alle weiteren Prozessabhängigkeiten der benötigten Geschäftsprozesse minimierend auswirken (Kaskadeneffekt).

Nachfolgend sind einige Beispiele dargestellt, wie notfallrelevante Prozessabhängigkeiten identifiziert werden können.

Beispiel:

Antragsbearbeitung: Der Geschäftsprozess *Antragsbearbeitung*, mit einer MTPD von 3 Tagen, ist vom Geschäftsprozess *Antragsprüfung* abhängig. Die Antragsprüfung hat eine geringere Prozessausführungszeit. Zudem sind erfahrungsgemäß immer mehr Anträge bereits geprüft, als in Bearbeitung (Arbeitsvorrat). Obwohl eine zeitkritische Abhängigkeit zwischen beiden Geschäftsprozessen besteht, kann der abhängige Geschäftsprozess *Antragsbearbeitung* wiederaufgenommen werden, ohne dass der benötigte Geschäftsprozess *Antragsprüfung* bereits läuft. Daher wird zwischen den Prozesseigentümern vereinbart, dass die MTPD des benötigten Geschäftsprozesses *Antragsprüfung* mit 7 Tagen deutlich größer sein kann, als die MTPD des abhängigen Geschäftsprozesses *Antragsbearbeitung.*

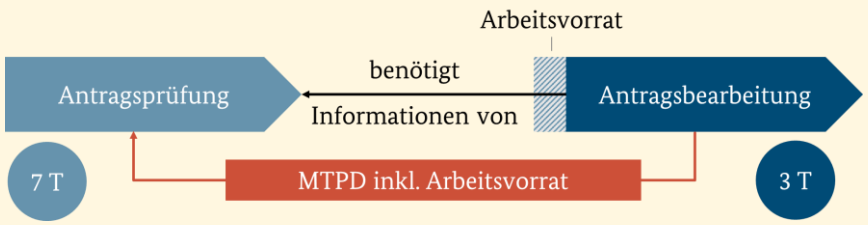

Abbildung 52: Beispiel einer informationsbasierten Prozessabhängigkeit

Kundenbetreuung: Der Geschäftsprozess *Kundenbetreuung* mit einer MTPD von 3 Tagen ist von einem ausgelagerten Geschäftsprozess *Telefon-Hotline-Dienst* abhängig. Dieser stellt sicher, dass Anrufe angenommen, die Anfragen geprüft und an das richtige Team in der *Kundenbetreuung* weitergeleitet werden. Da der benötigte Geschäftsprozess *Telefon-Hotline-Dienst* parallel zum abhängigen Geschäftsprozess *Kundenbetreuung* ausgeführt werden muss, wird entschieden, dass die MTPD des abhängigen Geschäftsprozesses übernommen wird.

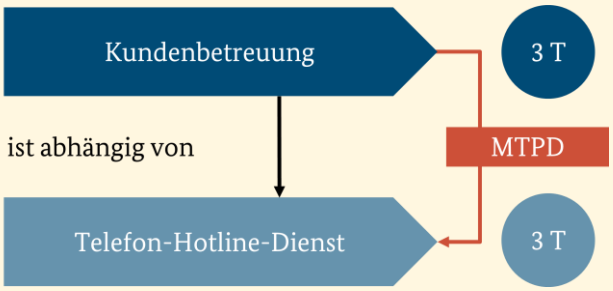

Abbildung 53: Beispiel einer parallelen Abhängigkeit zweier Geschäftsprozesse

Produktion: Der Geschäftsprozess *Produktion*, mit einer MTPD von 3 Tagen, ist vom nachgelagerten Geschäftsprozess *Distribution* abhängig. Da nur begrenzte Lagermöglichkeiten für die produzierten Güter bestehen, können diese maximal 2 weitere Tage aufbewahrt werden, bevor das Lagervolumen ausgeschöpft ist. Um einen kontinuierlichen Produktionsfluss zu gewährleisten, wird beschlossen die MTPD des benötigten Geschäftsprozesses *Distribution* auf 5 Tage festzulegen.

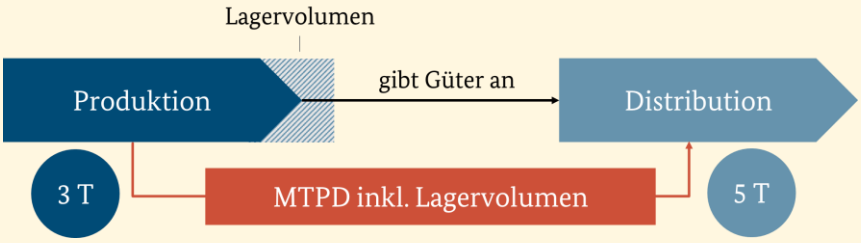

Abbildung 54: Beispiel einer güterbasierten Prozessabhängigkeit

Hinweis:

Bei der Identifizierung der Prozessabhängigkeiten im BCM geht es nicht darum, eine vollständige Prozesslandkarte für den Normalbetrieb zu erstellen. Auch handelt es sich nicht automatisch um eine notfallrelevante Abhängigkeit, wenn zwei Geschäftsprozesse im Normalbetrieb in einer bestimmten Reihenfolge ablaufen oder Informationen austauschen. Notfallrelevante Abhängigkeiten bestehen nur dann, wenn für den Wiederanlauf des untersuchten Geschäftsprozesses weitere Geschäftsprozesse zwingend benötigt werden, um das definierte Notbetriebsniveau zu erreichen.

In der Praxis ist es empfehlenswert, die Prozessabhängigkeiten iterativ zu erfassen, so wie in diesem Standard beschrieben. So fließen die Erkenntnisse aus zeitkritischen Prozessabhängigkeiten in die zukünftige Schadensbewertung der Geschäftsprozesse ein. Mit steigender Reife des BCMS steigt damit auch die Qualität der BIA und der Geschäftsfortführungspläne, da Geschäftsprozesse nicht isoliert betrachtet werden, sondern als Prozesskette verstanden werden.

6.5.2.3 Identifizierung der Ressourcenabhängigkeiten

Für alle Geschäftsprozesse mit einer MTPD müssen anhand der festgelegten Ressourcenkategorien (siehe Kapitel *4.4.1.3 Festlegung der Ressourcenkategorien und -cluster*) die für einen Notbetrieb erforderlichen Ressourcen ermittelt und den entsprechenden Geschäftsprozessen zugeordnet werden.

Erfahrungsgemäß wird nicht jede Ressource, die von einem Geschäftsprozess im Normalbetrieb genutzt wird, auch per se in einem Notbetrieb benötigt. Zum einen können Ressourcen entfallen, die lediglich für zurückgestellte Aktivitäten gemäß dem definierten Notbetriebsniveau benötigt werden. Zum anderen werden in der Praxis häufig Ressourcen eingesetzt, die einen Prozess im Normalbetrieb effizienter oder einfacher gestalten, aber nicht zwingend erforderlich sind, um das gewünschte Prozessergebnis auf dem definierten Notbetriebsniveau zu erreichen. Da im BCM prinzipiell nur die zwingend erforderlichen Ressourcen besonders abgesichert und in der weiteren Notfallplanung berücksichtigt werden sollen, kann auf die Angabe von Ressourcen, die nur im Normalbetrieb eingesetzt werden, bewusst verzichtet werden.

Mit steigender Reife des BCMS und sofern ausreichend Ressourcen hierzu bestehen, können jedoch auch die im Normalbetrieb genutzten Ressourcen miterfasst werden. Auch wenn die Normalbetriebsressourcen nicht zwingend für den Notbetrieb benötigt werden, kann deren Identifikation dabei helfen, in der späteren Notfallplanung oder ad hoc im Notfall den Notbetrieb komfortabler und effizienter zu gestalten.

Beispiel:

Ein Mitarbeiter kann über ein *Customer-Relationship-Management (CRM)-System* schnell Kontakte identifizieren und Zusatzinformationen abrufen. Im Notbetrieb genügt es aber möglicherweise auch, nur über die Kontaktdaten aus einem Adressbuch zu verfügen, um den Geschäftsprozess aufrecht zu erhalten.

In einer hohen Reife des BCMS kann gegebenenfalls das CRM-System, obwohl es nicht zeitkritisch ist, mit in der BIA erfasst und in der späteren Notfallplanung oder ad hoc im Notfall berücksichtigt werden. Der Mitarbeiter hat so die Möglichkeit gewonnen, den Geschäftsprozess im Notbetrieb effizienter als notwendig durchzuführen und somit nicht nur das Notbetriebsniveau zu erreichen, sondern dieses zu übertreffen.

Die Ressourcen(-cluster) sollten anhand vorgegebener Listen ermittelt und dokumentiert werden. So werden unterschiedliche Namen oder Schreibweisen für gleiche Ressourcen(-cluster) vermieden und Dubletten ausgeschlossen. Zusätzliche Aufwände in der BIA-Auswertung, um Dubletten zu identifizieren und zusammenzuführen, können damit vermieden werden. Je zeitkritischem Geschäftsprozess muss festgelegt und dokumentiert werden, welche Ressourcen(-cluster) benötigt werden, um das vorab definierte Notbetriebsniveau zu erreichen. Relevant für die weiteren Schritte in der Notfallplanung der Ressourcen sind die folgenden BIA-Kenngrößen:

- Geforderte Wiederanlaufzeit (RTO)
- Maximal zulässiger Datenverlust (RPO)

RTO

Anhand der MTPD des zeitkritischen Geschäftsprozesses muss die RTO der prozessnotwendigen Ressourcen(-cluster) abgeleitet werden. Da zwischen dem Eintritt eines Schadensereignisses und dem Beginn des Wiederanlaufs einer Ressource Zeit für die Detektion und Alarmierung verlorengeht, muss die RTO der Ressource kleiner als die MTPD des zeitkritischsten Geschäftsprozesses sein.

Hinweis:

Ähnlich wie die MTPD in den Prozessabhängigkeiten kann auch die RTO individuell abgestimmt werden. Diese ist abhängig von

- der zeitlichen Lücke, die sich aus dem Detektions- und Alarmierungsprozess ergibt,
- dem angestrebten Notbetriebsniveau und damit dem Leistungsumfang der Ressource sowie
- der Art der Prozessunterstützung (Die Ressource wird benötigt, um den Geschäftsprozess wiederanlaufen, ausführen oder abschließen zu können).

Da die Faktoren zum Zeitpunkt der BIA nur geschätzt werden können, kann die RTO näherungsweise mit der Angabe „<“ dokumentiert werden. Die Angabe sollte jedoch in der Weiterentwicklung des BCMS schrittweise konkretisiert werden.

Wenn mehrere Geschäftsprozesse auf dieselbe(n) Ressourcen(-cluster) zurückgreifen, muss die RTO kleiner als die MTPD des zeitkritischsten Geschäftsprozesses im Prozessumfang der BIA gewählt werden (Minimalprinzip).

Beispiel (sortiert nach Ressource):

Ressourcen, deren RTO auf Grund des Minimalprinzips ermittelt wurden, sind rot hervorgehoben.

Ressourcen-kategorie	Ressource	RTO	Geschäftsprozess	MTPD
IT	Telefonie	20 Stunden	Incident Management	24 Stunden
IT	Monitoringtool MT	< 3 Tage	Sicherstellung IT-Betrieb	3 Tage
IT	Monitoringtool MT	< 3 Tage	Berechtigungs-ma-nagement	7 Tage
IT	Identity & Access Man-agement Tool IAM	5 Tage	Berechtigungsma-nagement	7 Tage
Dienstleistun-gen	IT-Provider XYZ	8 Stunden	Sicherstellung IT-Betrieb	3 Tage
Dienstleistun-gen	IT-Provider XYZ	8 Stunden	Berechtigungsma-nagement	7 tage
Informatio-nen	Konfigurationsdaten	n/a	Sicherstellung IT-Betrieb	3 Tage

Tabelle 52: Beispiele für Ressourcenabhängigkeiten verschiedener Geschäftsprozesse

Tabelle 52 greift die Beispiele der Geschäftsprozesse aus Tabelle 49 auf und erweitert diese um die benötigten Ressourcen je Geschäftsprozess. Indem z. B. die Tabelle nach den Ressourcen sortiert wird, wird anhand der mehrfach genannten Ressourcen klar, wie die kleinste RTO daraus abgeleitet werden kann.

RPO

Bei informationsbasierten Ressourcenkategorien, wie im vorliegenden Beispiel IT und Informationen, muss zusätzlich die RPO festgelegt werden. Die RPO stellt in diesem Zusammenhang eine fachliche Anforderung des Prozesseigentümers dar, bis zu welchem Grad er eine Datensicherung voraussetzt, um mit geeigneten Informationen im Notbetrieb arbeiten zu können. Die RPO ist **unabhängig** von der MTPD und muss daher nicht darauf abgestimmt werden. Jedoch sollte analog zur RTO auch die RPO konsolidiert werden, wenn mehrere Geschäftsprozesse auf dieselbe(n) informationsbasierten Ressourcen(-cluster) zurückgreifen (Minimalprinzip).Tabelle 53 greift die Beispiele der Geschäftsprozesse aus Tabelle 49, analog zu Tabelle 52.

Beispiel:

Ressourcen-kategorie	Ressource	Konsolidierte RPO	Geschäftsprozess	RPO
Informationen	Konfigurationsdaten	Transaktionsgenau	Berechtigungsmanagement	Transaktionsgenau
Informationen	Konfigurationsdaten	Transaktionsgenau	Sicherstellung IT-Betrieb	Vortag

Tabelle 53: Beispiele für informationsbasierte Ressourcenabhängigkeiten verschiedener Geschäftsprozesse

Synergiepotenzial:

Die RPO sollte bereits innerhalb des Normalbetriebs z. B. als Datensicherungsintervall definiert worden sein und kann hier zugrunde gelegt werden. Sofern die RPO nicht definiert oder nicht bekannt ist, genügt an dieser Stelle die Information, welcher Datenverlust im Notbetrieb zulässig wäre. Üblicherweise bestehen im IT-Betrieb bereits verschiedene Stufen von Datensicherungsintervallen. Für die Angabe der RPO ist es empfehlenswert, sich auf diese Stufen zu beziehen oder abgestimmt mit dem IT-Betrieb diese Stufen zu erweitern.

Ressourcenbedarf in Abhängigkeit zur Dauer des Notbetriebs

Für bestimmte Ressourcenkategorien wie z. B. Personal und Arbeitsplätze, aber auch Maschinen oder Arbeitsmittel steigt die Anzahl der benötigten Ressourcen mit der Dauer des Notbetriebs erfahrungsgemäß an. Dies hat einerseits damit zu tun, das ansteigende Arbeitsvolumen aufzufangen (z. B. durch ein steigendes Notbetriebsniveau) als auch andererseits die weiteren, zeitkritischen Geschäftsprozesse bedienen zu können. Für diese Ressourcenkategorien ist es empfehlenswert, die Anzahl der benötigten Ressourcen über die definierten Zeithorizonte im Notbetrieb hinweg zu erheben.

Bei der Ressource Personal ist es empfehlenswert, zu berücksichtigen, ob sich die Anzahl je Geschäftsprozess aufsummiert oder unterschiedliche zeitkritische Geschäftsprozesse jeweils die gleichen Personen oder Rollen benötigen. In diesem Fall ist es empfehlenswert, die Anzahl kumuliert anstatt pro Geschäftsprozess zu erheben. Dies hat zum Ziel, Ressourcen, die für mehrere Geschäftsprozesse benötigt werden, nicht mehrfach oder als Anteil erfassen zu müssen. Tabelle 54 gibt ein Beispiel für die zeitlich gestaffelte Erhebung anhand des Arbeitsplatz- und Rollenbedarfs der Organisationseinheit wieder.

Beispiel: Benötigte Anzahl Arbeitsplätze oder Personal im Notbetrieb der OE IT-Betrieb

Ressourcen-kategorie	Ressource	Anmerkungen	24 Stunden	3 Tage	7 Tage	14 Tage	30 Tage
Arbeitsplatz	Standard-Arbeitsplatz		2	2	2	4	4
Personal	Teamleiter	arbeiten remote	1	2	2	2	2
Personal	Help Desk-Mitarbeiter		2	2	2	4	4
Personal	Datenbank-Administrator	arbeiten remote	1	2	3	3	3

Tabelle 54: Beispiel für Arbeitsplatz- und Personalabhängigkeiten

Im Beispiel wird angenommen, dass die Organisationseinheit über 2 Teamleiter, 4 Help Desk-Mitarbeiter, 4 System-Administratoren und 3 Datenbank-Administratoren verfügt. Jede dieser Personen verfügt im Normalbetrieb über einen eigenen Arbeitsplatz. Während eines eingeschränkten Notbetriebs werden innerhalb der ersten 24 Stunden zunächst nur 1 Teamleiter, 2 Help Desk-Mitarbeiter und 1 Datenbank-Administrator benötigt, da nur das Incident Management entsprechend zeitkritisch ist. Hierbei werden nur 2 Arbeitsplätze benötigt, damit die Help Desk-Mitarbeiter agieren können. Der Teamleiter und die Administratoren können. mobil arbeiten.

6.5.2.4 Identifizierung vorhandener Single Point of Failure

Wenn viele (sehr) zeitkritische Geschäftsprozesse eine einzelne Ressource benötigen, stellt diese ein erhöhtes Risiko für eine Geschäftsunterbrechung dar. Insbesondere wenn der Wiederanlauf oder die Wiederherstellung dieser Ressource voraussichtlich einen sehr hohen Aufwand hinsichtlich Dauer, Kosten oder Umfang erfordert. Üblicherweise werden solch Ressourcen als **Single Point of Failure** bezeichnet. Es gibt verschiedene Arten von Single Point of Failure:

Beispiel:

- **Wissen (Single Point of Knowledge, SPoK):** Eine Person, die als einzige über alle Fähigkeiten und spezifische Kenntnisse eines Prozesses oder Verfahrens verfügt.
- **Technik oder Dienstleistung (Single Point of Failure, SPoF):** Eine Anlage, eine Komponente, ein IT-System, ein Dienstleister etc., durch deren Ausfall ein Gesamtsystem nicht mehr betriebsbereit ist. Das trifft immer dann zu, wenn eine Komponente eine zentrale Funktion im Gesamtsystem übernimmt und beim Ausfall die Funktionen der anderen Komponenten beeinträchtigt.
- **Kontakte (Single Point of Contact, SPoC):** Eine Person, die der alleinige Ansprechpartner oder eine Schnittstelle, die alleinige Kommunikationsstelle für einen bestimmten Sachverhalt sind.
- Ressourcen, welche **von relativ vielen zeitkritischen Geschäftsprozessen benötigt** werden (Kumulationseffekt).

Um die Lesbarkeit zu vereinfachen, wird nachfolgend nur noch die Abkürzung **SPoF** verwendet. SpoFs stellen besonders verwundbare Stellen der Institution dar und sollten daher risiko-orientiert abgesichert werden. SpoFs sollten daher unbedingt in der BCM-Risikoanalyse untersucht und je nach Ergebnis in den BC-Strategien berücksichtigt werden.

6.5.3 Auswertung

Nachdem die BIA durchgeführt wurde, müssen die Ergebnisse im Rahmen der BIA-Auswertung qualitätsgesichert und zusammengefasst werden. Um ein einheitlich hohes Qualitätsniveau der BIA-Ergebnisse sicherzustellen, müssen die BIA-Ergebnisse dahingehend überprüft werden, dass diese vollständig, richtig und nachvollziehbar sind. Hierzu ist es empfehlenswert, zu überprüfen, ob sämtliche notwendigen Informationen erhoben sowie die Schadensbewertung formal korrekt vorgenommen wurde und ob die Begründung der Schadensbewertung plausibel erscheint. Zusätzlich ist es hilfreich zu prüfen, ob die RTO der Ressourcen korrekt aus der MTPD der zeitkritischen Prozesse abgeleitet wurde. Falls einzelne Ergebnisse nicht plausibel oder inkorrekt erscheinen, sollte Rücksprache mit den Ansprechpartnern gehalten und die Ergebnisse gemeinsam abgestimmt werden.

Nachdem die Ergebnisse qualitätsgesichert wurden, sollten die Einzelergebnisse zu einer Gesamtübersicht der zeitkritischen Geschäftsprozesse und Ressourcen zusammengefasst werden. Die Gesamtübersicht sollte mindestens die folgenden Inhalte umfassen:

- Übersicht der zeitkritischen Geschäftsprozesse und zugehöriger Ansprechpartner,

- Übersicht der Prozessabhängigkeiten sowie
- Übersicht der abhängigen Ressourcen und SpoF sowie deren RTO bzw. RPO.

Da nun bekannt ist, welche Anforderungen für den Wiederanlauf bestehen, sind die notwendigen Voraussetzungen geschaffen, um zu erfassen, was davon bereits erfüllt wird und daher mit dem Soll-Ist-Vergleich beginnen zu können.

6.6 Soll-Ist-Vergleich

Als Ergebnis der BIA liegen für alle betrachteten zeitkritischen Ressourcen die RTOs sowie gegebenenfalls die RPO vor. RTO und RPO stellen dabei gewünschte Soll-Werte dar. Die Ressourcenzuständigen müssen im Rahmen des Soll-Ist-Vergleichs die Frage beantworten, ob die RTO der Ressource durch vorhandene technische und organisatorische Maßnahmen erreicht werden kann. Hierzu wird der RTO (geforderte Wiederanlaufzeit) die **Recovery Time Achievable** (**RTA**, deutsch: erreichbare Wiederanlaufzeit), gegenübergestellt und die Zeitwerte miteinander verglichen. Die RTA einer zeitkritischen Ressource bezeichnet den real erreichbaren Zeitraum, von dem Zeitpunkt, an dem die Ressource ausfällt bis zum Zeitpunkt, an dem eine Notfall-Lösung produktiv gesetzt wird. Aus Vereinfachungsgründen wird nachfolgend nur bei Abweichungen im Vorgehen auf die RPO eingegangen. Ansonsten gilt das Vorgehen analog zum RTO Soll-Ist-Vergleich.

Die nachfolgenden Kapitel beschreiben die empfohlene Vorgehensweise, mittels derer der Soll-Ist-Vergleich durchgeführt wird. In Abbildung 55 sind die hierfür erforderlichen Schritte in einer Übersicht dargestellt.

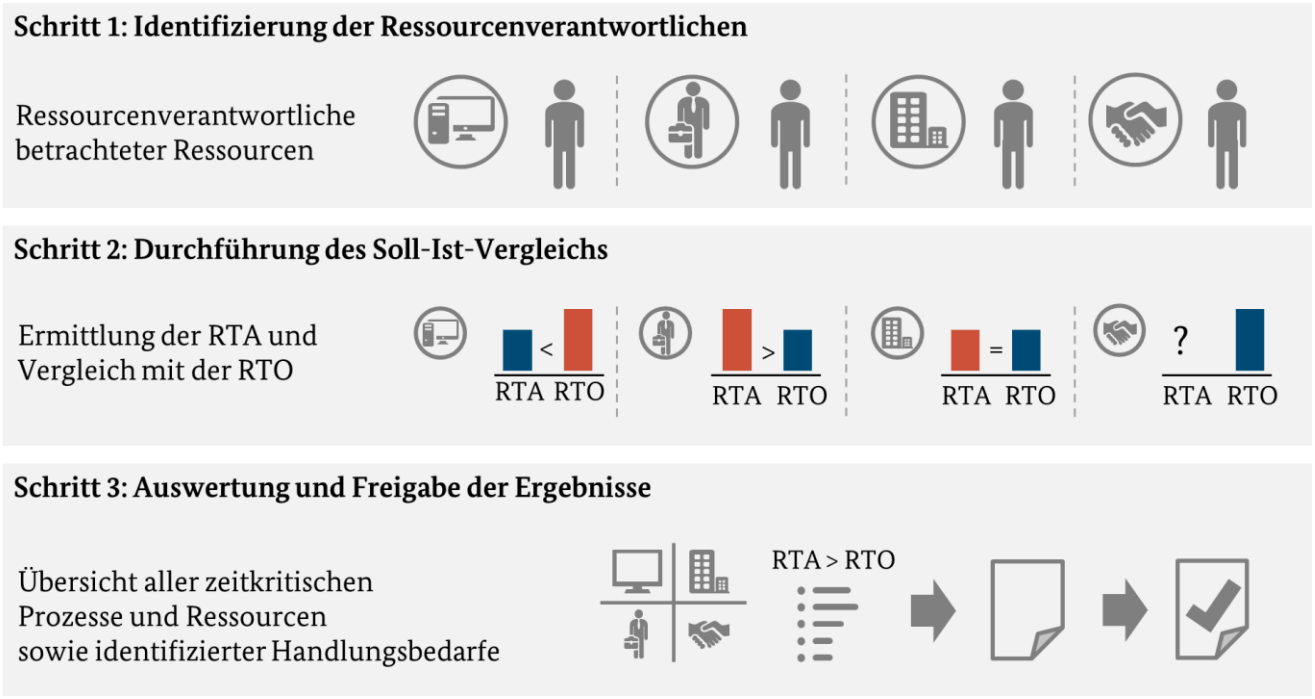

Abbildung 55: BCM-Prozessschritte des Soll-Ist-Vergleichs

6.6.1 Identifizierung der Ressourcenzuständigen

Vor dem Soll-Ist-Vergleich müssen die Ressourcenzuständigen identifiziert werden. Da der BCMB in der Regel über den besten Gesamtüberblick über die BIA-Ergebnisse verfügt, ist es empfehlenswert, dass er diese Aufgabe übernimmt. Hierzu kann er anhand der Ressourcenkategorien vorgehen. Tabelle 55 gibt beispielhaft die typischen Ansprechpartner je Ressourcenkategorie wieder. Falls die Institution abweichende Ressourcenkategorien benannt hat, so müssen diese entsprechend berücksichtigt werden.

Beispiel:

Ressourcenkategorie	Geschäftsprozess- bzw. Ressourcenzuständige
IT	Leiter IT
Personal	Leiter Personal
Arbeitsplätze	Leiter Gebäudeverwaltung/Haustechnik
Dienstleistungen	Leiter Einkauf/Provider Management oder dezentrale Provider/Supplier Manager
Informationen	• zentrale physische Daten: Leiter Aktensammelstelle/Archiv • dezentrale physische Daten: Leiter der jeweiligen Organisationseinheit (gemäß BIA) • Bei elektronischen Daten: Leiter IT
Infrastruktur	Leiter Infrastruktur/Werksleiter/Technischer Betriebsleiter
Maschinen/Geräte/ Anlagen/Fahrzeuge	Leiter Infrastruktur/Werksleiter/Technischer Betriebsleiter
Betriebsmittel (Sonstige)	Leiter Infrastruktur/Werksleiter/Technischer Betriebsleiter

Tabelle 55: Beispiele für Ressourcenzuständige

Einen direkten Überblick über die Verantwortlichkeiten einzelner Ressourcen haben die jeweiligen Leiter der Organisationseinheiten, die für die entsprechende Ressourcenkategorie zuständig sind. Die Leiter sollten darüber informiert werden, welche Angaben für den Soll-Ist-Vergleich benötigt werden und welche Relevanz diese Informationen für die weiteren Schritte im BCM haben. Die Leiter sollten die relevanten Ressourcenzuständigen benennen, um die erforderlichen Informationen einzuholen.

Für die Sensibilisierung der oben aufgeführten Leiter kann die *BIA Workshop-Präsentation* dienen (siehe Kapitel 6.5.1.5 *Vorbereitung der BIA-Hilfsmittel*). Diese kann im Rahmen einer Informationsveranstaltung vorgestellt oder als Begleitmaterial zu einer Informationsmail an die relevanten Personen gesendet werden.

Synergiepotenzial:

Falls bereits ein ISMS nach BSI-Standard 200-2 vorliegt und der Informationsverbund ähnlich zum Geltungsbereich des BCMS festgelegt ist, können die Ressourcenzuständigen anhand der Strukturanalyse ermittelt werden.

6.6.2 Durchführung des Soll-Ist-Vergleichs

Die Ressourcenzuständigen müssen im Rahmen des Soll-Ist-Vergleichs die Frage beantworten, ob die RTO der Ressource durch vorhandene technische und organisatorische Maßnahmen erreicht werden kann. Hierzu wird der RTO (geforderte Wiederanlaufzeit) die RTA (erreichbare Wiederanlaufzeit) gegenübergestellt und die Zeitwerte miteinander verglichen.

Die RTA kann im Rahmen von Übungen und Tests (siehe Kapitel 6.11 *Üben und Testen*) ermittelt und nachgewiesen werden. Für die Ressourcenkategorie *Dienstleistungen* muss in den bestehenden Verträgen oder Service Level Agreements geprüft werden, ob Aussagen zur Realisierbarkeit der RTO darin vorliegen.

Wird der PDCA-Lebenszyklus erstmalig durchlaufen, liegen im Regelfall noch keine Ergebnisse zu Notfallübungen und -Tests vor. In diesem Fall kann die RTA geschätzt werden. Da sich je nach Einschätzung der RTA

die Risikosituation anders darstellt, ist es wichtig, dass die Schätzung ein möglichst realistisches Bild wiedergibt und keinen erwünschten Zielzustand. Ist keine realistische Schätzung möglich oder es liegen keine technischen und organisatorischen Wiederanlaufmaßnahmen vor, so muss die RTA als unbekannt gekennzeichnet werden.

Der Soll-Ist-Vergleich kann per E-Mail oder über ein Tool abgefragt werden. Auch können Einzelgespräche, z. B. zwischen dem BCMB und den Ressourcenzuständigen, durchgeführt werden. Dies ist insbesondere bei kleinen Institutionen mit wenigen zeitkritischen Ressourcen sinnvoll. Hierzu sollten jeweils die vorliegenden Informationen aus der BIA sowie die benötigten Informationen für den Soll-Ist-Vergleich anhand eines einheitlichen Schemas abgefragt werden, um eine Auswertung über alle Ressourcen effektiv zu ermöglichen. Tabelle 56 zeigt dies am Beispiel von IT-Ressourcen.

Beispiel:

Ressourcen-kategorie	**Ressource**	**RTO**	**RTA**	**Nachweis**	**RTA ≤ RTO**
IT	Standard-IT-Ausstattung	< 3 Tage	2 Tage	Schätzung anhand des Regelprozesses	Ja
IT	Mailservice	< 1 Tag	05:45 h	Funktionstest	Ja
IT	Fileserver	< 1 Tag	unbekannt	nicht vorhanden	unbekannt

Tabelle 56: Beispiel eines Soll-Ist-Vergleichs der RTO anhand der Ressourcenkategorie IT

Für die Ressourcenkategorien, für die eine RPO festgelegt wurde, muss diese mit dem festgelegten Datensicherungszyklus gemäß des IT-Betriebs abgeglichen werden (siehe Tabelle 57).

Beispiel:

Ressource	**RPO**	**Datensicherungs-zyklus**	**Nachweis**	**Datensicherung ≤ RPO**
Kundendaten	Vortag	12 Stunden	Betriebshandbuch	Ja

Tabelle 57: Beispiel eines Soll-Ist-Vergleichs der RPO

6.6.3 Auswertung und Freigabe der Ergebnisse

Es muss eine Übersicht aller Ressourcen, insbesondere jedoch der unzureichend abgesicherten Ressourcen erstellt, der Institutionsleitung vorgestellt und mit dieser abgestimmt werden. Die Institutionsleitung sollte die folgenden Informationen zur Kenntnis nehmen und bestätigen:

- Übersicht der zeitkritischen Geschäftsprozesse gemäß BIA
- Übersicht der zeitkritischen Ressourcen gemäß BIA
- Übersicht der unzureichend abgesicherten Ressourcen gemäß Soll-Ist-Vergleich
- Einschätzung möglicher Risiken aus den identifizierten Lücken gemäß Soll-Ist-Vergleich

Der weitere Handlungsbedarf wird anhand der BCM-Risikoanalyse abgeleitet.

6.7 BCM-Risikoanalyse

Während die BIA die möglichen Auswirkungen auf den Geschäftsbetrieb untersucht, betrachtet die BCM-Risikoanalyse die möglichen Ursachen für den Ausfall des Geschäftsbetriebs. In der BCM-Risikoanalyse wird dazu untersucht, gegen welche Gefährdungen der Geschäftsbetrieb abgesichert werden soll, bzw. bei welchen Gefährdungen das Risiko so hoch ist, dass abgesichert werden soll. Als **Zielobjekte** in der BCM-Risikoanalyse dienen alle zeitkritischen Ressourcen, die vorab in der BIA identifiziert wurden.

Die Ergebnisse der BCM-Risikoanalyse schaffen die Voraussetzung in den Folgeschritten des BCMS gezielte Notfallvorsorgemaßnahmen und BC-Lösungen unter Kosten-Nutzen-Risiko-Gesichtspunkten ableiten zu können.

Hinweis:

Dieses Kapitel beschreibt die BCM-spezifischen Aspekte am Beispiel des Vorgehens zum BSI-Standard 200-3. Entsprechend werden auch die Begriffe und Phasen der Risikoanalyse gemäß BSI-Standard 200-3 angewendet. So werden z. B. die zu untersuchenden zeitkritischen Ressourcen nachfolgend als Zielobjekte bezeichnet.

Je nachdem, welche Methodik zum Risikomanagement institutionsspezifisch zugrunde gelegt wird, unterscheiden sich die durchzuführenden Schritte hinsichtlich ihrer Bezeichnung und Inhalte. Die Angaben müssen entsprechend institutionsspezifisch angepasst werden.

Abbildung 56 fasst die wesentlichen Schritte zusammen, wie anhand der Vorgehensweise nach BSI-Standard 200-3 eine BCM-Risikoanalyse durchgeführt wird. Abweichend davon könnte in der Praxis auch auf vorhandene Ergebnisse einer Risikoanalyse zurückgegriffen werden oder nur die Anforderungen an die BCM-Risikoanalyse in einer themenübergreifen Risikoanalyse mit erhoben werden. Beide Fälle werden hier nicht näher erläutert, setzen aber ebenfalls voraus, dass die zeitkritischen Ressourcen vollständig berücksichtigt und die spezifischen Anforderungen an die BCM-Risikoanalyse erfüllt sein müssen.

Hinweis:

Um für das BCM optimale Ergebnisse aus der Risikoanalyse ableiten zu können, sollte die Risikoanalyse möglichst zeitnah im Anschluss an den Soll-Ist-Vergleich erfolgen. Je größer der Zeitraum zwischen den Analysen ist, desto eher ist davon auszugehen, dass Informationen veralten oder sich die Rahmenbedingungen wieder verändern. Zudem sollte die Risikoanalyse ebenso häufig wie die BIA und der Soll-Ist-Vergleich stattfinden, z. B. jährlich. Dadurch kann sichergestellt werden, dass die betrachteten Zielobjekte stets vollständig und aktuell analysiert werden.

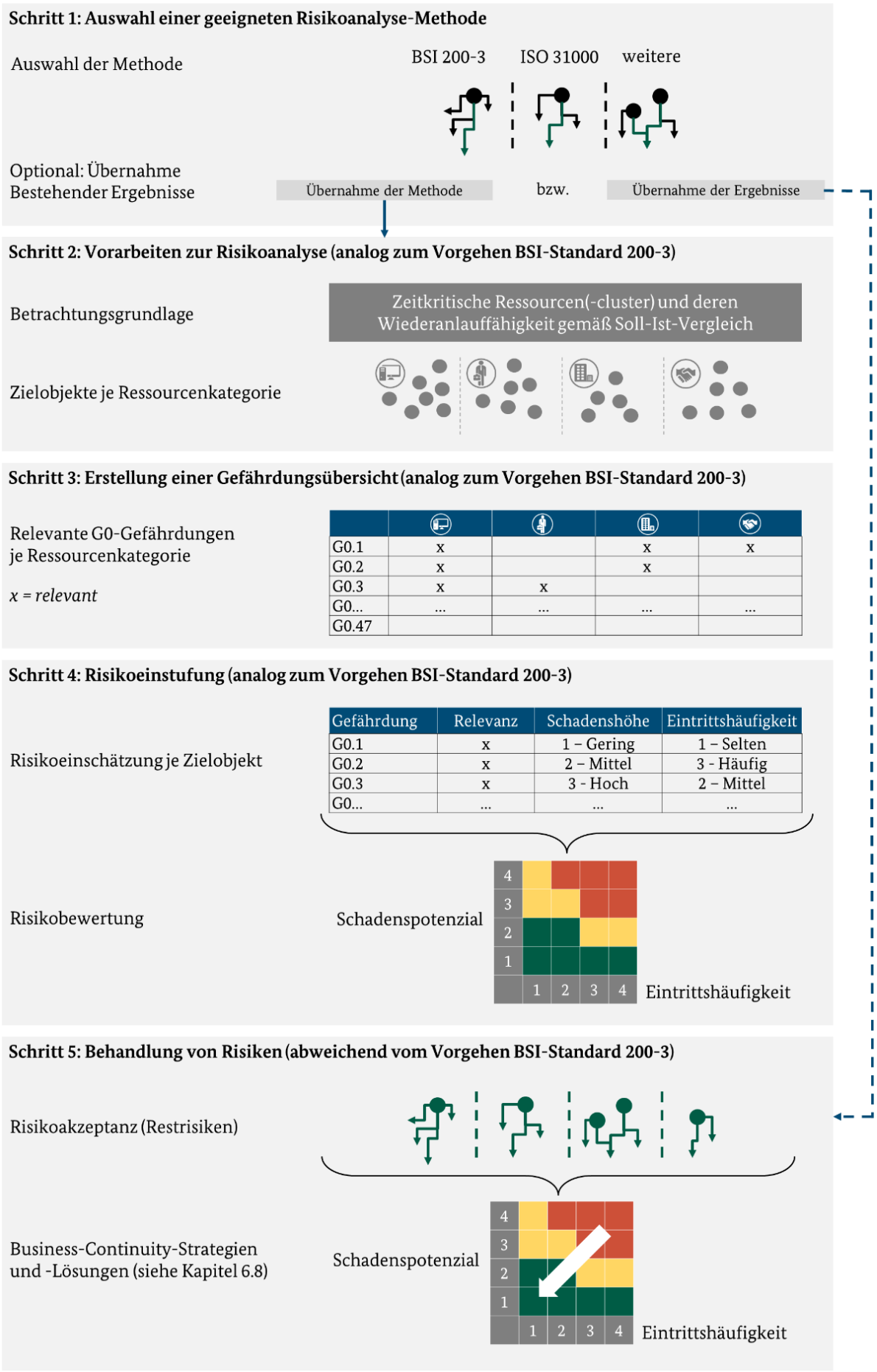

Abbildung 56: BCM-Prozessschritte der BCM-Risikoanalyse

6.7.1 Auswahl einer geeigneten Risikoanalyse-Methode

Eine BCM-Risikoanalyse unterscheidet sich methodisch nicht von Risikoanalysen aus anderen Managementdisziplinen, wie z. B. dem Informationssicherheitsmanagement, dem (IT-)Risikomanagement oder der Gebäudesicherheit. Üblicherweise fließen die Ergebnisse aller themenspezifischen Risikoanalysen in ein institutionsübergreifendes Risikomanagement ein und werden darin konsolidiert.

Der vorliegende Standard beschreibt keine eigenständige Methodik für eine BCM-Risikoanalyse. Vielmehr kann hierzu auf etablierte Risikomanagement-Standards zurückgegriffen werden. Diese Methoden müssen jedoch die Parameter Eintrittswahrscheinlichkeit und Schadenshöhe berücksichtigen. Unter anderem erfüllen die Risikomanagement-Standards BSI-Standard 200-3 *Risikomanagement* sowie die Norm DIN ISO 31000:2018 *Risikomanagement –Leitlinien* diese Voraussetzung.

Synergiepotenzial:

Es ist empfehlenswert, in einem ersten Schritt zu prüfen, inwieweit vorhandene Risikoanalyse-Methoden der Institution auch für die BCM-Risikoanalyse 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.

Zudem können Risiken, die zu einem Ausfall zeitkritischer Ressourcen führen, bereits anhand bestehender Risikoanalysen anderer Managementsysteme identifiziert, analysiert und bewertet worden sein. In diesem Fall kann nicht nur auf eine eigenständige Methodik, sondern auch auf eine eigenständige Risikoeinschätzung verzichtet werden, falls dabei die folgenden zwei Aspekte sichergestellt sind:

- Die betrachteten Zielobjekte der vorhandenen Risikoanalyse sollten die zeitkritischen Ressourcen abdecken.

Das Ergebnis der Risikoanalyse sollte einen Detailgrad besitzen, der es gestattet, konkrete BC-Lösungen im BCM daraus ableiten zu können.

Die nachfolgenden Unterkapitel fokussieren ausschließlich die Besonderheiten und spezifischen Anforderungen an eine BCM-Risikoanalyse. Diese sollten für eine BCM-Risikoanalyse berücksichtigt werden, um im Anschluss daraus geeignete Business-Continuity-Strategien entwickeln zu können.

6.7.2 Vorarbeiten zur Risikoanalyse

Durch den Soll-Ist-Vergleich liegt bereits die Liste der zeitkritischen Ressourcen und damit der relevanten Zielobjekte für die BCM-Risikoanalyse vor. Die Vorarbeiten zur Risikoanalyse gemäß BSI-Standard 200-3 beschränken sich daher auf eine geeignete Gruppenbildung der Zielobjekte. Hierzu kann in der BCM-Risikoanalyse auf die bereits definierten Ressourcencluster gemäß BIA zurückgegriffen werden. Auf Grund ihrer hohen Bedeutung ist es empfehlenswert, die in der BIA identifizierten SpoFs zusätzlich als eigenständige Zielobjekte in der BCM-Risikoanalyse zu untersuchen.

Analog zur BIA und dem Soll-Ist-Vergleich bieten sich für die BCM-Risikoanalyse ebenfalls Workshops an, um die Informationen zielgerichtet zu erheben. Das Vorgehen, um die Workshops vorzubereiten, kann analog zur Vorbereitung der BIA-Workshops erfolgen (siehe Kapitel 6.5.1.4 *Organisatorische Planung*). Auch der Einsatz von vorgegeben Hilfsmitteln bietet sich in der BCM-Risikoanalyse an (siehe Kapitel 6.5.1.5 *Vorbereitung der BIA-Hilfsmittel*). Insbesondere kann es hilfreich sein, eine Workshop-Präsentation vorzubereiten, in der auf die spezifischen Eigenschaften der BCM-Risikoanalyse eingegangen wird.

6.7.3 Erstellung einer Gefährdungsübersicht

Um eine Gefährdungsübersicht zu erstellen, kann in der BCM-Risikoanalyse analog zum BSI-Standard 200-3 vorgegangen werden. Die Risikoanalyse gemäß BSI-Standard 200-3 greift auf eine Liste von elementaren

Gefährdungen zurück, die als Ausgangsbasis zur Risikoeinstufung dient. Diese beinhalten bereits die üblichen Kombinationen aus Bedrohungen und Schwachstellen.

Für das BCM besteht die Besonderheit, dass aus dieser Liste nur jene Gefährdungen relevant sind, die sich auf das Schutzziel Verfügbarkeit beziehen. Gefährdungen, die sich auf andere Schutzziele auswirken, wie z. B. Gefährdungen die die Vertraulichkeit oder Integrität beeinträchtigen, werden innerhalb des BCM nicht behandelt. Sie können daher ausgelassen werden, sofern die Ergebnisse der Risikoanalyse ausschließlich für das BCM eingesetzt werden. Dies bietet den Vorteil, dass weniger Gefährdungen je Zielobjekt betrachtet werden müssen und damit der Aufwand in der Risikoeinstufung reduziert werden kann.

Tabelle 58 gibt am Beispiel ausgewählter, elementarer Gefährdungen ein mögliches Beispiel wieder, wie für das BCM relevante Gefährdungen selektiert werden können. Eine vollständige Liste der relevanten G0-Gefährdungen kann dem Hilfsmittel *BCM-Relevanz G0-Gefährdungen* entnommen werden.

Beispiel:

G0-Gefährdung gem. BSI 200-3	Verfügbarkeit	Vertraulichkeit	Integrität
G0.01 Feuer	X		X
…	…	…	…
G0.13 Abfangen kompromittierender Strahlung		X	
G0.14 Ausspähen von Informationen/Spionage		X	
…	…	…	…
G0.24 Zerstörung von Geräten oder Datenträgern	X		
…	…	…	…

Legende:

Relevant	Nicht relevant

Tabelle 58: Selektion der Elementaren Gefährdungen des BSI anhand der Schutzziele (Beispiele)

Ferner ist es empfehlenswert, die Gefährdungen vorab den Ressourcenkategorien zuzuordnen. Dadurch kann der Aufwand weiter minimiert werden, da nur eine Teilmenge aller Gefährdungen je Ressourcenkategorie betrachtet werden muss. Die Relevanz der Gefährdungen kann über folgende Stufen beschrieben werden (in Anlehnung an BSI-Standard 200-3, Kapitel 4.1 *Elementare Gefährdungen*):

- Direkt **relevant** bedeutet hier, dass die jeweilige Gefährdung auf das betrachtete Zielobjekt einwirken kann und deshalb im Rahmen der Risikoanalyse behandelt werden muss.
- **Indirekt relevant** meint hier, dass die jeweilige Gefährdung zwar auf das betrachtete Zielobjekt einwirken kann, in ihrem Schadenspotenzial aber nicht über andere (allgemeinere) Gefährdungen hinausgeht. In diesem Fall muss die jeweilige Gefährdung für dieses Zielobjekt nicht gesondert im Rahmen der Risikoanalyse behandelt werden.
- **Nicht relevant** heißt hier, dass die jeweilige Gefährdung nicht auf das betrachtete Zielobjekt einwirken kann und deshalb für dieses Zielobjekt im Rahmen der Risikoanalyse nicht behandelt werden muss.

Tabelle 59 gibt einige Beispiele für sinnvolle Zuordnungen wieder. Die Relevanz von Gefährdungen muss jedoch individuell für die Institution festgelegt werden.

Beispiel:

G0-Gefährdung gem. BSI 200-3	IT	Dienstleistung	Gebäude	Personal	...
...	...	...	...	...	...
G0.08 Ausfall oder Störung der Stromversorgung	Direkt relevant	Nicht relevant	Direkt relevant	Nicht relevant	...
...	...	...	...	...	...
G0.10 Ausfall oder Störung von Versorgungsnetzen	Indirekt relevant	Nicht relevant	Direkt relevant	Nicht relevant	...
G0.11 Ausfall oder Störung von Dienstleistern	Indirekt relevant	Direkt relevant	Nicht relevant	Nicht relevant	...
...	...	...	...	...	...
G0.33 Personalausfall	Indirekt relevant	Nicht relevant	Nicht relevant	Direkt relevant	...
...	...	...	...	...	...

Tabelle 59: Zuordnung der Gefährdungen zu den Ressourcenkategorien (Beispiele)

6.7.4 Risikoeinschätzung

Die Risikoeinschätzung stellt einen der elementarsten Schritte in der Risikoanalyse dar. In diesem BCM-Prozessschritt wird gemäß BSI-Standard 200-3, Kapitel *5.1 Risikoeinschätzung* anhand der relevanten Gefährdungen ermittelt, welches Risiko von diesen ausgeht. Die Risikoeinschätzung in der BCM-Risikoanalyse unterscheidet sich inhaltlich nicht vom Vorgehen des BSI-Standard 200-3. In der Praxis sind die Ressourcenzuständigen üblicherweise auch diejenigen, die am besten Aussagen über möglichen Risiken ihrer Ressource treffen können (**Risiko-Experten**). Da die Ressourcenzuständigen bereits aus dem Soll-Ist-Vergleich bekannt sind, ist es empfehlenswert, dass diese Ansprechpartner auch in der BCM-Risikoanalyse berücksichtigt werden.

Für die Risikoeinschätzung sollten die Risiko-Experten auf die elementaren Gefährdungen zurückgreifen. Darüber hinaus sollten die Risiko-Experten für die (gruppierten) Zielobjekte anhand der tatsächlichen Bedrohungen und Schwachstellen mögliche weitere Gefährdungen identifizieren, beispielsweise mit der Delphi-Methode. Wie hoch das Risiko ist, wird im BSI-Standard 200-3 von zwei Parametern bestimmt:

- Die **Eintrittshäufigkeit** definiert, mit welcher Wahrscheinlichkeit sich eine Gefährdung auf eine zeitkritische Ressource auswirkt.
- Die **Schadenshöhe** definiert die zu erwartende Höhe des Schadens, der bei Eintritt des Schadensereignisses entsteht.

Bei der Risikoeinschätzung müssen beide Einflussgrößen berücksichtigt werden.

Im Kontext des BCM kann die **Eintrittshäufigkeit** anhand von Realfällen sowie Statistiken und Daten eingeschätzt werden. Hierzu relevante Informationen können dem Hilfsmittel *Weiterführende Informationen zur Risikoeintrittshäufigkeit* abgerufen werden.

Im Kontext des BCM kann die **Schadenshöhe** zunächst aus dem Schadenspotenzial der ressourcenabhängigen, zeitkritischen Geschäftsprozesse abgeleitet werden. Über das Untragbarkeitsniveau in der BIA ist hierbei bereits festgelegt worden, dass hauptsächlich hohe und sehr hohe Schäden relevant sind. Die BIA-Ergebnisse können jedoch in der BCM-Risikoanalyse nicht unreflektiert als Schadenshöhe übernommen werden. In der BIA wird jeder Prozess einzeln hinsichtlich seiner Auswirkungen bei einem Ausfall analysiert. Diese umfasst keine Kumulation der potenziellen Schäden. Für bestimmte Ressourcen(-cluster), wie ein Gebäude

oder einen zentralen Server, von deren Verfügbarkeit mehrere Geschäftsprozesse abhängig sind, sollte das Schadenspotenzial dementsprechend höher eingeschätzt werden. Dem gegenüber werden in der Risiko-Analyse auch bereits etablierte risikoreduzierende Maßnahmen berücksichtigt, die auf die zeitkritischen Ressourcen wirken und die Schadenshöhe reduzieren können.

Hinweis:

Um ein möglichst realistisches Bild über die Verfügbarkeitsrisiken zu erhalten, sollte die Risikoeinschätzung alle vorhandenen risikoreduzierenden Maßnahmen berücksichtigen (**Netto-Risikoeinschätzung**). Die risikoreduzierenden Maßnahmen umfassen die vorhandenen Vorsorgemaßnahmen sowie die bereits umgesetzten BC-Lösungen und Notfallmaßnahmen. Die Netto-Risikoeinschätzung hat gegenüber einer Brutto-Risikoeinschätzung den Vorteil, dass die Wiederanlauffähigkeit der zeitkritischen Ressource oder SPoF anhand der realen Gegebenheiten berücksichtigt wird. Ist die Wiederanlauffähigkeit der Ressource gemäß RTO-Soll-Ist-Vergleich ausreichend, wird sich dies in der Praxis auch auf die Eintrittswahrscheinlichkeit oder Schadenshöhe der Risiken auswirken.

Beispiel:

Durch die Risiko-Experten wird ein Ausfall der Verfügbarkeit des Hauptstandortes bewertet. Im ersten Schritt werden anhand der elementaren Gefährdung G0.1 Feuer folgende, konkrete Gefährdungen abgeleitet:

- Fahrzeugbrand in der Tiefgarage
- Unzureichend gesicherte Heißarbeiten im Produktionsbereich
- Kabelbrand elektronischer Zündquellen im Kantinenbereich

Um die Eintrittshäufigkeit und Schadenshöhe zu bestimmen, werden durch den Risiko-Experten sowohl bestehende risikoreduzierende Maßnahmen als auch die Wiederanlauffähigkeit berücksichtigt.

Folgende risikoreduzierende Maßnahmen werden berücksichtigt:

- Es finden regelmäßige Brandschutz-Übungen und –Schulungen für alle Mitarbeiter statt.
- Eine automatische Brandmeldeanlage und eine Brandlöschanlage sind installiert.
- Das Gebäude wird regelmäßig auf Brandlasten untersucht, die jeweils zeitnah beseitigt werden.

Die Eintrittswahrscheinlichkeit wird daher durch den Risiko-Experten als selten eingestuft.

Die Wiederanlauffähigkeit wird wie folgt bewertet:

- Es handelt sich um das einzige Gebäude der Institution, in dem alle zeitkritischen Geschäftsprozesse ausgeführt werden (SpoF). Bei einem Gebäudeausfall wäre der gesamte Geschäftsbetrieb betroffen.
- Es liegt bereits eine BC-Lösung vor, dessen RTA < RTO ist.

Unter Abwägung des maximal möglichen Schadens und der hohen Wiederanlauffähigkeit wird das Schadenspotenzial durch den Risiko-Experten als mittel eingestuft.

6.7.5 Risikobewertung

Durch die Institution müssen die identifizierten Risiken hinsichtlich ihres weiteren Handlungsbedarfs bewertet werden. Wie in Abbildung 57 dargestellt, können verschiedene Risikokategorien anhand einer Risikomatrix festgelegt werden, (siehe *BSI-Standard 200-3, Kapitel 5.2 Risikobewertung*).

Beispiel:

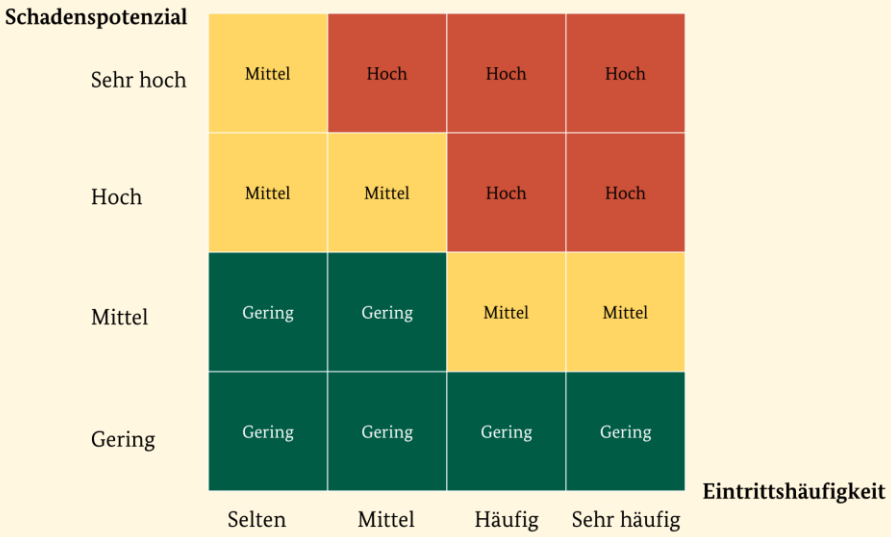

Abbildung 57: Beispiel einer Risiko-Matrix

Tabelle 60 enthält einen BCM-spezifischen Vorschlag zur Definition der verschiedenen Risikokategorien aus Abbildung 3 angelehnt an den BSI-Standard 200-3.

Beispiel:

Risikokategorien	Erläuterung
gering	Die Vorsorge- und Notfallmaßnahmen bieten einen **ausreichenden Schutz**. In der Praxis ist es üblich, geringe Risiken zu akzeptieren und die Gefährdung dennoch zu beobachten.
mittel	Die Vorsorge- und Notfallmaßnahmen reichen **möglicherweise nicht aus**.
hoch	Die Vorsorge- und Notfallmaßnahmen bieten **keinen ausreichenden Schutz** vor der jeweiligen Gefährdung, z. B. weil die RTA nicht ausreichend ist.

Tabelle 60: Definition der Risikokategorien

Hinweis:

Es ist empfehlenswert, die Risikobewertung anhand einer Risikomatrix in Zonen einzuteilen und daraus die weitere Behandlung von Risiken abzuleiten (z. B. geringe, mittlere und hohe Risiken). In der Praxis hat es sich bewährt, *geringe Risiken* zu akzeptieren, *mittlere Risiken* fallweise auf ihren Handlungsbedarf zu untersuchen und *hohe Risiken* unbedingt einer weiteren Risikobehandlung durch risikoreduzierende Maßnahmen zu unterziehen.

6.7.6 Risikobehandlung

Die Risikobehandlung im BCMS orientiert sich grundlegend an den vier Risikobehandlungs-Optionen des BSI-Standard 200-3 (siehe *BSI-Standard 200-3*, Kapitel *6.1 Risikobehandlungsoptionen*). Jedoch ist der *Transfer von Risiken* im BCM nur bedingt geeignet. Zum einen können daraus keine Maßnahmen zur Sicherstellung eines kontinuierlichen Geschäftsbetriebs abgeleitet werden. Zum anderen bleibt die Erfüllung von gesetzlichen oder vertraglichen Vorgaben davon unberührt. Aus denselben Gründen muss auch genau geprüft wer-

den, ob eine Risikoakzeptanz möglich ist. Insbesondere Institutionen, die eine Versorgungssicherheit zu garantieren haben, z. B. im KRITIS-Umfeld, sollten daher den Fokus darauf legen Risiken zu *vermeiden* oder zu *reduzieren.*

Die weitere Risikobehandlung erfolgt im BCM anhand von Business-Continuity-Strategien und -Lösungen, die im nachfolgenden Hauptkapitel näher erläutert werden. Alle Risiken, die einer weiteren Risikobehandlung unterzogen werden sollen, müssen in der Festlegung der Business-Continuity-Strategien berücksichtigt werden. Die Ergebnisse der BCM-Risikoanalyse sollten in einem Bericht zusammengefasst und der Institutionsleitung mitgeteilt werden. Insbesondere auf bestehende Restrisiken sollte explizit im Bericht hingewiesen werden.

Hinweis:

Auch nach Umsetzung angemessener Business-Continuity-Strategien und Lösungen können unter Kosten-Nutzen-Risiko-Aspekten entsprechende Restrisiken verbleiben. Diese Restrisiken können im Kontext des BCM durch die Institution toleriert werden, wenn entsprechende Geschäftsfortführungspläne vorliegen, die die Folgeschäden eingrenzen (siehe Kapitel 6.9 *Geschäftsfortführungsplanung*). Sollte es zum Eintritt eines unwahrscheinlichen Risikos kommen, können anhand der Geschäftsfortführungspläne zumindest die Folgeschäden eingedämmt werden.

6.8 Business-Continuity-Strategien und -Lösungen

Für die zeitkritischen Ressourcen wurden in der Risikobeurteilung die notwendigen Handlungsbedarfe abgeleitet, welche die Grundlage der weiteren Notfallplanung bilden. Diese Handlungsbedarfe müssen mit Business-Continuity-Strategien und –Lösungen (BC-Strategien und -Lösungen) behandelt werden. Die Notfallplanung kann dabei auf unterschiedliche Art und Weise erfolgen. Findet die Notfallplanung je Organisationseinheit separat statt, sind erfahrungsgemäß höhere Koordinationsaufwände, höhere Gesamtkosten oder gar widersprüchliche Notfallplanungen zu erwarten. Insofern ist es wichtig, übergreifend nach Lösungen zu suchen, die zusätzlich zu der Ausrichtung der Institution passen.

Mithilfe von Business-Continuity-Strategien (BC-Strategien) muss die Institutionsleitung daher für den gesamten Geltungsbereich des BCMS strategisch festlegen, wie sie die Notfallplanung allgemein gestalten und umsetzen lassen möchte. Sie kann zu diesem Zweck für jede in der BIA identifizierte Ressourcenkategorie den Schwerpunkt vorgeben.

Beispiel: BC-Strategien bei einem Gebäudeausfall

- Verteilte Geschäftstätigkeit
- Mobiles Arbeiten
- Nutzung dedizierter interner Arbeitsplätze an einem Ausweichstandort
- Zeitlich begrenzte Anmietung externer Büroarbeitsflächen und -Infrastruktur

Welche BC-Strategien für die Institution dabei am besten geeignet sind, hängt jedoch nicht ausschließlich von den Anforderungen an die Notfallplanung ab. So sollte berücksichtigt werden, welche Ziele die Institution im Allgemeinen verfolgt, welche rechtlichen und regulatorischen Vorgaben auf die Institution wirken und ob die angestrebten BC-Strategien technisch, baulich, personell und organisatorisch überhaupt in der Institution umgesetzt werden können. BC-Strategien können auch Chancen für den Normalbetrieb generieren, die ebenfalls mitberücksichtigt werden können.

BC-Strategien zu entwickeln ist umso bedeutender, wenn bislang keine einheitliche Notfallplanung bestand oder im Rahmen eines Reaktiv-BCMS ausschließlich bestehende Maßnahmen und Lösungen des Normalbetriebs genutzt wurden. Die BC-Strategien können in diesem Fall dabei unterstützen, die Notfallplanung effektiver und effizienter zu gestalten sowie die individuelle Risikosituation zu berücksichtigen.

Synergiepotenzial:

Erfahrungsgemäß bestehen in vielen Institutionen bereits Prozesse, mittels derer strukturiert Strategieoptionen identifiziert und bewertet sowie durch die Institutionsleitung ausgewählt werden. Die Entwicklung von BC-Strategien und -lösungen kann auf diese Prozesse zurückgreifen, sofern die in diesem Kapitel beschriebenen Anforderungen eingehalten werden.

Die nachfolgenden Kapitel beschreiben die empfohlene Vorgehensweise, mittels derer die BC-Strategien und -Lösungen entwickelt und umgesetzt werden können. In Abbildung 58 sind die hierfür erforderlichen Schritte in einer Übersicht dargestellt.

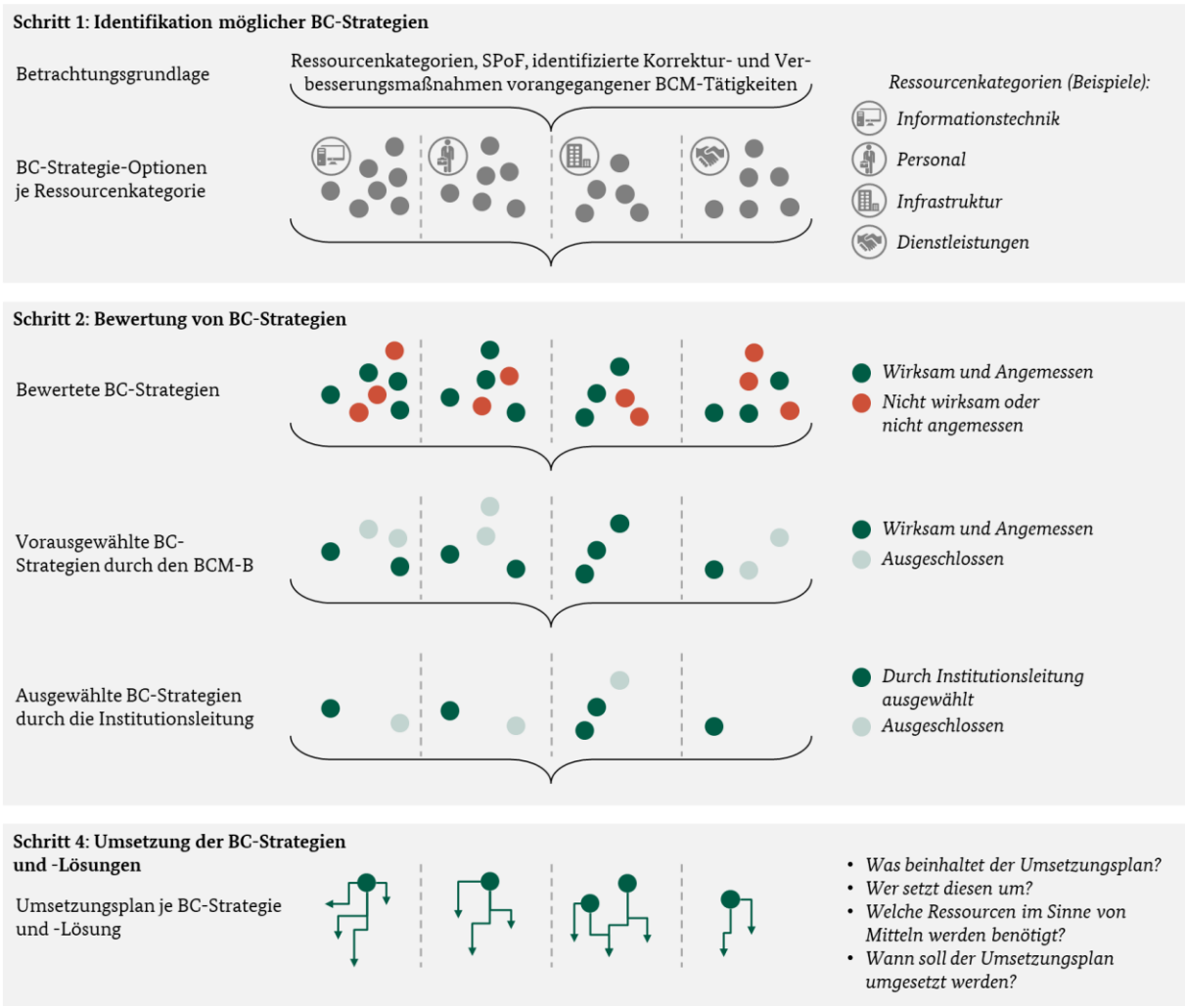

Abbildung 58: BCMS-Prozessschritte zur Entwicklung von BC-Strategien und -Lösungen

Hinweis:

Werden BC-Strategien explizit für die Ressourcenkategorie Dienstleister entwickelt oder sollen Dienstleister Teil einer BC-Strategie sein, so müssen Besonderheiten wie etwa Verträge oder allgemeine Vorgaben an Dienstleister berücksichtigt werden. Die zu beachtenden Besonderheiten werden im Kapitel 7 *BCM im Rahmen des Outsourcings und von Lieferketten* gesondert erläutert.

Um BC-Strategien zu entwickeln und zu dokumentieren, kann die Dokumentenvorlage *Bewertungstabelle für BC-Strategien* aus den Hilfsmitteln verwendet werden. Zusätzlich befinden sich in den Hilfsmitteln Beispiele für BC-Strategien. Die einzelnen Schritte werden nachfolgend anhand der Ressourcenkategorien Gebäude und Infrastruktur beispielhaft erläutert.

6.8.1 Identifikation möglicher BC-Strategien

Um entscheiden zu können, welche die beste BC-Strategie für eine Institution ist, muss anhand der Ergebnisse des Soll-Ist-Vergleichs und der Risikoanalyse festgestellt werden, was durch BC-Strategien überhaupt abgesichert werden muss und welche BC-Strategien grundsätzlich konzipiert werden könnten, um dies zu erreichen. Üblicherweise übernimmt diese Tätigkeit der BCMB.

Hierzu kann sich der BCMB zunächst an den in der BIA festgelegten Ressourcenkategorien orientieren. Für jede Ressourcenkategorie ist es empfehlenswert, zu prüfen, welche grundsätzlichen BC-Strategien möglich wären, um die jeweilige Ressourcenkategorie abzusichern. Eine BC-Strategie kann sowohl dazu geeignet sein, die Eintrittswahrscheinlichkeit eines Ressourcen- oder Geschäftsprozessausfalls durch Vorsorgemaßnahmen zu senken, als auch einen Notbetrieb durch BC-Lösungen sowie Notfallmaßnahmen zu ermöglichen.

Hinweis:

Erfahrungsgemäß beschränkt sich eine BC-Strategie nicht auf eine einzelne Vorsorgemaßnahme, BC-Lösung oder Notfallmaßnahme. In der Regel setzt sich eine wirksame und angemessene BC-Strategie aus mehreren der genannten Komponenten zusammen. So können Notfallmaßnahmen zum Beziehen eines Ausweichstandortes erst dann beschrieben werden, wenn ein Ausweichstandort im Rahmen einer BC-Lösung konzipiert wurde. Gleichzeitig ist es wahrscheinlich sinnvoll, einen Standort mittels Vorsorgemaßnahmen präventiv soweit abzusichern, dass die Wahrscheinlichkeit eines Gebäudeausfalls auf ein akzeptables Maß gesenkt werden kann.

Zusätzlich kann es zweckmäßig sein, einzelne Ressourcenkategorien weiter zu unterteilen. Dies ist etwa dann sinnvoll, wenn für unterteilte Ressourcenkategorien durch unterschiedliche BC-Strategien ein besseres Gesamtergebnis der BC-Strategien möglich wird. Die Ressourcenkategorien Gebäude und Infrastruktur kann etwa einen gesamten Standort, ein einzelnes Gebäude oder gar einzelne Gebäudeteile umfassen. Bei einem gesamten Standortausfall könnte die BC-Strategie lauten, sämtliche Tätigkeiten oder eine vorhandene Produktion an einen Ausweichstandort zu verlagern. Fallen hingegen nur einzelne Gebäudeteile aus, dann kann eine BC-Strategie dazu lauten, die Arbeitsplätze oder die Produktion innerhalb des Gebäudes oder Standortes zu verlagern.

Während der BCMB mögliche BC-Strategien identifiziert, muss er identifizierte SPoFs sowie Korrekturbedarfe und Verbesserungsmöglichkeiten vorangegangener BCMS-Zyklen berücksichtigen. Zu den identifizierten Korrekturbedarfen und Verbesserungsmöglichkeiten vorangegangener BCMS-Zyklen zählen etwa Lücken, die mit den bestehenden personellen, finanziellen oder zeitlichen Ressourcen bislang nicht behandelt werden konnten oder bewusst nicht behandelt wurden. Dies gilt insbesondere für initiale Entwicklungsstufen wie dem Reaktiv-BCMS.

Beispiel:

In Bezug auf das Beispiel eines Gebäude- und Infrastrukturausfalls könnte innerhalb des Reaktiv-BCMS als Notfallmaßnahme definiert worden sein, dass Organisationseinheiten ohne zeitkritische Tätigkeiten an (noch) intakten Standorten verdrängt werden, um freie Arbeitsplätze für zeitkritische Organisationseinheiten zu schaffen. Als Verbesserungsmöglichkeit wurde im Reaktiv-BCMS jedoch bereits dokumentiert, dass langfristig ein unabhängiger Ausweichstandort geplant werden soll. Im Zuge der aktuellen BC-Strategien wird diese Option mit aufgenommen.

Synergiepotenzial:

Speziell für die Ressourcenkategorien IT und digitale Informationen ist es empfehlenswert neben den klassischen Ausfallgründen wie etwa Hardwaredefekte oder höhere Gewalt auch Ausfälle aufgrund von Cyberangriffen zu berücksichtigen. Durch Cyberangriffe werden gesonderte Anforderungen an den Notbetrieb gestellt (siehe Kapitel 2.4.1 *BCM und Informationssicherheit*), die bereits in den jeweiligen BC-Strategien berücksichtigt werden können. Hierzu zählen etwa Schadensereignisse wie z. B. Schadsoftware-Angriffe, die primär die Vertraulichkeit oder Integrität von Informationen gefährden, sich aber in weiterer Folge auch auf die Verfügbarkeit auswirken können. Dies kann etwa der Fall sein, wenn der IT-Betrieb heruntergefahren werden muss, um zu verhindern, dass sich das Schadensereignis weiter auswirkt oder die Organisationseinheiten die korrumpierten Daten weiter nutzen können. Sofern ein ISMS besteht, können hierbei die Anforderungen an die jeweiligen BC-Strategien sowie mögliche Vorsorgemaßnahmen, die mitunter im ISMS bereits bestehen, gemeinsam abgestimmt und in eine BC-Strategie überführt werden.

Hinweis:

Für mögliche Beispiele von BC-Strategien kann das Hilfsmittel *BC-Strategievorschläge* genutzt werden. Zusätzlich kann der BCMB weitere Geschäftsprozess- und Ressourcenzuständige der Institution hinsichtlich möglicher BC-Strategieoptionen für den von ihnen verantworteten Ressourcenbereich hinzuziehen

Als Ergebnis dieses Abschnitts verfügt der BCMB je Ressourcenkategorie über eine Liste möglicher BC-Strategien.

6.8.2 Bewertung von BC-Strategien

Nachdem der BCMB die grundsätzlich möglichen BC-Strategien identifiziert hat, muss er bewerten, ob diese für die Institution **wirksam** und **angemessen** sind. Eine BC-Strategie ist dann **wirksam**, wenn durch die umgesetzte BC-Strategie die Eintrittswahrscheinlichkeit eines Ausfalls auf ein akzeptables Maß gesenkt werden kann oder die zeitkritischen Geschäftsprozesse innerhalb der MTPD auf dem Notbetriebsniveau fortgeführt werden können. **Angemessen** ist eine BC-Strategie dann, wenn sie den allgemeinen Zielen der Institution entspricht, die geltenden rechtlichen und regulatorischen Anforderungen einhält und der Nutzen die Kosten überwiegt. Um die BC-Strategien bewerten zu können, sollte der BCMB verschiedene Bewertungskriterien festlegen. Anhand der Bewertungskriterien können die BC-Strategien qualitativ und quantitativ bewertet und gegeneinander abgewogen werden. Sollte sich frühzeitig herausstellen, dass eine BC-Strategie nicht wirksam oder angemessen ist, muss diese nicht weiter bewertet werden. Im Folgenden werden einige Bewertungskriterien benannt, die mindestens berücksichtigt werden müssen:

Einhalten der RTO: Für die betrachteten BC-Strategien muss geprüft werden, ob nach deren Umsetzung der Notbetrieb der entsprechenden Ressourcen innerhalb der RTO hergestellt werden kann.

Erreichbares Notbetriebsniveau: Es muss geprüft werden, ob die betrachteten BC-Strategien in der Lage sind, das Notbetriebsniveau sicherzustellen. Wird durch eine Maßnahme zwar die RTO erreicht, jedoch nicht das Notbetriebsniveau, dann ist die betrachtete BC-Strategie nicht geeignet oder muss um weitere Maßnahmen ergänzt werden.

Verbleibendes Restrisiko: Es muss geprüft werden, welches Restrisiko eines Ressourcenausfalls bestehen bleibt, trotz umgesetzter BC-Strategie. Wird etwa ein Ausweichstandort geplant, der in der Nähe des primären Standortes liegt, verbleibt ein mögliches Restrisiko, dass beide Standorte durch ein Ereignis betroffen sind (etwa durch eine Bombenentschärfung). Werden die Tätigkeiten hingegen bereits im Vorhinein auf unterschiedliche Standorte verteilt, die ausreichend entfernt voneinander sind, würde der Ausfall eines Standortes mitunter gar nicht erst zum Ausfall des Geschäftsprozesses führen. Dies wäre dann der Fall, wenn die Leistung der verbliebenen Standorte ausreicht, den Geschäftsprozess auf dem Notbetriebsniveau fortsetzen zu können.

Finanzielle Aufwände: Es muss geprüft werden, welche finanziellen Aufwände mit den identifizierten BC-Strategien einhergehen und ob diese in einem angemessenen Verhältnis zu den erwarteten Schäden der ausgefallenen Geschäftsprozesse stehen. Finanzielle Aufwände beinhalten die Anschaffungskosten, die erforderlichen Kosten um die BC-Strategien aufrechtzuerhalten (etwa die laufenden Kosten eines Ausweichstandortes) sowie die notwendigen Kosten während und nach einem Notfall.

Hinweis:

Im Rahmen der Ressourcenplanung des BCMS (siehe Kapitel 3.2.4 *Ressourcenplanung*) hat die Institutionsleitung den BCMB mit angemessenen finanziellen Ressourcen im Sinne von Mitteln für den Aufbau, Betrieb und die kontinuierliche Verbesserung des BCMS ausgestattet. Die Kosten für BC-Strategien können jedoch häufig erst näher beziffert werden, wenn diese bewertet wurden. BC-Strategien, die das vorhandene Budget des BCMS übersteigen, sollten daher nicht bereits im Vorhinein ausgeschlossen werden. Sofern der Nutzen der BC-Strategie die entsprechenden finanziellen Ressourcen rechtfertigt, sollten diese stattdessen auch weiterhin in der Auswahl der BC-Strategien berücksichtigt werden.

Einhaltung interner und externer Anforderungen: Es sollte geprüft werden, ob die betrachteten BC-Strategien den Rahmenbedingungen der Institution entsprechen. So sollten die BC-Strategien etwa dahingehend geprüft werden, ob sie mögliche rechtliche und regulatorische Anforderungen einhalten, die Interessen interner und externer Interessengruppen einbeziehen sowie den allgemeinen Risikoappetit der Institutionsleitung berücksichtigen. Mögliche interne und externe Anforderungen wurden bereits mit den erweiterten Rahmenbedingungen zum BCMS erfasst (siehe Kapitel 6.1 *Analyse der erweiterten Rahmenbedingungen*).

Beispiel:

Für ausgewählte Organisationseinheiten könnte etwa gelten, dass die durchgeführten Tätigkeiten als vertraulich eingestuft wurden. In diesem Fall käme bei einem Gebäudeausfall eine angemietete gemeinschaftlich genutzte Bürofläche nicht in Betracht, ein geschützter gesonderter Ausweichstandort mitunter schon.

Maximal mögliche Notbetriebsdauer: Es sollte geprüft werden, wie lange die eingesetzten BC-Strategien einen Notbetrieb ermöglichen können, bis alternative Lösungen gefunden oder der Normalbetrieb wiederhergestellt sein muss. Die maximal mögliche Notbetriebsdauer der betrachteten BC-Strategie muss ermittelt werden, da bei einem langfristigen Ressourcenausfall weitere Schäden entstehen könnten. So könnten etwa verdrängte, im Betrachtungszeitraum der BIA nicht zeitkritische Arbeitsplätze langfristig auch zeitkritisch werden und ebenfalls Ausweicharbeitsplätze benötigen. Auch können die Kosten der aktivierten Notfallmaßnahmen ab einem bestimmten Zeitpunkt die erwarteten Schäden der ausgefallenen Ressourcen und Geschäftsprozesse übertreffen. Dies kann etwa der Fall sein, wenn zusätzliche Büroflächen über einen sehr langen Zeitraum angemietet werden müssen.

Neben den mindestens zu betrachtenden Bewertungskriterien können weitere optionale Bewertungskriterien betrachtet werden, wie etwa die folgenden:

Organisatorische Aufwände: Es wird empfohlen zu prüfen, welche organisatorischen Aufwände mit den identifizierten BC-Strategien einhergehen und ob diese im Verhältnis zu den erwarteten Schäden der ausgefallenen Ressourcen stehen.

Beispiel:

Im Beispiel eines Gebäudeausfalls könnten organisatorische Aufwände etwa damit verbunden sein, Tätigkeiten auf mehrere Standorte zu verteilen und damit Nachteile in der Kommunikation im Normalbetrieb zu erzeugen.

Die BC-Strategie „Mobiles Arbeiten“ kann möglicherweise nur umgesetzt werden, wenn die damit verbundenen rechtlichen Begebenheiten mit den jeweiligen Arbeitnehmervertretern abgestimmt werden.

Entstehende Risiken: Es wird empfohlen zu prüfen, ob die betrachteten BC-Strategien zu neuen Risiken führen können. Werden etwa gleiche Tätigkeiten auf mehrere Standorte verteilt, könnte dies in der Folge zu Effizienzverlusten oder einem mangelnden Wissensaustausch der beteiligten Mitarbeiter führen.

Entstehender Zusatznutzen: Es wird empfohlen zu prüfen, ob die betrachteten BC-Strategien auch im Normalbetrieb zu Verbesserungen führen. In diesem Hinblick kann der BCMB auch prüfen, ob Synergien zwischen den BC-Strategien oder zu anderen Tätigkeiten in der Institution bestehen oder geschaffen werden können.

Beispiel:

Für eine Institution stellt mobiles Arbeiten eine grundsätzlich mögliche BC-Strategie dar. Möglicherweise könnte mobiles Arbeiten bereits aus anderen Interessen der Institution heraus realisiert worden sein, etwa um flexibel von unterschiedlichen Standorten aus arbeiten zu können. Die BC-Strategie könnte so mit vergleichsweise geringem technischem Aufwand realisiert werden.

Sollte mobiles Arbeiten bislang nicht möglich sein, könnte die umgesetzte BC-Strategie zu Synergien in anderen Bereichen der Institution führen. So könnte der Austausch der Hardware dazu genutzt werden, die bestehende Hardwarelandschaft zu modernisieren oder zu vereinheitlichen. Auch könnte die Möglichkeit zukünftig flexibel arbeiten zu können sich positiv auf das jeweilige Geschäftsmodell auswirken. Die BC-Strategie wäre somit nicht nur im Rahmen der Notfallplanung sinnvollerweise weiter zu betrachten, sondern könnte auch in weiteren Themenbereichen der Institution zu strategischen Vorteilen führen.

Um die notwendigen Informationen zu erheben, kann der BCMB beispielsweise auf die Ressourcenzuständigen und Prozesseigentümer zugehen, in deren Zuständigkeitsbereich die BC-Strategien umgesetzt werden. Auch kann er mit Anbietern entsprechender Lösungen in Kontakt treten.

Die Bewertung der BS-Strategien kann in der Dokumentenvorlage *Bewertungstabelle BC-Strategien* aus den Hilfsmitteln dokumentiert werden. Tabelle 61 zeigt beispielhaft die bewertete BC-Strategie für mobiles Arbeiten:

Beispiel:

Bewertungskriterium	**Bewertung der BC-Strategie „mobiles Arbeiten“**
Einhalten der RTO	Mitarbeiter können ihre Arbeit selbstständig an ihren Heimarbeitsplatz verlagern und das Equipment starten (RTA [2 Stunden] ≤ RTO [24 Stunden]).
Erreichbares Notbetriebsniveau	Das notwendige Notbetriebsniveau wird erreicht.
Verbleiben des Restrisiko	Fällt der Standort etwa durch Feuer aus und nehmen Mitarbeiter ihre Laptops nicht immer über Nacht oder am Wochenende mit nach Hause, würde auch das notwendige Equipment für die BC-Strategie zerstört werden.
Finanzielle Aufwände	Alle in zeitkritische Geschäftsprozesse eingebundenen Mitarbeiter benötigen entsprechendes Equipment. Es müssen die technischen Voraussetzungen für die Arbeit außerhalb der Organisation geschaffen werden. Schätzung: Erstbeschaffung: 100.000€ Aufrechterhaltung der Infrastruktur: 10.000€ pro Jahr

Bewertungskriterium	Bewertung der BC-Strategie „mobiles Arbeiten“
Einhaltung interner und externer Anforderungen	Arbeitszeiten müssen auch bei temporärer Heimarbeit erfasst werden. Mittels digitaler Zeiterfassung wird dieser Anforderung entsprochen.
Maximal mögliche Notbetriebsdauer:	Bei regelmäßigen physischen Arbeitstreffen in angemieteten Konferenzräumen zeitlich nicht begrenzt.
Organisatorische Aufwände	Es muss eine allgemeine Heimarbeitsplatz-Richtlinie mit den Arbeitnehmervertretern abgestimmt werden.
Entstehende Risiken:	Bei falscher Dimensionierung des VPN-Netzes und im Notfall hoher Nutzerzahlen könnte das interne Netz überlastet werden. Es besteht ein erhöhtes Risiko einer Informationssicherheitslücke durch möglicherweise nicht ausreichende Sicherheitsmaßnahmen an Heimarbeitsplätzen.
Entstehender Zusatznutzen	Mitarbeitern könnte es ermöglicht werden, auch im Normalbetrieb mobiles Arbeiten zu nutzen. Gleichzeitig könnten die vorhandenen Arbeitsflächen des Unternehmens selbst bei einer wachsenden Zahl an Mitarbeitern ausreichend bleiben.

Tabelle 61: Beispiel für die Bewertung der BC-Strategie „Mobiles Arbeiten“

Als Ergebnis verfügt der BCMB über eine Übersicht prinzipiell sinnvoller BC-Strategien und inwieweit diese sowohl wirksam als auch angemessen sind. Es ist empfehlenswert, dass der BCMB die aus seiner Sicht passendsten BC-Strategien vorauswählt. Dies erleichtert es der Institutionsleitung, die bestmöglich geeignete BC-Strategie festzulegen. Dazu ist es hilfreich, dass der BCMB prüft, welche der BC-Strategien die Anforderungen an die Notfallplanung sowie die Rahmenbedingungen der Institution bestmöglich vereinen.

Nachdem der BCMB die BC-Strategien geprüft hat, kann er je Ressourcenkategorie eine oder mehrere BC-Strategien vorauswählen. Insbesondere für Notfallmaßnahmen kann es sinnvoll sein, mehrere prinzipiell mögliche BC-Strategien vorzuschlagen, etwa wenn die BC-Strategien nicht von allen Organisationseinheiten gleichermaßen genutzt werden können.

Beispiel:

Innerhalb einer Institution werden für das Szenario eines Gebäudeausfalls mehrere parallele BC-Strategien entwickelt, die gleichermaßen als wirksam und angemessen bewertet wurden. Die möglichen BC-Strategien umfassen gleiche Tätigkeiten auf mehrere Standorte zu verteilen, mobiles Arbeiten vorzubereiten sowie einen Ausweichstandort bereitzustellen. Eine Organisationseinheit könnte sich dazu entscheiden, ihre Tätigkeiten präventiv auf mehrere Standorte aufzuteilen und somit die Wahrscheinlichkeit zu senken, dass eine kritische Menge an Mitarbeitern gleichzeitig ausfällt.

Eine weitere Organisationseinheit hat in der BIA angegeben, keine dedizierten Arbeitsplätze zu benötigen, sondern flexibel arbeiten zu können. Für diese Organisationseinheit bietet sich folglich die BC-Strategie „mobiles Arbeiten“ an. Eine letzte Organisationseinheit hat in der BIA angegeben, aufgrund spezieller Anforderungen an den Arbeitsplatz (etwa Maschinen-Arbeitsplätze) einen dedizierten Ausweicharbeitsplatz zu benötigen. Für diese Organisationseinheit bietet sich folglich die BC-Strategie eines vorbereiteten Ausweichstandortes an.

Als Ergebnis dieser Phase verfügt der BCMB für jede Ressourcenkategorie über mindestens eine mögliche BC-Strategie, die der Institutionsleitung im folgenden Schritt vorgestellt werden muss.

6.8.3 Auswahl der BC-Strategien durch die Institutionsleitung

Nachdem der BCMB mögliche BC-Strategien vorausgewählt hat, muss die Institutionsleitung in ihrer Rolle als Gesamtverantwortliche für das BCM sowie aufgrund der Reichweite der BC-Strategien über die letztlich umzusetzenden BC-Strategien entscheiden. Die Institutionsleitung muss hierzu die Wirksamkeit der BC-Strategien sowie die erwarteten Kosten und ihre Risikobereitschaft gegeneinander abwägen.

Es ist empfehlenswert, die BC-Strategien im Rahmen einer Entscheidungspräsentation vorzustellen und abzustimmen. Die Entscheidungspräsentation ermöglicht es dem BCMB die BC-Strategien, die relevanten Inhalte sowie Vor- und Nachteile strukturiert und visuell gegenüberzustellen sowie seine jeweiligen Favoriten zu empfehlen. Es ist empfehlenswert, folgende Inhalte in der Entscheidungspräsentation zu berücksichtigen:

Die allgemeinen Ziele von BC-Strategien vorstellen: Da die Institutionsleitung erfahrungsgemäß nur zu bestimmten Ereignissen mit der Thematik von BC-Strategien mit einbezogen wird, ist es empfehlenswert, dass der BCMB zu Beginn der Entscheidungspräsentation auf die Ziele der BC-Strategien eingeht. Er kann hierzu erläutern, was unter BC-Strategien zu verstehen ist, welche Aufgabe die Institutionsleitung hierbei hat und welche Schritte auf die Entscheidung der Institutionsleitung folgen.

Betrachtungsgrundlage der BC-Strategien vorstellen: Um der Institutionsleitung zu verdeutlichen, was in der Notfallplanung durch die BC-Strategien abgesichert werden muss, kann der BCMB die betrachteten Ressourcenkategorien und Teilkategorien vorstellen. Er kann hierbei auch auf identifizierte Single-Points-of-Failure und Verbesserungsbedarfe vorangegangener BCMS-Tätigkeiten eingehen, die durch die BC-Strategien berücksichtigt werden sollten.

Empfohlene BC-Strategien sowie deren Vor- und Nachteile erläutern: Je vorgestellter Ressourcenkategorie kann der BCMB die empfohlenen BC-Strategien vorstellen sowie die jeweiligen Vor- und Nachteile erläutern. Hierbei kann er auch auf mögliche Synergien, Abhängigkeiten und Konflikte eingehen, die mit den jeweiligen BC-Strategien einhergehen.

Umzusetzende BC-Strategien auswählen: Auf Basis der empfohlenen BC-Strategien ist die Institutionsleitung in der Lage, sich eine fachliche Übersicht über die möglichen BC-Strategien zu verschaffen und zu entscheiden, wie Sie die Notfallplanung ausrichten möchte. Auch kann die Institutionsleitung über die BC-Strategien steuern, wie weit die Ressourcenkategorien mit entsprechenden Aufwänden abgesichert werden sollen, wie Vorteile genutzt werden können und welches Restrisiko sie bereit ist zu übernehmen.

Die Institutionsleitung kann sich entscheiden, je Ressourcenkategorie eine oder mehrere BC-Strategien auszuwählen, verschiedene BC-Strategien zu kombinieren oder eine eigene BC-Strategie auszuwählen.

Beispiel:

Die Ressourcenkategorie Gebäude und Infrastrukturen wird in die beiden Teilkategorien Bürogebäude und Produktionsgebäude unterteilt. Die Institutionsleistung entscheidet sich, die Bürogebäude durch folgende BC-Strategien abzusichern:

- Mitarbeiter, die mobil arbeiten können, sollen mit entsprechender Technik ausgestattet werden, um im Falle eines Gebäudeausfalls von zu Hause arbeiten zu können.
- Falls kein mobiles Arbeiten möglich ist, verdrängen Mitarbeiter mit zeitkritischen Aufgaben andere Mitarbeiter ohne zeitkritische Aufgaben von ihrem Arbeitsplatz.

Die Produktion innerhalb der Produktionsgebäude kann im Falle eines Gebäudeausfalls nicht verlagert werden. Auch können die eingesetzten Maschinen aufgrund der hohen Investitionskosten nicht redundant vorgehalten werden. Die Institutionsleitung entscheidet sich die Produktionsgebäude soweit durch Vorsorgemaßnahmen abzusichern, dass die Ausfallwahrscheinlichkeit auf ein akzeptables Niveau gesenkt und das verbleibende Restrisiko durch die Institutionsleitung übernommen wird. Als Vorsorgemaßmaßnahmen werden zusätzlich zu den rechtlich verbindlichen Maßnahmen wie Brandschutz weitere Maßnahmen, wie eine Netzersatzanlage, installiert.

Nachdem die BC-Strategien durch die Institutionsleitung ausgewählt und freigegeben wurden, sollte diese Entscheidung dokumentiert werden. Die dokumentierte Entscheidung ist der Auftrag an den BCMB, einen Umsetzungsplan zu erstellen. Sollte aus Sicht der Institutionsleitung keine der vorgeschlagenen BC-Strategien ausreichend wirksam oder angemessen erscheinen, kann sie den BCMB auch damit beauftragen neue BC-Strategien zu entwickeln. Sind auch die neu entwickelten BC-Strategien aus ihrer Sicht unwirksam oder unangemessen, kann sich die Institutionsleitung auch dazu entscheiden, keine BC-Strategie umzusetzen. Dies kann etwa der Fall sein, wenn das Risiko oder der mögliche Schaden ausgefallener Ressourcen oder Geschäftsprozesse die Aufwände der BC-Strategien aus Sicht der Institutionsleitung nicht rechtfertigen würden. In diesem Fall muss die Institutionsleitung das Restrisiko übernehmen, solange es keine regulatorischen oder gesetzlichen Verpflichtungen gibt, die dies verbieten. Das jeweilige Risiko muss im Rahmen der Risikobeurteilung dokumentiert, regelmäßig neu bewertet und daraufhin geprüft werden, ob das Risiko durch neue BC-Strategien gesenkt werden kann (siehe Kapitel 6.7 *BCM-Risikoanalyse*).

6.8.4 Umsetzung der BC-Strategien und -Lösungen

Nachdem die Institutionsleitung die BC-Strategien freigegeben hat, muss festlegt werden, wer für diese zuständig ist und wer das hierzu notwendige Fachwissen besteuern kann. Gemeinsam mit dem BCMB können diese abstimmen, wie die BC-Strategien umgesetzt werden. Hierzu ist es empfehlenswert, zunächst zu prüfen, aus welchen Vorsorgemaßnahmen, BC-Lösungen und Notfallmaßnahmen sich die ausgewählte BC-Strategie zusammensetzt. Vorsorgemaßnahmen und BC-Lösungen können im Rahmen von Projekten oder innerhalb der AAO umgesetzt werden, da diese in der Regel umfassender sind und oft verschiedene Organisationseinheiten, Stellen und Ansprechpartner betreffen.

Beispiel:

Eine Institution möchte die BC-Strategie eines Ausweichstandortes im Rahmen eines Projektes umsetzen. Als beteiligte Projektansprechpartner sind vorgesehen:

- Die Gebäudeverwaltung für alle gebäudespezifischen und infrastrukturellen Fragestellungen
- Die IT für alle Fragestellungen hinsichtlich der Anbindung und IT-spezifischen Ausstattung des Standortes
- Das Controlling für alle finanziellen Fragestellungen
- Das Projektmanagement-Büro, um das Projekt mit dem BCMB übergreifend zu steuern.

Nachdem der BCMB die jeweiligen Ressourcenzuständigen ermittelt hat, muss ein Umsetzungsplan erstellt werden. Erfahrungsgemäß wird dieser von den Ressourcenzuständigen erstellt. Der Umsetzungsplan muss mindestens folgende Informationen enthalten:

- die konkreten Handlungsschritte, die notwendig sind, um die jeweilige BC-Lösung umsetzen zu können
- die finanziellen, personellen und zeitlichen Ressourcen, die benötigt werden, um die Handlungsschritte umsetzen zu können
- die Personen, die die Handlungsschritte des Umsetzungsplans umsetzen sollen
- die Zeiträume, in denen die Handlungsschritte umgesetzt werden sollen

Während der Umsetzungsplan erstellt wird, können sich mitunter zusätzlich notwendige Ressourcen im Sinne von Mitteln oder Maßnahmen ergeben, die bisher noch nicht bedacht wurden. Die erstellten Umsetzungspläne müssen folglich dahingehend überprüft werden, ob das erwartete Gesamtergebnis im Hinblick auf die ausgewählten BC-Strategien weiterhin wirksam und angemessen ist.

Nachdem die Umsetzungspläne und benötigten Ressourcen im Sinne von Mitteln von der Institutionsleitung freigegeben wurden, müssen die Maßnahmen durch die Zuständigen im festgelegten Zeitraum umgesetzt

werden. Der BCMB sollte die Umsetzung dieser Maßnahmen steuern und kontrollieren. Hierzu ist der Maßnahmenplan ein sehr geeignetes Mittel (siehe Kapitel 6.13 *Korrektur und Verbesserung des BCMS*). Die Notfallmaßnahmen werden im Rahmen der Geschäftsfortführungsplanung sowie Wiederanlaufplanung behandelt (siehe Kapitel 6.9 *Geschäftsfortführungsplanung* und Kapitel 6.10 *Wiederanlauf- und Wiederherstellungsplanung*).

Innerhalb von **Geschäftsfortführungsplänen (GFP)** wird dokumentiert, wie eine Institution auf der Prozessebene auf eine Geschäftsunterbrechung nach einem Ressourcenausfall reagiert. Hierzu werden konkrete Notfallmaßnahmen und Verfahren aus den BC-Strategien und -Lösungen abgeleitet, wie zeitkritische Geschäftsprozesse bis zur Wiederherstellung der ausgefallenen Ressourcen im erforderlichen Umfang aufrechterhalten werden können.

Innerhalb von **Wiederanlaufplänen (WAP)** wird dokumentiert, wie die Institution ausgefallene Ressourcen etwa durch umgesetzte BC-Lösungen oder Ersatzlösungen auf dem für die Geschäftsfortführung notwendigen Umfang kompensiert.

Innerhalb von **Wiederherstellungsplänen (WHP)** wird dokumentiert, wie die ausgefallenen Ressourcen in den Normalbetrieb zurückversetzt werden können.

Die beschriebenen Dokumente bilden zusammen mit den Informationen aus dem Aufbau und der Befähigung der BAO die Inhalte des Notfallhandbuchs. Das Notfallhandbuch ist die zentrale Dokumentensammlung zur erfolgreichen Notfallbewältigung. Abbildung 59 verdeutlich die Beziehung der Dokumente untereinander.

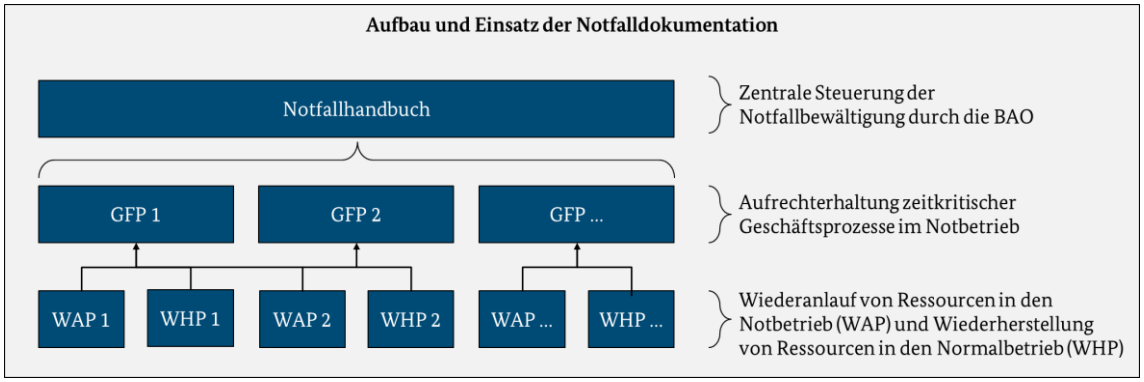

Abbildung 59: Aufbau und Einsatz der Notfalldokumentation

Hinweis:

Die verschiedenen Notfallpläne können sowohl nacheinander als auch parallel erstellt werden. Es ist hilfreich, die GFP und WAP parallel zu erarbeiten, da bestehende Abhängigkeiten so besser aufeinander abgestimmt werden können. Es ist wichtig dabei zu beachten, dass dies kurzfristig zu einem höheren Bedarf an benötigten personellen und organisatorischen Ressourcen führen kann.

6.9 Geschäftsfortführungsplanung

Im Rahmen der Geschäftsfortführungsplanung beschreibt die Institution, wie sie im Notfall die festgelegten BC-Strategien und -Lösungen auf Prozessebene anwenden wird. Die Geschäftsfortführungsplanung muss für alle zeitkritischen Geschäftsprozesse erstellt und dokumentiert werden. Dies gilt auch unabhängig davon, ob gemäß der Risikoanalyse nur ein geringes Risiko besteht, dass der Geschäftsprozess (bzw. die zugrundeliegenden Ressourcen) ausfallen könnte.

Um die Geschäftsfortführungspläne (GFPs) zu dokumentieren, kann die Dokumentenvorlage *Geschäftsfortführungsplan* aus den Hilfsmitteln verwendet werden. Anhand dieser Dokumentenvorlage werden einige in diesem Kapitel aufgeführten Beispiele und Hinweise dargestellt.

Da die Geschäftsfortführungspläne üblicherweise von den Organisationseinheiten selbst erstellt werden, ist es sinnvoll diesen Schritt zentral innerhalb der Notfallvorsorgeorganisation vorzubereiten. Die Geschäftsfortführungsplanung ist abgeschlossen, sobald alle GFPs zentral abgelegt und die Institutionsleitung über den Abschluss der Geschäftsfortführungsplanung informiert wurde.

Die folgende Abbildung gibt einen Überblick über die notwendigen Schritte zur Vorbereitung, Erstellung sowie Qualitätssicherung und Freigabe der GFPs. Diese werden in den folgenden Kapiteln näher beschrieben.

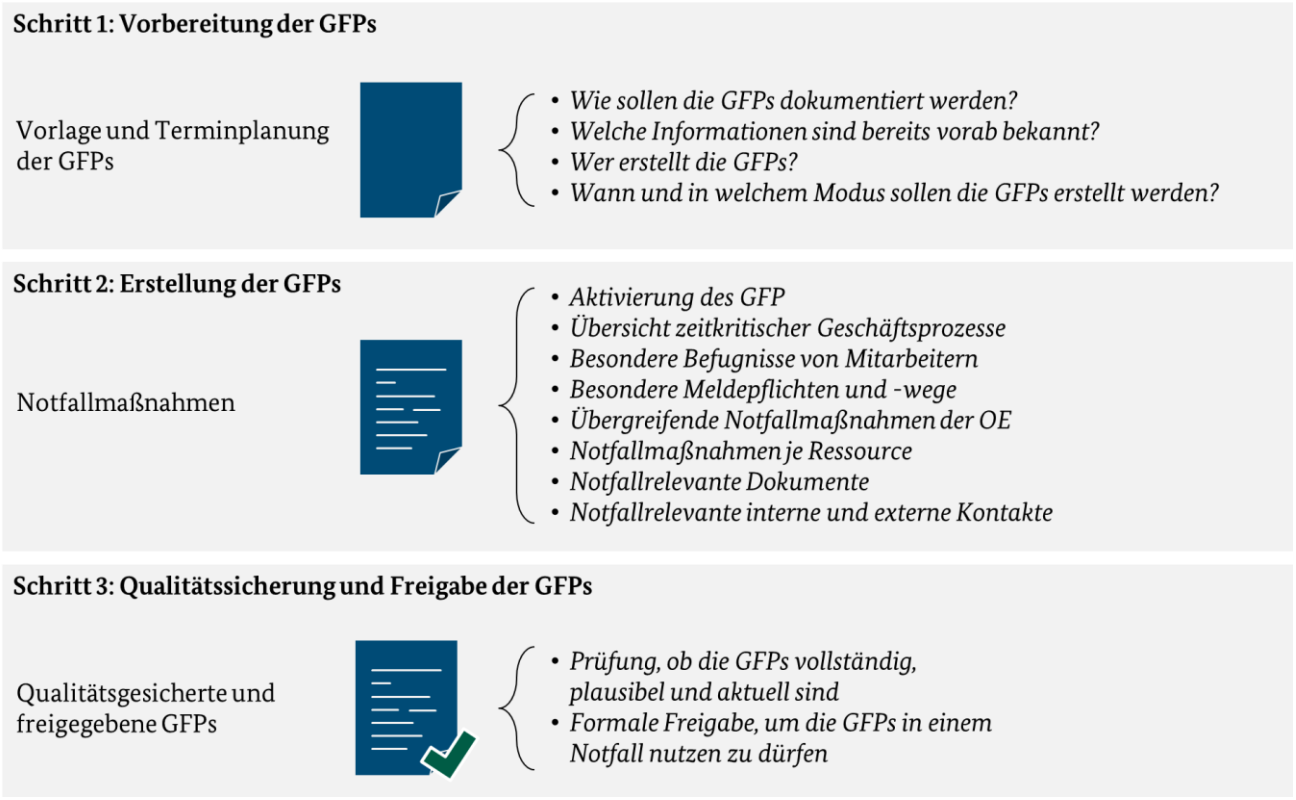

Abbildung 60: BCM-Prozessschritte zur Geschäftsfortführungsplanung

Hinweis:

Sofern die Institution bereits über GFPs verfügt, die etwa im Rahmen des Reaktiv-BCMS erstellt wurden, müssen diese entsprechend des Kapitels 4.8.4 *Übergang in das Folge-BCMS* ergänzt werden. Zusätzlich müssen die bestehenden Notfallmaßnahmen dahingehend überprüft werden, ob diese den im Standard-BCMS festgelegten BC-Strategien und -Lösungen entsprechen und falls erforderlich angepasst werden sollten.

6.9.1 Vorbereitung der GFPs

Eine effektive Vorbereitung der GFPs ist die Voraussetzung dafür, dass

- die Erstellung der GFPs effizient, vergleichbar und valide durchgeführt werden kann,
- die Teilnehmer optimal auf die Fragestellungen vorbereitet werden, sowie
- im Notfall die Leser die GFPs gut lesen und schnell anwenden können.

Die Erstellung der GFPs sollte daher vorbereitet werden. Es ist empfehlenswert, dass die Vorbereitung durch den BCMB erfolgt, da dieser über das notwendige Fachwissen zum BCM-Prozess verfügt und diesen zeitlich steuert. Er kann vorbereitende Tätigkeiten ganz oder teilweise an weitere Rollen im BCM delegieren, z. B. an lokale BCMB, BCMK oder ein Notfallvorsorgeteam (siehe Kapitel 3.2.2 *Definition der BCM-Aufbauorganisation*). Die Aufgaben in der Vorbereitung der GFPs werden in den nachfolgenden Unterkapiteln näher erläutert.

6.9.1.1 Organisatorische Aufteilung der GFPs

Der BCMB muss festlegen, wie die GFPs im Hinblick auf die zugrundeliegende Struktur der Institution aufgeteilt werden sollen. Es gibt viele Möglichkeiten, wie Geschäftsfortführungspläne organisatorisch aufgeteilt werden könnten. So könnte ein GFP je Geschäftsprozess erstellt werden oder für ein bestimmtes Ausfallszenario die jeweils relevanten Ressourcen wiedergeben. Entscheidend für eine schnelle Notfallreaktion ist jedoch, dass

- eine anschauliche Übersicht über die zeitkritischen Geschäftsprozesse und Ressourcen ermöglicht wird sowie
- die Zuständigkeiten der im GFP beschriebenen Maßnahmen möglichst klar geregelt sind.

Hierbei hat es sich in der Praxis bewährt, einen GFP je Organisationseinheit zu erstellen. Dieses Vorgehen bietet viele Vorteile. Die zuständigen Ansprechpartner, die den GFP erstellen und aktualisieren, können eindeutig der Organisationseinheit zugeordnet werden. Zudem wird eine überschaubare Anzahl an Dokumenten erzeugt und die GFPs spiegeln die vertraute Organisationsstruktur wider. Die GFPs lassen sich so leichter voneinander abgrenzen.

Im Einzelfall kann es sinnvoll sein, von dieser Struktur abzuweichen. Dies ist etwa der Fall, wenn

- Verantwortungs- und Tätigkeitsbereiche nicht klar voneinander abgrenzbar sind, z. B. in einer Matrix-Organisation, oder
- Organisationseinheiten standortübergreifend agieren und auf unterschiedliche Ressourcen zugreifen.

Zusätzlich können länderspezifische Anforderungen und Gegebenheiten unter Umständen dazu führen, dass für gleiche Geschäftsprozesse und Ressourcen im GFP unterschiedliche Notfallmaßnahmen an unterschiedlichen Standorten beschrieben werden müssen. Alternativ können GFPs auch nach Geschäftsprozessen unterteilt werden, was jedoch zu einer hohen Anzahl an Dokumenten führen kann.

Hinweis:

Ob die GFPs sinnvoll aufgeteilt und voneinander abgegrenzt wurden, kann mitunter erst im Rahmen der Erstellung der GFPs fundiert bewertet werden. Der BCMB sollte daher die Aufteilung der GFPs im Rahmen der Erstellung der GFPs mit den entsprechenden Ansprechpartnern diskutieren und gegebenenfalls den Geltungsbereich des GFP anpassen bzw. in mehrere GFPs aufteilen.

Um die Erläuterungen in den folgenden Kapiteln zu vereinfachen, wird davon ausgegangen, dass die GFPs entsprechend der Organisationseinheiten aufgeteilt wurden. Werden die GFPs in der Institution anderweitig aufgeteilt, so sollten die Inhalte dieses Standards angepasst auf die eigene Vorgehensweise angewendet werden.

6.9.1.2 Erstellung einer GFP-Dokumentenvorlage

Um die Geschäftsfortführung im Notfall zu erleichtern, sollte der BCMB sicherstellen, dass die GFPs einheitlich aufgebaut und nachvollziehbar dokumentiert sind. Hierzu sollte eine GFP-Dokumentenvorlage erstellt werden. Die nachfolgenden Aspekte müssen darin berücksichtigt werden:

Der **Geltungsbereich** beschreibt den organisatorischen und räumlichen Bereich, in welchem die Maßnahmen und Verfahren eines GFP gelten. Die Beschreibung des Geltungsbereichs stellt sicher, dass der GFP sowie die darin beschriebenen Maßnahmen ausschließlich in dem für ihn vorgesehenen Umfeld eingesetzt werden. Es könnte z. B. vorkommen, dass die beschriebenen Maßnahmen nicht in anderen Organisationseinheiten sowie Standorten eingesetzt werden können oder den dort notwendigen Maßnahmen widersprechen.

In der **Zielstellung des GFP** muss beschrieben werden, was durch den GFP erreicht werden soll und was explizit nicht durch den GFP forciert wird. Die Beschreibung der Zielstellung stellt sicher, dass der GFP nur

zu seinem gedachten Zweck eingesetzt wird und nicht etwa im Rahmen des Tagesbetriebs zweckentfremdet oder mit anderen Themen vermischt wird (siehe auch Aktivierungsprozess).

Der **Aktivierungsprozess** wird in Kapitel 6.9.2.1 *Festlegung organisatorischer Maßnahmen* näher erläutert.

Die **gesonderten Rechte und Pflichten der Mitarbeiter** werden in Kapitel 6.9.2.1 *Festlegung organisatorischer Maßnahmen* näher erläutert.

Die **besonderen Melde- und Berichtspflichten** werden in Kapitel 6.9.2.1 *Festlegung organisatorischer Maßnahmen* näher erläutert.

Innerhalb des GFP müssen alle **zeitkritischen Geschäftsprozesse** einer Organisationseinheit sowie deren MTPD dokumentiert werden. Die Dokumentation hat zum Ziel, dem Stab im Notfall eine Übersicht über die zeitkritischen Geschäftsprozesse im Geltungsbereich sowie deren MTPD zu verschaffen. Die Auflistung schafft Transparenz über die bestehenden zeitkritischen Geschäftsprozesse sowie über die zeitliche Reihenfolge, in welcher diese wieder in einem Notbetrieb anlaufen müssen

Zusätzlich müssen die identifizierten **Abhängigkeiten zwischen zeitkritischen Geschäftsprozessen** dokumentiert werden. Hierunter fallen auch prozessuale Abhängigkeiten, die etwa zwischen Organisationseinheiten bestehen. Dadurch ist es möglich im Notfall schnell festzustellen, welche Geschäftsprozesse durch einen vor- oder nachgelagerten oder parallelen Prozessausfall betroffen sind. Die Tätigkeiten im Notbetrieb können so leichter institutionsweit priorisiert werden.

Alle **zeitkritischen Ressourcen** der betrachteten Organisationseinheit sowie die identifizierten RTAs oder RTOs sowie die RPOs müssen innerhalb des GFP dokumentiert werden. Anhand der aufgelisteten Ressourcen müssen innerhalb des GFP Notfallmaßnahmen abgeleitet werden, wie die Organisationseinheit mit den im Rahmen der Wiederanlaufplanung bereitgestellten Ressourcen arbeitet. Die Notfallmaßnahmen zielen darauf ab, die Geschäftsprozesse bei Ausfall der Ressourcen innerhalb der RTO auf dem vorgegebenen Notbetriebsniveau fortzuführen.

Innerhalb des GFP müssen sämtliche internen sowie externen **Kontakte** dokumentiert werden, die im Rahmen der Geschäftsfortführung **relevant** sind. Hierunter fallen etwa Mitarbeiter aus anderen Fachbereichen, interne oder externe Fachexperten sowie innerhalb der Organisationseinheit benötigte Dienstleister. Die Dokumentation der relevanten Kontakte ermöglicht einen schnellen Zugriff auf die entsprechenden Stellen sowie eine Unabhängigkeit von anderen, möglicherweise nicht verfügbaren Kontakt-Quellen wie digitalen Telefonbüchern. Sofern die Kontakt-Informationen bereits ausfallsicher an anderer Stelle dokumentiert sind, genügt es, im GFP die Kontakt-Informationen zu referenzieren und im Notfall verfügbar zu machen.

Innerhalb des GFP sollten alle zur Geschäftsfortführung **relevanten Dokumente** sowie ihre jeweiligen Ablageorte notiert werden. Mögliche Dokumente sind etwa Prozessbeschreibungen oder Handlungsanweisungen. Für den Fall eines Notfalls kann durch die Verweise schnell auf die relevante Information in den jeweiligen Dokumenten zugegriffen werden. Voraussetzung ist, dass die für die Notfallbewältigung benötigten Dokumente schnell zu erfassen sind und konkrete Notfallmaßnahmen leicht daraus abgeleitet werden können Es muss jedoch sichergestellt werden, dass die Ablageorte entsprechend des Schutzbedarfs abgesichert und auch im Notfall zugänglich sind.

Hinweis

Sofern für die Geschäftsfortführung auf Informationen in anderen Dokumenten zurückgegriffen werden soll, ist es empfehlenswert, dass alle im GFP aufgeführten Dokumente am Ende des GFP noch einmal in einer Gesamtliste der benötigten Dokumente namentlich aufgeführt werden. Zusätzlich sollte dann je Dokument der jeweilige Ablageort referenziert werden.

6.9.1.3 Vorausfüllen der GFPs

Es ist empfehlenswert, dass die erstellte GFP-Vorlage mit den bereits bekannten Informationen aus BIA und Soll-Ist-Vergleich je Geltungsbereich vorausgefüllt wird. Zu den bereits bekannten Informationen gehören

- der Geltungsbereich des GFP,
- die zeitkritischen Geschäftsprozesse in diesem Geltungsbereich,
- die Abhängigkeiten zu diesen zeitkritischen Geschäftsprozessen,
- die MTPD und das Notbetriebsniveau jedes gelisteten Geschäftsprozesses sowie
- die zeitkritischen Ressourcen mit ihrer jeweiligen RTA bzw. /RTO sowie RPO.

Um ursachenbasiert konkrete Notfallmaßnahmen zu beschreiben, bietet es sich in einem GFP an, die relevanten Informationen den Ressourcenkategorien zuzuordnen. Dies erlaubt einen schnellen Zugriff auf die Informationen im Notfall.

6.9.1.4 Organisatorische Planung

Die Geschäftsfortführungsplanung kann weitestgehend analog zum Vorgehen in der BIA organisiert werden (siehe Kapitel 4.4.1.4 *Organisatorische Planung*). Insbesondere, wenn GFPs erstmalig erstellt werden, sollte der BCMB dies im Rahmen von Workshops durchführen. Er kann hierbei die Methodik und die Inhalte des GFP erläutern und den Workshop moderieren.

Es ist empfehlenswert, dass die gleichen Personen wie in den vorangegangenen Schritten zur BIA am Workshop teilnehmen. Dieser Personenkreis verfügt in der Regel über umfangreiches Wissen über die Geschäftsprozesse und die dafür benötigten Ressourcen und kann entsprechend qualitative Aussagen zur Geschäftsfortführung tätigen. Der Teilnehmerkreis bleibt so überschaubar, kann jedoch bei Bedarf durch weitere Prozess- und Ressourcenexperten ergänzt werden.

6.9.2 Erstellung der GFPs

In diesem Kapitel wird beschrieben, wie die Inhalte der GFPs erarbeitet werden.

6.9.2.1 Festlegung organisatorischer Maßnahmen

Die Festlegung organisatorischer Maßnahmen beinhaltet alle übergreifenden Aspekte, die nicht dazu dienen, die Geschäftsfortführung einzelner Geschäftsprozesse zu regeln. Diese werden im Nachfolgenden beschrieben.

In einem ersten Schritt muss die Organisationseinheit beschreiben, wie die relevanten **Mitarbeiter im Falle eines Notfalls alarmiert und informiert** werden, nachdem der GFP durch den Stab formal aktiviert wurde. Die Organisationseinheit kann sich hierzu an den Erläuterungen des Kapitels 6.4.2.3 *Alarmierung der BAO* ausrichten und den festgelegten Alarmierungs- und Eskalationspfad für die Organisationseinheit fortschreiben. Hierzu wird empfohlen, für die Organisationseinheit intern festzulegen,

- welche Personen bzw. Funktionen in Kenntnis gesetzt werden sollen,
- über welche Kommunikationsmittel die Alarmierung im Notfall erfolgen soll sowie
- welche weiteren Schritte sich aus der Alarmierung ergeben.

Zu alarmierende Kontaktpersonen können Mitglieder des Notfallteams, weitere Mitarbeiter, externe Fachexperten oder externe Stellen sein. Die Kontaktlisten können als Anhang zum GFP hinterlegt werden, um personenbezogene oder vertrauliche Kontaktdaten ihrem Schutzbedarf entsprechend ablegen zu können.

Innerhalb des Kapitels 6.4.4.1 *Konstituierung und Auflösung der BAO* ist beschrieben, nach welchen Kriterien GFPs durch den Stab aktiviert werden. Innerhalb dieses Abschnitts im GFP werden diese Kriterien aufgegriffen und konkretisiert.

Für die Dauer des Notfalls kann es notwendig sein, allen oder einzelnen Mitarbeitern im Geltungsbereich des GFP **besondere Rechte und Pflichten** zuzuteilen. Diese beschreiben etwa, welche gesonderten Zuständigkeiten und (Zugangs-, Zutritts- und Zugriffs-) Rechte Mitarbeitern im Notfall zugeteilt werden. Gesonderte Rechte umfassen auch solche im Rahmen von Freigabeprozessen oder Führungsaufgaben. Die gesonderten Rechte gelten von dem Zeitpunkt an, ab dem der GFP aktiviert wurde bis zu dem Zeitpunkt, an dem der Notfall deeskaliert wird.

Fallen Geschäftsprozesse innerhalb des Geltungsbereichs des GFP aus, können **besondere Melde- und Berichtspflichten an interne und externe Stellen** bestehen. Diese sollten innerhalb des GFP dokumentiert werden, sofern diese von denen des Normalbetriebs abweichen und nur für die Dauer des Notfalls gelten. Die besonderen Melde- und Berichtspflichten richten sich sowohl an interne als auch externe Interessengruppen. Hierunter fallen etwa andere Organisationseinheiten der Institution, Aufsichtsbehörden, Kunden, Dienstleister und Lieferanten, die für die Dauer des Notfalls gesondert informiert werden müssen. Dies kann etwa häufigere Meldungen oder Berichte umfassen oder gesonderte Inhalte der Meldungen. Hierzu ist es empfehlenswert, folgende Informationen zu beschreiben:

- Stelle, an die gemeldet oder berichtet werden soll
- Rolle, die melden oder berichten soll
- Medium, mit dem gemeldet oder berichtet werden soll
- Inhalt, der gemeldet oder berichtet werden soll
- Zeitpunkt bzw. Häufigkeit, zu dem gemeldet oder berichtet werden soll

6.9.2.2 Entwicklung von Notfallmaßnahmen

Innerhalb der Erstellung der GFPs müssen Notfallmaßnahmen entwickelt und dokumentiert werden, um ausgefallene Geschäftsprozesse in einen definierten Notbetrieb wiederaufzunehmen. Diese werden üblicherweise von den zuständigen Ansprechpartnern der GFPs erstellt. Hierzu muss beschrieben werden, wie auf Basis der festgelegten BC-Strategien und -Lösungen die Geschäftsprozesse innerhalb der erforderlichen Zeit und auf dem Notbetriebsniveau wiederaufgenommen werden sollen.

Folgende Leitfragen können dabei helfen, die erforderlichen Notfallmaßnahmen zu ermitteln:

Welche Informationen sollen an wen auf welche Weise weitergegeben werden?

- Welche Notfallmaßnahmen müssen eingeleitet werden, um den gewünschten Zustand zu erreichen (z. B. Notbetriebsniveau)?
- Wie lange würde die Durchführung der Notfallmaßnahmen dauern?
- Welche Voraussetzungen müssten gegeben sein, um die Notfallmaßnahmen durchführen zu können?
- Welche Reaktionen würden von anderen erwartet?

Darüber hinaus sollten die Notfallmaßnahmen mit der aktuellen Wiederanlaufplanung abgestimmt werden. Abschließend muss beschrieben werden, wie die Geschäftsprozesse vom Notbetrieb in den Normalbetrieb überführt und mit notwendigen Nacharbeiten, wie Arbeitsrückständen, verfahren werden soll.

Es wird empfohlen, die Notfallmaßnahmen am Ablauf der Notfallbewältigung auszurichten:

- Maßnahmen, um den Notbetrieb zu erreichen (Wiederanlauf in den Notbetrieb)
- Maßnahmen für die Geschäftsfortführung (Notbetrieb)
- Maßnahmen zur Rückführung in den Normalbetrieb (Nacharbeiten im Störbetrieb)

Beispiel:

Für einen Gebäudeausfall wird den Organisationseinheiten im Rahmen der festgelegten BC-Strategie und Lösung ein gleichwertiger Ausweichstandort zur Verfügung gestellt. Innerhalb des Wiederanlaufplans werden die Maßnahmen beschrieben, um den Ausweichstandort mit den benötigten Arbeitsmaterialien bereitzustellen. Innerhalb der GFPs wird beschrieben, wie die Organisationseinheiten die zeitkritischen Mitarbeiter an den Ausweichstandort entsenden und dort die Arbeit wiederaufnehmen. Dies umfasst etwa Transportmöglichkeiten abzustimmen, notwendige Zutrittsberechtigungen zu erhalten oder die Mitarbeiter auf die vorhandenen Arbeitsplätze zu verteilen. Darüber hinaus wird festgelegt, welche Maßnahmen für die Dauer des Notbetriebs an den Ausweichstandort gelten. Dies umfasst z. B. Regelungen,

- wie mit vertraulichen Dokumenten am Ausweichstandort umgegangen wird,
- wie Informationen auf Papier, z. B. Postsendungen, nachgesendet werden und
- wie alternative, vor Ort befindliche Geräte, Maschinen oder Anlagen eingesetzt werden.

Abschließend wird beschrieben, wie die Organisationseinheiten vom Notbetrieb wieder in den Normalbetrieb zurückkehren können. Dies umfasst etwa Mitarbeiter wieder auf die regulären Arbeitsplätze zu verteilen, den vertraulichen Transport von im Notbetrieb erstellten Dokumenten zu beauftragen oder temporäre Zutrittsberechtigungen zu löschen.

Sofern aus Sicht der Organisationseinheit der Geschäftsbetrieb durch zusätzliche Notfallmaßnahmen noch weiter abgesichert werden kann und die Maßnahmen leicht umsetzbar sind, ist es empfehlenswert, diese der Vollständigkeit halber mit in den GFP zu übernehmen. So können neben den hauptsächlich anzuwenden Maßnahmen auch alternative Varianten aufgeführt werden.

Der Detailgrad der beschriebenen Maßnahmen sollte dabei so gewählt sein, dass eine fachkundige dritte Person in der Lage wäre, die Geschäftsfortführung anhand des GFP umzusetzen.

Hinweis:

Um die Notfallmaßnahmen strukturiert abarbeiten zu können, kann es hilfreich sein, diese anhand von Checklisten zu dokumentieren.

Werden Notfallmaßnahmen definiert, kann es hilfreich sein, innerhalb eines GFP die zeitkritischen Ressourcen anhand unterschiedlich schwerer Ausfallszenarien zu betrachten. Ein Gebäudeausfall kann den Ausfall eines gesamten Standortes, eines einzelnen Gebäudes oder gar einzelner Gebäudeteile bedeuten. Bei einem gesamten Standortausfall könnte es etwa notwendig sein, sämtliche Tätigkeiten oder eine vorhandene Produktion an einen Ausweichstandort zu verlagern. Fallen hingegen nur einzelne Gebäudeteile aus, kann die Verlagerung der Arbeitsplätze oder der Produktion innerhalb des Gebäudes oder Standortes ausreichend sein.

Beispiel:

Für die Ressource Gebäude bestehen in einer Institution die BC-Strategie, Mitarbeiter an eine Aufweichlokation oder in Home-Offices zu verlagern. Um die Notfallmaßnahme für das Szenario eines Gebäudeausfalls besser umsetzen zu können, entscheidet sich die Organisationseinheit das Szenario eines Gebäudeausfalls aufzuteilen. Für den Fall, dass nur einzelne Gebäudeteile ausfallen, verlagert sie die entsprechenden Mitarbeiter an den Ausweichstandort. Für den Fall, dass das gesamte Gebäude ausfällt, verlagert sie Mitarbeiter, die mobil arbeiten können, in Home-Offices, da die Kapazität des Ausweichstandorts begrenzt ist. Mitarbeiter, die nicht mobil arbeiten können, werden an den festgelegten Ausweichstandort verlagert.

Nicht alle Notfallmaßnahmen müssen neu dokumentiert werden, falls diese bereits leicht verständlich in anderen Dokumenten beschrieben sind. Dies kann etwa bereits existierende Prozessbeschreibungen oder Arbeitsanweisungen der AAO umfassen. In diesem Fall kann auf die jeweiligen Stellen in den bestehenden Dokumenten verwiesen werden. Um schnell auf die entsprechenden Stellen zugreifen zu können, sollten alle im GFP aufgeführten Dokumente am Ende des GFP noch einmal in einer Gesamtliste namentlich aufgeführt werden. Zusätzlich sollte je Dokument der jeweils relevante Abschnitt sowie der Ablageort referenziert werden. Es muss auch sichergestellt werden, dass die Ablageorte dem Schutzbedarf der Dokumente entsprechen und auch im Notfall zugänglich sind.

Zusätzlich kann es notwendig sein, im Rahmen der Entwicklung der Notfallmaßnahmen weitere Personen oder Stellen einzubinden. Um sicherzustellen, dass die entsprechenden Kontaktdaten in einem Notfall zur Verfügung stehen, können auch diese im Anhang des GFP aufgelistet werden. Die Bestimmungen des Datenschutzes müssen dabei eingehalten werden.

6.9.3 Qualitätssicherung und Freigabe

Um sicherzustellen, dass alle Vorgaben zur Geschäftsfortführungsplanung eingehalten wurden, sollten die erstellten GFPs formal qualitätsgesichert werden. Dabei sollten die folgenden Aspekte berücksichtigt werden:

- **Vollständigkeit**: Wurde die GFP-Dokumentenvorlage verwendet und bilden die Inhalte alle vorgegebenen Punkte ab? Wurden alle relevanten Inhalte der BIA innerhalb des GFP erfasst und Notfallmaßnahmen dazu beschrieben? Unvollständige GFPs können dazu führen, dass diese im Notfall nicht oder nur begrenzt einsetzbar sind.
- **Plausibilität**: Sind die beschriebenen Maßnahmen widerspruchsfrei und die getroffenen Annahmen für die Institution realistisch? Sind die Angaben innerhalb des GFP als auch die beschriebenen Abhängigkeiten zu anderen GFP oder WAP/WHP plausibel dargestellt?
- **Aktualität**: Sind die referenzierten Dokumente in der jeweils aktuellen Version hinterlegt? Wurden die relevanten Ansprechpartner auf Basis einer aktuellen Kontaktliste dokumentiert? Veraltete Informationen können dazu führen, dass die beschriebenen Maßnahmen wirkungslos sind oder nicht umgesetzt werden können und der GFP in Gänze nicht oder nur begrenzt einsetzbar ist.

Ferner kann durch die Qualitätssicherung der Detailgrad und das sprachliche Niveau der GFPs überprüft und aufeinander abgestimmt werden.

Hinweis:

Die Qualitätssicherung dient zu diesem Zeitpunkt lediglich dazu, sicherzustellen, dass die Vorgaben eingehalten wurden. Ob die in den GFPs beschriebenen Notfallmaßnahmen angemessen, vollständig und wirksam sind, kann erst anhand von Übungen und Tests ermittelt werden (siehe Kapitel 6.11 *Üben und Testen*).

Nachdem die GFPs qualitätsgesichert wurden, müssen diese offiziell freigegeben werden. Dies kann beispielsweise durch die Leitungen der Organisationseinheiten erfolgen. Dieser Schritt signalisiert, dass die Maßnahmen und Verfahren bestätigt wurden und der Plan offiziell in einem Notfall verwendet werden kann.

Nachdem die GFPs sowie die im folgenden Kapitel beschriebenen WAPs/WHPs erstellt, qualitätsgesichert und freigegeben sind, ist wesentlich transparenter, in welchem Maße die BC-Strategien und -Lösungen durch die Organisationseinheiten anwendbar sind und welcher tatsächliche Ressourcenbedarf für die Notfallmaßnahmen erforderlich ist. Es ist daher empfehlenswert, dass der BCMB die aktualisierten Informationen der Institutionsleitung mitteilt. Hierdurch kann der Institutionsleitung ein realistischeres Bild über die Risikosituation vermittelt werden, als es zu einem früheren Zeitpunkt möglich war.

6.10 Wiederanlauf- und Wiederherstellungsplanung

Die **Wiederanlaufplanung** konkretisiert anhand der festgelegten BC-Strategien und –Lösungen, wie ausgefallene Ressourcen in einen Notbetrieb gebracht werden können. Die Wiederanlaufplanung muss für alle zeitkritischen Ressourcen erstellt und dokumentiert werden.

Die **Wiederherstellungsplanung** fokussiert darauf, einen Zustand zu erreichen, in dem der Normalbetrieb wieder möglich ist. Ausgefallene Ressourcen können unter anderem neu beschafft, Ersatzteile eingesetzt oder Komponenten neu installiert und konfiguriert werden. Die Bedingungen und Maßnahmen zur Wiederherstellung sind von vielen Faktoren abhängig: Die Art der Ressource, welche Schäden an den Ressourcen entstanden sind und welche Mittel zur Verfügung stehen. Die Abbildung 61 stellt den Wiederanlauf und die Wiederherstellung anhand einer stark vereinfachten, schematischen Darstellung der Notfallbewältigung gegenüber.

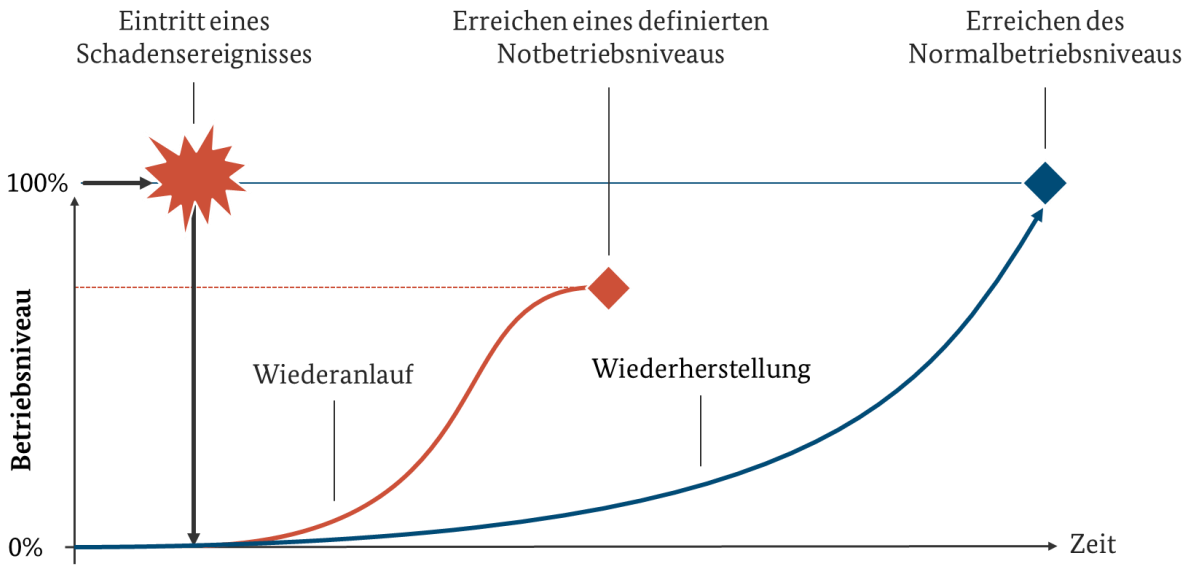

Abbildung 61: Darstellung der Phasen für den Wiederanlauf und die Wiederherstellung

Hinweis:

Abweichend zur Wiederanlaufplanung besteht für die Wiederherstellungsplanung eine andere, meistens deutlich längere Zeitvorgabe. Die maximal mögliche Notbetriebsdauer aus der BC-Strategie. In der Praxis erfolgt die Wiederherstellung ausgefallener Ressourcen typischerweise parallel zum Wiederanlauf. Zum Erreichen des Normalbetriebs muss nicht zwangsläufig exakt die Ressource wiederhergestellt werden, die ausgefallen ist. Mitunter kann eine Wiederherstellung auch bedeuten, dass ein verbesserter Zustand erreicht wird, z. B. weil eine Maschine neu beschafft statt repariert wird oder ein IT-System in einer aktuelleren Version neu aufgesetzt wird.

Um die Wiederanlauf- und Wiederherstellungsplanung zu planen, kann die Dokumentenvorlage *Wiederanlauf- und Wiederherstellungsplan* aus den Hilfsmitteln verwendet werden. Anhand dieser Dokumentenvorlage werden einige der in diesem Kapitel aufgeführten Beispiele und Hinweise dargestellt.

Beispiel:

Bei Ausfall eines Bürogebäudes wird der **Wiederanlauf** durch eine Ersatzlösung in Form mobilen Arbeitens ermöglicht. Grundsätzlich kann jeder Mitarbeiter jederzeit mobil arbeiten. Im Falle eines Notbetriebs würden jedoch sehr viele gleichzeitig auf die Ersatzlösung zugreifen. Die Wiederanlaufplanung fokussiert daher darauf, wie die zusätzlich erforderlichen Kapazitäten im geforderten Zeitraum zur Verfügung gestellt werden sollen.

Parallel zum Wiederanlauf kann das ausgefallene Bürogebäude **wiederhergestellt** werden. Wenn das komplette Bürogebäude so stark zerstört wurde, dass eine Instandsetzung nicht mehr sinnvoll ist, kann die Wiederherstellung statt des Wiederaufbaus auch die Suche nach einem neuen Gebäude sowie alle Maßnahmen zu dessen Inbetriebnahme beinhalten.

Analog zum Vorgehen in der Geschäftsfortführungsplanung gibt die folgende Abbildung 62 einen Überblick über die notwendigen Schritte zur Vorbereitung, Erstellung sowie Qualitätssicherung und Freigabe der Wiederanlauf- und Wiederherstellungspläne (WAP/WHP).

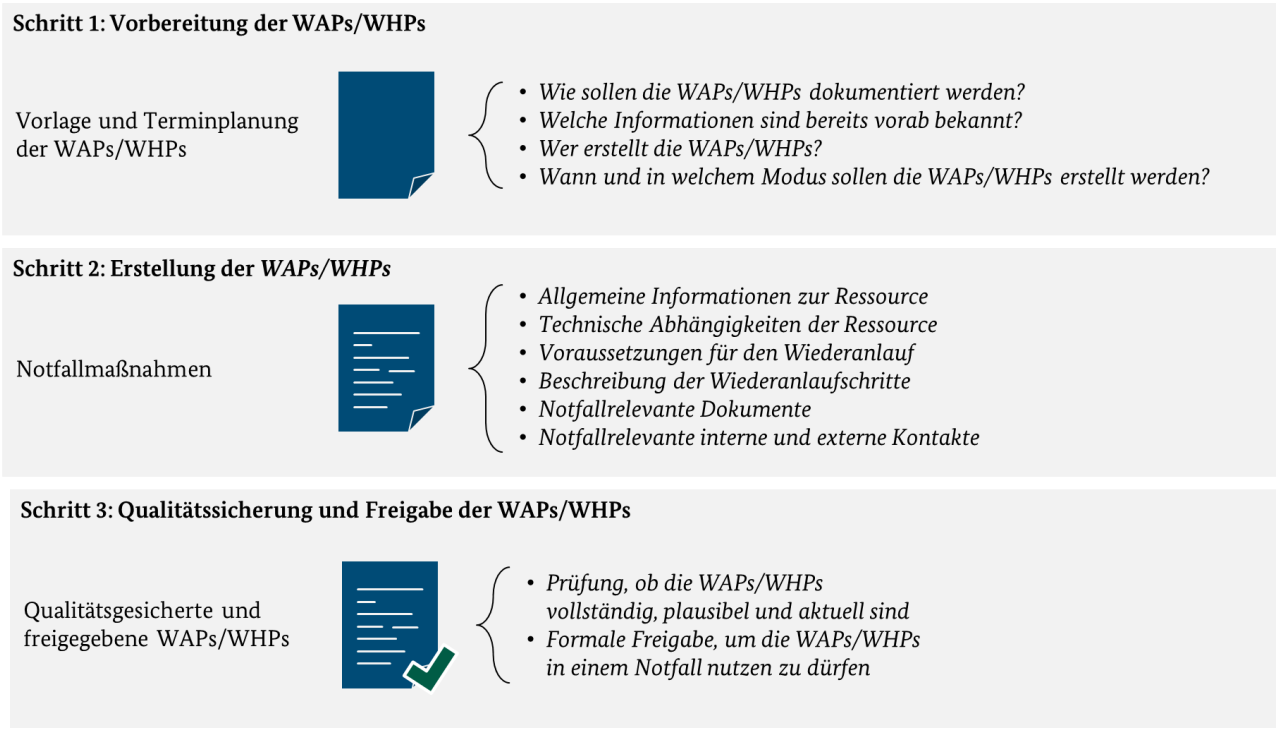

Abbildung 62: BCM-Prozessschritte zur Wiederanlauf- und Wiederherstellungsplanung

6.10.1 Vorbereitung der WAP/WHP

Die Vorbereitungsphase ist von großer Bedeutung, um die WAP/WHP effektiv und effizient erstellen zu können. Es ist empfehlenswert, dass die Vorbereitung durch den BCMB erfolgt. Er kann vorbereitende Tätigkeiten ganz oder teilweise an weitere Rollen wie etwa die Ressourcenzuständigen im BCM delegieren (siehe Kapitel 3.2.2 Definition der BCM-Aufbauorganisation). Die Aufgaben in der Vorbereitung der WAP/WHP werden in den nachfolgenden Unterkapiteln näher erläutert. Die Kapitel folgen einer logischen Reihenfolge, jedoch können sich verschiedene darin beschriebene Aufgaben in der Praxis zeitlich überlagern.

6.10.1.1 Organisatorische Aufteilung

Der BCMB muss festlegen, wie die WAP/WHP im Hinblick auf die zugrundeliegende Struktur der Ressourcen aufgeteilt werden sollen. Es gibt viele Möglichkeiten, wie WAP/WHP organisatorisch aufgeteilt werden könnten. So könnte ein Plan je einzelner Ressource erstellt werden oder umfangreichere Ressourcencluster umfassen. Entscheidend für eine schnelle Notfallreaktion ist jedoch, dass

- die zuständigen Stellen die jeweils für ihren Bereich relevanten Informationen erhalten,
- die Verfügbarkeit der Pläne gewährleistet ist sowie
- die Übergabepunkte zwischen den Plänen klar geregelt sind.

Hierbei hat es sich in der Praxis bewährt, einen Plan je Ressource zu erstellen, die von einer zuständigen Stelle bearbeitet wird. Dieses Vorgehen bietet folgende Vorteile:

- Die zuständigen Ansprechpartner, die den Plan erstellen und aktualisieren, können eindeutig einer abgegrenzten Ressource zugeordnet werden.
- Die Pläne spiegeln die vertraute Umgebung bzw. die eigenen Zuständigkeitsbereiche des Normalbetriebs wider und lassen sich so leichter voneinander abgrenzen.

Hinweis:

Ob die Pläne sinnvoll aufgeteilt und voneinander abgegrenzt wurden, kann mitunter erst im Rahmen der Planerstellung fundiert bewertet werden. Die Aufteilung der Pläne sollte daher im Rahmen der Erstellung mit den entsprechenden Ansprechpartnern diskutiert und gegebenenfalls angepasst, in mehrere Pläne aufgeteilt oder in verschiedene Pläne zusammengefasst werden.

6.10.1.2 Erstellung einer WAP-/WHP-Dokumentenvorlage

Um den Wiederanlauf bzw. die Wiederherstellung im Notfall zu erleichtern, sollte der BCMB sicherstellen, dass die WAPs/WHPs einheitlich aufgebaut und nachvollziehbar dokumentiert sind. Hierzu sollte eine WAP- und WHP-Dokumentenvorlage erstellt werden. Die nachfolgenden Aspekte müssen darin berücksichtigt werden:

Der **Zweck des WAP/WHP** beschreibt, was durch den WAP/WHP erreicht werden soll und was explizit nicht durch den WAP forciert wird. Die Beschreibung der Zielstellung stellt sicher, dass der WAP/WHP nur zu seinem gedachten Zweck eingesetzt wird und nicht etwa im Rahmen des Tagesbetriebs (siehe auch Aktivierungsprozess) zweckentfremdet oder mit anderen Themen vermischt wird.

Der **Aktivierungsprozess** des WAP/WHP muss dokumentiert werden. Dieser beschreibt, wie der WAP/WHP offiziell aktiviert wird. Die Definition eines eindeutigen Aktivierungsprozesses ist notwendig, da die Maßnahmen des WAP/WHP häufig nicht ohne Weiteres rückgängig gemacht werden können und ein frühzeitiges Auslösen des WAP/WHP verhindert werden soll.

Innerhalb des WAP/WHP werden alle zum Wiederanlauf **relevanten Dokumente** sowie ihre jeweiligen Ablageorte notiert. Mögliche Dokumente sind etwa Betriebshandbücher oder Handlungsanweisungen. Für den Fall eines Notfalls kann durch die Verweise schnell auf die relevante Information in den jeweiligen Dokumenten zugegriffen werden. Voraussetzung ist, dass die für die Notfallbewältigung benötigten Dokumente schnell zu erfassen sind und konkrete Notfallmaßnahmen leicht daraus abgeleitet werden können. Auch für referenzierte Dokumente muss sichergestellt werden, dass diese im Notfall verfügbar sind.

Die **betrachteten Ressourcen** definieren, auf welche Ressourcen sich der WAP/WHP bezieht.

Die **Voraussetzungen zum Wiederanlauf/Wiederherstellung der Ressource** regeln die organisatorischen sowie technischen Bedingungen, um die beschriebenen Notfallmaßnahmen initiieren zu können.

Die **Notfallmaßnahmen** stellen den Hauptteil des WAP/WHP dar und beschreiben konkreter die notwendigen Schritte um die spezifische Ressource wiederanlaufen bzw. wiederherstellen zu können.

Hinweis:

Damit der Aufwand für die Autoren möglichst geringgehalten wird, können die Pläne bereits im Vorfeld mit allgemeinen Informationen versehen werden. Dazu zählen insbesondere eine kurze Beschreibung der für die Ressource relevanten BIA-Informationen (z. B. RTO, Notbetriebsniveau) sowie möglicherweise benötigte Dokumente auf die in der Wiederanlauf- und Wiederherstellungsplanung referenziert wird.

6.10.1.3 Organisatorische Planung

Für die Erstellung der WAP/WHP wird ein hoher Grad an technischem Detailwissen benötigt. Daraus ergibt sich die Notwendigkeit, dass das Dokument idealerweise durch die gleichen Mitarbeiter erstellt werden sollte, die im Rahmen eines Notfalls auch die beschriebenen Maßnahmen durchführen.

Abhängig von dem notwendigen Fachwissen kann es erforderlich sein, weitere Experten unterstützend hinzuziehen. Dies ist dann erforderlich, wenn für den Wiederanlauf oder die Wiederherstellung der Ressource weitere (Infrastruktur-)Ressourcen bzw. Komponenten benötigt werden, die nicht in den Zuständigkeitsbereich des Ressourcenzuständigen fallen oder durch dessen Fachwissen abgedeckt sind.

Ferner sollte gewährleistet werden, dass die verschiedenen WAP/WHP einheitlich strukturiert sind, damit sich im Notfall auch andere Mitarbeiter, mit gleichem Fachwissen, schnell zurechtfinden und die Maßnahmen durchführen können, auch in der Stresssituation eines Notfalls. Dies kann beispielsweise durch zentrale Leitfragen oder Checklisten geschehen, die innerhalb einer geeigneten Dokumenten-Vorlage hinterlegt werden. Alternativ kann der Erstellungsprozess auch im Rahmen eines Workshops durch einen BCM-Experten und den Ressourcen-Experten gemeinsam erarbeitet werden.

Darüber hinaus ist es empfehlenswert, dass bereits an anderer Stelle dokumentierte Inhalte wie in Betriebsdokumentationen nicht wiederholt, sondern stattdessen referenziert werden. Dies setzt eine Kenntnis dieser Dokumentationen voraus. Auch für referenzierte Dokumente sollte sichergestellt werden, dass diese im Notfall verfügbar und zugänglich und entsprechend des Schutzbedarfs abgelegt sind (siehe Kapitel 6.2 *Dokumentation im Standard-BCMS*).

6.10.2 Erstellung der WAP/WHP

Innerhalb der Wiederanlauf- und Wiederherstellungsplanung müssen alle erforderlichen Rollen und Rolleninhaber, ihre jeweiligen Vertreter sowie benötigte Dienstleister, benannt werden. Dieser Personenkreis kann auch in der Alarmierung und Eskalation berücksichtigt werden (z. B. als definiertes Notfallteam).

Damit die jeweiligen Rolleninhaber in einem Notfall ohne Verzögerung kontaktiert werden können, sollten deren Kontaktdaten, unter Berücksichtigung der Vertraulichkeit der Informationen, hinterlegt und aktuell gehalten werden. Neben den unbedingt notwendigen Mitarbeitern sollten zudem zusätzliche oder alternative Wissensträger identifiziert und ebenfalls aufgeführt werden (Stellvertreterregelung). Folgende Aspekte sollten in einem WAP/WHP möglichst detailliert und konkret beschrieben sein:

- Voraussetzungen zum Wiederanlauf/Wiederherstellung der Ressource
- Ablauf und konkrete Tätigkeiten zum Wiederanlauf/zur Wiederherstellung der Ressource
- Funktionstest, ob der Wiederanlauf erfolgreich war und Übergabe in den Notbetrieb

Der Detailgrad der beschriebenen Maßnahmen sollte dabei so gewählt sein, dass eine fachkundige dritte Person in der Lage wäre, den Wiederanlauf bzw. die Wiederherstellung anhand des WAP/WHP umzusetzen. Um die erforderlichen Notfallmaßnahmen zu ermitteln können die Leitfragen aus Kapitel 6.9.2.2 *Entwicklung von Notfallmaßnahmen* als Grundlage verwendet werden.

Synergiepotenzial:

Nicht in jedem Fall müssen die Maßnahmen zum Wiederanlauf und zur Wiederherstellung in einem WAP/WHP beschrieben sein. Häufig sind solche Angaben bereits in vorhandenen Dokumentationen zu finden, z. B.

IT-Betriebskonzepte (IT-Recovery, Datenwiederherstellung, Failover-Konzept),

eine Pandemieplanung (Maßnahmen zum Umgang mit massivem Personalausfall) sowie

abgestimmte Notfallkonzepte für Dienstleistungen bzw. Exit-Strategien.

In diesem Fall können die vorhandenen Dokumente weiter genutzt werden, sofern diese im Notfallhandbuch referenziert und im Notfall verfügbar sind. Es sollte dabei sichergestellt werden, dass alle nachfolgend beschriebenen Anforderungen an WAP/WHP auch in den bestehenden Dokumenten erfüllt werden.

Voraussetzungen zum Wiederanlauf bzw. Wiederherstellung der Ressource

Bevor der Wiederanlauf einer Ressource initiiert werden kann, müssen die notwendigen Voraussetzungen und (technischen) Abhängigkeiten von anderen Ressourcen erfüllt sein. Damit diese nicht erst während eines Notfalls identifiziert und geprüft werden müssen, müssen die Abhängigkeiten bereits dokumentiert werden, wenn die Pläne erstellt werden. Es werden zwei Gruppen von Voraussetzungen unterschieden:

- Unter **organisatorische Voraussetzungen** fallen die zum Wiederanlauf oder der Wiederherstellung benötigten Befugnisse und das benötigte Wissen verschiedener institutionsinterner oder externer Rollen.
- Unter **technische Voraussetzungen** fallen alle Abhängigkeiten von anderen Ressourcen sowie eventuelle zeitliche Reihenfolgen, in denen voneinander abhängige Ressourcen in einem Notbetrieb anlaufen müssen.

Ablauf und konkrete Tätigkeiten zum Wiederanlauf bzw. Wiederherstellung

Die für den Wiederanlauf der Ressource durchzuführenden Schritte sollten in Form von Handlungsanweisungen beschrieben werden. Es ist empfehlenswert, die Schritte mit Abhängigkeiten untereinander sowie parallel ausführbare Schritte zu kennzeichnen, z. B. anhand nummerierter Einträge innerhalb einer Checkliste. Die Beschreibung sollte eindeutig und nur so ausführlich wie unbedingt notwendig gestaltet sein. Auch Screenshots können da eingesetzt werden, wo sie einen Mehrwert bieten.

Pro Schritt sollte dokumentiert werden, welche Rolle diesen Schritt durchführt und wie lange es in der Regel dauert, bis dieser abgeschlossen ist. Falls es Abhängigkeiten zu einer anderen Maßnahme oder zu einem anderen Dokument gibt, sollten diese Informationen ebenfalls aufgeführt bzw. referenziert werden.

Alle für den Wiederanlauf bzw. Wiederherstellung benötigten Ressourcen, Dokumentationen und Abläufe sollten in den Plänen aufgeführt werden.

Spezifisch für den Wiederanlauf sollten die aus dem Notbetrieb der Ressource resultierenden Einschränkungen dokumentiert werden. Dies kann etwa eine eingeschränkte Kapazität der Ressource oder ein reduzierter Funktionsumfang bedeuten.

Spezifisch für die Wiederherstellung sollten die erforderlichen Maßnahmen zur Rückführung der Ressource in den Normalbetrieb beschrieben werden. Dies gilt insbesondere, wenn auf Grund des Notbetriebs abweichende Verfahren eingesetzt wurden und ein „Schwenk“ auf eine wiederhergestellte Ressource sichergestellt werden muss.

Erstellung der übergeordneten Wiederanlaufplanung

Über die Abhängigkeiten und Reihenfolgen der WAP/WHP kann sichergestellt werden, dass die jeweiligen Voraussetzungen für den Wiederanlauf jeder Ressource erfüllt sind. Anhand dessen sollten die Abhängigkeiten der verschiedenen WAP/WHP in einer übergeordneten Wiederanlauf- bzw. Wiederherstellungsplanung dokumentiert werden, z. B. innerhalb des Notfallhandbuchs. An dieser Stelle findet zudem die Priorisierung der durchzuführenden Maßnahmen für den Wiederanlauf statt. Diese richtet sich üblicherweise an der logischen Abhängigkeit von Ressourcen aus. Bei entsprechender Komplexität sollten mehrere Ebenen der übergeordneten Wiederanlaufplanung entwickelt werden.

Abbildung 63 gibt hierzu ein schematisches Beispiel anhand einer IT-Wiederanlaufplanung für den IT-Service E-Mail wieder, der seinerseits auf Services oder Infrastrukturkomponenten zurückgreift. Der Wiederanlauf einer Ebene ist jeweils erst dann möglich, wenn alle beschriebenen Komponenten der darunterliegenden Ebene zur Verfügung stehen. Aus Gründen der Vereinfachung wird auf Abhängigkeiten zwischen Komponenten innerhalb einer Ebene verzichtet.

Beispiel:

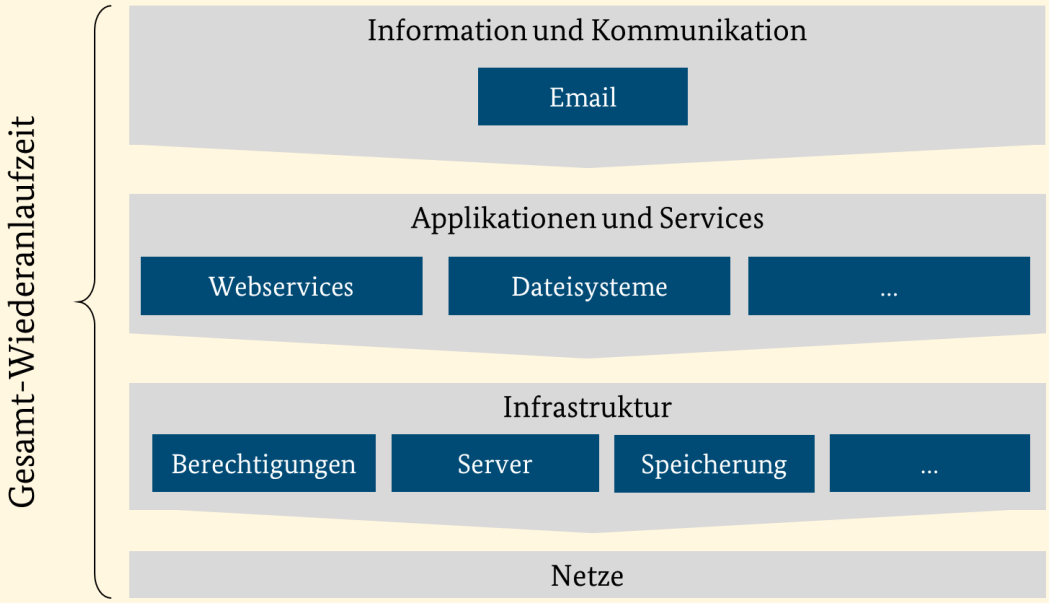

Abbildung 63: Beispiel einer übergeordneten IT-Wiederanlaufplanung

Die übergeordnete Wiederanlaufplanung muss sicherstellen, dass die Gesamt-RTA für eine zeitkritische Ressource auch unter Berücksichtigung der abhängigen Ressourcen die RTO nicht übersteigt.

6.10.3 Qualitätssicherung und Freigabe

Um sicherzustellen, dass alle Vorgaben zur Wiederanlaufplanung eingehalten wurden, sollten die erstellten WAPs/WHPs formal qualitätsgesichert werden. Dabei sollten die folgenden Aspekte berücksichtigt werden:

- **Vollständigkeit:** Bilden die Inhalte der erstellten WAP/WHP alle vorgegebenen Punkte ab? Wurden alle relevanten Inhalte der BIA innerhalb der WAP/WHP erfasst. Wurden Maßnahmen über alle Phasen beschrieben? Unvollständige WAP/WHP können dazu führen, dass diese im Notfall nicht oder nur begrenzt einsetzbar sind.
- **Plausibilität:** Sind die beschriebenen Maßnahmen widerspruchsfrei und die getroffenen Annahmen für die Institution realistisch?
- **Aktualität:** Sind die referenzierten Dokumente in der jeweils aktuellen Version hinterlegt? Wurden die relevanten Ansprechpartner auf Basis einer aktuellen Kontaktliste dokumentiert? WAP/WHP

Hinweis:

Die Qualitätssicherung dient zu diesem Zeitpunkt lediglich dazu, sicherzustellen, dass die Vorgaben eingehalten wurden. Ob die in den WAPs beschriebenen Notfallmaßnahmen angemessen, vollständig und wirksam sind, kann erst anhand von Übungen und Tests ermittelt werden (siehe Kapitel 6.11 *Üben und Testen*).

Nachdem die WAPs/WHPs qualitätsgesichert wurden, müssen diese offiziell freigegeben werden. Dies kann beispielsweise durch die Leitungen für die Ressourcen zuständigen Organisationseinheiten erfolgen. Dieser Schritt signalisiert, dass die Maßnahmen und Verfahren bestätigt wurden und der Plan offiziell in einem Notfall verwendet werden kann.

Nachdem die WAP/WHP erstellt, qualitätsgesichert und freigegeben sind, ist wesentlich transparenter, in welchem Maße die BC-Strategien und -Lösungen anwendbar sind und welcher tatsächliche Ressourcenbedarf für die Notfallmaßnahmen erforderlich ist. Es ist daher empfehlenswert, dass der BCMB die aktualisierten Informationen der Institutionsleitung mitteilt. Hierdurch kann der Institutionsleitung ein realistischeres Bild über die Risikosituation vermittelt werden, als es zu einem früheren Zeitpunkt möglich war. Können die identifizierten Probleme mit einfachen Mitteln gelöst werden, sollten diese im Maßnahmenplan aufgenommen und zeitnah verfolgt werden.

6.11 Üben und Testen

Wenn die BAO aufgebaut und befähigt wurde und die zeitkritischen Geschäftsprozesse angemessen abgesichert wurden ist die Institution theoretisch für den Notfall gut gerüstet. Um jedoch sicher zu sein, dass dies auch tatsächlich der Fall ist, müssen die umgesetzten Maßnahmen, die organisatorischen Strukturen und die erstellten Pläne kontinuierlich überprüft werden. Die Bewältigung von Notfällen erfordert von den Beteiligten Höchstleistungen sowie eine schnelle und angemessene Reaktion, um Schäden so weit wie möglich abzuwenden. Unvollständige oder nicht funktionierende Pläne können verheerende Folgen haben und wertvolle Zeit kosten. Regelmäßige Übungen und Tests helfen, Verbesserungsbedarfe im BCM zu identifizieren und die Reaktionsfähigkeit zu erhöhen. Durch ein abgestimmtes Programm von Übungen und Tests sollte erreicht werden, dass

- alle für die Notfallbewältigung relevanten Informationen aktuell, plausibel und vollständig sind (insbesondere Notfallhandbuch, Geschäftsfortführungspläne, Kontaktlisten zur Alarmierung),
- die für die Notfallbewältigung benötigten Räumlichkeiten, die IT und alle weiteren Ressourcen einsatzbereit sind,
- die Abläufe im Notfall wie geplant funktionieren und sowohl angemessen als auch effizient sind sowie
- die Mitarbeiter auf den Notfall vorbereitet sind, eigene Erfahrungen sammeln können und dadurch in die Lage versetzt werden, im Notfall überlegt zu handeln.

Hinweis:

Eine scharfe Trennung der Begriffe Übung und Test ist nicht immer möglich und sinnvoll. Im internationalen Standard ISO 22398 ist der Begriff Test definiert als eine besondere Art von Übung, bei der ein objektiv gemessenes „Pass or Fail"-Ergebnis (Bestehen oder Nichtbestehen) erwartet und entsprechend als Ziel definiert wird. Bei Übungen sind die Ziele generischer formuliert und dienen üblicherweise dazu, praktische Erfahrungen im Umgang mit den Notfallplänen und Notfallmaßnahmen zu sammeln sowie Korrektur- und Verbesserungsmaßnahmen zu identifizieren. Der BSI-Standard 200-4 folgt der Begriffsdefinition aus den ISO-Standards der 22300-Reihe. Der Begriff Übung wird als Oberbegriff verwendet. Tests stellen eine spezielle Form von Übungen dar. Aus Gründen der besseren Lesbarkeit wird nachfolgend primär von Übungen gesprochen, was Tests einschließt.

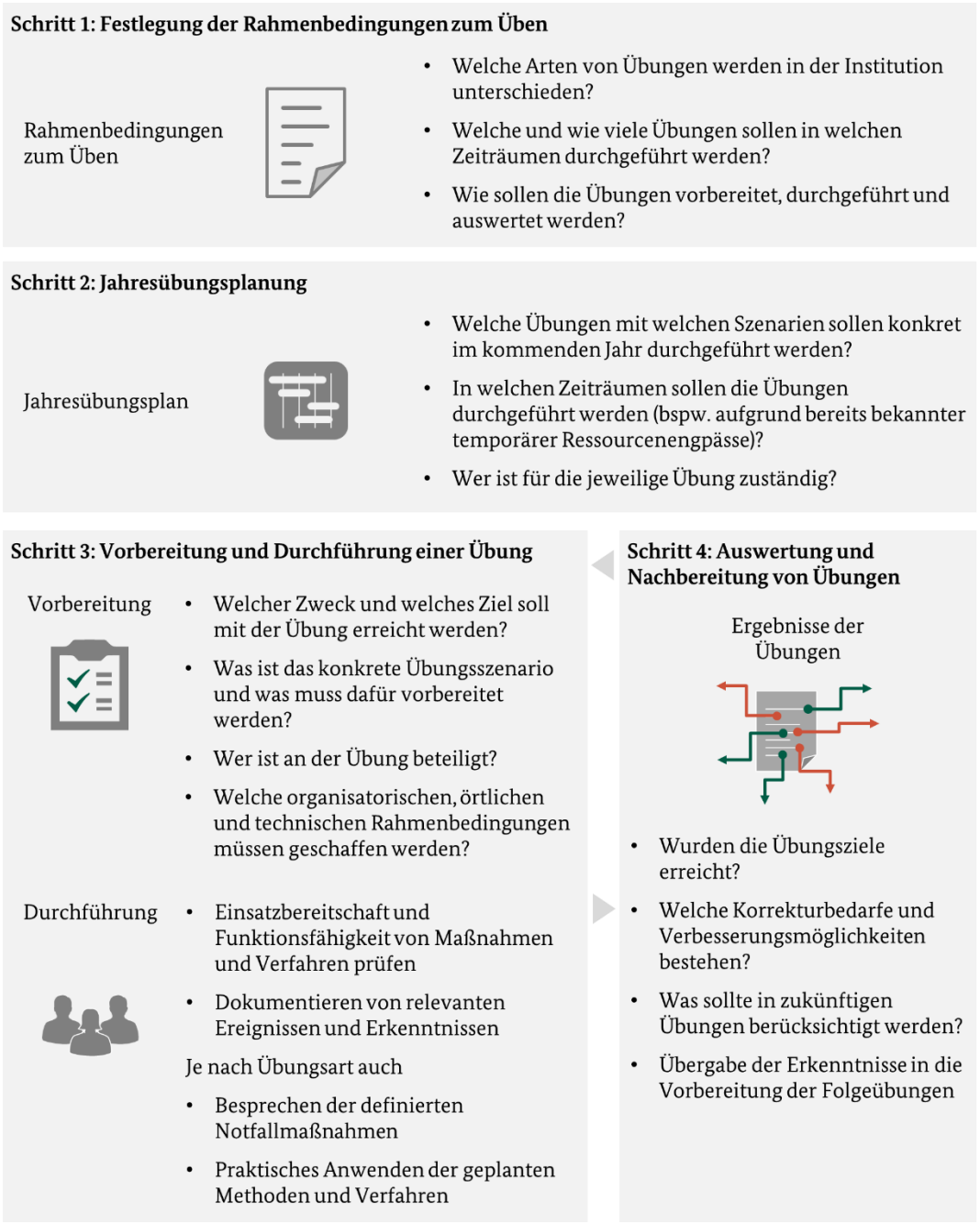

Abbildung 64: BCM-Prozessschritte zum Üben und Testen

Synergiepotenzial:

Wenn in anderen Themenfeldern wie dem ITSCM bereits Übungen durchgeführt werden und eigenständige Übungsarten definiert sind, sollte dies bei der Jahresübungsplanung und den Rahmenbedingungen berücksichtigt werden. Es wird empfohlen, die Begriffe zwischen dem BCM, Krisenmanagement, ITSCM sowie weiteren Übungen durchführenden Stellen, einheitlich zu definieren oder namentlich klar voneinander abzugrenzen.

6.11.1 Festlegung der Rahmenbedingungen zum Üben

Für alle Übungen des BCM sollte sichergestellt werden, dass sie geplant und vorbereitet ablaufen. Um dies zu erreichen und um störende Auswirkungen auf den Geschäftsbetrieb so gering wie möglich zu halten, muss der BCMB die Rahmenbedingungen zum systematischen Üben festlegen. Diese bilden die Grundlage für die Jahresübungsplanung und die Schritte zur Vorbereitung, Durchführung und Nachbereitung der einzelnen

Übungen. Um die Rahmenbedingungen zum Üben festzulegen, sollten die folgenden Fragen beantwortet und dokumentiert werden (z. B. in einem Übungshandbuch oder anderweitigen Anweisung):

- Welche Arten von Übungen werden in der Institution unterschieden?
- Wie sind diese Übungen definiert?
- Welche übergreifenden Übungsziele sollen mit welchen Übungsarten erreicht werden?
- Welche Aufwände sind mit den einzelnen Übungsarten verbunden (Schätzung)?
- Wie viele Übungen sollten in welchen Zeiträumen durchgeführt werden?
- Welche Zielgruppe/n soll/en mit welcher Übungsart adressiert werden? An wie vielen Übungen sollen Mitglieder jeder Zielgruppe im Jahr/in einem mehrjährigen Zeitraum mindestens und maximal teilnehmen?
- Welche Ausfallszenarien sollten wie oft geübt werden?
- Welche Anforderungen an die Realitätsnähe und Komplexität müssen die Übungen erfüllen?
- Wie erfolgt die Risikoeinschätzung, falls Übungen sich auf den Geschäftsbetrieb auswirken?
- Wie sollen die Übungen, abhängig von der Übungsart, vorbereitet, durchgeführt und auswertet werden? Wie sollen diese Schritte jeweils dokumentiert werden?
- Welche Rollen werden bei der Planung und Durchführung von Übungen unterschieden? Welche Aufgaben, Rechte und Zuständigkeiten haben diese?

Da Übungen mit Aufwand und Kosten verbunden sind, sollte der BCMB die festgelegten und dokumentierten Rahmenbedingungen mit der Institutionsleitung abstimmen und durch diese freigeben lassen.

Im Folgenden werden die wichtigsten Rahmenbedingungen zum Üben anhand von Beispielen näher erläutert. Wie die Dokumentation dieser Rahmenbedingungen im Detail gestaltet wird, muss jede Institution für sich entscheiden, abhängig von ihren individuellen Rahmenbedingungen und ihrer BCMS-Reife. Die folgenden Abschnitte geben Hilfestellungen dazu.

Übungsarten

In unterschiedlichen Standards und Publikationen zu den Themen BCM und Krisenmanagement werden verschiedene Übungsarten mit jeweils individuellen Definitionen beschrieben. Dieser Standard verwendet die in Tabelle 62 aufgeführten Übungsarten. Alle hier genannten Übungsarten müssen in der Institution berücksichtigt, dokumentiert und regelmäßig durchgeführt werden. Die Bezeichnungen und Definitionen der jeweiligen Übungsarten können institutionsspezifisch angepasst werden, sofern sichergestellt wird, dass der jeweilige Inhalt der Übungsart berücksichtigt wird.

Übungsart	Inhalt und Ziel	Beispiele
Planbesprechung („Schreibtischtest“)	Moderierte Besprechung eines Notfallplans. Ziel: Planinhalte hinsichtlich ihrer realistischen Anwendbarkeit prüfen. In der Regel wird dazu fachlich überprüft, ob die Pläne plausibel, vollständig korrekt und aktuell sind. Darüber hinaus kann geprüft werden, ob die untersuchten Pläne untereinander widerspruchsfrei sind.	Ein BCM-relevantes Dokument mit darin vorgesehenen Rolleninhabern durchsprechen, ohne dass Handlungsschritte real ausgeführt werden (GFP, Alarmierungsplan, RZ-Umschaltung, Vertragsklauseln in SLA etc.).

Übungsart	Inhalt und Ziel	Beispiele
Stabsübung	Praktisches Üben der Stabsarbeit, um ein vorgegebenes Notfallszenario zu bewältigen. Ziel: die Zusammenarbeit der Mitglieder des Stabs und die Grundelemente der Stabsarbeit üben, z. B. Führungszyklus, Lagebesprechungen, Protokollierung, Visualisierung etc. Wenn für das Szenario bestimmte stabsnahe Unterstützungsrollen benötigt werden, sind diese Teil der Stabsübung.	Stab aktivieren und im Stabsraum zusammenkommen. Anschließend die simulierte Bewältigung eines realitätsnahen Notfallszenarios durch den Stab durchführen.
Stabsrahmenübung	Erweiterte Form der Stabsübung, bei der weitere Stellen der Institution eingebunden werden. Ziel: Üben der übergreifenden Kommunikation und Zusammenarbeit zwischen dem Stab und ausgewählten Stellen der Notfallbewältigung Neben dem Stab und seinen Unterstützungsrollen sind auch operative Teams an der Übung beteiligt, wie etwa das Kommunikationsteam oder Organisationseinheiten mit zeitkritischen Geschäftsprozessen.	Notfallstab aktivieren und im Stabsraum zusammenkommen, um anschließend die simulierte Bewältigung des Notfallszenarios „Ausfall Gebäude“ durch den Stab durchzuführen. Zeitgleich simulieren ausgewählte Organisationseinheiten mit zeitkritischen Prozessen das Verlagern zum und Arbeiten am Ausweichstandort anhand ihrer Notfallpläne und kommunizieren mit dem Stab.
Alarmierungsübung	Aktivieren und Durchlaufen der Alarmierungskette Ziel: Technische Kommunikationsmittel, organisatorische Abläufe sowie vorhandene Dokumentationen zur Alarmierung und Eskalation prüfen.	Alarmierungskette durch einen Anruf bei der zuständigen Meldestelle auslösen und systematisch die Erreichbarkeits- und Rückrufquote innerhalb eines Zeitfensters nachverfolgen.

Übungsart	Inhalt und Ziel	Beispiele
Funktionstest	Reale Ausführung eines Notfallplans Ziel: Einsatzbereitschaft und Funktionsfähigkeit von einzelnen oder mehreren baulichen, technischen oder organisatorischen Maßnahmen bzw. Ressourcen prüfen, die für die Notfallbewältigung benötigt werden.	Test eines Notfallarbeitsplatzes durch einen Mitarbeiter; Test eines IT-Administrations-Arbeitsplatzes (Berechtigungen im Notfall etc.); Umschalttest zwischen redundant ausgelegten Systemen; Wiederanlauftest von Systemen oder Komponenten; Restorationstest von Datenbank-Servern inklusive Datenbanken; Lesbarkeitstest von Backups; Notfallausrüstung im Stabsraum überprüfen, ob diese vorhanden und einsatzbereit ist

Tabelle 62: Übungsarten gemäß BSI-Standard 200-4

Es ist zudem empfehlenswert, auch die wesentlichen Merkmale der einzelnen Übungsarten zu benennen, z. B. Zielgruppe (=Übende), Voraussetzungen und Zuständigkeiten. In Tabelle 63 wird ein Beispiel hierfür dargestellt:

Beispiel:

Übungsart	Übungsziel	Übende	Voraussetzung	Zuständig für Vorbereitung
Planbesprechung	…	Rollen im Notfallplan	Plan liegt vor	Dokumenteneigentümer
Funktionstest	…	Notfallteam	Planbesprechung wurde durchgeführt	Ressourcenzuständiger
Stabsübung	…	Stabsmitglieder	Geschäftsordnung des Stabs liegt vor	BCMB
…	…	…		…

Tabelle 63: Übungsarten und wesentliche Merkmale

Synergiepotenzial:

Übungsarten, die in anderen Themenfeldern wie z. B. dem Krisenmanagement, ITSCM oder dem Gebäudemanagement bereits definiert sind, sollten bei den Rahmenbedingungen berücksichtigt werden, damit ein konsistentes Gesamtbild entsteht. Vorhandene Bezeichnungen von Übungsarten sowie ihre jeweiligen Ziele und Inhalte können so weitergenutzt oder auf die o. a. Übungsarten abgestimmt werden.

Vorgaben zu Ausfallszenarien

Grundsätzlich wird empfohlen, dass über einen Mehrjahreszeitraum alle für die Institution relevanten Ausfallszenarien berücksichtigt werden. Geeignete Szenarien sind Ausfälle bestimmter Ressourcenkategorien oder die Bewältigung eines Cyberangriffs, z. B. mit Datenverlust oder -manipulation. Hierzu sollte festgelegt werden, welche Ausfallszenarien in welchem Zeitraum anhand von Übungen berücksichtigt werden sollen.

Es wird dabei zwischen Ursachen- und Wirkungsszenarien unterschieden:

- Ein **Wirkungsszenario** geht von definierten Ausfällen bzw. Beeinträchtigungen aus (z. B. Ausfall eines Rechenzentrums), ohne die Ursachen zu berücksichtigen.
- Ein **Ursachenszenario** beinhaltet zusätzlich die zugrundeliegenden Ursachen (Stromausfall, Viren-Befall, Hacker-Einbruch etc.).

Wirkungsszenarien werden verwendet, wenn ursachenunabhängige Reaktionsprozesse im Fokus stehen oder interne und externe Abhängigkeiten ermittelt werden sollen. Dies wird auf die meisten Stabsübungen zutreffen.

Ursachenszenarien dagegen bieten sich an, wenn Ursachenerforschung, Problembehebungsvorgänge oder ursachenabhängige Schadensbegrenzungsprozesse geübt werden sollen. Je nach Übungsziel muss der Übungsautor entscheiden, welche der beiden Szenarioarten besser geeignet ist.

Hinweis

Die Bewältigung eines Cyberangriffs hat inhaltlich große Überschneidungen mit dem Szenario IT-Ausfall, da teilweise die gleichen Notfallmaßnahmen eingeleitet werden. Jedoch gibt es immer dann Besonderheiten zu beachten, wenn ein Teil der Notfallmaßnahmen aufgrund des Cyberangriffs nicht wie vorgesehen funktionieren, z. B. weil die Datenbestände und die Datensicherungen der letzten 4 Wochen kompromittiert wurden (siehe Hilfsmittel *Weiterführende Aspekte zur Bewältigung*). Beim Szenario Cyberangriff steht daher eher die Zusammenarbeit der einzelnen Themengebiete, wie z. B. Informationssicherheit, ITSCM und (IT-)Krisenmanagement im Vordergrund. Hierfür bieten sich Übungsarten wie eine Planbesprechung, Stabsübung oder Stabsrahmenübung an.

Vorgaben zur Dokumentation

Der BCMB sollte anhand von Mindestanforderungen sowie über entsprechende Vorlagen bzw. Hilfsmittel sicherstellen, dass die Dokumentation der Übungen innerhalb einer Übungsart möglichst einheitlich erfolgt und möglichst zielführend ausgerichtet ist. Die Vorlagen bzw. Hilfsmittel sollten sich an der Übungsart orientieren. Je einfacher eine Übungsart ist, desto einfacher kann die Dokumentation ausgestaltet sein.

Die folgende Abbildung zeigt ein Beispiel für die Dokumentation bei Übungen:

Beispiel:

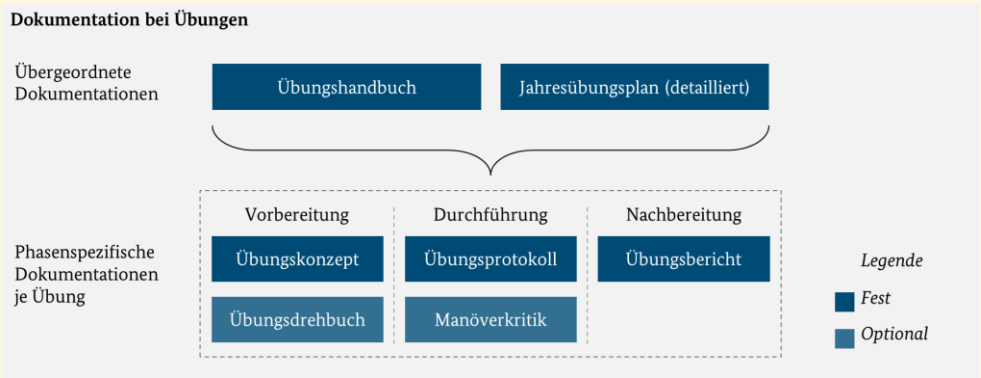

Abbildung 65: Beispiele einer Dokumentation bei Übungen

Die Dokumentation der Rahmenbedingungen (Übungshandbuch) sowie die Jahresübungsplanung sollten übergreifend durch den BCMB erstellt werden, da diese Dokumente den notwendigen Rahmen für alle Übungen bilden.

Für jede Übung muss in der Vorbereitungsphase ein **Übungskonzept** erstellt werden, welches die Rahmendaten aus der Jahresübungsplanung präzisiert und weiter detailliert. Hier sollte auch die weitere Dokumentation festgelegt werden. Für bestimmte, umfangreichere Übungsarten ist es empfehlenswert, zusätzliche Dokumente in der Vorbereitungsphase zu erstellen. Für ausgewählte Übungsarten bestehen darüber hinaus weitere Dokumentationsanforderungen, wie **Übungsdrehbücher** bei Stabs- und Stabsrahmenübungen.

Die Durchführung einzelner Übungen muss anhand von **Übungsprotokollen** dokumentiert werden. Bei komplexeren Übungen mit einer umfangreicheren Zielgruppe wie Stabsübungen ist es darüber hinaus empfehlenswert, direkt im Anschluss der Durchführung eine sogenannte **Manöverkritik** durchzuführen. In dieser werden die unmittelbaren Eindrücke der Teilnehmer dokumentiert.

Für jede Übung muss ein **Übungsbericht** angefertigt werden, der die wesentlichen Ergebnisse der Übung, wie Zielerreichungsgrad, Änderungsbedarfe und Verbesserungspotentiale zusammenfasst.

Die vorgestellten phasenspezifischen Dokumente können auch in einem einzigen Dokument je Übung gesammelt werden. Welche Informationen in diesen Dokumenten erfasst werden sollten, wird in den nachfolgenden Kapiteln je Übungsart individuell beschrieben.

Rollen bei Übungen

Neben dem BCMB, der die übergreifenden Aufgaben im Üben wahrnimmt, gibt es weitere Rollen zu berücksichtigen, die je nach Übungsart obligatorisch oder optional sind. Dies wird in den Unterkapiteln zu den einzelnen Übungsarten in Kapitel 6.11.3 *Vorbereitung und Durchführung einer Übung* erläutert.

Sofern erforderlich oder sinnvoll können Personen auch mehrere Rollen einnehmen. So wäre es etwa möglich, dass der Übungsleiter auch die Tätigkeiten des Übungsautors übernimmt oder ein Übender gleichzeitig die Rolle des Übungs-Protokollanten übernimmt. Das folgende Beispiel zeigt typische Rollen und deren Aufgaben bei Übungen.

Beispiel:

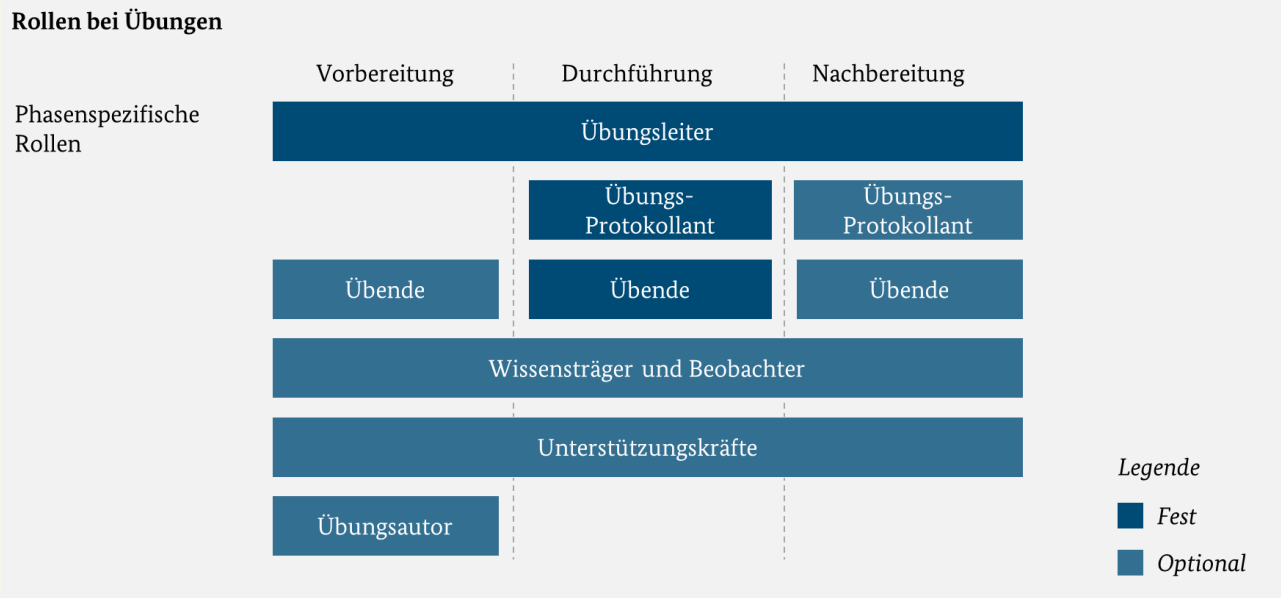

Abbildung 66: Beispiele verschiedener Rollen bei Übungen

Rolle	Typische Aufgaben
Übungsleitung	**Vorbereitung:** • Mit dem Übungsautor zusammenarbeiten • Übungskonzept freigeben **Durchführung:** • Übung insgesamt steuern, von der Eröffnung und Einleitung bis zum offiziellen Ende • Situative Entscheidungen treffen, z. B. ob und wie von der ursprünglichen Planung abgewichen werden kann • Abbruchkriterien fortlaufend prüfen **Nachbereitung:** • Protokolle auswerten • Übungsbericht erstellen • Beobachtungen in die Auswertung einbringen
Übungsautor	**Vorbereitung:** • Übungskonzept erstellen inkl. Übungsziele, organisatorischer Ablauf, Zielgruppe(n), Vorbereitungsmaßnahmen, Abbruchkriterien etc. • Weitere Übungsdokumente und -materialien erstellen bzw. vorbereiten, wie z. B. das Übungsdrehbuch, die Szenario-Einlagen oder die Übungsumgebung (abhängig von Übungsart) • Übende auswählen • Unterstützungskräfte koordinieren
Übungsprotokollant	**Durchführung:** • Übungsablauf detailliert im Protokoll erfassen **Nachbereitung:** • Beobachtungen in die Auswertung einbringen
Übende	**Vorbereitung:** • Einlesen in zur Vorbereitung bereitgestellte oder als Übungsvoraussetzung genannte Materialien **Durchführung:** • Übende Personen reagieren entsprechend ihrer vorgesehenen Funktionen oder Rollen auf die Szenarien und Einlagen bzw. auf die Anforderungen gemäß dem geplanten Übungsverlauf **Nachbereitung:** • An Nachbesprechung oder Debriefing teilnehmen, Fragebogen beantworten, Rückmeldung zur Übung geben.

Rolle	Typische Aufgaben
Beobachter	**Vorbereitung:** • Sich vertraut machen mit der Übung gemäß Übungskonzept und weiterer Dokumente **Durchführung:** • Übung aus neutraler Sicht beobachten **Nachbereitung:** Beobachtungen in die Auswertung einbringen
Wissensträger	**In allen Phasen:** • Andere Übungsrollen fachlich beraten **Durchführung:** • Anfragen der Teilnehmer aus fachlicher Sicht beantworten
Unterstützungskräfte	**Vorbereitung:** • Übungsautor unterstützen, wie z. B. das Drehbuch erstellen oder logistische Aufgaben erledigen **Durchführung:** • Übungsleitung unterstützen, wie z. B. die Einlagen gemäß Drehbuch einspielen **Nachbereitung:** • Beobachtungen in die Auswertung einbringen

Tabelle 64: Aufgaben der Rollen bei Übungen

Hinweis:

In anderen Publikationen, z. B. im LÜKEX Glossar des BBK (siehe [BBK2]), werden bestimmte Rollen ebenfalls verwendet, aber abweichend definiert.

Übungsumfang

Das Üben ist mit zeitlichen, technischen und personellen Aufwänden verbunden. Jede Institution muss daher genau abwägen, welche Arten von Übungen für welchen Zweck und in welchem Umfang sinnvoll sind. Pro Übungsart sollte vorgegeben werden, wie häufig und mit welcher Detailtiefe die Übungen durchgeführt werden sollen. Dabei kann ein risikoorientierter Ansatz verfolgt werden, d. h. der Übungsumfang kann z. B. abhängig von den in der BIA ermittelten RTO differenziert festgelegt werden (siehe Tabelle 65).

Beispiel:

Übungsart	Geschätzter Übungsumfang	Häufigkeit	Detailtiefe
Planbesprechung	niedrig	• zeitnah nach Planerstellung, • zeitnah nach wesentlichen Änderungen, betroffene Kapitel	alle Kapitel (möglicherweise verteilt über mehrere Planbesprechungen)

Übungsart	Geschätzter Übungsumfang	Häufigkeit	Detailtiefe
Funktionstest	mittel-hoch	• mindestens jährlich für Prozesse und Ressourcen mit RTO < 24 h • mindestens alle 3 Jahre für Prozesse und Ressourcen mit RTO < 5 Tage	einzelne Komponente einzelne Ressource Ressourcen-übergreifend
Stabsübung	niedrig-mittel	• mindestens jährlich,	alle Stabsmitglieder (Kernteam) und stabsnahe Unterstützungsfunktionen sowie alle Stellvertreter

Tabelle 65: Beispiel für differenzierte Angaben zum Übungsumfang

6.11.2 Erstellung einer Jahresübungsplanung

Um sicherstellen zu können, dass die definierten Prozesse, Ressourcen, Verfahren und Abläufe der Notfallbewältigung über einen längeren Zeitraum vollständig geübt werden können, muss der BCMB eine Jahresübungsplanung erstellen. Die Jahresübungsplanung sollte einen Zeitraum von mindestens zwölf Monaten umfassen. Dabei sollten die folgenden Aspekte berücksichtigt werden:

- die Rahmenbedingungen (z. B. der Übungsarten und deren Umfang)
- die zeitlichen und personellen Ressourcen der beteiligten Rollen
- die vorherigen Jahresübungspläne
- die gewonnenen Erkenntnisse aus den letzten Jahren
- aktuelle Ergebnisse der anderen BCMS-Prozessschritte
- die Erwartungen von Interessengruppen gemäß 6.1.1 *Identifizierung von Anforderungen an das BCMS*
- die Reife des BCMS
- die Übungserfahrung der Institution.

Dabei sollte sichergestellt werden, dass über einen festgelegten Zeitraum alle BC-Strategien und -Lösungen geübt wurden. Dies sorgt dafür, dass wirklich alle Maßnahmen, organisatorischen Strukturen und Pläne anhand von Übungen überprüft werden. Zusätzlich kann durch wechselnde Szenarien eine Fehlsteuerung vermieden werden. Wenn die Teilnehmer ihre Aufgaben nur noch routinemäßig in derselben Übungssituation bearbeiten, steigt die Gefahr von „Betriebsblindheit“. Dies kann zu Fehlhandlungen führen, aber auch dazu, dass Korrekturbedarfe und Verbesserungsmöglichkeiten nicht mehr erkannt werden.

Ergänzend zu den regelmäßigen Übungen, müssen auch anlassbezogene Übungen berücksichtigt werden. Diese können sich beispielsweise daraus ergeben, dass Notfallpläne aufgrund hinzugekommener Geschäftsprozesse oder Ressourcen aktualisiert und erneut geübt werden sollen.

Der Reifegrad der Übungen muss kontinuierlich gesteigert werden. Hierzu sollte die Institution risikoorientiert vorgehen, d. h. die Übungen müssen realistischer und handlungsorientierter werden, ohne jedoch unzumutbare Auswirkungen auf den eigentlichen Geschäftsbetrieb auszulösen. Zudem genügt es nicht, über Jahre hinweg nur einseitig technisch oder organisatorisch zu üben. Schrittweise müssen die technischen sowie organisatorischen Aspekte der Notfallbewältigung im Zusammenspiel geübt werden. Dies kann z. B. dadurch erreicht werden, dass korrespondierende Wiederanlaufpläne und Geschäftsfortführungspläne kombiniert getestet werden. Auch sollte sichergestellt werden, dass nicht nur die Hauptvertreter der BAO an Übungen eingesetzt werden, sondern auch die Stellvertreter berücksichtigt werden.

Pro Übung sollten mindestens folgende Punkte festgelegt und im Jahresübungsplan dokumentiert werden:

- konkretes Datum oder geplanter Zeitraum der Übung
- Übungsart
- Übungsziel
- zuständige Personen, welche die Übung vorbereiten
- zuständige Personen, welche die Übung durchführen
- Zielgruppe/n und geplante Übende
- Abschätzung der erforderlichen personellen, materiellen und finanziellen Ressourcen
- Abschätzung des zu erwartenden Einflusses der Übung auf den Normalbetrieb.

Das festgelegte **Datum bzw. der geplante Zeitraum** der Übung sollte mit den zuständigen Personen abgestimmt werden, welche die Übung vorbereiten und durchführen. Zusätzlich sollte die Verfügbarkeit aller Übungsteilnehmer berücksichtigt werden. Bei der Terminplanung sollte beachtet werden, dass Stabs- und Stabsrahmenübungen und manche Funktionstests eine längere Vorbereitungsphase benötigen, weil z. B. zuvor Übungsunterlagen erstellt und organisatorische oder technische Voraussetzungen geschaffen werden müssen.

Das **Übungsziel** beschreibt konkret, was mit dieser Übung erreicht werden soll. Es sollte sich an der Reife des BCMS sowie dem allgemeinen Übungsziel der Übungsart ausrichten und die Übungserfahrung der Institution berücksichtigen. Übungen sollten so geplant werden, dass sie einerseits herausfordernd für die Übenden sind, andererseits aber auch Erfolgserlebnisse und einen Erkenntnisgewinn für die Teilnehmer bieten. Entsprechend sollten in der Jahresübungsplanung reale Ereignisse aus der Vergangenheit oder realistisch denkbare Schadensereignisse für die Institution berücksichtigt werden. Es reicht für die Jahresübungsplanung aus, das übergeordnete Übungsziel jeder Übung festzulegen. Dieses Übungsziel kann anschließend in der Vorbereitung der einzelnen Übungen konkretisiert und in Teilziele unterteilt werden, anhand derer die Ergebnisse der Übung bewertet werden können.

Beispiel:

Folgende Übungsziele sind typisch für eine Stabsübung:

- Einüben der effektiven und effizienten Zusammenarbeit
    - innerhalb des Kernteams des Stabs selbst sowie mit den
    - unterstützenden Funktionen wie Protokollierung und Visualisierung
- Überprüfung der Angemessenheit und Funktionsfähigkeit der Dokumente und Methoden des Stabs
- Überprüfung der Angemessenheit und Funktionsfähigkeit des Stabsraums

Darüber hinaus ist es empfehlenswert, Übungen so zu gestalten, sodass diese aufeinander aufbauen. Eine Planbesprechung für einen GFP kann z. B. eine sinnvolle Vorbereitungsmaßnahme für einen späteren Funktionstest einer Maßnahme aus dem GFP sein und/oder der Kombination daraus.

Beispiel:

In einer Planbesprechung wird überprüft, ob die beschriebenen Aktivitäten, um einen Ausweicharbeitsplatz in Betrieb zu nehmen, schlüssig beschrieben sind. Basierend auf diesen Aktivitäten wird anschließend in einem Funktionstest überprüft, ob der beschriebene Arbeitsplatz auch technisch einsatzfähig ist.

Für jede Übung muss entschieden werden, ob diese in der Institution angekündigt wird oder nicht. Wenn Übungen im Voraus angekündigt werden, können sich alle Teilnehmer besser darauf vorbereiten. So können Terminkonflikte vermieden werden. Auf der anderen Seite kann dies auch Nachteile mit sich bringen, wie z. B. einen niedriger wahrgenommenen Realitätsgrad oder eine künstliche Vorbereitung. Für Institutionen ohne Übungserfahrung ist es sinnvoll, zu Beginn alle Übungen anzukündigen, um den Beteiligten die Möglichkeit zu geben, sich darauf vorzubereiten, die nötige Erfahrung zu sammeln und Hemmschwellen abzubauen. Mit steigender Übungserfahrung ist es empfehlenswert zu nicht angekündigten Übungen überzugehen, da diese einer realen Situation mehr entsprechen und die Übenden mehr fordert.

Der erstellte Jahresübungsplan sollte mit der Institutionsleitung abgestimmt und durch diese freigegeben werden. Der Hauptgrund hierfür ist, dass die Institutionsleitung die notwendigen personellen, materiellen und finanziellen Ressourcen freigeben muss. Darüber hinaus kann die Institutionsleitung so die Termine von Übungen steuern, an denen sie selbst beteiligt ist. Dies kann z. B. der Fall sein, wenn auf strategischer Ebene arbeitende Stäbe üben. In Tabelle 66 wird ein vereinfachtes Beispiel für einen Jahresübungsplan dargestellt:

Beispiel:

Nr.	Übungsart	Datum/Zeitraum	Ziel und Umfang der Übung	Zuständig	Ressourcen
2020-01	Planbesprechung	14.04.2020, 09-11 Uhr	GFP der IT-Abteilung im Szenario Standortausfall prüfen	Hr. Meier (IT)	2-3 Mitarbeiter IT, ca. 2 h je Teilnehmer
2020-02	Funktionstest	22.09.2020, 13-16 Uhr	Arbeitsfähigkeit ausgewählter IT-Mitarbeiter an den definierten Notfallarbeitsplätzen überprüfen	Hr. Meier (IT)	2-3 IT Mitarbeiter, ca. 1 Tag je Teilnehmer
2020-03	Alarmierungstest	13.11.2020, 08:30 Uhr	Meldewege und Alarmierung der Stabsmitglieder prüfen	BCMB	Mitglieder des Stabs, ca. 1 h je Teilnehmer
2020-04	Stabsübung	13.11.2020, 09-11 Uhr	Abläufe des Szenarios „Brand im RZ“ im Stab üben	BCMB	Mitglieder des Krisenstabs, Drehbuch und Einlagen, ca. 15 Tage zur Vorbereitung, Durchführung, Nachbereitung + 0,5 Tage je Teilnehmer

Tabelle 66: Beispiel für einen Jahresübungsplan

Hinweis:

Nicht angekündigte Stabsübungen (siehe Kapitel 6.11.3.2 *Stabsübung*) und Stabsrahmenübungen (siehe Kapitel 6.11.3.3 *Stabsrahmenübung*) können gut mit Alarmierungsübungen (siehe Kapitel 6.11.3.4 *Alarmierungsübung*) kombiniert werden. Die Alarmierungsübung wird dabei der Stabs- oder Stabsrahmenübung vorangestellt. In der Alarmmeldung wird den Übenden mitgeteilt, dass sie sich schnellstmöglich oder zu einem bestimmten Zeitpunkt im vorgesehenen Stabsraum einfinden sollen. Anschließend beginnt die eigentliche Stabs- bzw. Stabsrahmenübung.

Der BCMB sollte überwachen, dass alle geplanten Übungen stattfinden. Für ausgefallene, verschobene oder abgebrochene Übungen sollte zeitnah ein Ersatztermin gefunden werden. Treten technische oder organisatorische Probleme auf, sollte der BCMB prüfen, ob eine Wiederholung der Übung erforderlich ist, nachdem die Mängel behoben wurden.

Synergiepotenzial:

Vielfach werden bereits in anderen Sicherheitsthemen Übungen geplant und durchgeführt. So finden aufgrund gesetzlicher Vorgaben regelmäßig Brandschutz- und Räumungsübungen statt, für deren Planung der Brandschutz- oder Arbeitsschutz-Beauftragte zuständig ist. Im Rahmen des ITSCM werden unter anderem Recovery-Tests von IT-Systemen, Schwenktests bei redundanten Rechenzentren sowie Datenwiederherstellungstests durchgeführt. Auch das Krisenmanagement führt eigene Übungen durch. Daher empfiehlt es sich, die Jahresübungsplanung im BCM mit der Übungsplanung der anderen Managementsysteme abzustimmen, um Terminkollisionen und Ressourcenengpässe zu verhindern. Zusätzlich können bestimmte Übungen bewusst miteinander verbunden werden. So kann eine Räumungsübung z. B. mit einer Alarmierungsübung oder einem Funktionstest verbunden werden, was den Realitätsgrad für die übenden Personen weiter steigert.

6.11.3 Vorbereitung und Durchführung einer Übung

Passend zur Jahresübungsplanung müssen die folgenden Schritte je Übung durchlaufen werden:

- Die **Vorbereitung** beinhaltet alle Aktivitäten, die im Vorfeld für die Übung geplant werden müssen. Hierzu gehört z. B. ein Übungsszenario zu beschreiben, die Beteiligten zu bestimmen und die organisatorischen, örtlichen und technischen Rahmenbedingungen zu schaffen. Die Konzeption und Vorbereitung der Übung sollte am gesetzten Übungsziel ausgerichtet werden. Der Umfang der Vorbereitung hängt von der Art und Komplexität der Übung ab.
- Die **Durchführung der Übung** beinhaltet, dass die vorgesehenen Beteiligten einen vorgegebenen Übungsablaufbewältigen müssen z. B. indem die geplanten Ressourcen für den Notfall aktiviert und die Funktionsfähigkeit getestet werden. Ferner werden in diesem Schritt die Erkenntnisse aus der Übung zwecks späterer Auswertbarkeit nachvollziehbar protokolliert.

Da sich die konkreten Schritte je nach Übungsart unterscheiden, sind die Vorbereitung und Durchführung jeweils spezifisch für diese in den nachfolgenden Unterkapiteln zu jeder Übungsart beschrieben.

6.11.3.1 Planbesprechung

In Planbesprechungen werden einzelne Pläne der Notfallbewältigung, insbesondere die Geschäftsfortführungspläne, gemeinsam mit den Anwendern auf fachliche Plausibilität der Inhalte und der getroffenen Annahmen überprüft. Ziel der Planbesprechung ist es, die jeweiligen Pläne anhand eines Szenarios theoretisch durchzuspielen, um Korrekturbedarfe und Verbesserungsmöglichkeiten festzustellen.

Um die Planbesprechungen für die Teilnehmer greifbarer zu gestalten, können die Problemstellungen auch anhand fiktiver Lagen erörtert werden. Die beschriebenen Maßnahmen sollten in der Planbesprechung durch die Anwender dahingehend beurteilt werden, ob diese auch in einer Stresssituation verständlich, plausibel, vollständig und aktuell sind. Planbesprechungen sind vor allem geeignet Abhängigkeiten aufzudecken oder notwendige Voraussetzungen von Maßnahmen zu erkennen bzw. bewusst zu machen. Sie können aber auch eingesetzt werden, um die Teilnehmer zu sensibilisieren.

Vorbereitung einer Planbesprechung

Die Vorbereitung einer Planbesprechung kann der BCMB prinzipiell selbst übernehmen. Deutlich zielführender ist es jedoch, wenn die Übung durch einen Mitarbeiter aus der Organisationseinheit vorbereitet wird, in

dessen Zuständigkeitsbereich der Plan erstellt wurde. Dieser kann besser die Arbeitsbelastung und Terminsituation in der jeweiligen Organisationseinheit einschätzen und so geeignete Zeiträume festlegen, um die Planbesprechung durchzuführen. Zudem sind dem Mitarbeiter geeignete Personen bekannt, die an der Planbesprechung teilnehmen sollen.

Hinweis:

Planbesprechungen können jederzeit auch ohne geeignete organisatorische und technische Grundstrukturen zur Kommunikation und Notfallbewältigung durchgeführt werden. Die Pläne werden nur theoretisch innerhalb des jeweils geltenden Bereichs diskutiert und überprüft, jedoch nicht praktisch umgesetzt. Daher ist es empfehlenswert, gleich nach Erstellung eines Plans, diesen im Rahmen einer Planbesprechung weiter zu plausibilisieren und zu vervollständigen. Ein validierter Plan kann dann auch Grundlage einer Planbesprechung zur Sensibilisierung z. B. neuer Mitarbeiter sein.

Eine Planbesprechung sollte stets angekündigt erfolgen und an einem geeigneten zentralen Ort, z. B. in einem Besprechungsraum, stattfinden. Dieser sollte mit den erforderlichen Mitteln ausgestattet sein. Die Übungsdauer beträgt typischerweise zwei bis vier Stunden, abhängig vom Umfang des besprochenen Plans. Diese Details sollten, wie beschrieben, im Übungskonzept dokumentiert werden Die Übungsziele von Planbesprechungen werden oft „weich“ formuliert.

Beispiel:

- Sensibilisierung und Schaffung eines gemeinsamen Verständnisses aller in diesem Plan involvierten Stellen
- Klärung von Zuständigkeiten bei der Notfallreaktion
- Aufdeckung von internen und externen Abhängigkeiten
- Überprüfung vorhandener Notfallpläne auf Schwachstellen, bevor diese mit großem Aufwand realisiert und/oder praktisch geübt werden

Ein individuelles, dynamisch aufgebautes Szenario mit weiteren Einlagen, so wie es bei Stabsübungen üblich ist, ist für diese Übungsart nicht notwendig. Ein Szenario, das zu Beginn der Übung als Ausgangslage kommuniziert wird, ist vollkommen ausreichend zur Vermittlung der Problemstellung und des Handlungsbedarfs.

Synergiepotenzial:

Planbesprechungen können eine Plattform bilden, um die Notwendigkeit von Informationsaustausch und Zusammenarbeit aufzuzeigen und den Aufbau von Vertrauensnetz zu initiieren. Ein Beispiel hierfür ist das Szenario Cyber-Angriff, das gemeinsam mit Vertretern aus der IT-Abteilung und aus der Informationssicherheit im Rahmen einer Planbesprechung geübt werden kann. Hierbei steht auch das Identifizieren von Zielkonflikten im Fokus, z. B. hinsichtlich der Frage, ob IT-Systeme zugunsten der Informationssicherheit abgeschaltet oder zugunsten des BCM aufrechterhalten werden sollen.

Durchführung einer Planbesprechung

Die Planbesprechung hat die Form einer durch die Übungsleitung moderierten Besprechung mit Leitfragen zur konstruktiven Diskussion der folgenden Aspekte:

Vollständigkeit: Sind die Angaben zu den zeitkritischen Geschäftsprozessen, den Abhängigkeiten zu anderen Geschäftsprozessen sowie Ressourcen vollständig? Sind die Notfallmaßnahmen ausführlich genug beschrieben, um einen sachkundigen Dritten in die Lage zu versetzen, die zeitkritischen Geschäftsprozesse in

einem Notbetrieb wiederaufzunehmen, die Aufgaben im Notbetrieb zu priorisieren und wieder in den Normalbetrieb zurückzuführen?

Plausibilität: Sind die beschriebenen Maßnahmen widerspruchsfrei und im geforderten Zeitraum (RTO) realistisch umsetzbar? Sind die Angaben innerhalb des GFP sowie die beschriebenen Abhängigkeiten zu anderen GFP oder WAP/WHP plausibel dargestellt?

Aktualität: Sind die Angaben zu den zeitkritischen Geschäftsprozessen, den Abhängigkeiten zu anderen Geschäftsprozessen sowie Ressourcen aktuell? Sind die referenzierten Dokumente in der jeweils aktuellen Version hinterlegt? Wurden die relevanten Ansprechpartner auf Basis einer aktuellen Kontaktliste dokumentiert?

6.11.3.2 Stabsübung

Ziel der Stabsübung ist es, die Zusammenarbeit innerhalb der BAO sowie die Methoden zur Stabsarbeit zu üben. Im Gegensatz zur Stabsrahmenübung (siehe Kapitel 6.11.3.3 *Stabsrahmenübung*) wird die Stabsübung im BCM in einem „geschützten Raum“ durchgeführt, ohne Externe zu beteiligen. Der Stab muss die Grundelemente der Stabsarbeit praktisch anwenden, um ein vorgegebenes Notfallszenario zu bewältigen. Bei Stabsübungen nimmt dabei die Vorbereitung aufgrund der Komplexität den größten Umfang im Gegensatz zu den anderen Übungsphasen ein.

Folgende Vorlagen bzw. Hilfsmittel werden in der Regel innerhalb der Vorbereitung und Durchführung der Stabsübung erstellt:

- Übungskonzept
- Übungsdrehbuch und Einlagen
- Übungsprotokoll

Auf die wesentlichen Vorlagen bzw. Hilfsmittel wird im weiteren Verlauf detailliert eingegangen.

Vorbereitung einer Stabsübung

Die Vorbereitung wird in der Regel von einem benannten Übungsautor wahrgenommen. Diese Rolle kann durch den BCMB, durch die für die Übung zuständige Person oder weitere beauftragte Personen übernommen werden. Da Stabsübungen deutlich komplexer sind, sollte im Übungskonzept neben den bereits beschriebenen organisatorischen Eckpunkten die folgenden Punkte festgelegt und dokumentiert werden:

Organisatorische Eckpunkte

Die organisatorischen Eckpunkte für das Übungskonzept wurden bereits beschrieben. Für den Erfolg von Stabsübungen ist insbesondere eine klare Definition der Übungsziele wichtig. Die Übungsziele bei Stabsübungen liegen in der Regel auf einer höheren Abstraktionsebene, als bei anderen Übungen.

Beispiel: Typische Ziele von Stabsübungen

- Praktische Anwendung und Verinnerlichung der Abläufe und Grundlagen der Stabsarbeit
- Kennenlernen der beteiligten Personen und Rollen in einer Notfallsituation
- Überprüfung von Zuständigkeiten, Fähigkeiten und Kenntnissen der BAO
- Übung von Kommunikations- und Entscheidungsprozessen im Stab
- Aktive Einbindung und Überprüfung der Zusammenarbeit mit den Unterstützungsrollen Protokollierung und Visualisierung
- Training einer einheitlichen und abgestimmten Kommunikation nach innen und außen

Rahmenablauf

Um die Ziele und den zeitlichen Rahmen der Übung besser im Blick zu behalten, muss der Übungsautor den Rahmenablauf der Stabsübung planen. Hierbei müssen folgende Fragestellungen beantwortet werden:

- Soll die Übung den Teilnehmern vorab angekündigt werden und falls ja, wann und mit welchen Detailinformationen (z. B. Termin, Übungsdauer, Ort etc.)?
- Soll vor der Stabsübung eine Alarmierung der Teilnehmer erfolgen, z. B. anhand einer vorgeschalteten Alarmierungsübung?
- In welcher Form soll den Übenden Rückmeldung zu erwarteten und in der Übung beobachteten Entscheidungen gegeben werden?
- Sollen Rückmeldungen der Übenden erfasst werden?

Zusätzliche Zeitbedarfe für die Alarmierung oder Auswertung sollten sinnvollerweise bereits in der Vorbereitung der Übung eingeplant werden. Eine Auswertungsrunde erfolgt idealerweise möglichst direkt im Anschluss an die Stabsübung, um die erste Resonanz der Teilnehmer direkt und ungefiltert aufnehmen zu können. Zudem wird empfohlen, eine zweite Auswertungsrunde mit den Teilnehmern vorzusehen, um ein strukturiertes und konsolidiertes Feedback zu erhalten. Dieser Termin sollte mit etwas zeitlichem Abstand zur Übung stattfinden, damit sich alle Beteiligten darauf vorbereiten können. Die zweite Auswertungsrunde kann auch schriftlich stattfinden, z. B. mit Hilfe eines Fragebogens.

Übungsregeln

Damit im Verlauf der Übung keine Schäden verursacht werden, muss der Übungsautor die Regeln für die Übung wie folgt festlegen:

- Welche Abbruchbedingungen führen zu einem vorzeitigen Ende der Übung?
- Gibt es besondere Sicherheitsvorkehrungen, wie z. B. eine bestimmte Kennzeichnung von Dokumenten als Bestandteil der Übung?
- Ist den Teilnehmern eine Kommunikation mit Personen außerhalb des Übungsraums gestattet und falls ja, mit wen und wie?

Abbruchbedingungen für eine Stabsübung sind z. B. der Eintritt eines realen Notfalls, eine deutliche Überschreitung der Übungszeit oder wenn Schlüsselfunktionen die Übung ungeplant verlassen müssen.

Während der Übung sollte die Kommunikation außerhalb des Übungsraums nur in Ausnahmefällen gestattet werden, wenn z. B. eine Auskunft durch einen Fachexperten wichtig für eine bestimmte Entscheidung ist. In jedem Fall muss in der Kommunikation nach außen klar dargestellt werden, dass es sich um eine Anfrage im Kontext einer Übung handelt und nicht um einen echten Notfall. Gerade in einem sehr realistischen Übungsszenario können Teilnehmer dies in der Außenkommunikation schnell vergessen. Daher sollte ein Mitglied des Übungsteams die kommunizierende Person begleiten und dies sicherstellen.

Notfallszenario

Ein wesentlicher Erfolgsfaktor für Stabsübungen ist der Einsatz eines plausiblen und auf die Institution zugeschnittenen Notfallszenarios. Ein Szenario umfasst eine Ausgangssituation und in der Regel eine Abfolge von Ereignissen, auf welche die Teilnehmer reagieren müssen. Das Szenario kann reale oder fiktive realitätsnahe Vorfälle enthalten und liefert die für die Übung relevanten Grundinformationen oder Annahmen.

Das Szenario sollte dafür geeignet sein, die Zielsetzung der Stabsübung zu unterstreichen. Die Teilnehmer sollten die Grundelemente der Stabsarbeit anwenden und sich mit den Notfallplänen sowie mit den vorgesehenen Notfallmaßnahmen inhaltlich auseinandersetzen können.

Hinweis:

Für die ersten Stabsübungen reichen einfache Notfallszenarien mit einem Wirkungsszenario vollkommen aus, um die Grundlagen der Stabsarbeit zu überprüfen.

Übungsdrehbuch

Damit die Übungsleitung den Übungsablauf koordinieren und steuern kann, sollte aus der Gesamtheit der Einlagen durch den Übungsautor ein Übungsdrehbuch erstellt werden, das den gedachten Verlauf der Übung detailliert beschreibt. Tabelle 67 zeigt beispielhaft den Aufbau eines Übungsdrehbuchs

Beispiel:

Nr.	Zeit	Sender	Empfänger	Information bzw. Ereignis	Erwartete Handlung
…	…	…	…	…	…
2	09:15	Leiter RZ	Hr. Lorenz	Löscharbeiten im Rechenzentrum wurden durch die Feuerwehr abgeschlossen.	Funktionsfähigkeit des RZ prüfen und Erstmaßnahmen aus dem GFP initiieren
3	09:22	Mitarbeiter IT	Hr. Meier	Der Ausfall von Anwendung A führt zum Ausfall der zeitkritischen Prozesse X, Y und Z.	Prüfen der konkreten Ausfälle und Ermitteln der Betroffenen
…	…	…	…	…	…

Tabelle 67: Beispiel des Aufbaus eines Übungsdrehbuchs

Einlagen

Sogenannte **Ausgangslagen** beschreiben anhand des Szenarios die Übungsumgebung zur Ausgangssituation. Anhand von **Einlagen** während der Übung können Informationen im Szenario ergänzt, erweitert oder verändert werden, sodass die Teilnehmer dazu animiert werden, zu reagieren und zu handeln.

Beispiel:

Einlagen können z. B. eine Beobachtung, eine eingehende Meldung, ein Pressebericht oder ein weiterer Vorfall zur Lageverschärfung sein.

Je nach hierfür notwendiger Fachexpertise oder anderen Einflussfaktoren kann es erforderlich sein, weitere Personen hinzuzuziehen, die selbst Einlagen entwickeln oder den Übungsautor fachlich beraten.

Hinweis:

Der Übungsautor sollte anhand des Szenarios und der Einlagen sicherstellen, dass jede Funktion im Stab im Verlauf der Stabsübung mindestens eine Aufgabe bearbeiten muss. Gleichzeitig ist es empfehlenswert, wenn keine Funktion so überlastet wird, dass ein „Flaschenhals-Effekt“ entsteht.

Übungsrollen

In einem nächsten Schritt muss der Übungsautor die für die Übungsdurchführung relevanten Teilnehmer festlegen und mit konkreten Personen besetzen:

Übungsleitung: Eine Person wird benannt, welche die Übung insgesamt steuert.

Unterstützungskräfte: Die Übungsleitung sollte abhängig von der Komplexität des Szenarios durch weitere Personen unterstützt werden, insbesondere um Einlagen einzuspielen sowie für den Umgang mit Informationen oder Aufträgen aus dem Stab.

Übende: Dies sind alle weiteren Personen, die als Mitglieder des Stabs, Unterstützungsfunktionen (Protokollierung und Visualisierung) oder in zusätzlichen Funktionen an der Bewältigung des Übungsszenarios teilnehmen sollen.

Übungs-Protokollant: Eine oder mehrere Personen werden benannt, die den Verlauf der Übung nachvollziehbar im Übungsprotokoll erfassen. Der Übungs-Protokollant erfüllt nicht die Rolle des Protokollanten des Stabs, der innerhalb des Übungsszenarios mitwirkt und die Aktivitäten und Entscheidungen des Stabs protokolliert.

Beobachter (optional): Eine oder mehrere Personen werden benannt, welche die Übung neutral „aus der zweiten Reihe“ beobachten und hinsichtlich möglicher Verbesserungspotenziale bewerten.

Letzte Vorbereitungen

Im letzten Schritt der Vorbereitungsphase sollte dafür gesorgt werden, dass die Übung operativ stattfinden kann. Die hierfür notwendigen Aktivitäten ergeben sich typischerweise aus den vorherigen Schritten.

Beispiel:

- Sicherstellen, dass der Raum am Übungstag verfügbar ist und über die notwendige Ausstattung verfügt
- Frühzeitige Einladungen an alle Beteiligten versenden (bei angekündigten Übungen)
- Prüfung der Aktualität von Notfalldokumentationen, die während der Übung verwendet werden sollen
- Vorbereitung einer Kurzpräsentation zur Einführung in die Besonderheiten der Übung, wie z. B. die Regeln zur Kommunikation nach außen oder der Appell, das Übungsszenario nicht infrage zu stellen
- Prüfung, ob die vorgesehenen Übenden ausreichend geschult sind, um ihre Rolle in der Übung wahrzunehmen, z. B. anhand von Schulungsnachweisen
- Vorbereitung der Einlagen, z. B. als Präsentation, als Mails, als Skript zum Vorlesen oder als gedruckte Handouts
- Prüfung der Funktionsfähigkeit von eingesetzter Technik, wie z. B. Beamer, Telefonen etc.)
- Logistische Vorbereitung der Übung, wie z. B. die Verpflegung während der Übung oder die Unterbringung von Teilnehmern
- Durchführung von Briefings mit allen Teilnehmern der Übung

Bis zum Übungstag sollte der Übungsautor wiederkehrend prüfen, ob eventuell andere Ereignisse die Durchführung der Übung beeinflussen oder sogar verhindern können, z. B. weil der vorgesehene Raum oder Schlüsselfunktionen aufgrund anderer Termine nicht länger verfügbar sind.

Durchführung einer Stabsübung

Auch bei einer guten Vorbereitung können oft nicht alle Eventualitäten vorhergesehen werden. Daher können Übungen auch für die Übungsleitung Herausforderungen mit sich bringen Die Übungsleitung muss das

Übungsszenario unter Beachtung der Ziele und der Zeitplanung steuern. Darüber hinaus sollte die Übungsleitung den Übungsablauf koordinieren. Außerdem sollte die Übungsleitung das Recht besitzen, von der Zeitplanung abzuweichen oder die Übung abzubrechen. Alle Teilnehmer sollten sich während der Übung stets an die geltenden Übungsregeln und -künstlichkeiten halten, ohne jedoch ihren kreativen Handlungsraum zu beschränken.

Die Übungsleitung und die vorhandenen Unterstützungsrollen sollten darauf achten, die vorbereiteten Einlagen geeignet in den Übungsverlauf einzuspielen. Die Übungsleitung kann jederzeit entscheiden, dass eine Einlage früher, später oder überhaupt nicht eingespielt wird, wenn sich dies positiv auf den Übungsverlauf auswirkt. Der Übungs-Protokollant muss den Übungsverlauf und die Ergebnisse dokumentieren.

Beispiele:

- Notizen zum beobachteten Ablauf der Übung
- Hinweise von Teilnehmern als Input für die Übungsauswertung
- Erreichung oder Nicht-Erreichung von Übungszielen
- verwendete Dokumente, Werkzeuge, Ressourcen
- erkannte Korrekturbedarfe oder Verbesserungsmöglichkeiten

Werden Beobachter eingesetzt, sollten diese notieren, was gut funktioniert hat und was noch optimierbar ist. Dabei wird empfohlen, Personen als Beobachter einzusetzen, die viel Wissen zum BCM der Institution besitzen.

Die Protokollanten und Beobachter müssen sich während der Übungsdurchführung neutral verhalten und dürfen nicht in das Geschehen eingreifen. Erst in der Auswertung der Übung sollten die Protokollanten und Beobachter aktiv in die Auswertungsrunde einbezogen werden.

Die Übung muss durch die Übungsleitung offiziell beendet werden. Ein offizielles Ende ist zum einen wichtig, damit alle an der Übung Beteiligten wissen, dass die Übungsregeln nicht mehr gelten, insbesondere die Regelungen zur Außenkommunikation. Zum anderen können Übungen sehr emotional werden und die Teilnehmer können sich stark in das Szenario hineinversetzen. Ein klares Übungsende trägt dazu bei, dass Emotionen abflauen und alle Teilnehmer das durchlebte Szenario abschließen können.

6.11.3.3 Stabsrahmenübung

Stabsrahmenübungen im BCM stellen eine erweiterte Form der Stabsübung dar (siehe Kapitel 6.11.3.2 *Stabsübung*). Sie dienen dazu, neben der Stabsarbeit auch die Zusammenarbeit und Kommunikation zwischen dem Stab und weiteren Teams zu überprüfen und zu üben. Bei diesen Teams kann es sich um Unterstützungsteams wie z. B. zur Notfallkommunikation handeln. Es kann auch gemeinsam mit operativen Einheiten der Institution, wie etwa einer zeitkritischen Organisationseinheit, der IT-Abteilung oder dem Gebäudemanagement geübt werden. Gleiches gilt für mögliche extern Beteiligte oder Wissensexperten, welche die Übung beispielsweise als neutrale Beobachter begleiten sollen.

Wenn in der Institution noch keine größere Übungserfahrung vorhanden ist, können die Rollen, die nicht stabsnah sind, zunächst simuliert werden. Beschlossene Maßnahmen des Stabs werden somit nicht praktisch ausgeführt.

Beispiel:

Innerhalb der Stabsrahmenübung wird durch den Stab entschieden und angewiesen, dass betroffene Organisationseinheiten einen Ausweichstandort beziehen sollen. Weitere beteiligte Rollen innerhalb der Stabsrahmenübung, welche die betroffenen Organisationseinheiten repräsentieren, führen dies jedoch nicht real aus, sondern geben nur simuliert die Rückmeldung, dass der Ausweichstandort bezogen wurde.

Mit steigender Übungserfahrung sollten Stabsrahmenübungen einen immer stärkeren realen Bezug haben. So können Stabsrahmenübungen z. B. mit Funktionstests (siehe Kapitel 6.11.3.5 *Funktionstest*) kombiniert werden, um realitätsnah zu üben und damit Erkenntnisse zu gewinnen, die mit Simulationen alleine nicht erlangt werden können.

Hinweis:

Wenn die Übungserfahrung der Institution es zulässt, können Stabsrahmenübungen auch sehr realistisch und mit externer Beteiligung wie z. B. Aufsichtsbehörden, Feuerwehr, THW oder Statisten erfolgen. Je nach Ausmaß kann diese Übungsart in eine „Vollübung" übergehen.

Vorbereitung einer Stabsrahmenübung

Um eine Stabsrahmenübung vorzubereiten, müssen alle Schritte durchgeführt werden, die für die Vorbereitung einer Stabsübung erforderlich sind (siehe Kapitel 6.11.3.2 *Stabsübung*). Der zentrale Unterschied zwischen den beiden Übungsarten besteht darin, dass die Kommunikation der Teilnehmer nicht auf den Stabsraum beschränkt ist. Bei fortgeschrittener Übungserfahrung üben die Teilnehmer wie in einem realen Notfall auf ihre jeweiligen Standorte verteilt und nutzen auch die vorgesehenen Kommunikationskanäle dazwischen. Dies erfordert entsprechende Sicherheitsvorkehrungen, die im Vorfeld geklärt und geschaffen werden müssen. Im Folgenden werden einige Beispiele für solche Sicherheitsvorkehrungen genannt:

Beispiel:

- An jedem Übungsort sollte ein Mitglied des Übungsteams bzw. ein Beobachter anwesend sein oder per Videokonferenz zugeschaltet sein, um im Bedarfsfall eingreifen zu können.
- Einlagen und sonstige schriftliche Unterlagen müssen unter Angabe des Übungsdatums und Bezeichnung eindeutig und auffällig als Übungselemente bzw.-dokumente gekennzeichnet werden.
- Für die Stabsrahmenübung sollten Verhaltensregeln festgelegt werden. Dies betrifft insbesondere die mündliche Kommunikation aus dem Stabsraum heraus und die dafür zu nutzenden Kommunikationswege. Es muss unbedingt verhindert werden, dass Personen, die nicht Teil der Übung sind, fiktive Informationen für echt halten. Außerdem muss das Verhalten bei Eintritt einer Abbruchbedingung oder eines realen Notfalls geregelt sein.
- Die Verhaltensregeln können zu „Übungskünstlichkeiten" führen, da zum einen in der Übung nicht alles real nachvollzogen wird, was bei Notfällen passieren kann (z. B. Brandschäden, Ausfall von IT-Systemen, Datenverlust, Kontakt zu Medienvertretern, Wartezeiten und Pausen bis Maßnahmen umgesetzt sind). Zum anderen sind bestimmte Dinge mitunter nicht in der Übung verfügbar oder nicht möglich. Diese Übungskünstlichkeiten können im Vorfeld der Übung identifiziert werden. Es ist empfehlenswert, diese vor der Übung anzupassen, sodass diese sich „natürlich" einfügen und nicht störend wirken. Zudem ist es empfehlenswert, die Teilnehmer darüber zu informieren.
- Anhand von Schulungs- und Informationsveranstaltungen im Vorfeld der Übung kann ein vergleichbares Wissensniveau bei den an der Übung beteiligten Personen hergestellt werden.
- Insbesondere bei komplexen Stabsrahmenübungen kann der BCMB erwägen, den Ablauf zuvor mindestens einmal mit geeigneten Vertretern der Teilnehmer durchzuspielen. Durch diesen Probelauf werden Lücken und Ungereimtheiten im Szenario und im Übungsablauf beseitigt und etwaige Übungskünstlichkeiten so angepasst, dass sie sich „natürlich" einfügen und nicht störend wirken.
- Direkt vor der Übung ist es empfehlenswert, wenn die Übungsleitung alle wesentlichen Rahmenbedingungen und Prämissen sowie die Verhaltensregeln der Übung vorstellt. Zudem ist empfehlenswert, die Teilnehmer darauf hinzuweisen, dass die Übungsinhalte und -abläufe vertraulich behandelt werden sollen, damit die Geschehnisse und das Verhalten Einzelner nicht innerhalb der Institution thematisiert werden.

Wenn die Stabsrahmenübung mit anderen Übungsarten, wie z. B. Funktionstests, kombiniert werden, dann beinhaltet die Vorbereitungsphase auch deren Aspekte und Schritte.

Ein wesentlicher Bestandteil einer Stabsrahmenübung ist die Vorspiegelung bzw. Simulation der Außenwelt durch Personen, die nicht zur BAO gehören. Diese Personen unterstützen den Ablauf indem sie z. B.

- Szenario-Elemente wie einzuspielende Einlagen vorgeben
- Entscheidungen von außen treffen
- Aufträge der Übenden entgegennehmen
- Reaktionen der Außenwelt simulieren und an die Übenden zurückspielen

Je nach Komplexität der Übung ist es notwendig, dass die unterstützenden Personen untereinander und mit der Übungsleitung kommunizieren. Hierfür sollten in der Vorbereitungsphase entsprechende organisatorische und technische Rahmenbedingungen geschaffen werden. Tools können dabei unterstützen, Übungen zu planen und durchzuführen (siehe Hilfsmittel *Tools*). Bei sehr komplexen Stabsrahmenübungen ist es empfehlenswert, eine komplette Steuerungsorganisation (vgl. LÜKEX-Glossar des BBK, siehe [BBK2]) aufzubauen, die den Übungsablauf inklusive der Simulation der Außenwelt gesamthaft steuert.

Durchführung einer Stabsrahmenübung

Die Durchführung einer Stabsrahmenübung beinhaltet weitestgehend die gleichen Schritte wie die der Stabsübung (siehe Kapitel 6.11.3.2 *Stabsübung*). Durch die Übungsleitung müssen jedoch die zusätzlichen Aspekte, die im Rahmen der Vorbereitung ermittelt und festgelegt wurden, fortlaufend beachtet werden.

6.11.3.4 Alarmierungsübung

Die Alarmierungsübung zielt darauf ab, Fehlerquellen und Schwächen in der Alarmierung BAO zu identifizieren und die Wirksamkeit von Alarmierungsverfahren festzustellen. Eine erfolgreiche Alarmierung ist Grundlage für die weitere Notfallbehandlung und sollte somit schnellstmöglich erfolgen. Ausgehend von einer Information einer Meldestelle wird über die zentrale Entscheidungsinstanz eine Alarmierungsmeldung bzw. die Alarmierungskette ausgelöst und nachverfolgt. Alarmierungsübungen können unterschieden werden in technikorientierte Tests und anwendungsorientierte Übungen.

In technikorientierten Tests wird überprüft, ob die Kommunikationsmittel und -verfahren, die im Notfall eingesetzt werden, funktionsfähig sind. In anwendungsorientierten Übungen werden die organisatorischen Regelungen wie z. B. die Erreichbarkeit und Verfügbarkeit der relevanten Rolleninhaber, die Stellvertretungen, gegebenenfalls. die Geschwindigkeit der Reaktion und die vorhandene Alarmierungsdokumentation überprüft bzw. eingeübt.

Anwendungsorientierte Alarmierungsübungen setzen voraus, dass ein abgestimmter Alarmierungspfad mit aktuellen Kontaktdaten vorliegt und die zu nutzenden Kommunikationswege und -mittel zwischen den Teilnehmern organisatorisch und technisch festgelegt, dokumentiert, umgesetzt und funktionstüchtig sind.

Vorbereitung einer Alarmierungsübung

Der Aufwand einer Alarmierungsübung ist aufgrund der geringen Komplexität deutlich kleiner als der einer Stabsübung. Typischerweise übernimmt der BCMB selbst diese Aufgabe.

Neben den üblichen Einträgen im Übungskonzept, sollte abhängig vom definierten Alarmierungsprozess (siehe Kapitel 6.4.2.3 *Alarmierung der BAO*) der BCMB bei anwendungsorientierten Übungen entscheiden, ob die Erreichbarkeit nur innerhalb oder auch außerhalb der üblichen Dienstzeit getestet werden soll. Falls eine Erreichbarkeit auch außerhalb der Dienstzeit festgelegt wurde, ist es empfehlenswert, Alarmierungsübungen auch vereinzelt zu ungünstigen Zeiten abzuhalten. Beispiele hierfür sind die Mittagspause, kurz nach

Feierabend, nachts, am Wochenende oder an Feiertagen. Findet eine Übung zu ungünstigen Zeiten statt müssen die erforderlichen Stellen, wie der Betriebsrat oder die IT-Abteilung, vorab informiert werden.

Die Übungsziele ergeben sich aus der Übungsart und aus dem Alarmierungsprozess. Neben den oben genannten allgemeinen Zielen beinhalten die Übungsziele hier meistens zeitliche Parameter hinsichtlich der Erreichbarkeits- und Rückrufquote der Beteiligten.

Beispiel:

Ziel der Alarmierungsübung: Nach Auslösen der initialen Alarmmeldung dauert es maximal 30 Minuten, bis alle erforderlichen Rolleninhaber der BAO den Alarm positiv quittiert haben.

Notfallszenario

Ein Szenario ist für diese Übungsart nicht unbedingt notwendig. Eine einfache Ausgangslage, die während des Tests kommuniziert wird, ist vollkommen ausreichend.

Beispiel:

Einfache Ausgangslage für eine Alarmierungsübung:

„Übungsalarm! Ausfall von IT-Systemen durch Brand im Serverraum. Übungsalarm!“

Der BCMB sollte in seiner Jahresplanung darauf achten, dass über einen festgelegten Zeitraum alle definierten Alarmierungswege getestet werden.

Durchführung einer Alarmierungsübung

In der Praxis hat es sich bewährt, die Alarmierungsübung unangekündigt durchzuführen, um möglichst reale Voraussetzungen zu schaffen. Gegebenenfalls können die Teilnehmer aber zuvor vom BCMB informiert werden, dass eine Alarmierungsübung innerhalb eines vorgegebenen Zeitraums stattfinden wird, um deren Kooperationsbereitschaft weiterhin zu erhalten.

6.11.3.5 Funktionstest

Funktionstests, auch funktionale Tests genannt, sind in vielen Institutionen bereits fester Bestandteil des Qualitätssicherungsprozesses, z. B. in der Software- oder Systementwicklung. Es existieren unterschiedliche Definitionen zum Begriff Funktionstest. In diesem Standard wird der Begriff weit gefasst und schließt alle Tests mit ein, in denen funktionale Anforderungen auf systematischem Wege geprüft werden.

In einem Funktionstest werden die vorhandenen Vorsorgemaßnahmen und Notfallpläne bzw. Notfallmaßnahmen dahingehend überprüft, ob diese wie vorgesehen funktionieren. Anhand von Funktionstests sollte systematisch und, wenn vertretbar, realitätsnah überprüft werden, ob die Inhalte in der Betriebs- und Notfalldokumentation verständlich, vollständig und fachlich richtig sind. Außerdem wird überprüft, ob die Inhalte in der Notfalldokumentation verständlich, vollständig und fachlich richtig sind. Zudem kann verifiziert werden, ob die im Notfallplan enthaltenen Zeitvorgaben eingehalten werden können.

Beispiele für Funktionstests:

- Eine Auswahl von Mitarbeitern einer Fachabteilung an einen Auswahlort verlagern und dort arbeiten lassen. (Szenario Standortausfall)
- Geschäftsvorgänge anhand der Schritte, die im Geschäftsfortführungsplan beschrieben sind, durch einen Mitarbeiter einer anderen Abteilung erledigen lassen. (Szenario Personalausfall)
- Einen vorhandenen alternativen Dienstleister temporär nutzen. (Szenario Dienstleisterausfall)

- Mehrere untereinander abhängige Ausweichserver und alternative Netzverbindungen in Betrieb nehmen. (Szenario IT-Ausfall)
- Vorhandene IT-Wiederanlaufpläne und -Maßnahmen praktisch ausführen.
- Den Anlauf und Betrieb eines Notstromaggregats in der vorgegebenen Zeit überprüfen, eventuell auch für eine längere Dauer.

Hinweis:

Funktionstests dienen insbesondere dazu, die RTA bestimmen und nachweisen zu können. Dabei ist es nicht notwendig, bei jedem Test den kompletten Notfallbewältigungsprozess zu simulieren. Aufwand und Kosten einer kompletten Überprüfung sind unter Berücksichtigung des tatsächlichen Notfallrisikos oft nicht angemessen. Stattdessen ist es häufig ausreichend

- sich auf die zeitkritischen Aspekte des Notfallplans zu konzentrieren sowie
- Teilaspekte des Notfallplans in aufeinander aufbauenden Stufen zu testen

Vorbereitung eines Funktionstests

Eine Voraussetzung für die Funktionstests ist, dass die Verfügbarkeit und Inbetriebnahme von einzelnen Ressourcen, die für die Notfallvorsorge oder den Wiederanlauf im Notfall erforderlich sind, anhand von Komponententests durch die Ressourcenzuständigen Organisationseinheiten überprüft wurde. In Komponententests wird geprüft, ob die Notfallmaßnahmen für einzelne Hardwarekomponenten, wie z. B. Server, Router etc., oder Softwarekomponenten, wie z. B. Applikationen, Dienste etc., wirksam und angemessen sind. Dies erfolgt typischerweise anhand von Tests, die nicht primär im BCM liegen, jedoch damit korrespondieren und daher aufeinander abgestimmt werden sollten. Damit sind z. B. folgende Testarten gemeint:

- Schwenktests von IT-Systemen oder Rechenzentren
- Failover-Tests von Netzdiensten oder Clustern
- Wiederanlauf- bzw. Recovery-Tests von IT-Systemen oder einzelnen Komponenten
- Restorationstests von Datenbeständen oder Datenbanken
- Lesbarkeitstests von Datensicherungen
- Technische Betriebstests von Infrastrukturkomponenten, Maschinen oder Anlagen, die zur Notfallvorsorge oder für den Notfall vorgesehen sind

Die Übungsdauer reicht von wenigen Minuten für einen einfachen Funktionstest einzelner Komponenten bis hin zu mehreren Tagen, in denen die Testumgebung für einen umfangreicheren Funktionstest hergestellt und zurückgebaut wird.

Für Funktionstests sollten folgende Eckpunkte im Übungskonzept zusätzlich dokumentiert werden:

- Voraussetzungen (z. B. eine Testumgebung oder vorab durchgeführte Tests einzelner für den Funktionstest notwendiger Basisressourcen)
- Risikoeinschätzung und risikosenkende Maßnahmen

Funktionstests können reale Auswirkungen auf den Geschäftsbetrieb haben und diesen unter Umständen sogar unterbrechen, sowohl geplant als auch unbeabsichtigt. Der Übungsautor muss eine Risikoeinschätzung zum Funktionstest und zu den damit verbundenen Auswirkungen durchführen und, falls erforderlich, risikosenkende Maßnahmen ermitteln. Es wird empfohlen, für Funktionstests mit potenziell möglichen Auswirkungen auf den Geschäftsbetrieb eine Freigabe von der Institutionsleitung einzuholen. Zudem sollten Maßnahmen vorgesehen werden, die einen Abbruch des Funktionstests und eine schnellstmögliche Wiederherstellung des Ausgangszustands ermöglichen, falls unbeabsichtigte Auswirkungen auftreten.

Die meisten Funktionstests werden aufgrund des Risikos für den Geschäftsbetrieb angekündigt. Funktionstests finden in der realen Umgebung oder in einer gesonderten Testumgebung statt. Bei einer Testumgebung handelt es sich idealerweise um ein speziell geschaffenes, möglichst realitätsnahes, aber vom Produktionsbetrieb abgekapseltes Testumfeld. Dies soll verhindern, dass der Geschäftsbetrieb durch die Funktionstests eingeschränkt oder gefährdet wird. Wenn vor dem Test eine Testumgebung vorbereitet werden muss, muss der Funktionstest in der Institution angekündigt werden.

Hinweis:

Die Herstellung und der Rückbau der Testumgebung müssen geplant werden. Die Planung wird am besten von ausgewählten Spezialisten aus Notfallteams durchgeführt. Alle speziell für die Übung geschaffenen Vorkehrungen müssen nach Übungsende rückgängig gemacht werden.

Die Übungsziele von Funktionstests sind in der Regel die praktische Überprüfung reaktiver Maßnahmen hinsichtlich ihrer Funktionsfähigkeit

Beispiel:

Typische Übungsziele für Funktionstests sind:

- die Überprüfung von technischen Vorkehrungen und organisatorischen Verfahren, die für den Notfall vorgesehen sind
- die Überprüfung vorhandener Notfallpläne in Gänze oder in Teilen in Bezug auf Korrektheit, Aktualität und Vollständigkeit
- das Training der Mitarbeiter im Umgang mit dem Notfallplan
- die Überprüfung, ob die Zielvorgaben aus dem Notfallplan eingehalten werden können

Durchführung eines Funktionstests

Funktionstests finden auf Basis der Ressourcenkategorien statt, die dem Notfallplan zugrunde liegen. Der Ablauf sollte den vorgesehenen Maßnahmen aus dem Notfallplan entsprechen und wird durch die Übungsleitung gesteuert. Bei sehr einfachen Funktionstests, z. B. dem Testen eines Notfall-Laptops, kann die Übungsleitung durch die testende Person selbst wahrgenommen werden. Bei komplexen Funktionstests hingegen, sollte die Übungsleitung durch eine separate Person besetzt sein, welche die Vorgänge koordiniert. Ein Protokollant oder weitere Unterstützungsrollen können den Ablauf sowie die Auswertung unterstützen und die anderen Beteiligten damit entlasten.

Die in dem Funktionstest aufgedeckten Korrekturbedarfe und Verbesserungsmöglichkeiten sollten nachvollziehbar protokolliert werden. Es ist empfehlenswert, anhand einer einheitlichen Protokollvorlage pro getesteter Maßnahme bzw. Ressource zu dokumentieren, ob diese „ohne Befund“ funktioniert hat oder ob es Auffälligkeiten bzw. Anmerkungen gab. Die Inhalte des Protokolls sollten prägnant und für sachverständige Dritte verständlich formuliert sein.

Die Tabelle 68 zeigt einen exemplarischen Aufbau für ein Testprotokoll.

Beispiel: Funktionstest Ausweichstandort

Zu testende Ressource	Testaktivität	Ergebnis	Bemerkung	Korrekturmaßnahme
Gebäude	Zugang zum Gebäude über Wachdienst prüfen	**Nicht erfolgreich**	Wachdienst war nicht in seine Aufgaben in einem Notfall eingewiesen.	Schulungsunterlagen und -maßnahmen prüfen
Notfallarbeitsplatz	Vollständigkeit der Ausstattung prüfen	**Erfolgreich**	Alle Materialien des Notfallarbeitsplatzes vorhanden.	
Notfallarbeitsplatz	Anmeldung mit Nutzerkennung prüfen	**Teilweise erfolgreich**	Anmeldung erfolgreich, aber der Notfallarbeitsplatz wurde nicht regelmäßig aktualisiert. Durch eine systemseitige Aktualisierung kommt es zu einer deutlichen Verzögerung.	Aktualisierungs-prozess prüfen
Notfallarbeitsplatz	Notfallrelevante Software prüfen	**Nicht erfolgreich**	E-Mail und Warenwirtschaftssystem verfügbar. Kundenkartei nicht erreichbar.	Kundenkartei für standortübergreifende Zugriffe freischalten

Tabelle 68: Beispiel für den Aufbau eines Testprotokolls

Ein Protokollant oder weitere Unterstützungsrollen können den Ablauf sowie die Auswertung unterstützen und die anderen Beteiligten damit entlasten. Zwingend notwendig ist dies jedoch nicht.

6.11.4 Auswertung und Nachbereitung von Übungen

Die Auswertung und Nachbereitung jeder Übung ist Voraussetzung, um das BCM weiterentwickeln und Korrekturbedarfe und Verbesserungsmöglichkeiten identifizieren zu können. Alle durchgeführten Übungen müssen ausgewertet und nachbereitet werden. In der Auswertung wird zum einen analysiert, ob und wie gut die gesetzten Ziele erreicht wurden.

Zum anderen werden Korrekturbedarfe und Verbesserungsmöglichkeiten abgeleitet. Dies können sowohl dokumentarische oder technische Änderungsbedarfe in den Notfallplänen und -Maßnahmen sein, als auch Anpassungen an der BCM-Aufbauorganisation oder dem BCM-Prozess bzw. der Notfallbewältigungsprozess. Zusätzlich können aus der Übung funktions- bzw. rollenspezifische Verbesserungs- und Unterstützungsbedarfe hervorgehen, z. B. zu den individuellen Aufgaben und Befugnissen einzelner Rollen. Auch Schulungs- oder Trainingsbedarfe für die Rolleninhaber des Stabes zählen dazu.

Sowohl die für die Übung herangezogenen Dokumente, wie die Notfallpläne, als auch in der Übung erstellte Dokumente sollten ausgewertet werden. Erstellte Dokumente sind zum einen Übungsprotokolle und Feedbackbögen der Übungsteilnehmer. Zum anderen geben auch Ergebnisobjekte der Stabsübung, wie Visualisierungen, Protokolle oder fiktive Pressemitteilungen, Auskunft über die Reife des BCM. Alle Übungsergebnisse und identifizierten Korrekturbedarfe und Verbesserungsmöglichkeiten sollten in einem Übungsbericht dokumentiert werden. Der BCMB sollte daraus ableiten, wie ausgereift das BCM der Institution bereits ist.

Hinweis:

Mit der *Darstellung des Übungserfolges* ist hier nicht gemeint, dass beurteilt wird, ob die Teilnehmer immer „richtig", d. h. wie geplant bzw. aus fachlicher Sicht sinnvoll, gehandelt und entschieden haben. Vielmehr sollte im Rahmen der Auswertung und Nachbereitung dargestellt werden, welcher Lerneffekt erzielt und welche Korrekturbedarfe oder Verbesserungsmöglichkeiten erkannt werden konnten. Eine „fehlerfreie" Übung ist hingegen kein Erfolgskriterium für eine Übung. Wurden alle Übungsziele erreicht, kann dies als Erfolg angesehen werden. Im Umkehrschluss kann aber auch dann von einer erfolgreichen Übung gesprochen werden, wenn darin Korrekturbedarfe und Verbesserungsmöglichkeiten identifiziert wurden und diese Erkenntnisse genutzt werden, um das BCMS weiter zu verbessern.

Zusätzliche Aspekte zur Auswertung und Nachbereitung einer Stabs(rahmen)übung

Falls im Anschluss an eine Stabsübung eine Auswertungsrunde (Manöverkritik) vorgesehen ist, ist es empfehlenswert, wenn diese zum vorgesehenen Zeitpunkt durch die Übungsleitung oder einen im Vorfeld festgelegten, geeigneten Moderator gestartet wird. Die Teilnehmer können darin ihre persönlichen Eindrücke und die Zielerreichung einschätzen sowie identifizierte Korrekturbedarfe und Verbesserungsmöglichkeiten darstellen. Es kann aus psychologischen Gründen hilfreich sein, wenn erst die aktiven Teilnehmer zu Wort kommen, bevor die beobachtenden Rollen sich zur Übung äußern. In der Auswertungsrunde können auch Fragebögen genutzt werden. Die Auswertungsrunde sollte protokolliert werden, um Erkenntnisse für die weitere Auswertung daraus ableiten zu können. Neben den Beobachtungen und Rückmeldungen der Übenden und Übungsbeobachter muss die Übungsleitung hierfür auch die erstellten Unterlagen der Übenden für die Auswertung zusammentragen und entsprechend der Zielstellung auswerten. Zu den erstellen Unterlagen zählen etwa Visualisierungen, Protokolle und fiktive Pressemitteilungen zusammen mit während der Übung erstellten Unterlagen der Protokollanten und Beobachter,

Zusätzliche Aspekte zur Auswertung einer Alarmierungsübung

Die Ergebnisse der Alarmierungsübung müssen protokolliert werden. Wird eine Alarmierungssoftware eingesetzt ist es empfehlenswert, die von der IT-Anwendung erzeugten Protokolle auszuwerten. Die im Übungsverlauf erzeugten Protokolle erlauben es im Anschluss der Übung diese auszuwerten.

Ergebnisvorstellung und Festlegung der Folgeschritte

Das Übungsergebnis sowie die identifizierten Korrekturbedarfe und Verbesserungsmöglichkeiten müssen durch die Übungsleitung an den BCMB kommuniziert werden. Der BCMB sollte diese im Maßnahmenplan aufgreifen und dadurch in der Korrektur und Verbesserung des BCMS weiterbehandeln (siehe Kapitel 6.13 *Korrektur und Verbesserung des BCMS*).

6.12 Leistungsüberprüfung und Berichterstattung

Um das BCMS aufrechtzuerhalten und kontinuierlich verbessern zu können, muss regelmäßig überprüft werden, ob das BCMS angemessen, wirksam und effizient ist. Anhand der Leistungsüberprüfung kann festgestellt werden, ob die jeweiligen Vorgaben des BCMS eingehalten und Ziele des BCMS erreicht werden. Außerdem werden Korrekturbedarfe und Verbesserungsmöglichkeiten sowie Abweichungen zu den definierten Vorgaben im BCM aufgedeckt, die durch die der Korrektur und Verbesserung des BCMS behandelt werden (siehe Kapitel 6.13 *Korrektur und Verbesserung des BCMS*). Die Institutionsleitung erhält durch die Berichte aus der Leistungsüberprüfung die Möglichkeit, potenzielle Fehlentwicklungen zu identifizieren und proaktiv darauf reagieren zu können. Abbildung 67 gibt einen Überblick über die notwendigen Schritte zur Leistungsüberprüfung und Berichterstattung.

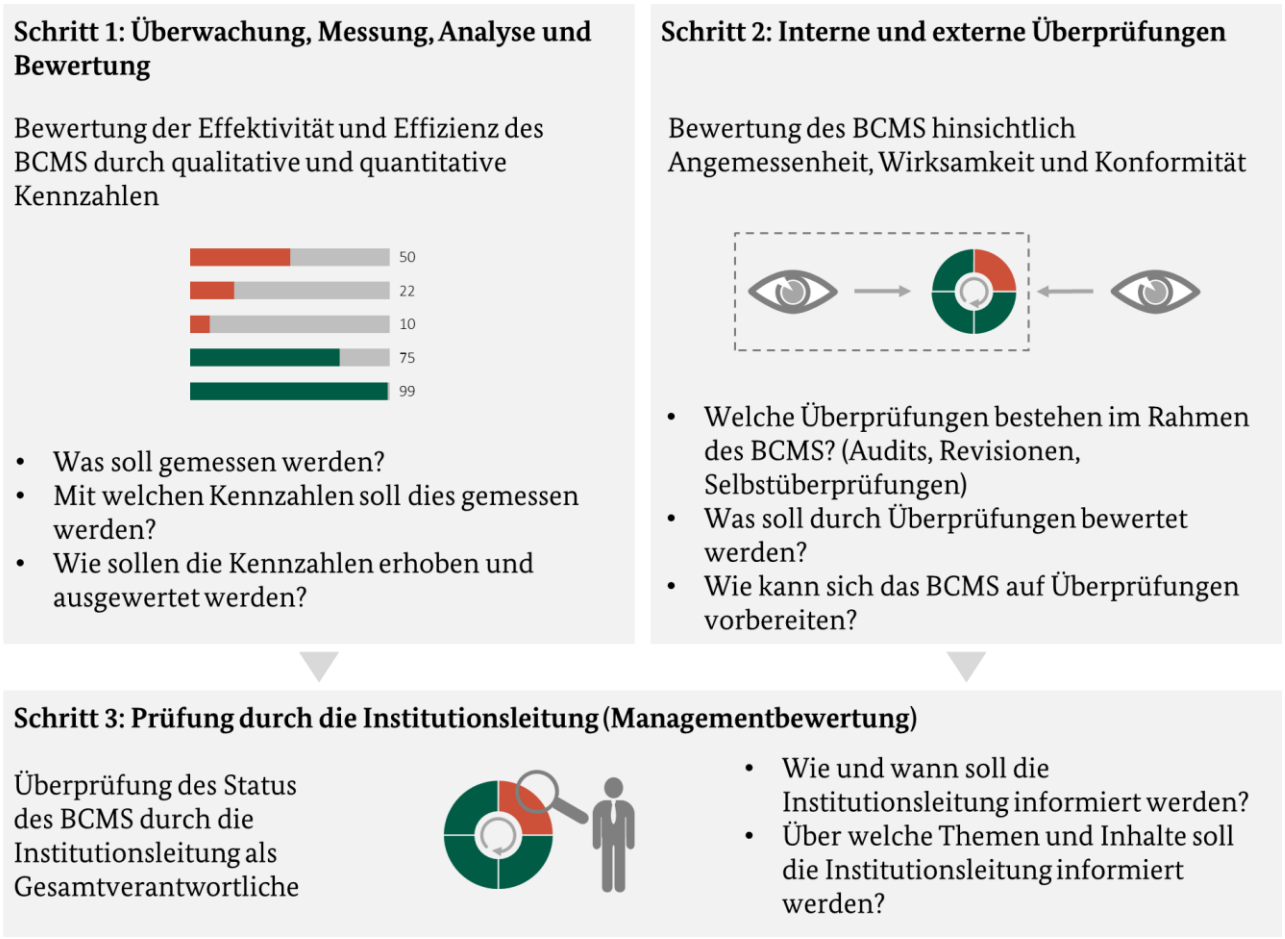

Abbildung 67: BCM-Prozessschritte zur Leistungsüberprüfung

6.12.1 Überwachung, Messung, Analyse und Bewertung

Um die Effektivität und Effizienz des BCMS sicherzustellen, bedarf es einer regelmäßigen Überwachung, Messung, Analyse und Bewertung aller BCM-Prozessschritte. Hierzu sollten Kennzahlen definiert und erhoben werden, die dann mit definierten Zielwerten abgeglichen werden.

Auswahl von Kennzahlen und Zielwerten

Im ersten Schritt sollte festgelegt werden, was gemessen werden soll. Hierfür werden in der Praxis zumeist Kennzahlen erhoben, die sich auf das konkrete Ergebnis eines oder mehrerer BCM-Prozessschritte beziehen. Aber auch konkrete Ergebnisobjekte, die sich aus den BCM-Prozessschritten ergeben, können anhand einer

Kennzahl untersucht werden. Daher sollten messbare Kennzahlen identifiziert und definiert werden, die eine Aussage über die Effektivität und Effizienz des BCMS ermöglichen.

Hinweis:

Anstelle von Kennzahlen wird in einigen Institutionen die englische Bezeichnung **Key Performance Indicator (KPI)** genutzt.

Bei der Auswahl der Kennzahlen muss berücksichtigt werden, welches Ziel durch die Erhebung der Kennzahlen verfolgt wird und ob zur Erhebung der Kennzahlen eine sinnvolle Datengrundlage besteht. Die ausgewählten Kennzahlen sollten quantitative und qualitative Aspekte berücksichtigen, um zu überprüfen, ob BCM-Prozessschritte sowie deren Ergebnisse vollständig, aktuell, angemessen, wirksam, plausibel und effizient sind.

Ein **quantitativer Aspekt** ist beispielsweise der Abdeckungsgrad des Untersuchungsgegenstandes. In der BIA entspricht dies der Anzahl analysierter Geschäftsprozesse im Vergleich zur Gesamtheit aller Geschäftsprozesse der Institution.

Qualitative Aspekte werden gemessen, indem die Abweichungen zu den Vorgaben der BCMS-Prozessschritte überprüft wird. Beispielsweise können hierzu Kennzahlen zur Aktualität oder Konsistenz der Daten sowie zu Fehlern festgelegt werden.

In Tabelle 69 sind beispielhafte quantitative und qualitative Kennzahlen aufgeführt, die Aussagen über den Reifegrad und die Effektivität der BIA, der Geschäftsfortführungsplanung sowie der Überprüfung von GFP anhand von Tests und Übungen treffen.

Beispiel:

Geschäftsprozess	In BIA betrachtet?	Zeitkritisch?	Im GFP vorhanden?	Qualität des GFP?	Anhand des GFP geübt?
A	Ja	Ja	Ja	Angemessen und plausibel	GFP ist funktionsfähig und wirksam
B	Nein	*Fehlende Daten*	*Fehlende Daten*	*Fehlende Daten*	*Fehlende Daten*
…	…	…	…	…	…
Z	Ja	Nein	Nicht relevant	Nicht vorhanden	Nicht vorhanden
Gesamt	**25/26 (96 % aller Geschäftsprozesse)**	**6/26 (23 % aller Geschäftsprozesse)**	**6/6 (100 %)** **1 unbekannt**	**4/6 (66,6 % aller GFP aktuell, angemessen und plausibel)** **1 unbekannt**	**3/6 (50 % aller GFP wirksam)** **1 unbekannt**

Tabelle 69: Beispiele für quantitative und qualitative Kennzahlen ohne Zielwerte

Kennzahlen lassen sich immer im Kontext der Institution unterschiedlich interpretieren. So könnte eine insgesamt hohe Prozentzahl zeitkritischer Geschäftsprozesse entweder bedeuten, dass die BIA-Methodik daraufhin überprüft werden sollte, ob die Parameter angemessen sind oder ob die Schadensbewertung durch die Prozessexperten angemessen eingeschätzt wurde. In einer anderen Institution könnte dasselbe Ergebnis

hingegen deutlich machen, in welchem risikobehaftetem Umfeld die Institution steht und daher die Bedeutung des BCMS unterstreichen.

Um Abweichungen zu den jeweiligen Kennzahlen aufzuzeigen, sollten Zielwerte für diese festgelegt werden. Insbesondere die Zielsetzungen des BCMS (siehe Kapitel 3.1.1 *Zielsetzung*), die allgemeinen Anforderungen (siehe Kapitel 6.1.1 *Identifizierung von Anforderungen an das BCMS*) sowie der aktuelle und gewünschte Reife sollten dabei beachtet werden.

Tabelle 70 enthält verschiedene Beispiele für Kennzahlen und deren Zielwerte. Weitere Beispiele von Kennzahlen können dem Hilfsmittel *Kennzahlen im BCMS* entnommen werden.

Beispiel:

Kennzahl	BCM-Prozess-schritt	Zielwert
Abdeckungsgrad der Geschäftsprozesse gemäß Prozesslandkarte in der BIA	BIA	N = 100 %
Aktualität der BIA-Daten	BIA	Letzte Aktualisierung < 365 Tage
Anteil zeitkritischer Geschäftsprozesse	BIA	N < 50%
Abdeckungsgrad zeitkritischer Geschäftsprozesse in den GFP	GFP	N = 100 %
Aktualität der GFP	GFP	Letzte Aktualisierung < 365 Tage
Abdeckungsgrad zeitkritischer Ressourcen in der Übungsplanung	Üben und Testen	N = 100 % über 3 Jahre
Abdeckungsgrad der Wiederanlaufpläne in der Übungsplanung	Üben und Testen	N = 100 % über 3 Jahre
Abdeckungsgrad der Geschäftsfortführungspläne in der Übungsplanung	Üben und Testen	N = 100 % über 3 Jahre
Termintreue in der Bearbeitung offener Maßnahmen der Maßnahmenliste	Kontinuierliche Verbesserung	N = 100 %

Tabelle 70: Beispiele für Kennzahlen mit definierten Zielwerten.

Erhebung und Messung der Kennzahlen

Kennzahlen des BCMS müssen regelmäßig erhoben werden, um einen aktuellen Überblick über den Status des BCMS und die einzelnen BCM-Prozess-Schritten zu erhalten. Hierbei muss insbesondere der Maßnahmenplan mit einbezogen werden (siehe Kapitel 6.13.3 *Umsetzung und Überwachung von Korrektur- und Verbesserungsmaßnahmen*). Die Institution muss festlegen, durch wen und in welchen Abständen die Kennzahlen erhoben und ausgewertet werden. Die definierten Kennzahlen können dabei zentral durch den BCMB oder dezentral durch die BCM-Koordinatoren oder andere zuständige BCM-Rollenträger erhoben werden.

Der BCMB kann für die dezentrale Erhebung Kennzahlen Fragebögen oder Berichtsvorlagen entwerfen, in denen die Kennzahlen definiert und abgefragt werden. Zudem sollte die Qualität und Richtigkeit der erhobenen Kennzahlen stichprobenartig im 4-Augen-Prinzip nachvollzogen werden.

Analyse und Bewertung der Kennzahlen

Die erhobenen Kennzahlen müssen zentral dokumentiert und auf Vollständigkeit überprüft werden. Sobald alle angeforderten Kennzahlen erhoben und zusammengefasst sind, kann der Status des BCMS zu einem spezifischen Zeitpunkt ermittelt werden, indem die Kennzahlen ausgewertet werden.

Die erhobenen Kennzahlen müssen mit den Zielwerten verglichen und Abweichungen identifiziert und bewertet werden. Darüber hinaus sollten Trends ermittelt werden.

Alle identifizierten Abweichungen müssen analysiert und bewertet werden. Hierzu sollte zum einen die Ursache identifiziert und zum anderen die Schwere der Abweichung bewertet werden. Zusätzlich ist es empfehlenswert, auch eindeutig negative Trends näher zu untersuchen. Grobe Abweichungen vom Zielwert können im anschließenden kontinuierlichen Verbesserungsprozess priorisiert behandelt werden. Identifizierte Ursachen helfen dabei, konkrete Korrektur- und Verbesserungsmaßnahmen abzuleiten.

Beispiel:

Kennzahl	BCM-Geschäftsprozess	Zielwert	Ist-Wert	Abweichung	Ursache	Schweregrad
Abdeckungsgrad der Geschäfts-prozesse gemäß Prozesslandkarte in der BIA	BIA	N = 100 %	95 %	Ja	Kürzlich zwei neue Geschäftsprozesse implementiert.	mittel
Abdeckungsgrad zeitkritischer Geschäftsprozesse in GFP	Notfallkonzept	N = 100 %	50 %	Ja	In mehreren OE sind keine BCM-Koordinatoren benannt.	hoch
Abdeckungsgrad zeitkritischer Geschäftsprozesse in der Übungsplanung	Notfallkonzept	N = 100 %	50 %	Nein	In mehreren OE sind keine BCM-Koordinatoren benannt.	hoch

Tabelle 71: Beispiel zur Priorisierung von Abweichungen

Hinweis:

Da anhand von Kennzahlen der Fortschritt oder der Erfüllungsgrad einer Anforderung oder eines gewünschten Zielzustands gemessen werden kann, sind sie auch ein geeignetes Mittel für Selbstüberprüfungen im BCMS. Insbesondere aus qualitativen Kennzahlen können Verbesserungspotenziale oder die Reife des BCMS abgeleitet werden.

6.12.2 Interne und externe Kontrollen

Das BCMS muss in regelmäßigen Abständen daraufhin kontrolliert werden, ob es angemessen, wirksam und anforderungsgerecht ist. Die Kontrolle kann anhand von Revisionen, Audits oder Selbstüberprüfungen erfolgen.

Hinweis:

Es besteht ein unterschiedliches Verständnis über die Bedeutung der Begriffe Audit und Revision. Der BSI-Standard 200-4 verwendet diese Begriffe wie folgt:

Ein **Audit** prüft gegen einen Standard zum Zwecke der Zertifizierung und wird daher in der Regel durch Externe durchgeführt.

Eine **Revision** prüft ebenfalls einen bestimmten Bereich mit einem festgelegten Vorgehen. Ziel der Revision ist dabei allerdings nicht die Zertifizierung, sondern nur die Ermittlung von Schwachstellen, Mängeln und Handlungsempfehlungen. Revisionen werden wie folgt unterschieden:

- Eine **externe Revision** wird durch Externe durchgeführt.
- Eine **interne Revision** wird durch Mitarbeiter der Institution durchgeführt.

Ferner kann eine **Selbsteinschätzung** zum BCMS, z. B. durch den BCMB selbst, erfolgen.

Audits

Audits des BCMS werden entweder freiwillig oder auf Grund der Anforderungen externer Interessensgruppen durch die Institution angefordert. In regulierten Branchen, wie z. B. im Banken- und Versicherungssektor, können Audits auch von Aufsichtsorganen initiiert werden. Mit der Durchführung von Audits werden in der Regel qualifizierte unabhängige Dritte, wie Wirtschaftsprüfer oder zugelassene Auditoren, beauftragt. Durch Audits wird festgestellt, ob das BCMS konform zu den Anforderungen anerkannter Standards ist. Die Methoden und die Vorgehensweise sind durch Vorgaben und Standards der Berufsverbände, wie beispielsweise des *Instituts der Wirtschaftsprüfer in Deutschland e.V. (IDW)* geregelt. Für selbst beauftragte Audits zum BCMS muss der BCMB zusammen mit der Institutionsleitung die Ziele und den Geltungsbereich abstimmen. Der Geltungsbereich muss sich nicht immer auf die gesamte Institution beziehen.

Externe Revisionen

Die externe Revision ist eine unabhängige Überprüfung, die von der Institutionsleitung beauftragt wird. Mögliche Gründe für eine externe Revision können aufsichtsrechtliche Anforderungen oder andere Anforderungen von Interessengruppen sein. In der externen Revision wird der aktuelle Zustand des BCMS bewertet, z. B. ob dieses hinsichtlich der Rahmenbedingungen und Ziele im BCM wirksam, aktuell, vollständig und angemessen ist.

Interne Revisionen

Interne Revisionen basieren auf einer unabhängigen Bewertung durch die Institution selbst. Sie sollte von Mitarbeitern durchgeführt werden, die weder an der Planung noch am Aufbau des BCMS beteiligt waren.

Die interne Revision muss die bestehenden Anforderungen an das BCMS widerspiegeln sowie ausgewählte BCM-Prozessschritte und Methoden des BCMS umfassen. Korrektur- und Verbesserungsmaßnahmen als Ergebnis vorangegangener Überprüfungen müssen als Grundlage einer aktuellen Kontrolle herangezogen werden. Interne Revisionen sollten jährlich geplant, durchgeführt und selbstkritisch ausgewertet werden. Audits sowie externe Revisionen können die jährliche interne Revision ersetzen.

Hinweis:

Weitergehende Informationen zur Methodik von Revisionen können unter anderem dem Kapitel 4.1.2 aus dem BSI-Dokument *Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz* entnommen werden (siehe [BSI4]).

Selbsteinschätzung (optional)

Der BCMB kann anhand von Selbsteinschätzungen (engl.: **Self-Assessments**) die korrekte Umsetzung der Vorgaben oder die Effizienz des BCMS überprüfen oder durch weitere Rollen im BCM überprüfen lassen. Dabei wird unter anderem kontrolliert, ob die BCM-Prozessschritte korrekt angewendet und die zur Verfügung gestellten Hilfsmittel und Dokumentenvorlagen eingesetzt werden. Hierbei können auch die Kennzahlen sehr hilfreich sein.

Die Selbsteinschätzung kann auch dabei helfen, die Reife des BCMS zu bestimmen und sich auf andere Kontrollen vorzubereiten. Bei einer Selbsteinschätzung obliegt es dem Untersuchenden selbst zu entscheiden wann und wie die aufgedeckten Mängel bzw. Korrekturbedarfe und Verbesserungsmöglichkeiten behandelt werden. Die Selbsteinschätzung ist im Standard-BCMS optional.

Vorbereitung von Revisionen und Audits

Da alle Kontrollen mit entsprechendem zeitlichem und personellem Aufwand verbunden sind, sollte der BCMB eine zeitliche Übersicht der verschiedenen, geplanten Kontrollen erstellen. Diese zeitliche Übersicht dient dazu, mögliche Engpässe der Mitarbeiter und Ressourcen feststellen und die notwendigen Vorarbeiten leisten zu können. In der zeitlichen Übersicht ist es hilfreich die folgenden Punkte zu dokumentieren

- Zeitplanung der angestrebten Audits und Revisionen
- Umfang der Audits und Revisionen (diese können einen Teilausschnitt des BCMS oder eine Gesamtüberprüfung betrachten)
- Fokus der Audits und Revisionen (Korrektur- und Verbesserungsmaßnahmen als Ergebnis vorangegangener Überprüfungen sollten als Grundlage einer aktuellen Überprüfung dienen)
- Ressourcenbedarf zur Unterstützung
- benötigte Dokumente und Informationen

Der BCMB sollte definieren, wie auf Revisions- und Audit-Ankündigungen angemessen und zielgerichtet reagiert werden kann und welche Dokumente und Informationen innerhalb einer Überprüfung bereitgestellt werden sollen. Der BCMB sollte die eigenen Aktivitäten im BCM auf die Revisions- und Audit-Termine abstimmen.

Zudem sollte der BCMB bei einer Revisionsanfrage die BCM-Rollenträger über die bevorstehende Überprüfung informieren und die Revisoren aktiv bei der Auswahl der Dokumente und Interviewpartner unterstützen. Für eine externe Revision sind folgende Aspekte relevant:

- aktuell gültige Dokumente des BCM
- Nachweise der Umsetzung und Ergebnisobjekte aller BCM-Prozess-Schritte
- aktueller Maßnahmenkatalog
- aktuell erhobene Kennzahlen
- frühere Ergebnisse von Kontrollen
- Nachweise geschlossener Abweichungen vorangegangener Kontrollen

Es kann hilfreich sein, die oben genannten Informationen, Dokumentationen, Verfahren und Ergebnisse in aktueller Version in einem ständigen Revisionsordner vorzuhalten. So können bei Audit- und Revisionsankündigungen die relevanten Informationen schnell zur Verfügung gestellt werden.

Nachbereitung von Revisionen und Audits

Im Anschluss an Audits und Revisionen werden Audit- bzw. Revisionsberichte erzeugt. Die darin festgestellten Abweichungen müssen aus Sicht der Institution eingeschätzt und entsprechende Korrekturbedarfe und Verbesserungsmöglichkeiten müssen abgeleitet werden. Analog zu den Vorgaben des vorangegangenen Kapitels (siehe Kapitel 6.12.1 *Überwachung, Messung, Analyse und Bewertung*) müssen die Ergebnisse, Abweichungen und daraus abgeleiteten Korrekturbedarfe und Verbesserungsmöglichkeiten für die Institutionsleitung aufbereitet und an diese kommuniziert werden.

Die Institution muss sicherstellen, dass festgestellte Mängel und Korrekturbedarfe des BCMS sowie deren Ursachen zeitnah untersucht und durch Korrekturmaßnahmen behandelt werden (siehe Kapitel 6.13 *Korrektur und Verbesserung des BCMS*). Zusätzlich muss geprüft werden, ob ähnliche Abweichungen bereits aufgetreten sind oder auftreten könnten.

Hinweis:

Um die Ursachen einer Abweichung strukturiert identifizieren zu können, können die zuständigen Stellen eine Reihe möglicher Methoden einsetzen. Dazu gehören beispielsweise die Fehler-Ursachen-Analyse, das Fischgräten- oder auch sogenannte Ishikawa-Modell sowie das Multiple Cause Diagram.

6.12.3 Prüfung durch die Institutionsleitung (Managementbewertung)

Der BCMB sollte die Institutionsleitung regelmäßig über den Status des BCMS informieren. Der BCMB sollte dafür die Ergebnisse der Leistungsüberprüfung zielgruppengerecht aufbereiten und die notwendigen Handlungsbedarfe seitens der Institutionsleitung konkret kommunizieren.

Anhand des Status des BCMS kann die Institutionsleitung den Entwicklungsstand des BCMS nachvollziehen, Fehlentwicklungen identifizieren und die eigenen Ziele kritisch hinterfragen. Je nach Einschätzung der Ergebnisse kann es erforderlich sein, dass die Institutionsleitung strategische oder taktische Entscheidungen treffen muss, um eine Neuausrichtung des BCMS zu erreichen und Fehlentwicklungen entgegenzuwirken. Hierzu müssen folgende Punkte adressiert werden (angelehnt an ISO 22301):

- Status von Maßnahmen aus dem vorangegangenen BCMS-Zyklus oder aus den Entscheidungen der Institutionsleitung
- interne und externe Veränderungen des Umfeldes des BCMS
- identifizierte Abweichungen und Trends aus Nicht-Konformitäten (non-conformities), Kontrollen (siehe Kapitel: 6.12.1 Überwachung, Messung, Analyse und Bewertung) und internen und externen Überprüfungen (siehe Kapitel: 6.12.2 Interne und externe Überprüfungen)
- Rückmeldungen von Interessengruppen zum BCMS
- Bewertung der Angemessenheit der Leitlinie und der Ziele des BCMS
- Verfahren und Ressourcen, um die Effektivität oder Effizienz des BCMS zu steigern
- Ergebnisse der Business Impact Analyse und BCM-Risikoanalyse
- Ergebnisse der Dokumentenüberprüfung (siehe Kapitel 6.2 *Dokumentation im Standard-BCMS*)
- Unzureichend abgesicherte Risiken vorangegangener BCM-Risikoanalysen
- Erkenntnisse aus Störungen mit Notfallpotenzial und eingetretenen Notfällen sowie
- Chancen zur Verbesserung

Der BCMB sollte mit der Institutionsleitung vereinbaren, wie häufig der Status zum BCMS berichtet werden soll. Die Institutionsleitung kann entscheiden, ob der BCMB neben dem BCM-Bericht weitere zyklische Berichte oder Ad-hoc-Berichte bereitstellen soll.

Basierend auf dem Status zum BCMS muss die Institutionsleitung regelmäßig überprüfen, inwieweit das BCMS geeignet, angemessen und effektiv ist. Hierzu muss die Institutionsleitung mindestens folgende Punkte berücksichtigen:

- Notwendige Änderungen des Geltungsbereichs des BCMS
- Korrekturbedarfe und Verbesserungsmöglichkeiten der Analyse-Methoden des BCMS, der BC-Strategien und –Lösungen sowie der Notfallpläne

- Korrekturbedarfe und Verbesserungsmöglichkeiten an Verfahren und Kontrollen, auf Grund interner oder externer Anforderungen
- Korrekturbedarfe und Verbesserungsmöglichkeiten an der Leistungsüberprüfung um deren Effizienz und Effektivität zu steigern

Die Ergebnisse der Prüfung durch die Institutionsleitung müssen dokumentiert und den relevanten internen und externen Interessengruppen kommuniziert werden. Grundlage bilden die in der Planung und Konzeption identifizierten Interessengruppen (siehe Kapitel 6.1.1 *Identifizierung von Anforderungen an das BCMS)* sowie die festgelegten Informationsansprüche (siehe Kapitel 6.2.1 *Festlegung von Dokumenteninformationen*).

Hinweis:

Auch wenn ein Bericht zum Gesamtstatus des BCMS immer nur eine Momentaufnahme darstellt, können über einen zeitlichen Verlauf hinweg, Trends und Entwicklungen daraus abgeleitet werden. Insbesondere wenn die Veränderungen gegenüber dem vorherigen Bericht herausgestellt werden, kann die Reife des BCMS konkreter eingeschätzt und Verbesserungen kenntlich gemacht werden.

6.13 Korrektur und Verbesserung des BCMS

Anhand der identifizierten Korrekturbedarfe und Verbesserungsmöglichkeiten sollten im Rahmen der **Korrektur und Verbesserung des BCMS** konkrete Maßnahmen entwickelt und umgesetzt werden:

- **Korrekturmaßnahmen** dienen dazu, Abweichungen des Managementsystems und der Notfallplanung zu den identifizierten Anforderungen an das BCMS zu korrigieren. Sofern erforderlich können über Korrekturmaßnahmen auch innerhalb des BCMS definierte Anforderungen korrigiert werden.
- **Verbesserungsmaßnahmen** dienen dazu, das BCMS sowie einzelne bauliche, technische oder organisatorische Maßnahmen zu verbessern.

Hinweis:

Die Korrektur und Verbesserung des BCMS obliegt nicht ausschließlich dem BCMB, sondern ist Aufgabe vieler verschiedener Rollen im BCMS. So muss etwa die Institutionsleitung ihrerseits Korrekturbedarfe und Verbesserungsmöglichkeiten auf strategischer Ebene identifizieren und durch Neuausrichtung der Ziele und Rahmenbedingungen des BCMS behandeln.

Die Korrektur und Verbesserung des BCMS erfolgt nicht in einem zeitlich abgeschlossenen Zeitraum. Das BCMS zu korrigieren und zu verbessern ist vielmehr ein Aspekt, der stetig und zu jeder Zeit in allen Phasen des PDCA-Zyklus` mitberücksichtigt und forciert werden muss. Nur so kann gewährleistet werden, dass kurzfristig auf Abweichungen und Verbesserungsmaßnahmen, sowie auf veränderte Rahmenbedingungen reagiert werden kann. Dies stellt wiederum sicher, dass die BCM-Prozessschritte sowie die Notfallplanung stets den geltenden Anforderungen entsprechen.

Sofern über einen längeren Zeitraum oder aus einzelnen BCM-Prozessschritten keine neuen Korrektur- oder Verbesserungsmaßnahmen identifiziert und in den BCM-Maßnahmenplan aufgenommen werden, kann dies einen stagnierenden Reifegrad des BCMS bedeuten. Dies gilt selbst für vermeintlich ausgereifte BCMS, da sich die internen und externen Rahmenbedingungen des BCMS erfahrungsgemäß stetig weiterentwickeln und so auch das BCMS regelmäßig angepasst werden muss. Der BCMB muss daher stetig prüfen, ob erkannte Abweichungen dokumentiert, korrigiert und Verbesserungsmöglichkeiten in das BCMS überführt werden und gegebenenfalls die Korrektur und Verbesserung des BCMS weiter intensivieren.

Die folgende Abbildung gibt einen Überblick über das Vorgehen zur Korrektur und Verbesserung des BCMS.

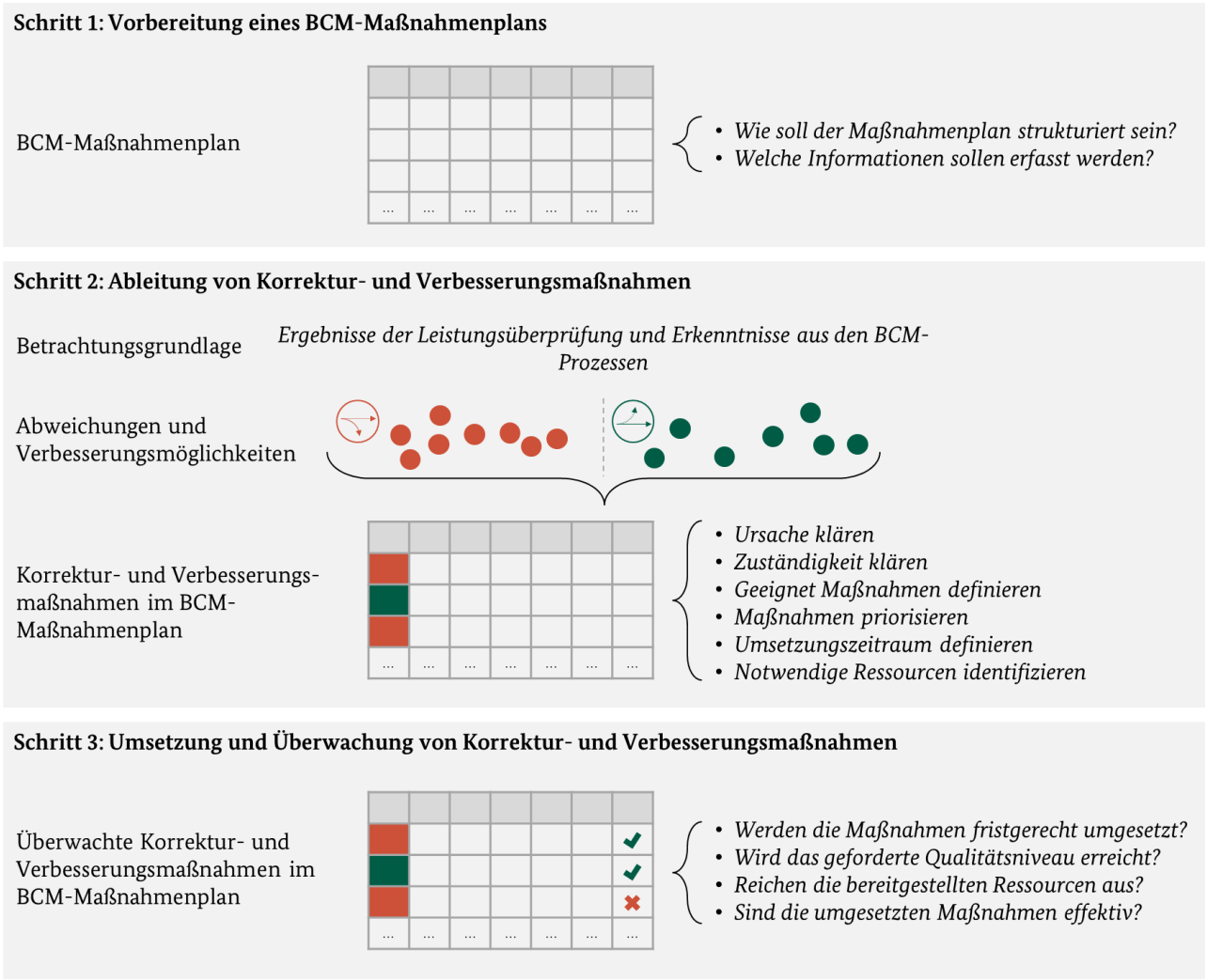

Abbildung 68: BCM-Prozessschritte zur Korrektur und Verbesserung des BCMS

Um Korrektur- und Verbesserungsmaßnahmen des BCMS zu dokumentieren und nachzuhalten, kann die Dokumentenvorlage *BCM-Maßnahmenplan* aus den Hilfsmitteln verwendet werden.

Synergiepotenzial:

Die Korrektur und Verbesserung ist ein Teilprozess eines jeden zyklischen Managementsystems. Vor diesem Hintergrund können im Rahmen weiterer Managementsysteme der Institution, wie etwa einem Qualitätsmanagementsystem, ISMS oder Datenschutzmanagementsystem, bereits bestehende Vorgehensweisen sowie Tools zur Korrektur und Verbesserung des jeweiligen Managementsystems bestehen. Sollte dies der Fall sein, kann einerseits die bestehende Vorgehensweise für das BCMS adaptiert werden. Andererseits können identifizierte Korrektur- und Verbesserungsmaßnahmen der verschiedenen Managementsysteme auch aufeinander abgestimmt werden. Dies bietet sich etwa an, wenn Korrektur- oder Verbesserungsmaßnahmen auch anderen Managementsystemen zugutekommen.

6.13.1 Vorbereitung eines BCM-Maßnahmenplans

Um den Gesamtüberblick über alle Korrektur- und Verbesserungsmaßnahmen zu behalten und diese leichter steuern zu können, sollte der BCMB eine Dokumentenvorlage für einen BCM-Maßnahmenplan vorbereiten und nutzen. Die wesentlichen Inhalte eines BCM-Maßnahmenplans werden im folgenden Beispiel veranschaulicht und im Kapitel 6.13.2 *Ableitung von Korrektur- und Verbesserungsmaßnahmen* näher beschrieben.

Falls nicht das Hilfsmittel Dokumentenvorlage *BCM-Maßnahmenplan* benutzt wird, sollten die aufgeführten Punkte in der Dokumentenvorlage berücksichtigt werden:

Beispiel:

Eindeutige Kennung der Maßnahme	**BCM-Korrektur-0001a**	**BCM-Korrektur-0001b**
Korrekturbedarf oder Verbesserungsbedarf	Im Rahmen der durchgeführten Übungen und Tests wurde festgestellt, dass die Geschäftsfortführungspläne der Organisationseinheiten Bürgerbüro und IT-Help Desk weder vollständig noch aktuell waren. So fehlten zeitkritische Ressourcen aus dem Soll-Ist-Vergleich und es wurde auf nicht länger bestehende Dokumente verwiesen.	Siehe BCM-Korrektur-0001a Mitarbeiter sind nicht in die Bearbeitung von Geschäftsfortführungsplänen eingewiesen worden.
Ursache	Grund für die BCM-Korrektur-0001a ist, dass die zuständigen Mitarbeiter nicht in die Bearbeitung von Geschäftsfortführungsplänen eingewiesen worden sind.	Ursache hierfür ist, dass diese Mitarbeiter sich nicht im Schulungs- und Sensibilisierungsplan befanden. Grund hierfür ist, dass diese dem BCMB nicht als neue Mitarbeiter gemeldet wurden. Mit der Organisationseinheit Personal wurde bislang kein Meldeprozess definiert für den Fall, dass Mitarbeiter die Organisationseinheit wechseln oder die Institution verlassen.
Vorgesehene Korrektur- oder Verbesserungsmaßnahme	Zur kurzfristigen Behandlung der Abweichung werden die Geschäftsfortführungspläne gemeinsam mit den BCMK aktualisiert und im Rahmen einer Planbesprechung erneut geübt. (Maßnahmen zur langfristigen Behandlung siehe BCM-Korrektur-0001b)	Um die Abweichung langfristig abzustellen, soll der Prozess für Mitarbeiterwechsel und Benennung von BCM-Rollenträgern gemeinsam mit der Organisationseinheit Personal überarbeitet und entsprechende Kontrollmechanismen entwickelt werden.
Zuständige Stelle(n)	BCMB, BCMK	Organisationseinheit Personal
Festgelegte Priorität	**Hoch** – ~~Mittel~~ – ~~Gering~~	~~Hoch~~ – **Mittel** – ~~Gering~~
Geplanter Fertigstellungstermin	16.08.2020 (Heute + 2 Wochen)	31.12.2020
Notwendige Ressourcen	Verfügbarkeit der zuständigen BCMK und der zuständigen Mitarbeiter	Verfügbarkeit der Mitarbeiter der Organisationseinheit Personal
Umsetzungsstatus	~~Offen~~ – ~~in Umsetzung~~ – **abgeschlossen** –	**Offen** – ~~in Umsetzung~~ – ~~abgeschlossen~~ – ~~abgeschlossen und Wirksamkeit geprüft~~

Eindeutige Kennung der Maßnahme	BCM-Korrektur-0001a	BCM-Korrektur-0001b
	~~abgeschlossen und Wirksamkeit geprüft~~	
Umsetzungsdetails	01.08.: Maßnahme freigegeben durch BCMB 14.08.: GFP wurden aktualisiert.	01.08.: Maßnahme freigegeben durch BCMB

Tabelle 72: Struktur des BCM-Maßnahmenplans am Beispiel einer fiktiven Abweichung

6.13.2 Ableitung von Korrektur- und Verbesserungsmaßnahmen

Anhand des BCM-Maßnahmenplans sollte der BCMB alle Korrektur- und Verbesserungsmaßnahmen dokumentieren und steuern. Der BCMB muss den Umsetzungsstatus der Maßnahmen überwachen und umgesetzte Maßnahmen dahingehend prüfen, ob diese wirksam sind. Um die Korrektur- oder Verbesserungsmaßnahmen erfolgreich planen und umsetzen zu können, müssen die folgenden Inhalte pro Maßnahme ermittelt und dokumentiert werden:

- Beschreibung des Korrekturbedarfs bzw. der Verbesserungsmöglichkeit
- Beschreibung der Ursache des Korrekturbedarfs bzw. der Verbesserungsmöglichkeit
- Beschreibung der Korrektur- oder Verbesserungsmaßnahmen, die angemessen und dazu geeignet sind, die Korrekturbedarfe bzw. der Verbesserungsmöglichkeiten umzusetzen
- Fertigstellungstermin der Korrektur- oder Verbesserungsmaßnahmen
- Umsetzungsstatus der Korrektur- oder Verbesserungsmaßnahme(n)
- Für die Umsetzung zuständige Stellen

Ferner ist es empfehlenswert, die folgenden Inhalte im Maßnahmenplan zusätzlich zu dokumentieren.

- Eindeutige Kennung der Korrektur- oder Verbesserungsmaßnahmen
- Priorisierung der Maßnahme
- Notwendige Ressourcen (finanziell, personell und zeitlich)
- Dokumentation relevanter Umsetzungsdetails

Hinweis:

Üblicherweise behandeln Korrektur- und Verbesserungsmaßnahmen einzelne Teilprozesse des BCMS sowie der Notfallplanung. Bei taktischen oder strategischen Korrektur- und Verbesserungsmaßnahmen kann es jedoch notwendig sein, grundsätzlich zurück in die Initiierungsphase des BCMS zu gehen, da die Korrektur- oder Verbesserungsmaßnahmen sich auch auf alle weiteren Teilprozesse des BCMS auswirken können. Dies kann etwa der Fall sein, wenn im Rahmen der Maßnahmen die Rahmenbedingungen und Ziele des BCMS neu definiert werden müssen.

6.13.3 Umsetzung und Überwachung von Korrektur- und Verbesserungsmaßnahmen

Nachdem die Korrektur- oder Verbesserungsmaßnahmen geplant und dokumentiert wurden, müssen diese durch die jeweils zuständigen Stellen freigegeben und umgesetzt werden. Der BCMB sollte den Umsetzungsstatus regelmäßig überwachen, um Fehlentwicklungen in Bezug auf die Qualität oder den geplanten Fertigstellungstermin frühzeitig erkennen und diesen entgegenwirken zu können.

Nachdem die jeweiligen Korrektur- und Verbesserungsmaßnahmen umgesetzt wurden, sollte der BCMB diese in der CHECK-Phase des BCMS dahingehend untersuchen, ob sie angemessen und wirksam sind. Das Ergebnis der Untersuchung sollte der BCMB anschließend im Maßnahmenplan dokumentieren. Wenn das Ergebnis der Untersuchung zeigt, dass die umgesetzten Korrektur- und Verbesserungsmaßnahmen nicht wirksam sind, sollten erneute Korrektur- und Verbesserungsmaßnahmen geplant und umgesetzt werden.

7 BCM im Rahmen des Outsourcings und von Lieferketten

Wie in Kapitel 2.4.4 *BCM und Outsourcing sowie Lieferketten* erläutert, kann der Einsatz von Dienstleistern vielseitige Vorteile mit sich bringen. Zugleich ist deren Einsatz aber auch mit Risiken verbunden. Minderleistungen des Dienstleisters oder in der Lieferkette wirken sich in der Regel unmittelbar auf die Institution aus. Ein Beispiel hierfür ist ein Reputationsverlust, da aus Sicht der Interessengruppen die eigene Institution oftmals weiterhin als direkter Leistungserbringer wahrgenommen wird. Für die Interessengruppen ist es dabei oftmals unerheblich, ob die Minderleistung auf die Versäumnisse eines Dritten zurückzuführen ist. Die geringere Möglichkeit, Leistungsqualität zu beeinflussen, wird umso gravierender, wenn Aktivitäten in zeitkritischen Geschäftsprozessen extern erbracht werden oder externe Güter benötigt werden, um den Geschäftsprozess ausführen zu können. Abbildung 69 gibt eine Übersicht, welche BCM-Aspekte im Rahmen des Outsourcings und bei Lieferketten berücksichtigt werden sollten. Diese werden im Folgenden beschrieben.

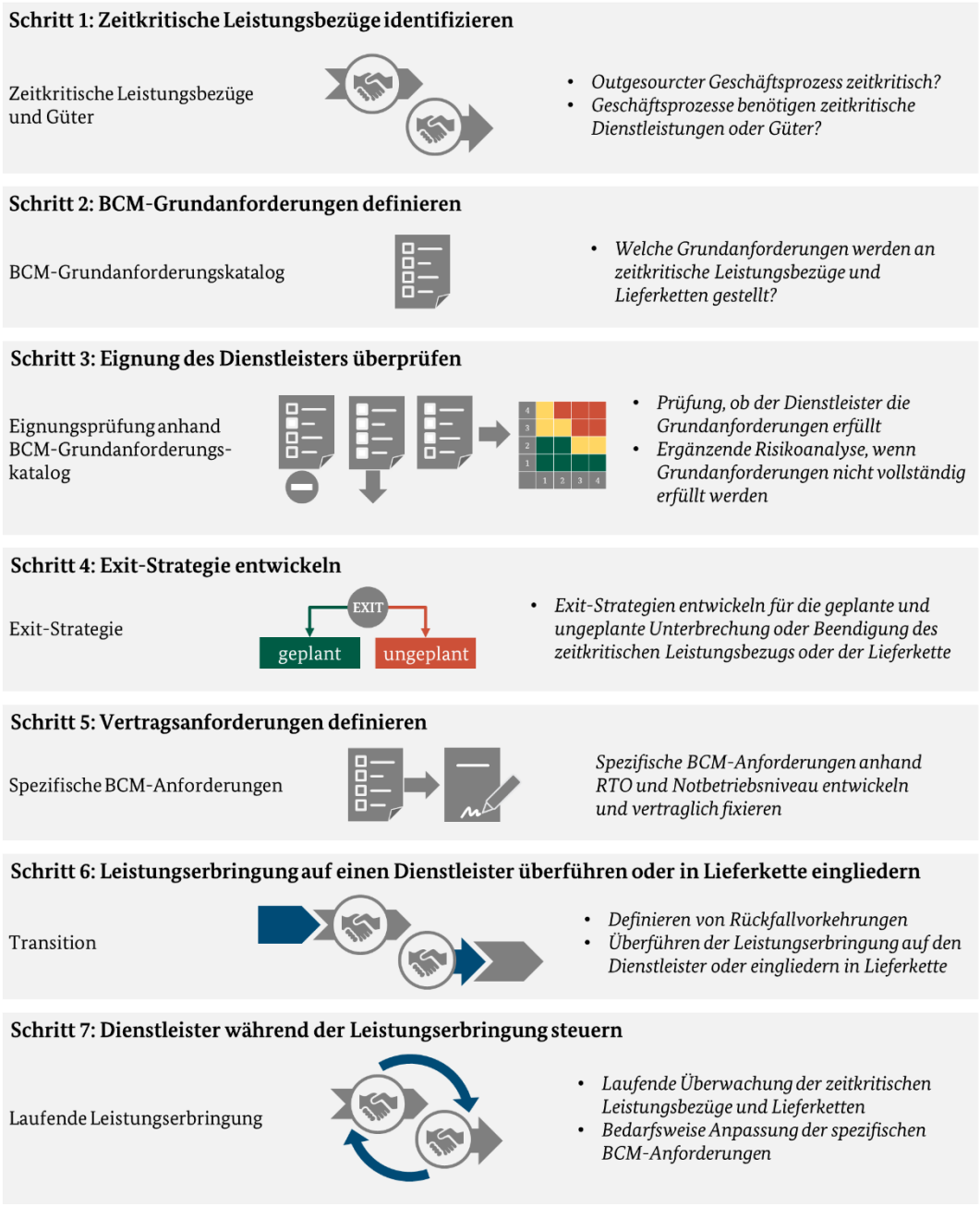

Abbildung 69: BCM-Prozessschritte für BCM im Outsourcing und in Lieferketten

Je nach vertraglichen Möglichkeiten sollten die genannten Schritte auch für die bereits etablierten Dienstleister durchgeführt werden. Die genannten Tätigkeiten unterstützen die Institution darin, sicherzustellen, dass der Dienstleister einen ebensolchen unterbrechungsfreien Geschäftsbetrieb gewährleistet, wie die Institution selbst.

7.1 Identifizierung zeitkritischer Leistungsbezüge

Sobald BCM-Anforderungen an einen Leistungsbezug gestellt werden, ist dies mit einem Aufwand auf Seiten des Dienstleisters verbunden. Dieser wird in der Regel die Kosten dafür mit in die Leistung einrechnen. Als Folge erhöhen sich die Kosten für die beauftragende Institution. Für diese entsteht zudem ein Kontroll- und Steuerungsaufwand. Aus diesem Grund sollten BCM-Anforderungen als wesentlicher Kostenfaktor bei einem zeitkritischen Leistungsbezug berücksichtigt werden und nur dann an einen Leistungsbezug gestellt werden, wenn dies in einem angemessenen Verhältnis zu dem tatsächlichen Risiko steht.

Primär wird dieses Risiko daraus abgeleitet, ob der Leistungsbezug für den Notbetrieb eines zeitkritischen Geschäftsprozesses relevant ist und damit eine RTO vorliegt. Falls der betroffene Geschäftsprozess zum Zeitpunkt der Prüfung noch nicht im Rahmen einer aktuellen BIA berücksichtigt wurde, sollte der Prozesseigentümer sicherstellen, dass die BIA vor Vertragsabschluss durchgeführt oder aktualisiert wurde.

Hinweis:

Sofern zum Vertragsabschluss keine aktuellen BIA-Ergebnisse vorliegen, besteht das Risiko, dass Verträge nicht den aktuellen BCM-Anforderungen der Institution entsprechen. Dadurch könnten weitere Kosten aufgrund von nachträglichen Vertragsanpassungen entstehen, da der Dienstleister die BCM-Anforderungen als zusätzliche Leistung interpretieren könnte. Im schlechtesten Fall können Verträge zu einem späteren Zeitpunkt nicht mehr angepasst werden, da der Institution die rechtliche Grundlage fehlt, um den Dienstleister auf angemessene präventive und reaktive Maßnahmen im BCM verpflichten zu können.

7.2 Definition von BCM-Grundanforderungen

Für den möglichen Fall, dass zeitkritische Leistungen bezogen werden sollen, muss der BCMB BCM-Anforderungen definieren, die bei der Dienstleisterauswahl berücksichtigt werden müssen.

Um die Anzahl der potentiellen Dienstleister sinnvoll einzuschränken, muss zunächst überprüft werden, inwieweit diese überhaupt über die notwendigen Voraussetzungen verfügen, um angemessen auf Notfälle reagieren zu können. Hierzu sollte ein Grundanforderungskatalog erstellt werden. Dabei kann auf das Hilfsmittel *Grundanforderungskatalog BCM* oder Informationen vergleichbarer einschlägiger Regelwerke, wie z. B. den ISO-Standard 22318 (siehe [22318]), zurückgegriffen werden.

Beispiele für BCM-Grundanforderungen

- Die Rollen für das BCM sind beim Dienstleister angemessen festgelegt, z. B. in Form eines zentralen BCMB und dezentraler BCM-Koordinatoren.
- Zeitkritische Geschäftsprozesse und Ressourcen, die die zeitkritische Leistung betreffen, werden regelmäßig identifiziert und analysiert, z. B. mittels einer BIA.
- Es sind Notfallpläne und Maßnahmen für die zeitkritische Leistung implementiert, die eine effektive Notfallbewältigung und einen schnellen Wiederanlauf ermöglichen.
- Eine Übungsplanung ist beim Dienstleister vorhanden und wird aktiv angewendet, sodass alle wesentlichen Pläne und Maßnahmen des BCM regelmäßig und anlassbezogen geübt werden.

7.3 Überprüfung der Eignung des Dienstleisters

Jeder Dienstleister, der für einen zeitkritischen Leistungsbezug in Betracht gezogen wird, muss im Vorfeld der Vertragsgestaltung auf seine BCM-Fähigkeit anhand des BCM-Grundanforderungskatalogs überprüft werden. Damit soll vermieden werden, dass grundsätzlich ungeeignete Dienstleister im Rahmen der Dienstleisterauswahl näher betrachtet werden. Im Zuge dessen sollten angemessene Evidenzen geprüft werden. Als solche können beispielsweise Zertifikate, eine BCM-Leitlinie, ein Notfallkonzept, Geschäftsfortführungs- und Wiederanlaufpläne sowie schriftliche Nachweise in Form von Übungs- und Testprotokollen herangezogen werden. Sofern ein Dienstleister ausgewählt wird, der sich auf Basis der Überprüfung als ungeeignet erweist oder dessen Eignung nicht ausreichend festgestellt werden kann, sollten die damit verbundenen Risiken analysiert und angemessene Risikobehandlungsmaßnahmen abgeleitet werden.

7.4 Entwicklung einer Exit-Strategie

Für zeitkritische Leistungsbezüge sollte eine angemessene Exit-Strategie entwickelt werden. Diese sollte sowohl die geplante als auch die ungeplante Beendigung des Leistungsbezugs berücksichtigen. Inhaltlich muss diese Exit-Strategie dabei für jeden Leistungsbezug individuell definiert werden.

Hinweis:

Die bereits festgelegten BC-Strategien und -Lösungen für zeitkritische Dienstleister zielen primär darauf ab, eine ungeplante aber temporäre Unterbrechung des Dienstleisters zu behandeln. Eine Exit-Strategie korrespondiert mit den festgelegten BC-Strategien und –Lösungen, deckt aber zusätzlich auch den Fall ab, dass der Dienstleister seine Leistung dauerhaft nicht mehr erbringen wird (z. B. im Falle eines Konkurses).

Eine Exit-Strategie im Outsourcing und bei Lieferketten kann die folgende Fragestellung thematisieren:

1. **Zu welchen Dienstleistern können die Aktivitäten und Geschäftsprozesse bei Bedarf verlagert werden und auf welche Weise kann dies erfolgen?**

   Bzw.

2. **Auf welche Weise können die benötigten Güter in erforderlicher Zeit, Qualität und Quantität bei Bedarf durch einen anderen Dienstleister geliefert werden?**

   In diesem Zusammenhang können mögliche Ersatzdienstleister identifiziert werden, die ebenfalls geeignet sind, die avisierten Leistungen zu erbringen und zugleich den BCM-Anforderungen der Institution entsprechen. Dabei kann es sinnvoll sein, vertragliche Vereinbarungen mit geeigneten Ersatzdienstleistern zu schließen, um deren kurzfristigen Einsatz auch im Falle einer ungeplanten Beendigung des Leistungsbezugs zu gewährleisten.

   Das Ausfallrisiko einer Geschäftsunterbrechung in Folge fehlender Güter kann insbesondere dadurch reduziert werden, indem ein bestimmtes Gut parallel von verschiedenen Dienstleistern bezogen wird. Da diese BC-Strategie jedoch in der Praxis mit einem Effizienzverlust sowie erhöhten Kosten im Normalbetrieb verbunden ist, ist es empfehlenswert, den Nutzen der BC-Maßnahmen dem Ausfallrisiko und den Kosten gegenüberzustellen.

Eine weitere Exit-Strategie im Fall von Outsourcing kann die folgende Fragestellung thematisieren:

- **Auf welche Weise können die zu erbringenden Aktivitäten und Geschäftsprozesse wieder selbst durch die Institution durchgeführt werden?**

Bei einer geplanten Beendigung des Leistungsbezugs kann dies z. B. mit Hilfe von vertraglich vereinbarten Transferleistungen des Dienstleisters erfolgen. Darüber hinaus kann die Institution benötigte Ressourcen und benötigtes Know-how für die betroffenen Tätigkeiten weiterhin intern vorhalten. Im Falle einer ungeplanten Beendigung können diese dann kurzfristig abgerufen werden.

7.5 Definition von Vertragsanforderungen

Im Vorfeld der Vertragsgestaltung sollten die zuvor definierten BCM-Grundanforderungen in Form von spezifischen BCM-Anforderungen konkretisiert werden. Hierbei sollten die konkreten Verfügbarkeitsanforderungen (RTO und Notbetriebsniveau gemäß BIA) für den jeweiligen Leistungsbezug ergänzt werden. Um zielgerichtete BCM-Vertragsanforderungen zu definieren, kann die Anzahl, der Umfang und der Detailgrad der spezifischen BCM-Anforderungen von dem potenziellen Schaden einer Minderleistung des Dienstleisters abgeleitet werden.

Beispiel:

Zusätzlich zu den Verfügbarkeitsanforderungen im Normalbetrieb (siehe Service Level und Reaktionszeit bei Störungen), gelten die folgenden Anforderungen an das BCM:

- Bei Ausfall des Service muss, ungeachtet der Wiederherstellungszeit, ein Wiederanlauf auf dem definierten Notbetriebsniveau binnen 24 Stunden erfolgen (RTO).
- Der Nachweis, dass die geforderte Wiederanlaufzeit erreicht werden kann, muss durch Übungen und Tests mindestens jährlich erbracht werden.
- Die Planung von Übungen und Tests muss dokumentiert werden.
- Alle Übungen und Tests müssen auf mögliche Korrekturbedarfe und Verbesserungsmöglichkeiten untersucht werden.
- Abgebrochene oder abgesagte Übungen und Tests sowie Übungen und Tests, in denen das festgelegte Ziel nicht erreicht wurde, müssen zeitnah wiederholt bzw. neu geplant werden.
- Die Ergebnisse durchgeführter Übungen und Tests sowie daraus abgeleiteter Maßnahmen müssen dem Auftraggeber im Rahmen eines Gesamtberichts einmal jährlich zur Verfügung gestellt werden.

Auf diese Weise kann eine angemessene Verhältnismäßigkeit zwischen dem potentiellen Schaden und den spezifischen BCM-Anforderungen sowie dem damit verbundenen Kontroll- und Steuerungsaufwand gewährleistet werden. Alle BCM-Anforderungen müssen für jeden zeitkritischen Leistungsbezug vertraglich festgehalten werden. Auf diese Weise wird der Dienstleister dazu verpflichtet, die Anforderungen umzusetzen und die Institution ist in der Lage, den Dienstleister zu kontrollieren und zu steuern.

Beispiel:

Die folgenden Tätigkeiten sind bezüglich der Vertragsgestaltung von besonderer Relevanz:

- Ansprechpartner und Kontaktpersonen für den Normalbetrieb sowie für den Notfall festlegen.
- Definitionen abstimmen, z. B. Störung, Notfall, Krise.
- Bedeutung einschlägiger Begriffe klären, z. B. MTPD, RTO und RPO.
- Melde- und Eskalationswege sowie Schwellenwerte und meldepflichtige Ereignisse festlegen.
- Rechte und Pflichten beider Vertragsparteien vor, während und nach einem Notfall vereinbaren.
- Kontroll- und Weisungsrechte der Institution gegenüber dem Dienstleister festlegen.
- Berichtspflichten des Dienstleisters vereinbaren.

- Spezifische Anforderungen festlegen, z. B. Zusicherung einer bestimmten RTO innerhalb der üblichen Geschäftszeiten und je nach Bedarf inklusive Wochenenden, Feiertagen, über Nacht etc.
- Spezifische Maßnahmen vereinbaren, z. B. Art und Häufigkeit von Übungen und Tests mit oder ohne Beteiligung der beauftragenden Institution sowie Audits und Überprüfungen.

Um die Steuerung des Dienstleisters sowie das Berichtswesen im Normalbetrieb zu vereinfachen, ist es empfehlenswert, KPIs festzulegen (siehe Kapitel 6.12.1 *Überwachung, Messung, Analyse und Bewertung*). Diese sollten durch die Dienstleistersteuerung bzw. die Rechtsabteilung vertraglich fixiert werden. In diesem Zusammenhang kann z. B. gemessen werden, inwieweit die für die Leistungserbringung relevanten Geschäftsprozesse des Dienstleisters regelmäßig in der BIA berücksichtigt, geplante Übungen und Tests erfolgreich durchgeführt oder präventive und reaktive BCM-Dokumente aktuell gehalten werden.

7.6 Einbindung des Dienstleisters

Nachdem die Vertragsgestaltung abgeschlossen ist, kann die Leistungserbringung für die vereinbarten Tätigkeiten auf den Dienstleister überführt bzw. der Dienstleister in die Lieferkette integriert werden. Die Leistungserbringung verlässt in diesem Moment ganz oder teilweise den direkten Einflussbereich der Institution. Dies beschränkt mitunter auch die Möglichkeiten der Institution, adäquate Notfallmaßnahmen zu ergreifen, sobald die Leistungsüberführung gestört oder unterbrochen wird. Insbesondere wenn IT-Geschäftsprozesse überführt werden, ist diese Überführungs- oder Integrationsphase daher oftmals mit erheblichen Risiken für den stabilen Geschäftsbetrieb verbunden. Es sollten daher im BCM angemessene Vorkehrungen getroffen werden, die einen unterbrechungsfreien Ablauf der Überführungs- oder Integrationsphase unterstützen. In diesem Zusammenhang kann es sinnvoll sein, Rückfallvorkehrungen (engl. Fallback) zu schaffen, um Störungen oder Ausfälle kompensieren zu können.

Beispiel:

Die Rückfallvorkehrung im Outsourcing kann z. B. in Form eines temporären Parallelbetriebes erfolgen, der durch die Institution selbst sichergestellt wird, bis eine stabile Leistungserbringung durch den Dienstleister gewährleistet werden kann. Soll ein neuer Dienstleister in eine Lieferkette integriert werden, kann eine Zeit lang das bisherige Dienstleistungsverhältnis fortgeführt werden, bis der neue Dienstleister die erforderliche Leistungsqualität und –quantität ausreichend sicherstellen kann.

Die BCM-Maßnahmen, die für die Rückfallvorkehrung benötigt werden, und die dafür benötigten Ressourcen sollten im Vorfeld festgelegt und dokumentiert werden, bevor der Dienstleister eingebunden wird. Sowohl auf Seiten der Institution als auch auf Seiten des Dienstleisters sollten klare Verantwortlichkeiten definiert und zuständige Ansprechpartner genannt werden. Im Zuge der Einbindung des Dienstleisters ist es empfehlenswert, wenn sich beide Seiten stetig über aktuelle Fortschritte und eventuelle Komplikationen informieren.

7.7 Steuerung des Dienstleisters

Es sollte sichergestellt werden, dass die vertraglich festgelegten BCM-Anforderungen über den gesamten Zeitraum der Leistungserbringung durch den Dienstleister erfüllt werden. Andernfalls kann nicht gewährleistet werden, dass der Dienstleister im Falle einer Unterbrechung des Geschäftsbetriebes in der Lage ist, negative Auswirkungen auf die Institution möglichst gering zu halten bzw. zu vermeiden.

Mittels der zuvor definierten KPIs und regelmäßiger Dienstleisterberichte kann effizient kontrolliert werden, inwieweit der Dienstleister die an ihn gestellten BCM-Anforderungen erfüllt. Darüber hinaus sollte jeder zeitkritische Dienstleister risikobasiert, z. B. abhängig von der RTO, oder anlassbezogen kontrolliert werden. Hierzu kann gegebenenfalls auf die vertraglich zugesicherten Kontrollrechte zurückgegriffen werden. Zu den

üblichen Kontrollen zählen beispielsweise Dokumentenprüfungen, Vor-Ort-Audits und Revisionen in den Räumlichkeiten des Dienstleisters oder gemeinsam durchgeführte Übungen.

Die Tätigkeiten während der Leistungserbringung sollten nicht allein darauf beschränkt werden, dass der Dienstleister kontrolliert wird. Vielmehr ist es empfehlenswert, wenn ein kontinuierlicher Informationsaustausch zwischen den vertraglich festgelegten Kontaktpersonen erfolgt, z. B. durch regelmäßige Gremientreffen. Ziel dieses Informationsaustauschs ist es, eine anforderungsgerechte Leistungserbringung zu gewährleisten, indem z. B. veränderte Einflussfaktoren rechtzeitig kommuniziert werden und die Zusammenarbeit zwischen der Institution und dem Dienstleister nachhaltig gestärkt und optimiert wird.

Während des gesamten Leistungszeitraums können sich die Rahmenbedingungen und Einflussfaktoren verändern. Daher sollten auch die BCM-Anforderungen an den Dienstleister regelmäßig kontrolliert und bei Bedarf angepasst werden. Sofern sich BCM-Anforderungen verändern, sollte überprüft werden, inwieweit auch die betroffenen vertraglichen Vereinbarungen angepasst werden können, um der veränderten Risikolage gerecht zu werden. Hierbei ist es empfehlenswert, abzuwägen, ob der wirtschaftliche Mehraufwand in einem angemessenen Verhältnis zu dem bestehenden Risiko steht.

8 Anhang A: Anforderungskatalog

Die Anforderungsliste wird innerhalb der Community-Draft-Phase online auf der Website des BSI zur Verfügung gestellt.

9 Anhang B: Hinweise zu den Hilfsmitteln

Das BSI bietet ergänzend zum BSI-Standard 200-4 verschiedene Hilfsmittel und Dokumentenvorlagen an, die den Anwender darin unterstützen sollen, die beschriebenen Prozesse und Methoden im BCM effektiv umzusetzen.

Die Hilfsmittel des BSI zum BCM werden kontinuierlich weiterentwickelt und ausgebaut. Sie beinhalten:

- Weiterführende Aspekte zur Bewältigung
- Weiterführende Informationen zu Tools
- ein Migrationskonzept zum abgelösten BSI-Standard 100-4
- viele Dokumentenvorlagen, inklusive Beispieltexten
- Weiterführende Informationen zur Eintrittshäufigkeit von Ausfallrisiken
- ein Glossar zu den wichtigsten Begriffen
- einen Dokumenten- und Anforderungsvergleich BSI-Standard 200-4 zu ISO 22301:2019

Um die Liste der Hilfsmittel aktuell zu halten und kontinuierlich zu erweitern, ist diese auf der Website des BSI hinterlegt.

Literaturverzeichnis

[820-2] DIN 820-2, ‚DIN e. V. (Hrsg,), Normungsarbeit - Teil 2: Gestaltung von Dokumenten (ISO/IEC-Direktiven - Teil 2, 2018

[22301] ISO 22301:2019, International Organization for Standardization (Hrsg.), Security and resilience — Business continuity management systems — Requirements, ISO/TC 292, 2019

[22313] ISO 22313:2020, International Organization for Standardization (Hrsg.), Security, Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301, ISO/TC 292, 2020

[22317] ISO/TS 22317:2015, International Organization for Standardization (Hrsg.), Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA), ISO/TC 292, 2015

[22318] ISO/TS 22319:2015, International Organization for Standardization (Hrsg.), Societal security — Business continuity management systems — Guidelines for supply chain continuity, ISO/TC 292, 2015

[22398] ISO 22398:2013, International Organization for Standardization (Hrsg.), Guidelines for exercises and testing, ISO/TC 292, 2013

[27001] ISO/IEC 27001:2013, International Organization for Standardization (Hrsg.), Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC JTC 1/SC 27, 2013

[27031] ISO/IEC 27031:2011, International Organization for Standardization (Hrsg.), Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity, ISO/IEC JTC 1/SC 27, 2011

[BBK1] BBK Glossar - Ausgewählte zentrale Begriffe des Bevölkerungsschutzes, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.), 2. überarbeitete Auflage, Juni 2019, https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Praxis_Bevoelkerungsschutz/Glossar_2018.pdf?__blob=publicationFile

[BBK2] *LÜKEX-Glossar* - Zentrale Begriffe zur Mitarbeit an der Länder- und Ressortübergreifenden Krisenmanagementübung LÜKEX, , Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.), Ausgabe 1, Oktober 2018, *https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Broschueren_Flyer/Glossar_LUEKEX_18.pdf?__blob=publicationFile*

[BCMN] BCM-Info Newsletter des BSI, Bundesamt für Sicherheit in der Informationstechnik, 2020, https://www.bsi.bund.de/DE/Service/Aktuell/Newsletter/Newsletterbestellen/newsletterbestellen_node.html

[BRLN] Katastrophenschutzgesetz des Landes Berlin, http://gesetze.berlin.de/jportal/portal/t/150e/page/bsbeprod.psml/action/portlets.jw.MainAction?p1=5&eventSubmit_doNavigate=searchInSubtreeTOC&showdoccase=1&doc.hl=0&doc.id=jlr-KatSchG-BEpP2&doc.part=S&toc.poskey=#focuspoint

[BSI1] Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 200-1, Version 1.0, Oktober 2017, https://www.bsi.bund.de/grundschutz

[BSI2] IT-Grundschutz-Methodik, BSI-Standard 200-3, Version 1.0, Oktober 2017, https://www.bsi.bund.de/grundschutz

[BSI3] Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 200-3, Version 1.0, Oktober 2017, https://www.bsi.bund.de/grundschutz

[BSI4] Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz, Version 3.0, Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), März 2018, https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/ISRevision/Leitfaden/leitfaden_node.html

[BW1] Verwaltungsvorschrift der Landesregierung und der Ministerien zur Bildung von Stäben bei außergewöhnlichen Ereignissen und Katastrophen des Landes Baden-Württemberg, Landesregierung Baden-Württemberg (Hrsg.), 2011, http://www.landesrecht-bw.de/jportal/?quelle=jlink&docid=VVBW-VVBW000017504&psml=bsbawueprod.psml&max=true

[BW2] Gesetz über den Katastrophenschutz des Landes Baden-Württemberg, http://www.landesrecht-bw.de/jportal/;jsessionid=1FC02569B454A0890B439D4AEBAF9498.jp91?quelle=jlink&query=KatSchG+BW&psml=bsbawueprod.psml&max=true&aiz=true#jlr-KatSchGBW1999V1P1

[BMI1] Umsetzungsplan Bund - Leitlinie für Informationssicherheit in der Bundesverwaltung, Bundesministerium des Innern (Hrsg.), 2017, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.pdf?__blob=publicationFile&v=3

[BMI2] Konzeption Zivile Verteidigung, Bundesministerium des Innern (Hrsg.), 2016, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/bevoelkerungsschutz/konzeption-zivile-verteidigung.pdf;jsessionid=459C7813A932821D337491401D2C07CE.2_cid364?__blob=publicationFile&v=1

[GPG] Good Practice Guidelines, Business Continuity Institute (Hrsg.), 2018, https://www.thebci.org/product/good-practice-guidelines-2018-edition---download.html

[ITIL] Information Technology Infrastructure Library, Axelos (Hrsg.), 2020, https://www.axelos.com/best-practice-solutions/itil

[RFC2119] Key words for use in RFCs to Indicate Requirement Levels, Harvard University (Hrsg.), 1997, https://www.ietf.org/rfc/rfc2119.txt