Bundesamt
für Sicherheit in der
Informationstechnik

Business Continuity Management

BSI-Standard 200-4

Reguvis

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Reguvis Fachmedien GmbH
Amsterdamer Straße 192
50735 Köln

www.reguvis.de

Beratung und Bestellung:
wirtschaft@reguvis.de

ISBN (Print): 978-3-8462- 1518-0

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

Herstellung: Günter Fabritius
Satz: Cicero Computer GmbH, Bonn
Druck und buchbinderische Verarbeitung: Appel & Klinger Druck und Medien GmbH, Schneckenlohe

Printed in Germany

Inhalt

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 als praxisnahe Anleitung zur Umsetzung der ISO-Norm 22301:2019: Anpassung an ISO-Norm 22301:2019 Einführung eines Stufenmodells 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-Vergleich Berücksichtigung der Schnittstellen und Synergien des BCM, unter anderem mit ISMS, ITSCM und Krisenmanagement Ausführlichere Beschreibung der Bewältigungsorganisation
August 2022	CD 2.0	Umstrukturierung des Standards, sodass sich der Kapitelaufbau fortan 1 zu 1 am BCM-Prozess orientiert Integration des Outsourcings in den BCM-Prozess und Auslagerung der Outsourcing-BC-Strategien in das Hilfsmittel BC-Strategien Vereinfachung der Voranalyse und Integration verschiedener Ansätze Klarere Trennung der Begriffe, BC, BCM und BCMS. Umbenennung vieler Rollen von BCM-Rolle zu BC-Rolle.
Mai 2023	Version 1.0	Anpassung der Definition zur RTO und Einführung der BAO-Reaktionszeit Umbenennung der Voranalyse in BIA-Vorfilter Allgemeine Fehlerkorrektur und Umformulierung des gesamten Standards in geschlechtergerechte Sprache

Tabelle 1: Änderungshistorie

1 Einleitung

1.1 Adressatenkreis

Der BSI-Standard 200-4 richtet sich an Business-Continuity-Beauftragte, Krisenstabsmitglieder, Zuständige für Sicherheitsthemen, Sicherheitsfachleute und -beratende, Institutionsleitungen sowie an 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 **Business-Continuity-Management (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 BCM aufzubauen und zu betreiben.

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 des globalen Wettbewerbs, der fortschreitenden Digitalisierung sowie verschiedener Interessengruppen, d. h. von Aufsichtsbehörden, Kunden und Kundinnen usw. Infolgedessen werden Institutionen immer abhängiger von Informationstechnik (IT), funktionierenden Lieferketten und den Leistungen von Drittanbietenden wie beispielsweise Dienstleistungs-, Zulieferungs- und Versorgungsunternehmen. 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 in hohem 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 bzw. Cybersicherheit sowie mit IT-Service Continuity Management (ITSCM) 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 zu einer allgegenwärtigen Bedrohung entwickelt.

Zudem sorgt die fortschreitende Effizienzsteigerung von Geschäftsprozessen dafür, dass Leerlauf- und Pufferzeiten auf ein Minimum reduziert werden. Darüber hinaus werden auch in der Logistik und der Produktion benötigte Ressourcen auf ein Mindestmaß reduziert, um Lagerflächen einzusparen.

Infolgedessen verkleinern sich in der Praxis die Zeitfenster, innerhalb derer auf Ausfälle der Geschäftsprozesse angemessen reagiert und unmittelbare Folgewirkungen eingedämmt werden können. Entsprechend steigt die Notwendigkeit, gegen Ausfälle des Geschäftsbetriebs umfassend vorzusorgen sowie für den Schadensfall angemessene Möglichkeiten zur Geschäftsfortführung vorzubereiten (engl. **Business Continuity** oder **BC**).

Mit Hilfe eines angemessenen **Business-Continuity-Managements (BCM)** können sich Institutionen vor den Auswirkungen solcher Schadensereignisse schützen, die den Geschäftsbetrieb in nicht akzeptablem bis hin zu existenzbedrohendem Maße beeinträchtigen können. Ziel des BCM ist es sicherzustellen, dass der Geschäftsbetrieb selbst bei massiven Schadensereignissen nicht unterbrochen wird oder nach einer Unterbrechung in angemessener Zeit auf einem definierten Mindestniveau fortgeführt werden kann**.** Das BCM umfasst organisatorische, technische, bauliche und personelle Maßnahmen. Institutionen können dabei teilweise auf vorhandene Sicherheitsmaßnahmen weiterer Managementsysteme zurückgreifen und diese gegebenenfalls erweitern. Synergien ergeben sich z. B. mit dem Managementsystem für Informationssicherheit (ISMS).

Dieser BSI-Standard erleichtert den Einstieg in ein BCM, indem ein Stufenmodell mit Einstiegsstufen angeboten wird (siehe Kapitel 2.6 *BCMS-Stufenmodell*).

Darüber hinaus bietet dieser BSI-Standard eine Anleitung, um ein vollständiges, zur Norm ISO 22301:2019 konformes BCM einzuführen, aufrechtzuerhalten und zu verbessern. Erfahrene Anwendende, die gegebenenfalls mit einem bereits existierenden BCM arbeiten, können den Anforderungskatalog nutzen, um sich auf schnelle und effektive Weise nach diesem Standard auszurichten (siehe Anhang A: *Anforderungskatalog*).

BCM ist kein einmaliges Projekt, sondern bedarf eines zielgerichteten **Business-Continuity-Management-Systems (BCMS)**, das sich fortlaufend weiterentwickelt. Ein BCMS muss kontinuierlich verbessert und an die sich stetig verändernden Rahmenbedingungen der Institution angepasst werden (siehe Kapitel 2.2 *Grundlagen eines Managementsystems*). So wird ein dauerhafter Prozess geschaffen, um organisatorische Resilienz (Widerstandsfähigkeit) aufzubauen.

Die organisatorische Resilienz einer Institution ist die Fähigkeit, auf Veränderungen zu reagieren und sich diesen Veränderungen anzupassen. Je „resilienter" eine Institution ist, umso besser kann sie Risiken und Chancen durch Veränderungen erkennen und flexibel darauf reagieren. Dies gilt sowohl für plötzliche als auch für allmähliche, sowohl für interne als auch für externe Veränderungen.

Organisatorische Resilienz wird nicht durch ein einzelnes Managementsystem aufgebaut, sondern entsteht erst durch das Zusammenspiel verschiedener Management-Disziplinen. Dieser Standard berücksichtigt die Informationssicherheit, das Business Continuity Management, die Krisenbewältigung und IT-Service Continuity als Eckpfeiler, die gemeinsam Resilienz schaffen können (siehe Abbildung 1).

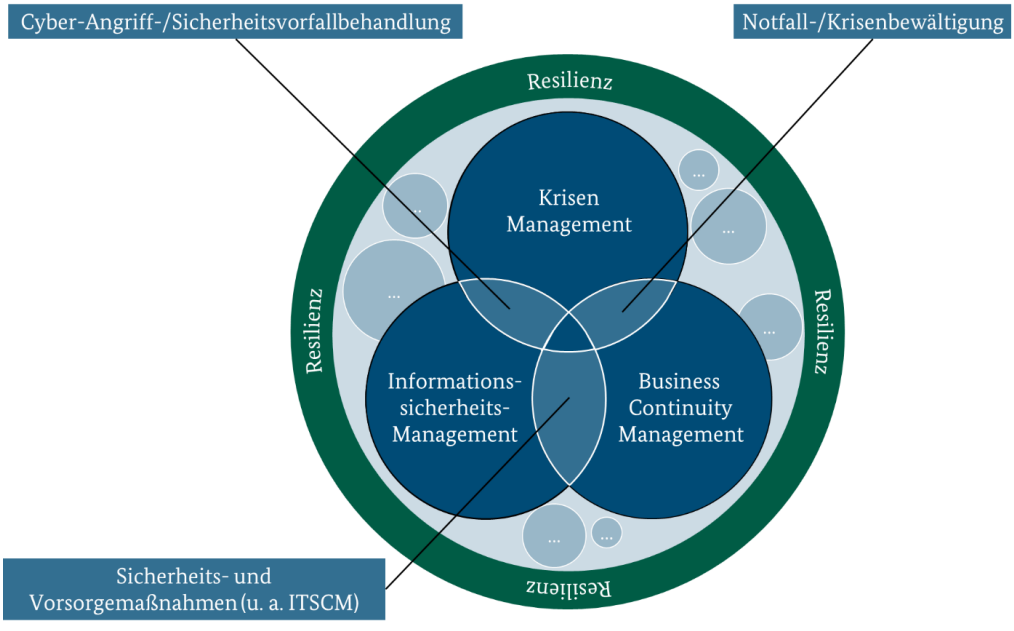

Abbildung 1: Resilienz schaffen durch verschiedene Sicherheitsthemen

Hinweis

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

Gemäß ISO 22316:2017 *Security and resilience – Organizational resilience* (siehe [22316]) 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 vorliegende BSI-Standard 200-4 *Business Continuity Management* wird beschrieben, mit welchen Methoden BCM in einer Institution generell initiiert, implementiert und gesteuert werden kann. Er 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.

Grundsätzlich werden Institutionen durch diesen Standard in die Lage versetzt, alle Arten von Notfällen erfolgreich und auch Krisen zumindest rudimentär zu bewältigen, da die organisatorischen Vorrausetzungen zur Bewältigung für Notfälle und Krisen nahezu identisch sind.

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. Der BSI-Standard 200-4 setzt die Reihe der BSI-Standards 200-1 *Management für Informationssicherheit (ISMS)*, 200-2 *IT-Grundschutz-Methodik* und 200-3 *Risikomanagement* 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*).

Dieser BSI-Standard setzt folgende Elemente ein, um besondere Aspekte hervorzuheben:

Hinweis

Hinweisboxen dieser Art heben besonders relevante Informationen hervor.

Beispiele

Beispiele, mit Ausnahme von in Teilsätzen eingeschobenen Beispielen, werden auf diese Weise hervorgehoben. Sie dienen nur als Veranschaulichung und sind nicht dazu gedacht, unbesehen übernommen zu werden.

Synergiepotenzial

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

Zusätzlich werden viele auf den Standard abgestimmte Hilfsmittel und Dokumentvorlagen angeboten, die auf der Webseite des BSI heruntergeladen werden können. Die Dokumentvorlagen beinhalten nicht nur Elemente zur Strukturierung, sondern zum großen Teil Textbausteine und Beispiele, die auch losgelöst von den Vorlagen verwendet werden können.

Der vorliegende BSI-Standard 200-4 gestattet es, die Umsetzung und Vorgehensweise individuell an die zeitlichen, finanziellen und personellen Möglichkeiten der jeweiligen Institution anzupassen. Das BCMS kann schrittweise in den drei Stufen aufgebaut werden: 1. Reaktiv-BCMS, 2. Aufbau-BCMS und 3. Standard-BCMS (siehe Kapitel 2.6 *BCMS-Stufenmodell*).

Die Stufe Standard-BCMS ist konform zu den Anforderungen der ISO-Norm 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 *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 dieser Standard auch Lösungsansätze für einzelne Aufgabenstellungen, beispielsweise für die Konzeption

bestimmter Methoden, BC-Strategien und Notfallpläne oder für die Durchführung von Revisionen und Zertifizierungen im Bereich des BCM. Je nach Anwendungsbereich bilden bereits einzelne Umsetzungshinweise, Hilfsmittel oder Synergiepotenziale, die mit dem BSI-Standard 200-4 zur Verfügung gestellt werden, hilfreiche Grundlagen für die Arbeit im BCM. Alle Empfehlungen dieses Standards müssen stets im Kontext der jeweiligen Institution betrachtet und an die jeweiligen Rahmenbedingungen angepasst werden, z. B. an rechtliche, regulatorische und vertragliche Anforderungen.

Insbesondere in Tabellen werden Rollen in diesem Standard im Plural verwendet, um die Geschlechtsneutralität zu wahren. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

Aufbau des BSI-Standards 200-4

Ab Kapitel 3 werden die Themen in diesem Standard nach derjenigen Handlungsreihenfolge beschrieben, in der die einzelnen BCM-Prozessschritte umgesetzt werden, um ein BCMS aufbauen, betreiben und weiterentwickeln zu können. Zu Beginn jedes Kapitels werden in einer Übersicht die Unterkapitel zu den einzelnen Prozessschritten dargestellt. Hier wird ferner erläutert, ob eine chronologische, schrittweise Vorgehensweise empfohlen wird oder ob einzelne Schritte parallelisiert werden können.

Grundsätzlich sind die meisten Kapitel für alle Stufen anwendbar. Nur wenige Kapitel unterscheiden sich je nach Stufe oder gelten nur für einzelne Stufen. Daher wird ab Kapitel 3 hinter der Kapitelüberschrift angegeben, für welche Stufen das Kapitel jeweils gilt. (R) steht für Reaktiv-BCMS, (A) für Aufbau-BCMS und (S) für Standard-BCMS. Viele Kapitel gelten für alle Stufen, was durch (R+AS) ausgedrückt wird. Einige weitere Kapitel gelten nur für das Aufbau- und Standard-BCMS (AS), andere nur für das Reaktiv-BCMS (R). Die Buchstaben AS werden zusammengeschrieben, weil die Vorgehensweisen bei den Stufen Aufbau- und Standard-BCMS in den meisten Fällen identisch sind. Anwendende, die vorerst z. B. ausschließlich das Reaktiv-BCMS umsetzten möchten, brauchen nur diejenigen Kapitel zu lesen, bei denen hinter der Kapitelüberschrift auch ein R in der Klammer steht.

In einigen Fällen gilt zwar das Kapitel für alle Stufen, aber es gibt kleinere Unterschiede innerhalb des Kapitels. Diese Unterschiede sind jeweils durch eine Box mit dem entsprechenden Kürzel markiert. Das folgende Beispiel zeigt einen Textbaustein, der nur für Aufbau- und Standard-BCMS relevant ist:

Texte in einer solchen Box gelten nur für das Aufbau- und das Standard-BCMS.	**AS**

Für Personen, die über keine Vorerfahrung zum Aufbau eines Managementsystems im Allgemeinen sowie zum BCM im Speziellen verfügen, wurde das *Kapitel 2 Was ist Business Continuity Management (BCM)* verfasst. Es erläutert die wichtigsten Begriffe und Definitionen zum BCM und die die wichtigsten Schnittstellen zu anderen Managementsystemen. Personen und Institutionen mit Vorerfahrung zum BCM sollten mindestens die Kapitel 2.1 *Begriffe,* 2.3 *(zeitlicher) Ablauf der Bewältigung* sowie 2.6 *BCMS-*

Stufenmodell (Reaktiv-, Aufbau und Standard-BCMS) gelesen haben, um die im BSI-Standard 200-4 genutzten Begriffe und deren Definitionen zu kennen.

Institutionsleitungen sind grundsätzlich für das BCM verantwortlich. Sie sollten aufgrund dieser Verantwortung mindestens die Inhalte des Kapitels 3 *Initiierung des BCMS durch die Institutionsleitung (R+AS)* kennen und beachten.

Kapitel 14 *Anhang A: Anforderungskatalog* verweist auf den normativen Anforderungskatalog. Dieser fasst die Anforderungen zusammen, damit BCM-erfahrene Leser einen schnellen Überblick gewinnen können.

Kapitel 15 *Anhang B: Hinweise zu den Hilfsmitteln* enthält Informationen über weiterführende Hilfsmittel auf der Webseite des BSI.

Kontaktmöglichkeiten

Kommentare jeglicher Art, unabhängig davon, ob es sich um eine orthografische oder inhaltlich-fachliche Anmerkung handelt, können an

it-grundschutz@bsi.bund.de

gerichtet werden. Jeder Kommentar und der damit verbundene Austausch mit den Anwendenden ist sehr willkommen. Das BSI informiert über Updates zum BSI-Standard 200-4 über die etablierten Kanäle.

2 Was ist Business Continuity Management (BCM)?

Dieses Kapitel bietet eine Übersicht zu allen zentralen, wichtigen Begriffen, Definitionen und Bestandteilen dieses Standards. Darüber hinaus ermöglicht das Kapitel Institutionen ohne Vorerfahrung einen schnellen Einstieg in das Thema BCM.

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:

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 in dem gesamten Standard unter dem Begriff Geschäftsprozess auch Fachaufgaben verstanden.

Für die im BCM betrachteten Geschäftsprozesse ist eine mittlere Detaillierungsebene ausreichend. Eine feingliedrige Beschreibung der Einzeltätigkeiten, wie sie z. B. in der Organisationsanalyse anhand einer Prozessmodellierung erhoben und dokumentiert werden, sind für das BCM nicht notwendig.

Als **zeitkritisch** gelten alle Geschäftsprozesse, deren Ausfall innerhalb eines zuvor festgelegten Zeitraums zu einem nicht tolerierbaren, unter Umständen existenzgefährdenden Schaden für die Institution führen kann. So kann z. B. ein Ausfall, der gegen entsprechende regulatorische Anforderungen verstößt, zu existenzbedrohenden Folgen führen. Falls andere Geschäftsprozesse, wie beispielsweise Unterstützungsprozesse, oder Ressourcen, wie beispielsweise Personal, IT-Systeme oder Dienstleistungsunternehmen, benötigt werden, um die zeitkritischen Geschäftsprozesse aufrecht zu erhalten, müssen auch diese als zeitkritisch angesehen werden. Hingegen kann es in einer Institution auch Geschäftsprozesse geben, die im Alltag sehr wichtig, aber nicht zeitkritisch sind.

Hinweis

Im BCM werden ausschließlich die zeitkritischen Geschäftsprozesse berücksichtigt. Ein Prozess ist nur dann nicht zeitkritisch, wenn genügend Zeit zur Verfügung steht, um auf eine Störung oder einen Ausfall dieses Prozesses angemessen zu reagieren.

Üblicherweise werden Schadensereignisse durch die **Allgemeine Aufbauorganisation (AAO)** im täglichen Dienst- bzw. Geschäftsbetrieb (**Normalbetrieb**) bewältigt. Die **AAO** ist die ständige Organisationsform der Institution für die Aufgaben des täglichen Service- 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 zu bewältigen sind. In diesem Fall wird in der Regel eine **Besondere Aufbauorganisation (BAO)** eingesetzt.

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

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

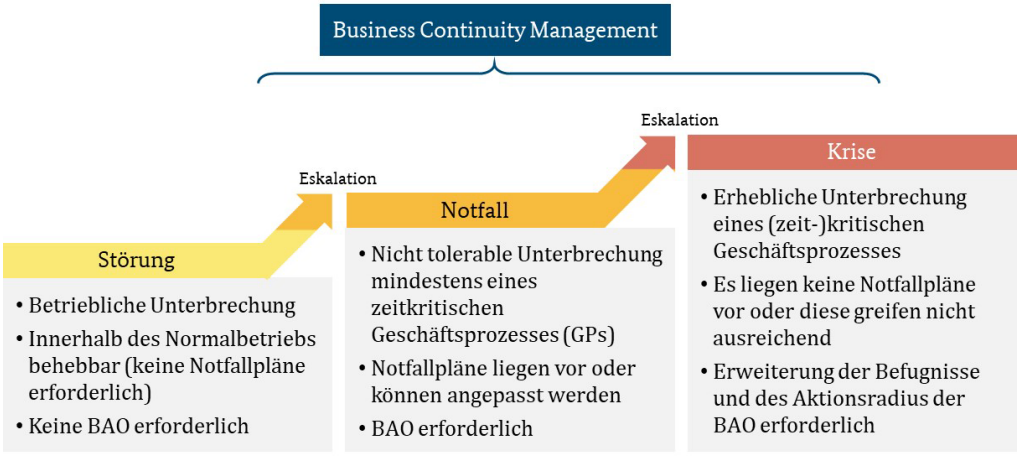

Abbildung 2: Abgrenzung Störung, Notfall, Krise

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 Vorfallmanagements (auch Incident-Management genannt) zurückgegriffen. Daher sind Störungen nicht Betrachtungsgegenstand dieses Standards. **Störungen können jedoch zu einem Notfall eskalieren**, wenn sie nicht in einer angemessenen Zeit behoben werden können.

Ein Notfall im Sinne dieses Standards ist eine Unterbrechung des Geschäftsbetriebs, die mindestens einen zeitkritischen Geschäftsprozess betrifft, der nicht im Normalbetrieb innerhalb der maximal tolerierbaren Ausfallzeit wiederhergestellt werden kann (siehe Kapitel 6.2 *Konkretisierung des Begriffs zeitkritisch (R+A)*). Im Gegensatz zu Störungen wird

zur Bewältigung von Notfällen eine BAO benötigt. Im Gegensatz zur Krise liegen geeignete Pläne zur Bewältigung vor oder bestehende Pläne können adaptiert werden. Der Notfall kann auch ausgerufen werden, bevor das Schadensereignis zu einer Unterbrechung des Geschäftsbetriebs führt, um schnell reagieren zu können. Es genügt die Gefahr, dass durch das Schadensereignis der Geschäftsbetrieb unterbrochen wird.

Hinweis

Der Begriff Notfall wird hier im Kontext BCM definiert. In anderen Themengebieten kann es abweichende Definitionen eines Notfalls geben, z. B. im Sinne des Brandschutzes oder Schutz von Leib und Leben. Wenn im BSI-Standard 200-4 nachfolgend von Notfall gesprochen wird, ist immer der BCM-Notfall gemeint.

Als **Krise** im Sinne dieses Standards wird ein Schadensereignis bezeichnet, das sich in erheblicher 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 solcher Schadensereignisse 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, weil er einen großen Gebäudebereich umfasst, so können weite Bereiche der Institution nicht mehr einsatzfähig und wesentliche Arbeiten nicht mehr durchführbar sein. 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, liegt eine **Krise** vor. Die vorhandenen Notfallmaßnahmen sind nicht mehr ausreichend und die BAO muss ad hoc über geeignete Maßnahmen entscheiden, z. B. kann ein Notstromaggregat für 3 Tage eingesetzt werden.*

Hinweis

Viele weitere Definitionen der gängigen BCM-Literatur differenzieren die Begriffe Störung, Notfall, Krise primär anhand der Auswirkungen. Im Rahmen dieses 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 Notfallpläne 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.*

Es ist möglich, dass sich Krisen nicht nur ausschließlich auf die eigene Institution und die Geschäftspartner und -partnerinnen, sondern auch darüber hinaus auswirken. In der Bewältigung treten dann gegebenenfalls weitere Parteien in Erscheinung, wie Aufsichtsbehörden oder **Behörden und Organisationen mit Sicherheitsaufgaben** (BOS), wie z. B. Polizei und Feuerwehr. 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])). BCM behandelt die Auswirkung von Schadensereignissen auf die eigene Institution. Da der Umgang innerhalb der Institution mit einer Katastrophe nicht anders ist als mit 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 Anhang B: *Hinweise zu den Hilfsmitteln*).

2.2 Grundlagen eines Managementsystems (BCMS)

Ein Managementsystem umfasst alle Regelungen, die dazu dienen, eine Institution so zu steuern und zu lenken, dass die jeweiligen Ziele des Managementsystems erreicht werden (siehe [BSI1]). Bei einem Managementsystem für Informationssicherheit liegt das Ziel in der Verbesserung der Informationssicherheit. Bei einem Managementsystem für Business Continuity ist das Ziel, die zeitkritischen Geschäftsprozesse gegen Ausfälle abzusichern. Für jedes Managementsystem gilt es, die gesteckten Ziele effektiv und effizient zu erreichen und die sich stetig verändernden Rahmenbedingungen und Anforderungen der Institution zu berücksichtigen. Ein Business Continuity Management System (BCMS) kann sicherstellen, dass die Reife des BCM und somit der Resilienz gegen Geschäftsunterbrechungen kontinuierlich und systematisch gesteigert wird.

Anders als ein Projekt, das ein einmaliges Vorhaben mit konkretem Ziel darstellt und zeitlich terminiert ist, 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):

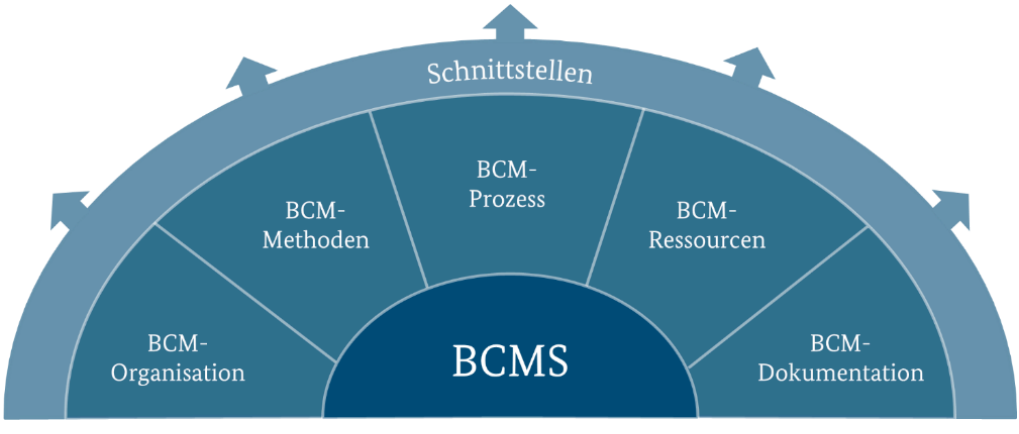

Abbildung 3: BCMS-Bestandteile

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:

- **Strategische Ebene** (Diese legt die allgemeinen, langfristig wirkenden Rahmenbedingungen, den Geltungsbereich und die Ziele fest und trägt die Verantwortung.)

- **Taktische Ebene** (Diese definiert mittelfristig wirkende Vorgaben, Aktivitäten und Methoden anhand der Rahmenbedingungen und Ziele und überwacht die Umsetzung.)
- **Operative Ebene** (Diese beinhaltet konkrete kurzfristige Handlungen, um die gesteckten Ziele zu erreichen. Sie berücksichtigt hierbei die definierten Vorgaben und Methoden und setzt die Vorgaben um.)

Hinweis

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

Die **BCM-Methoden** sind die Werkzeuge, die benötigt werden, um das BCM umzusetzen. Hierzu gehören die Business-Impact-Analyse, die BCM-Risikoanalyse sowie Methoden, um Business-Continuity-Strategien (BC-Strategien), Lösungen und Notfallpläne zu entwickeln.

Der **BCM-Prozess** dient dazu, das BCMS aufzubauen, zu betreiben und kontinuierlich weiterzuentwickeln. Gegenüber einigen anderen Managementsystemen weist ein BCMS die Besonderheit auf, dass es neben dem BCM-Prozess den (zeitlichen) 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 den Ablauf der Bewältigung und bereitet diese vor. Umgekehrt fließen Erkenntnisse aus der Bewältigung in die Weiterentwicklung und Verbesserung des BCM-Prozesses ein. Der **Ablauf der Bewältigung** wird im nachfolgenden Kapitel konkreter erläutert (siehe Kapitel 2.3 *(zeitlicher) 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).

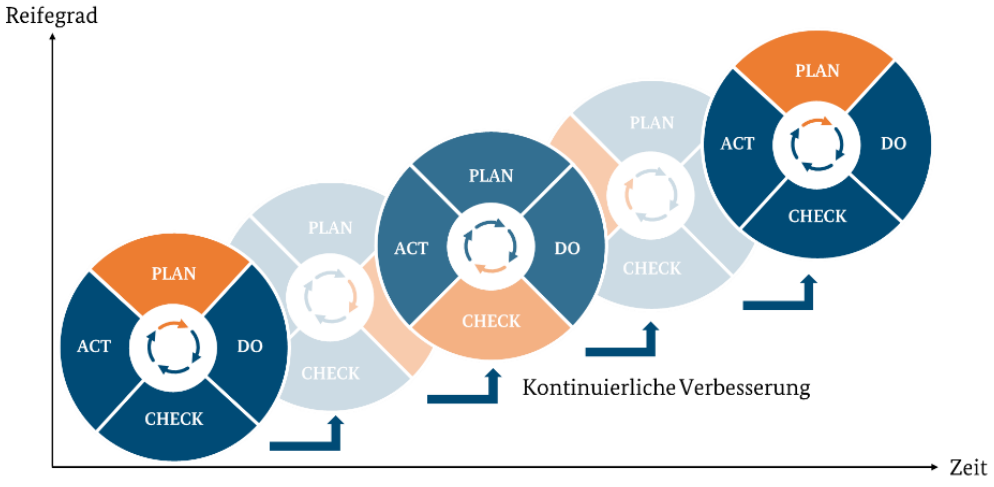

Abbildung 4: PDCA-Zyklus eines Managementsystems

Die Phasen PLAN, DO, CHECK, ACT werden jeweils zu einem PDCA-Zyklus zusammengefasst, der sich kontinuierlich wiederholt (siehe Abbildung 4). Der Reifegrad des Managementsystems steigert sich mit jedem weiteren PDCA-Zyklus. Wie der BCM-Prozess anhand eines PDCA-Zyklus aufgebaut ist, hängt von der gewählten BCMS-Stufe ab. Dies wird in Kapitel 2.6.2 *Übersicht über den BCMS-Prozess* 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 *Initiierung des BCMS durch die Institutionsleitung (R+AS)*).

Die **BCM-Dokumentation** beinhaltet sowohl Dokumente, die das BCMS selbst beschreiben als auch das Notfallhandbuch, das in der Notfallbewältigung eingesetzt wird. Die Besonderheiten der BCM-Dokumentation werden in Kapitel 4.4 *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 (zeitlicher) Ablauf der Bewältigung

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

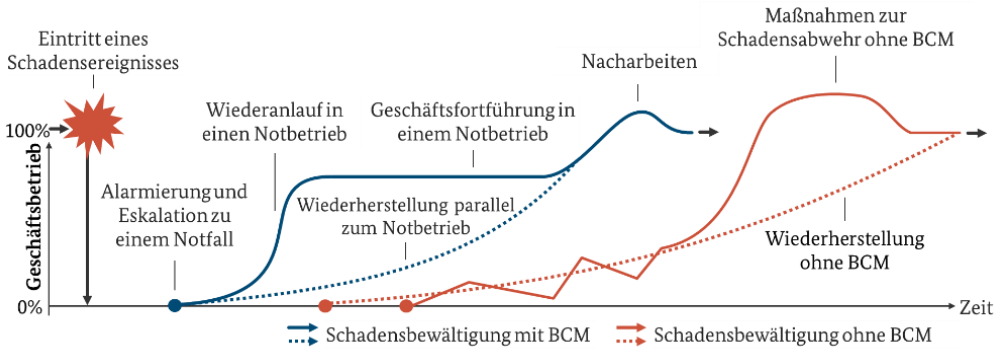

Abbildung 5: Bewältigung eines schwerwiegenden Schadensereignisses mit und ohne BCM

Ohne BCM 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 zeitlich unkritischere Prozesse zuerst gestartet werden. Werden infolgedessen zeitkritische Prozesse zu spät gestartet, kann dies schnell die Existenz der gesamten Institution gefährden. Ohne BCM wird auch deutlich mehr Zeit gebraucht, um 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. 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, d. h. es gibt z. B. keine Pläne und kein Entscheidungsgremium.

Mit BCM kann ein Schadensereignis anhand festgelegter Kriterien schnell an kompetente Entscheidungsinstanzen 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 der 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 dieses Standards näher erläutert.

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 sie überschneiden sich oder laufen parallel zueinander. Insbesondere die Schritte Sofortmaßnahmen und Alarmierung sind situationsspezifisch und können zeitlich auch in umgekehrter Reihenfolge ausgeführt werden.

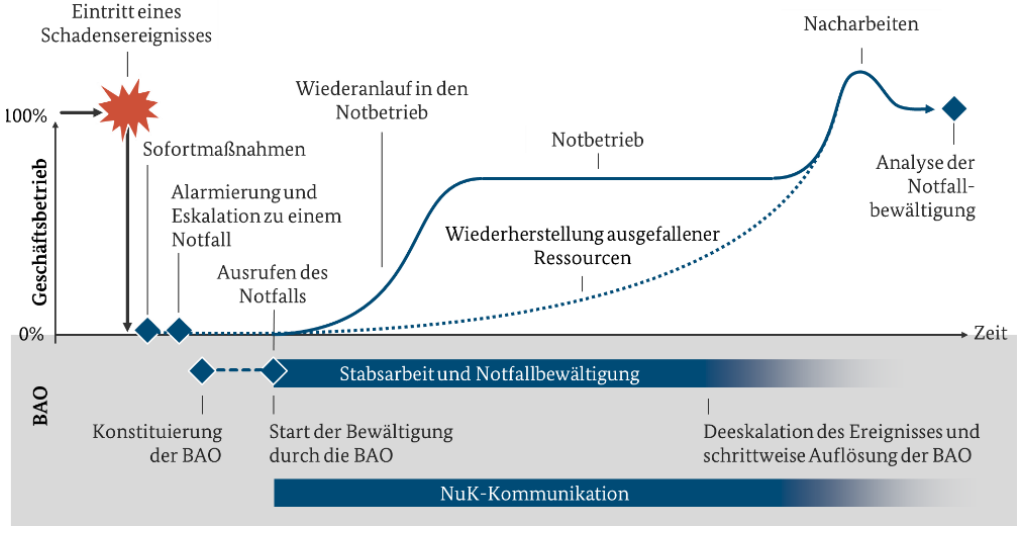

Abbildung 6: Ablauf der Bewältigung mit BCM

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, bevor das Ereignis zu einem Notfall eskaliert wird, um weiteren Schaden 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 die BAO in die Lage versetzen, ihre Arbeit aufzunehmen. 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 verabschieden Maßnahmen müssen operativ umgesetzt und anschließend nachverfolgt werden, z. B. ob sie wirksam sind. Nach Ausrufen des Notfalls weist der Stab situationsbezogen die betroffenen Organisationseinheiten an, den Geschäftsbetrieb wiederanlaufen zu lassen, indem dieser in einen stabilen Notbetrieb zu überführt wird.

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-Systeme, Notfallarbeitsplätze etc.), Prozesse und Tätigkeiten auf einen möglicherweise reduzierten Notbetrieb umzustellen oder die Mitarbeitenden in die definierten alternativen Prozesse 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 oder alternativer Prozessschritte durchgeführt werden können. Innerhalb dieser Phase können beispielsweise Ersatzsysteme genutzt oder Tätigkeiten innerhalb von Geschäftsprozessen zurückgestellt, modifiziert oder anders priorisiert werden.

Die **Wiederherstellung** hat einen Zustand zum Ziel, in dem der Normalbetrieb wieder möglich ist. Ausgefallene Ressourcen können z. B. 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 häufig parallel zum Wiederanlauf und zum Notbetrieb. Typischerweise erfolgt die Wiederherstellung ausgefallener Ressourcen durch die ressourcenzuständigen Organisationseinheiten. Sie sind üblicherweise nicht Teil der BAO, sondern arbeiten parallel zu deren Maßnahmen. Jedoch sollten die Maßnahmen zur Wiederherstellung mit den Maßnahmen zum Wiederanlauf und zum Notbetrieb zwischen den beteiligten Zuständigen abgestimmt werden, um unter anderem die notwendige Dauer des Notbetriebs ableiten zu können.

Die **Notfall- und Krisenkommunikation** (**NuK-Kommunikation**) dient dazu, Informationen während der Bewältigung zu sammeln, zu verifizieren sowie adressatengerecht nach innen und außen zu verteilen. Ferner werden im Rahmen der NuK-Kommunikation vorab definierte Regeln zum Umgang mit Medien, Presse und gegebenen-

falls (Aufsichts-)Behörden angewendet und es wird 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, was 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,
- Überprüfung und Wiederherstellung der Datenaktualität und Datenkonsistenz in IT-Anwendungen, z. B. Status von Batchläufen und Schnittstellen zu anderen Systemen, sowie
- Schwenk von Ausweich- zu wiederhergestellten Hauptsystemen.

Üblicherweise fallen Nacharbeiten an, die sich aus dem Notbetrieb ergeben. Die erforderlichen Nacharbeiten sind nicht unbedingt Teil der Bewältigung. Dies gilt, solange die regulären Prozesse zur Störungsbeseitigung greifen.

Hinweis

Die Praxis zeigt, dass die Zeit der Nacharbeiten weiterhin eine arbeitsintensive Zeit für die Institution ist. In 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 während der Nacharbeiten, sobald die Institution entscheidet, dass die BAO nicht mehr benötigt wird. Es kann sinnvoll sein, dass die BAO die Nacharbeiten noch eine Weile begleitet, z. B. wenn es 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.

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

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

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

Beispiel

In Bezug auf die Ressourcenkategorien Gebäude und Infrastruktur könnten mehrere Vorsorgemaßnahmen umgesetzt werden, um die Ausfallwahrscheinlichkeit eines Gebäudes zu senken. So können Mitarbeitende 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 im Vorfeld 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 Mitarbeitenden im Notfall ortsungebunden weiterarbeiten zu können.

Unter **Notfallmaßnahmen** fallen alle Maßnahmen, die im Vorfeld erarbeitet jedoch erst im Schadensfall umgesetzt werden, um den Schaden zu begrenzen und Geschäftsprozesse fortzuführen. Dazu gehören alle Maßnahmen zum Wiederanlauf und zur Geschäftsfortführung sowie alle Sofortmaßnahmen.

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 umgesetzt werden sollen.

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

2.4 Abgrenzung und Synergien

Wie bereits in Kapitel 1.2 *Zielsetzung* dargestellt, tragen eine Reihe von Themen und Managementsystemen dazu bei, eine organisatorische Resilienz aufzubauen. In diesem Sinne ist es auch nicht zielführend, ein BCMS als Insellösung zu betrachten, sondern es bedarf einer Gesamtsicherheitsstrategie, in der alle wesentlichen Themen zur organisatorischen Resilienz zusammen betrachtet werden. Ein BCMS sollte im Rahmen einer solchen 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, Ausfall- und Schadensszenarien zu machen.

Die größten thematischen Überschneidungspunkte besitzt das BCM zu den Managementsystemen und Disziplinen ISMS, ITSCM, Krisenmanagement und Outsourcing. 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 Synergieboxen ergänzt (siehe hierzu auch Kapitel 1.3 *Anwendungsweise*). Synergieboxen zeigen auf, welche konkreten Möglichkeiten bestehen, um die Arbeit mit den angrenzenden Managementsystemen und Disziplinen zu erleichtern oder abzustimmen.

2.4.1 BCM und Informationssicherheit

BCM und Informationssicherheit gehören in Institutionen zu den wichtigsten Säulen einer ganzheitlichen Sicherheitsstrategie. 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 fi-

nanzielle, 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. Falls die Geschäftsprozesse nicht schon aus einem Geschäftsprozessmanagement bekannt sind, können die Ergebnisse aus der Strukturanalyse nach IT-Grundschutz als gemeinsame Datenbasis verwendet werden.

In den Analysen zum Schutzbedarf (siehe [BSI2]) und zum Business Impact werden oftmals dieselben Kontaktpersonen und ähnliche Bewertungsmethoden herangezogen. Einheitliche Stammdaten und aufeinander abgestimmte Methoden steigern die Akzeptanz in der Institution, reduzieren die Aufwände und vermeiden Missverständnisse bei den Kontaktpersonen. Unter Umständen kann eine gemeinsame Datenerhebung sinnvoll sein. In diesem Fall ist es wichtig zu beachten, dass nur die Daten der Bereiche, die von beiden Managementsystemen untersucht werden, auch gemeinsam erhoben werden.

Risikoanalyse 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 und Methoden zur Risikobewertung zurückgreifen. Beim BCM steht jedoch die Identifizierung von Gefährdungen im Vordergrund, da die potenzielle Schadenshöhe schon in der Business-Impact-Analyse bewertet wird. Eine gemeinsame Übersicht der relevanten Risiken in Form 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 die Verfügbarkeit verbessern, sind sowohl für das BCM als auch für die Informationssicherheit relevant. Sind z. B. Ressourcen bereits in einem der beiden Managementsysteme redundant ausgelegt und wird deren Verfügbarkeit regelmäßig getestet, dann profitiert das jeweils andere Managementsystem davon.

Neben dem Schutz der IT umfasst die Informationssicherheit auch den Schutz von Informationen aller Art, z. B. auch von solchen auf Papier oder in den Köpfen. Für Informationen 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 Eintrittshäufigkeit reduzieren. So kann z. B. der Verlust der Integrität von essenziellen IT-Systemen in letzter Konsequenz für die betroffenen Geschäftsprozesse gleichbedeutend damit sein, dass die IT-Systeme nicht zur Verfügung stehen.

Informationsfluss

Beide Managementsysteme informieren regelmäßig die internen Interessengruppen über Tätigkeiten, Maßnahmen und Risiken (Informationsfluss). Oftmals erfolgt diese Kommunikation an die gleichen Rollen innerhalb der Institution durch die jeweilige Beauftragten-Funktion. Eine gemeinsame Berichterstattung hat insbesondere in der Risikobewertung und Risikobehandlung viele Vorteile. Zum einen können Zusammenhänge zwischen BCM und ISMS aufgezeigt werden, was Entscheidungen auf Grundlage einer besseren Informationsbasis ermöglicht. Zum anderen werden doppelte Berichte vermieden und somit Ressourcen eingespart, auch auf Leitungsebene. Im Sinne einer Gesamtsicherheitsstrategie können zudem die Interessengruppen für beide Themengebiete übergreifend geschult werden.

Notfallbewältigung

Auch innerhalb der Notfallbewältigung ist ein Zusammenspiel von BCM und ISMS von Vorteil. Zwar ist im BCM die Ursache eines Ausfalls vernachlässigbar, um einen Geschäftsfortführungsplan zu aktivieren und so einen Notbetrieb sicherzustellen. 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 sorgt die Geschäftsfortführungsplanung des BCMS für einen Notbetrieb, der den Ausfall zeitkritischer Ressourcen überbrückt und so die Überlebensfähigkeit der Institution steigert. Zeitgleich bereinigt das ISMS zusammen mit dem ITSCM die IT und stellt diese wieder für einen Normalbetrieb zur Verfügung. Somit sorgen das BCMS und das ISMS zusammen mit dem ITSCM für organisatorische Resilienz.

Ausweichverfahren im BCMS mit dem primären Ziel der Verfügbarkeit sollten grundsätzlich auch darauf achten, Vertraulichkeit und Integrität zu wahren. Das Risiko, dass diese Schutzziele verletzt werden, wird daher auch in den BC-Strategien untersucht und die Schutzziele werden gegebenenfalls gegeneinander abgewogen. 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 Schutzziele **gemäß ISMS** (u. a. Verfügbarkeit und Integrität im Normalbetrieb) und **betriebliche Kontinuitätsanforderungen an Informationen und die IT gemäß BCMS** (Verfügbarkeit und ausreichende Integrität im Notfall) voneinander abgegrenzt werden. Die Verfügbarkeit im Normalbetrieb muss z. B. nicht zwangsläufig der Verfügbarkeit im Notbetrieb entsprechen:

- Durch ein ISMS soll die Verfügbarkeit von Informationen so weit 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 Operational Level Agreements (SLA oder OLA) 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 BC-Lösungen dienen dazu, längere Ausfallzeiten des Geschäftsbetriebs zu verhindern. Die Anforderungen im BCM werden beispielsweise in Form von Wiederanlaufzeiten, maximalen Ausfallzeiten im Notfall und einem zugesicherten Mindestniveau innerhalb von SLAs bzw. OLAs angegeben. D. h., dass auch im Schadensfall diese Anforderungen garantiert sein müssen.

Beispiel

Ein Prozess zur Kundschaftsbetreuung nutzt eine Anwendung, um die Kundschaftsbeziehungen zu verwalten (Customer Relationship Management, CRM). Diese Anwendung erlaubt es, schnell und effizient auf Kontaktdaten zurückzugreifen und Informationen zu vorangegangen Geschäftsaktivitäten abzurufen. Aufgrund 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 anders bewertet. Sie erhält, bezogen auf existenzbedrohende Auswirkungen auf das Unternehmen, keine Kontinuitätsanforderung, da sie für einen Notbetrieb nicht zwingend erforderlich ist. Die Informationen können auch durch die Kontaktbetreuenden 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 ebenfalls eine Bewertung der ERP-Anwendung. Hier wird festgestellt, dass der Geschäftsprozess maximal 6 Stunden ausfallen darf, bevor unzumutbare Auswirkungen eintreten. Um dies zu erreichen, ist es notwendig, dass die ERP-Anwendung innerhalb von 4 Stunden wieder zur Verfügung steht, damit noch zwei Stunden Puffer für Alarmierungund fachliche Inbetriebnahme nach Wiederanlauf verbleiben. Die im ISMS geforderten 99,9 % Verfügbarkeit entsprechen 8,76 Stunden maximale Ausfalldauer pro Jahr in Summe für alle Ausfälle. Dabei wird, statistisch gesehen, nicht

davon ausgegangen, dass die gesamte tolerierbare Ausfalldauer durch ein einzelnes Ereignis überschritten wird. Gemäß BCMS könnte jedoch bereits ein zeitkritischer Geschäftsprozess, der binnen 6 Stunden wiederanlaufen muss, als schlimmster anzunehmender Fall zu nicht tolerierbaren Auswirkungen für die Institution führen. Somit weicht die geforderte Wiederanlaufzeit von der bisher zugesicherten Verfügbarkeit von 99.9 % ab und verschärft die Anforderungen an die Verfügbarkeit der Anwendung in der Art, dass diese nach 4 Stunden wiederanlaufen muss.

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. So sollen zeitkritische IT-Services und deren zugrundliegenden IT-Systeme und IT-Ressourcen auch in einem IT-Notfall aufrechterhalten werden oder rasch wiederanlaufen können. Analog zum BCM nutzt das ITSCM dazu einen eigenen Management-Zyklus (PDCA – siehe auch ISO 27031 (siehe [27031]).

Dieser Standard setzt kein ITSCM voraus und beschreibt daher Aufgaben, die gegebenenfalls schon im ITSCM durchgeführt werden. Zu diesen Aufgaben gehören alle Aspekte, um die Ressource IT abzusichern. 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 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. Da jedoch aus einem Major Incident gemäß ITSCM leicht eine nicht tolerierbare Geschäftsunterbrechung entstehen kann, 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 redundantes Servercluster in Folge eines Hardwaredefektes aus. Aufgrund von Failover-Lösungen läuft der Betrieb ohne Unterbrechung über das verbleibende Servercluster weiter. Es handelt sich hierbei zwar aufgrund des Ausfalls der Redundanz um einen IT-Notfall, jedoch nicht unbedingt um einen Notfall im Sinne des BCM, da kein zeitkritischer

Geschäftsprozess unterbrochen ist. Die BAO sowie der oder die BC-Beauftragte werden über den Vorfall informiert und beobachten diesen weiter. Der Vorfall wird als IT-Notfall im Rahmen der Möglichkeiten des ITSCMs behoben. Ein aktiver Eingriff der BAO des BCMS ist nicht erforderlich.

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

- Rollen der BAO des BCM, sodass keine separaten Stabsstrukturen zwischen BCM und ITSCM entstehen,
- Alarmierungs- und Eskalationsverfahren,
- Informationsflüsse im (IT-)Notfall und in der Krise,
- Aufgabenmanagement im (IT-)Notfall und in der Krise,
- (IT-)Notfallpläne,
- Vermeidung separater (IT-)Notfall- und Krisenkommunikationsverfahren von BCM und ITSCM,
- Schulungen, Trainings, (IT-)Notfall- und Krisenübungen sowie
- technische Infrastrukturen für die (IT-)Notfall- und Krisenbewältigung.

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 dieses 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. Bei der Krise handelt es sich um eine außergewöhnliche Situation, für die keine BC-Planung möglich ist oder für die eine vorhandene BC-Planung 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 entschei-

den und umsetzen zu können. Die vorhandenen Notfallpläne werden in einer Krise so weit 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 Aspekte zur Bewältigung* näher ein. Dieses Hilfsmittel beschreibt auch die spezifischen Unterschiede zwischen einem Notfallstab und einem Krisenstab, falls z. B. in einer größeren bzw. international angesiedelten Institution mehrere Stäbe etabliert werden.

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 sowie
- 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 diskutiert werden, was wertvolle Zeit in Anspruch nimmt.

2.4.4 BCM und Outsourcing sowie Lieferketten

Outsourcing und der Bezug von externen Gütern in Lieferketten ist heutzutage in vielen Institutionen gängige Praxis. Im Rahmen des **Outsourcings** werden Geschäftsprozesse einer Institution vollständig oder teilweise durch externe Dienstleistungsunternehmen erbracht und somit nicht mehr ausschließlich durch die Institution selbst.

Hierzu können zuliefernde und dienstleistende Institutionen selbst wieder auf Zuliefernde und Dienstleistungsunternehmen zurückgreifen. Dadurch entsteht eine **Lieferkette** (engl. supply chain).

Hinweis

Grundversorger wie Strom-, Wasser- oder Gasanbieter werden im Kontext dieses Standards nicht als zuliefernde Institutionen einer Lieferkette verstanden, da die üblichen BC-Strategien zur Absicherung einer Lieferkette auf diese oftmals nicht angewendet werden können. Sie werden in diesem Standard als benötigte Ressource innerhalb der Business-Impact-Analyse und Risikoanalyse betrachtet. Geeignete BC-Strategien berücksichtigen den Ausfall eines Grundversorgers als Standortausfall.

Um sicherzustellen, dass mögliche Ausfallrisiken des Geschäftsbetriebes vermieden oder reduziert werden können, ist es erforderlich, BCM-Anforderungen an das Dienstleistungsunternehmen zu stellen. Dazu ist es notwendig, das Thema Outsourcing von zeitkritischen Dienstleistungen auch im BCMS zu verankern und Schnittstellen zu zeitkritischen Dienstleistungsunternehmen zu etablieren.

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 das Dienstleistungsunternehmen sicherstellen, dass der unterbrechungsfreie Geschäftsbetrieb seiner Leistung gewährleistet wird. Die beziehende Institution hat darauf keine oder nur begrenzte Einflussmöglichkeiten.

Sofern zeitkritische Geschäftsprozesse von externen Dienstleistungsunternehmen erbracht oder unterstützt werden, liegt es daher nicht mehr allein im Einflussbereich der güter- oder leistungsbeziehenden Institution, angemessen auf Notfälle zu reagieren und diese zu bewältigen. Notfälle auf Seiten von Dienstleistungsunternehmen wirken sich meistens unmittelbar auf den Geschäftsbetrieb der leistungsbeziehenden Institution aus und daher ist es wichtig, die zeitkritische Dienstleistung angemessen abzusichern. Folgende Sicherungsmaßnahmen sind möglich:

- die relevanten Ressourcen und Geschäftsprozesse von Dienstleistungsunternehmen in die eigene Notfallbewältigung mit einbinden und beide aufeinander abstimmen
- auf geeignete andere Dienstleistungsunternehmen zurückgreifen
- die Fähigkeit gewährleisten, die Dienstleistung umgehend wieder in der eigenen Institution zu erbringen

Die BC-Strategien für einen Ausfall eines Dienstleistungsunternehmenswerden für zeitkritische Dienstleistungsunternehmen im Rahmen des Prozessschritts 10 *Business-Continuity-Strategien und -Lösungen (AS)* ausgewählt. Hier ist es essenziell, dass das angestrebte Leistungsniveau des oder der Dienstleistenden in einem Notfall dem Anspruch der leistungsbeziehenden Institution gerecht wird. Da hier viele Aspekte wichtig sind, werden ausführliche Hilfestellungen zu den einzelnen BC-Strategien im Bereich Outsourcing im Hilfsmittel *BC-Strategievorschläge* gegeben.

2.5 Überblick über Normen und Standards

BCM wird in verschiedenen Normen sowie nationalen und internationalen Standards behandelt. Die 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.

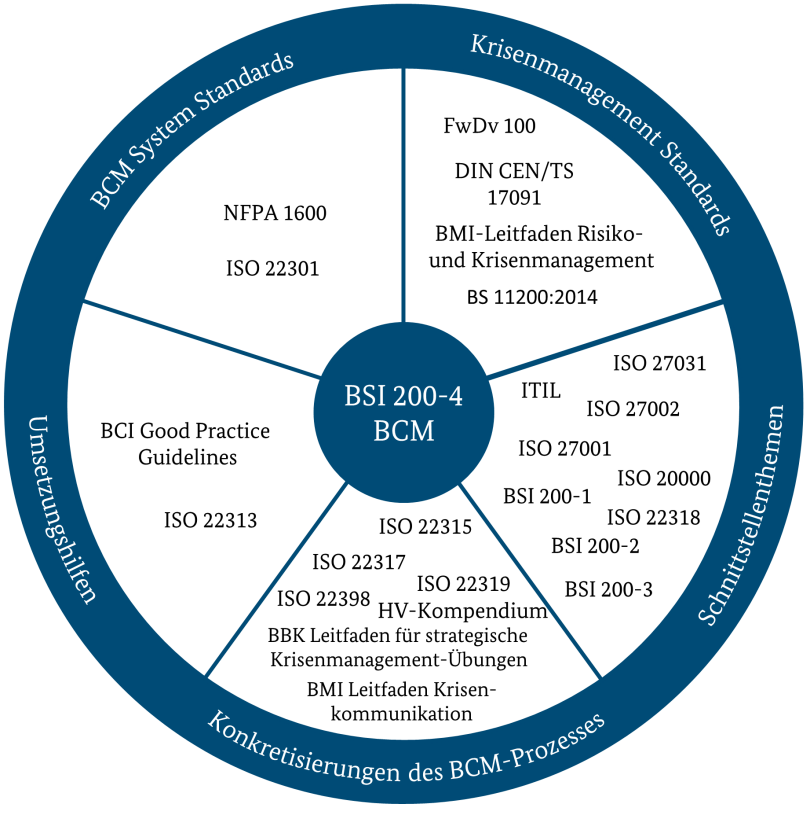

Abbildung 7: Übersicht über BCM-Standards sowie korrespondierende Sicherheitsthemen

ISO 22301:2019 (abgekürzt ISO 22301)

Die ISO-Norm 22301 „Security and resilience – Business continuity management systems – Requirements“ (siehe [22301]) ist der erste internationale Standard zum BCM, der auch eine Zertifizierung ermöglicht. Diese Norm unterstützt Institutionen dabei, die Risiken von Betriebsunterbrechungen jeglichen Ursprungs zu reduzieren. Beschrieben werden alle Anforderungen, um ein BCMS planen, einrichten, betreiben, überwachen, überprüfen und kontinuierlich verbessern zu können.

Die internationale Norm erschien erstmalig im Jahr 2012 und ersetzte die Reihe des British Standard BS 25999. Die ISO 22301 wurde 2019 überarbeitet und der BSI-Standard 200-4 ist kompatibel zu dieser überarbeiteten Version. Im Gegensatz zu diesem BSI-Standard stellt die ISO-Norm 22301 Anforderungen auf abstrakterer Ebene.

Ergänzende ISO-Standards der ISO-Reihe 22300 konkretisieren einzelne Aspekte oder Schnittstellen zum BCM. Dazu gehören z. B. die folgenden Normen:

- 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])

- ISO 22318:2015 „Societal security – Business continuity management systems – Guidelines for supply chain continuity“ (siehe [22318])
- ISO 22398:2013 „Societal security — Guidelines for exercises" (siehe [22398])

BSI-Standards

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

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 Analyse 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 Vorgehensweise kann auch im Rahmen der BCM-Risikoanalyse des BSI-Standards 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 im Bereich des BCM zu setzen und Kompetenz aufzubauen. Im Jahre 2002 wurden zum ersten Mal die Good Practice Guidelines herausgegeben, die von Mitgliedern des Business Continuity Institutes (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 zum einen eine Anleitung, wie die Anforderungen in der Krisenkommunikation analysiert werden können, und zum anderen einen Musteraufbau, um einen Krisenkommunikationsplan zu erarbeiten.

ITIL

ITIL (Information Technology Infrastructure Library) wird von AXELOS herausgegeben, gepflegt und weiterentwickelt (siehe [ITIL]). ITIL erläutert, wie Institutionen anhand von Technologien und Werkzeugen das Servicemanagement digital transformieren können. Sie berücksichtigt aktuelle Trends wie Agile Softwareentwicklung, DevOps und Lean IT-Management.

Da in der Praxis der IT-Betrieb häufig nach ITIL ausgerichtet ist, kann das BCM auf diese Strukturen zurückgreifen, insbesondere auf das Incident und das IT-Service Continuity Management.

Leitfäden der Bundesländer zum Krisenmanagement

Verschiedene Bundesländer veröffentlichen länderspezifische Leitfäden zum Krisenmanagement, z. B:

- den *Leitfaden Krisenmanagement durch Krisenstäbe im Land 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 (Reaktiv-, Aufbau- und Standard-BCMS)

Der BSI-Standard 200-4 richtet sich an Institutionen jeglicher Art, Branche und Größe. Entsprechend sind auch die zeitlichen, finanziellen und personellen Möglichkeiten sowie die Vorerfahrungen, um ein BCMS aufzubauen, in jeder Institution unterschiedlich. Um den verschiedenen Vorerfahrungen und den unterschiedlichen Möglichkeiten aller Institutionen Rechnung zu tragen, bietet dieser Standard ein Stufenmodell mit den drei Stufen Reaktiv-, Aufbau- und Standard-BCMS:

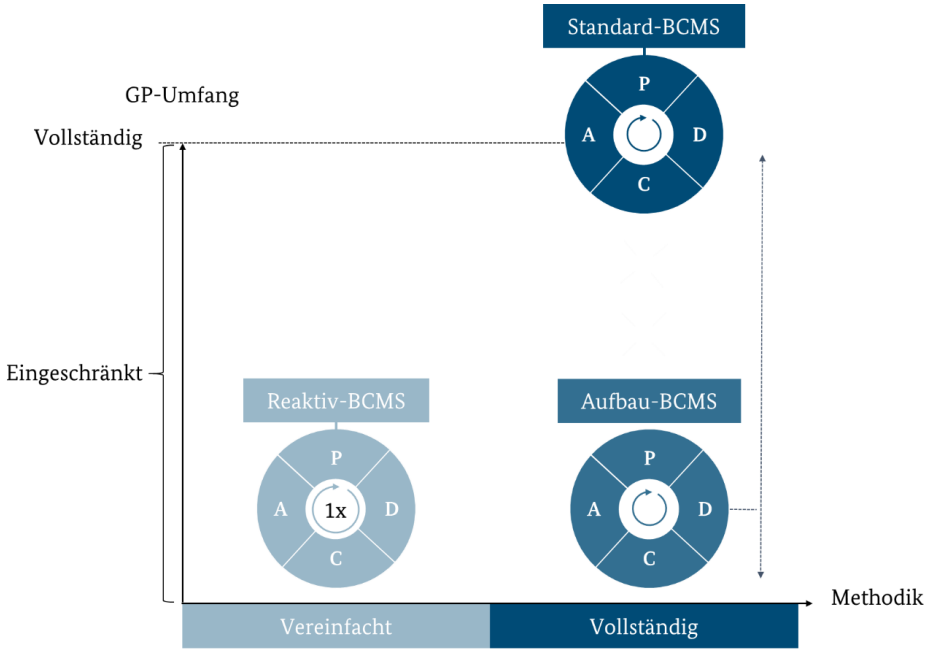

Abbildung 8: Übersicht über das BCMS-Stufenmodell

Wie in Abbildung 8: *Übersicht über das BCMS-Stufenmodell* ersichtlich ist, wird das Stufenmodell in 2 Dimensionen vereinfacht:

Methodik: Die Methodik kann im Reaktiv-BCMS vereinfacht werden, indem diejenigen Analysemethoden zeitlich zurückgestellt werden, die der detaillierteren Analyse der Rahmenbedingungen des BCMS oder der Notfallvorsorge dienen. Detaillierte Analysen werden dann erst in einer der beiden nachfolgenden Stufen mit vollständiger Methodik bearbeitet. In der vollständigen Methodik, die im Aufbau- und Standard-BCMS angewendet wird, werden Aspekte der Notfallvorsorge und der Notfallbewältigung gleichermaßen berücksichtigt. Auch die jeweiligen Methoden der einzelnen BCMS-Prozessschritte sind im Aufbau- und Standard-BCMS erweitert, um detailliertere Ergebnisse zu ermöglichen. In diesem beiden Stufen mit vollständiger Methodik kann so zum einen das BCMS deutlich effektiver und zielgerichteter aufgebaut werden. Zum anderen kann die BAO konkreter und bedarfsorientierter definiert werden.

GP-Umfang (Geschäftsprozessumfang): Im Rahmen der Initiierung des BCMS wird dessen Geltungsbereich festgelegt. Unabhängig vom Geltungsbereich des BCMS kann anhand eines eingeschränkten GP-Umfangs der Ressourcenaufwand zunächst reduziert werden (Reaktiv- und Aufbau-BCMS). Anschließend kann der GP-Umfang mit jedem weiteren Zyklus schrittweise gesteigert werden, bis alle Geschäftsprozesse im Geltungsbereich des BCMS betrachtet werden (Standard-BCMS).

2.6.1 Übersicht zum Stufenmodell

Für jede Institution sollte das Ziel darin bestehen, ein Standard-BCMS zu erreichen und zu etablieren, um alle zeitkritischen Geschäftsprozesse angemessen abzusichern. Falls nicht von Anfang an ein Standard-BCMS etabliert wird, stellen sowohl das Reaktiv-BCMS als auch das Aufbau-BCMS eine dezidierte Einstiegstufe dar, wobei das Aufbau-BCMS für fortgeschrittene Anwendende geeignet ist. Das Aufbau BCMS erleichtert zudem erheblich den Übergang vom Reaktiv- zum Standard-BCMS:

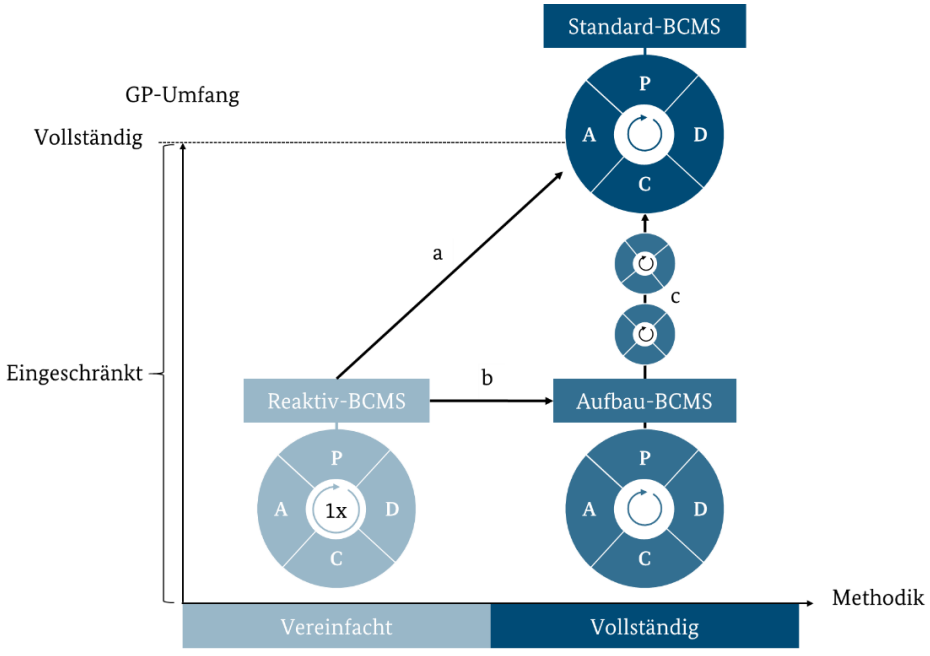

Abbildung 9: BCMS-Stufen und Übergang zwischen den Stufen

Während der Initiierung des BCMS kann jede Institution die für sie optimale BCMS-Stufe auswählen. Wie in Abbildung 9 dargestellt, bestehen verschiedene Möglichkeiten, um von den Einstiegsstufen zur höchsten Stufe, dem Standard-BCMS, zu gelangen.

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 gesteigerte Resilienz der Institution
Nachteile	Lücken in der Absicherung von Bereichen, die nicht oder nur teilweise betrachtet werden	Bereiche, die in der Absicherung der Institution nicht betrachtet werden	Größerer Ressourcenbedarf in einem Zyklus 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, soweit mit vorhanden Mitteln oder kleineren Investitionen möglich. Weitere Maßnahmen im BCM, für die zunächst der Geschäftsbetrieb einge-

hender analysiert werden müsste, werden bewusst zeitlich zurückgestellt und erst durch den Wechsel zu einem Standard-BCMS (Pfad a in Abbildung 9) oder Aufbau-BCMS (Pfad b Abbildung 9) 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 nur ein Ausschnitt des BCMS-Geltungsbereichs, nämlich der eingeschränkte GP-Umfang, näher analysiert und innerhalb des BCM abgesichert wird. Dieser GP-Umfang wird so gewählt, dass möglichst viele der zeitkritischsten Geschäftsprozesse darin enthalten sind (siehe Kapitel 6 *BIA-Vorfilter (R+A)).* 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 9). Ist einmal ein Aufbau-BCMS erreicht, ist die nötige Kenntnis vorhanden, um die Weiterentwicklung bis hin zum Standard-BCMS gut planen und skalieren zu können. 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 analysiert, die sich im Geltungsbereich des BCMS befinden. 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. **Ein Reaktiv-BCMS ist grundlegend für den Einstieg geeignet, sofern keine regulatorischen Anforderungen dagegensprechen**. Die im Folgenden aufgeführten Kriterien behandeln besondere Situationen, in denen eher die beiden weiteren Stufen Aufbau- und Standard-BCMS zum Einstieg empfohlen werden:

- **Gesetzliche oder regulatorische Anforderungen** (Die Institution muss gesetzliche oder regulatorische Anforderungen erfüllen. Diese setzen voraus, dass alle da-

von betroffenen Geschäftsprozesse im BCMS zeitnah untersucht und angemessen abgesichert werden.)

- **Vorerfahrung mit Managementsystemen** (Die Institution greift auf Erfahrungen zum Aufbau und Betrieb eines Managementsystems zurück, z. B. weil bereits ein ISMS auf Basis von IT-Grundschutz oder ISO 27001 (siehe [27001]) etabliert wurde.)
- **Vorerfahrung in einzelnen Aspekten des BCM oder der Krisenbewältigung** (Die Institution hat bereits eine BAO zur Bewältigung von Notfällen oder Krisen etabliert oder hat bereits Erfahrungen mit BCM und Krisenmanagement.)
- **BCMS ist bereits etabliert** (Die Institution hat bereits ein BCMS nach BSI-Standard 100-4 oder ISO 22301 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 (sofern alle regulierten GPs im GP-Umfang liegen)	X
Es existiert solide Vorerfahrung mit Managementsystemen	X	
Es existiert Vorerfahrung in einzelnen Aspekten des BCM oder der Krisenbewältigung	X	
BCMS ist bereits etabliert		X
Ressourcenausstattung ist gut	X	X

Tabelle 3: Gegenüberstellung der BCMS-Stufen anhand verschiedener Kriterien

2.6.2 Übersicht über den BCMS-Prozess

Das vorliegende Kapitel gibt eine grundlegende Übersicht über den BCM-Prozess, der sich an den einzelnen Phasen des PDCA-Zyklus orientiert (siehe Abbildung 10).

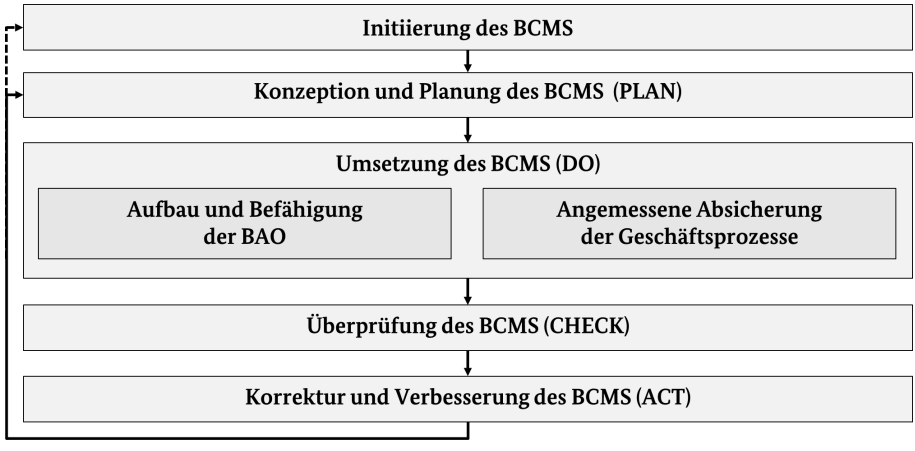

Abbildung 10: PDCA-Struktur des BCMS-Prozesses

Die einzelnen Phasen teilen sich in unterschiedliche BCMS-Prozessschritte auf, die in der nachfolgenden Übersicht in Abbildung 11 dargestellt werden. Abbildung 11 bezieht sich auf das Standard-BCMS, da dieses alle Schritte beinhaltet, um ein vollständiges, angemessenes und interessengruppengerechtes BCMS zu etablieren. Reaktiv- und Aufbau-BCMS weichen in gewissen Prozessschritten von dieser Übersicht ab. Dies ist im Folgenden sowohl in der Abbildung 11 als auch in den Beschreibungen der Prozessschritte entsprechend gekennzeichnet. Nach allen Prozessschritten sind die weiteren Kapitel dieses Standards strukturiert.

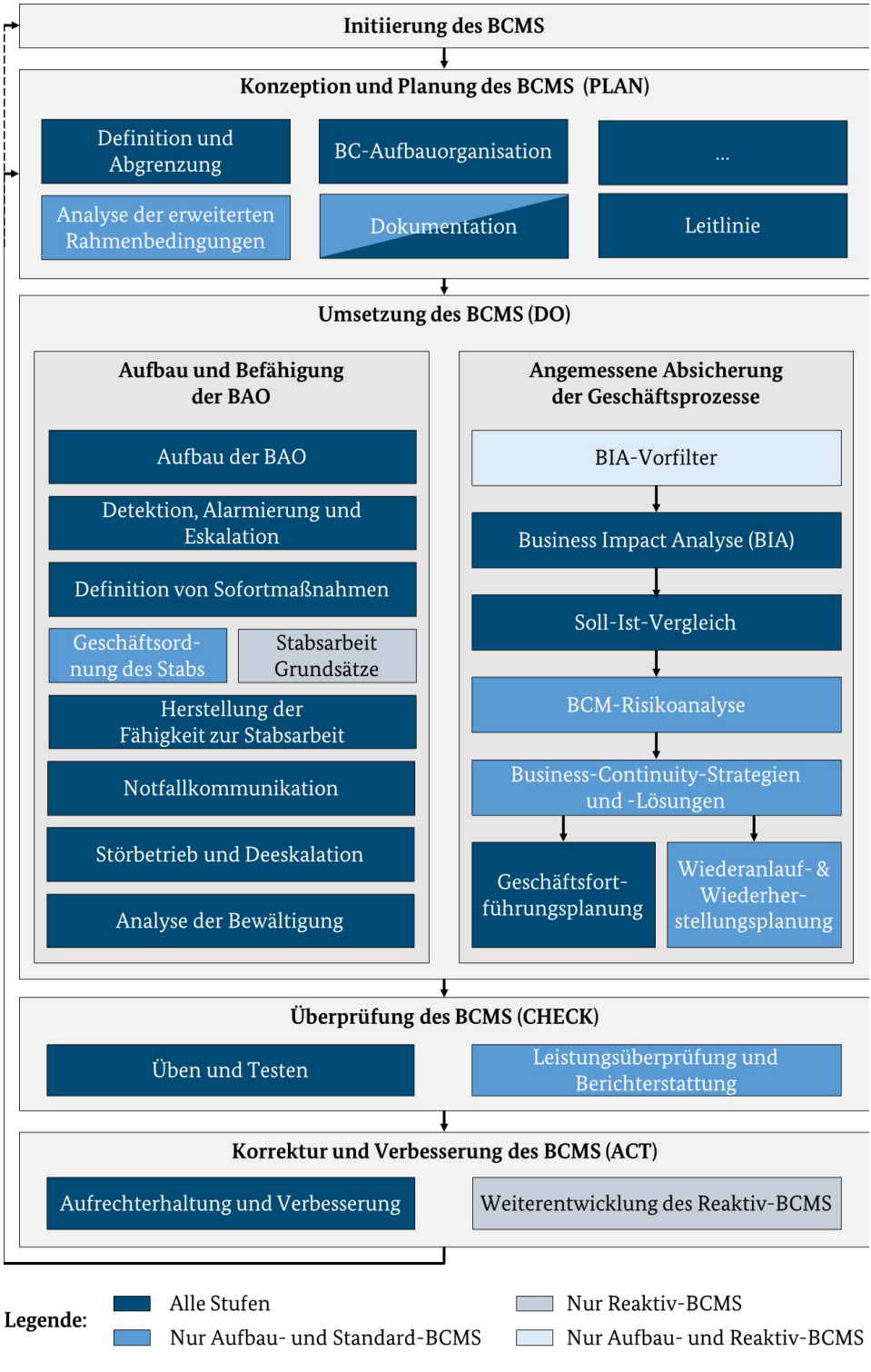

Abbildung 11: BCM-Prozess Gesamtübersicht

Initiierung

Um ein Managementsystem erstmals aufzubauen und einen PDCA-Zyklus zu starten, sind zu Beginn zusätzliche Tätigkeiten erforderlich, die in der **Initiierung** stattfinden. Dieser Schritt wird von allen **BCMS-Stufen** benötigt und richtet sich primär an die **Institutionsleitung**. In diesem Schritt bekennt sich die Institutionsleitung zu ihrer Verantwortung, legt die Zielsetzung und den Geltungsbereich des BCMS fest, wählt eine geeignete BCMS-Stufe für den Einstieg aus und beauftragt eine oder einen BCB.

Dieser Schritt wird im Gegensatz zu der nachfolgenden **Plan-Phase** nicht im selben Detailgrad in den nachfolgenden PDCA-Zyklen durchlaufen. Daher erhält er auch keinen eigenen Buchstaben in der Abkürzung PDCA. Die Ergebnisse der Initiierung fließen in die **Leitlinie BCMS** ein.

Plan-Phase

In der Plan-Phase werden in **allen BCMS-Stufen** grundlegende Aspekte geregelt, ohne die das BCMS nicht etabliert werden kann, z. B. die **BC-Aufbauorganisation**, die **Definition und Abgrenzung**, sowie die **Dokumentation** zur Reaktion. Im **Aufbau**- und **Standard-BCMS** werden die Vorgaben an die Dokumentation formaler geregelt, damit alle Dokumente des BCMS auf einem gleichbleibenden, hohen Qualitätsniveau sind.

Für den Erfolg des **Aufbau- und Standard-BCMS** ist es ferner entscheidend, die **Rahmenbedingungen** zu dem BCMS genau zu **analysieren** und das BCMS auf die berechtigten Bedürfnisse und Anforderungen von relevanten Interessengruppen auszurichten. Nur so kann sichergestellt werden, dass das BCMS anforderungsgerecht aufgebaut und betrieben wird. Demgegenüber können diese erweiterten Analysemethoden im **Reaktiv-BCMS** ausgelassen werden, da dieses darauf abzielt, schnellstmöglich eine rudimentäre Reaktionsfähigkeit in Notfällen und Krisen herzustellen.

Für alle Stufen dokumentiert die Institutionsleitung in der **Leitlinie BCMS** ihre Selbstverpflichtung und legt die Rahmenbedingungen für das BCMS fest, z. B. die Ressourcenausstattung.

Do-Phase

Der Prozessschritt **Aufbau und Befähigung der BAO** beinhaltet alle Aspekte, um eine funktionierende BAO zu etablieren, die im Not- und Krisenfall sofort erreichbar und arbeitsfähig ist. Die Institution wird so im Fall von Schadensereignissen unmittelbar handlungsfähig, unabhängig davon, ob bereits Notfallpläne für die Fortführung von Geschäftsprozessen vorliegen. Im **Reaktiv-BCMS** kann hierbei auf die Geschäftsordnung des Stabes als formale Dokumentation und Organisation für eine rudimentäre Vorfallbehandlung verzichtet werden.

Alle weiteren Prozessschritte in der **DO-Phase** dienen der **angemessenen Absicherung der zeitkritischen Geschäftsprozesse**. Fast jeder dieser Schritte verbessert die Möglichkeiten, einen Vorfall in einer geordneten BC-Planung zu behandeln anstatt nur reaktiv in einer Krise.

Die **Business-Impact-Analyse** untersucht näher, was innerhalb des Untersuchungsbereichs abgesichert werden soll. Dazu analysiert die Institution, welche Geschäftsprozesse im Untersuchungsbereich zeitkritisch sind, wie lange diese ausfallen dürfen und welche Ressourcen sie im Notbetrieb benötigen. Da die Business-Impact-Analyse mit einem erhöhten Aufwand verbunden ist und eine langwierige Untersuchung eine schnelle BC-Planung verzögern kann, wird ihr im **Reaktiv-** und **Aufbau-BCMS** ein **BIA-Vorfilter** vorangestellt. Dieser BIA-Vorfilter filtert den Untersuchungsbereich der BIA grob vor, sodass in dieser nur noch die zeitkritischsten Einheiten untersucht werden. Mit dem Ergebnis beider Schritte kann die BAO bereits deutlich gezielter auf Schadensereignisse reagieren und frühzeitig erkennen, welche Ressourcen z. B. als erstes wieder anlaufen müssen sowie diesen Wiederanlauf koordinieren. Die BAO erkennt auch frühzeitig, wenn dies nicht möglich ist, und kann gegebenenfalls entsprechende Gegenmaßnahmen einleiten.

Im **Soll-Ist-Vergleich** wird festgestellt, ob die benötigten Ressourcen schon ausreichend abgesichert sind. Mit diesen Informationen kann die BAO in einem Schadensfall direkt erkennen, wo lediglich der Wiederanlauf gestartet werden muss und wo noch weitere Aktionen benötigt werden.

Anschließend unterscheidet sich die Vorgehensweise des Reaktiv-BCMS elementar von derjenigen im Aufbau- sowie Standard-BCMS. Das **Reaktiv-BCMS** sieht im Anschluss nur eine rudimentäre BC-Planung im Rahmen der **Geschäftsfortführungspläne** vor. Einerseits bestehen auf dieser Stufe große Lücken in der Analysephase, sodass umfangreiche, zielgerichtete Investitionen zur BC-Planung nur eingeschränkt getätigt werden können. Andererseits fokussiert das Reaktiv-BCMS in der BC-Planung bewusst bereits vorhandene Lösungen sowie schnell und einfach umsetzbare Maßnahmen, damit schnellstmöglich eine rudimentäre BC-Planung erstellt werden kann.

Demgegenüber verfolgen das **Aufbau**- und **Standard-BCMS** einen vollständigen Ansatz zur BC-Planung. In diesen beiden Stufen wird in der **BCM-Risikoanalyse** 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**, bezogen auf Geschäftsprozesse, und die **Wiederanlaufpläne**, bezogen auf Ressourcen, die Handlungsschritte, die im Notfall durchgeführt werden müssen, damit die zeitkritischen Geschäftsprozesse innerhalb der geforderten Zeit fortgeführt werden können. Die **Wiederherstellungspläne** geben Hilfestellungen, welche Handlungsschritte nötig sind, um wieder ausreichend Ressourcen 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. Dieser Schritt ist auch für das **Reaktiv-BCMS** essenziell, da eine ungeübte Lösung extrem fehleranfällig sein kann. Zusätzlich wird im **Aufbau-** und

Standard-BCMS 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, die **im Aufbau- und Standard-BCMS** umgesetzt und auch weiter nachverfolgt werden. In einem **Reaktiv-BCMS** wird in der Act-Phase zusätzlich der gezielte Übergang in eine folgende Stufe geplant.

Umsetzungsreihenfolge der Do-Phase

Wie in Abbildung 11 dargestellt, können der Aufbau der BAO und die angemessene Absicherung der Geschäftsprozesse prinzipiell parallel erfolgen. Da aber häufig nur eingeschränkte Ressourcen zur Verfügung stehen und natürlich auch inhaltliche Querverbindungen zwischen den beiden parallelen Prozessreihen bestehen, stellt sich die Frage, in welcher Reihenfolge diese beiden Aspekte bearbeitet werden sollten.

Zur Übersicht zeigt Abbildung 12, welche Aspekte der Notfallbewältigung jeweils vorbereitet werden.

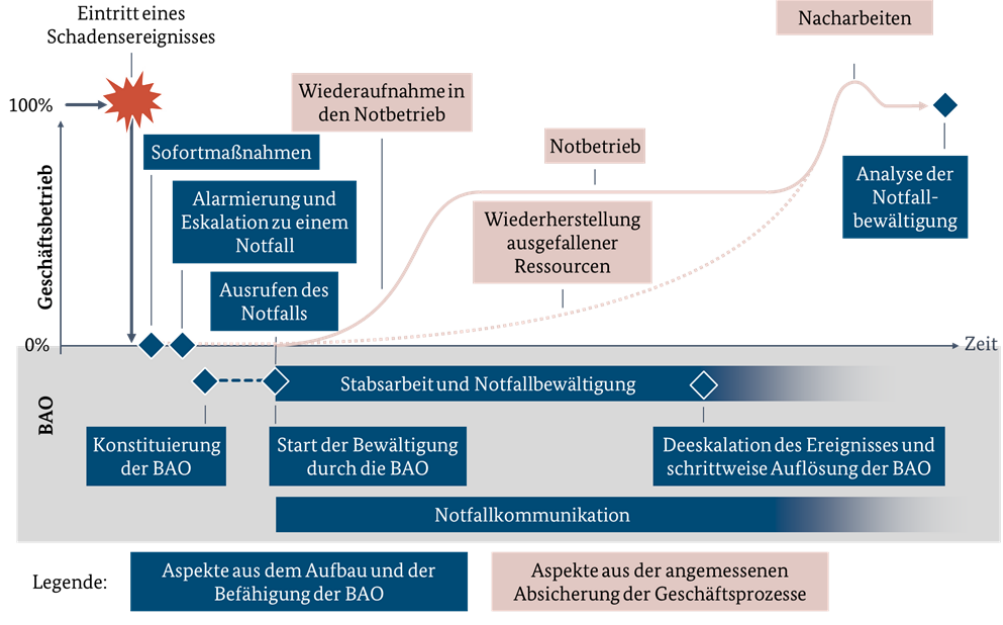

Abbildung 12: Vorbereitung der Notfallbewältigung

Im Rahmen des **Reaktiv-BCMS** ist es sinnvoll, immer zuerst mit dem Aufbau der BAO zu beginnen, da Anwendende eines Reaktiv-BCMS in der Regel noch über gar keine Absicherung verfügen und eine BAO zumindest eine rudimentäre Bewältigung ermöglicht. Anschließend verbessert jeder Zwischenschritt aus der angemessenen Absicherung der

Geschäftsprozesse die Möglichkeiten, ein Schadensereignis geordnet als Notfall zu bewältigen.

Demgegenüber kann auf der Stufe des Aufbau- oder Standard-BCMS frei entschieden werden, ob die BAO **vor**, **gleichzeitig mit** oder **nach** der angemessenen Absicherung der Geschäftsprozesse aufgebaut und befähigt wird. Es bestehen unterschiedliche Vorteile, die im Folgenden erläutert werden:

Wird die BAO **vor der angemessenen Absicherung der Geschäftsprozesse aufgebaut und befähigt**, ermöglicht dies schneller eine allgemeine Reaktionsfähigkeit in einem Schadensereignis. In diesem Fall ist es sinnvoll, die Teams, die das Schadensereignis bewältigen (siehe hierzu auch 5.1 *Aufbau der BAO (R+AS)*), nach Untersuchung der Geschäftsprozesse gegebenenfalls noch einmal anzupassen und sich dabei konkreter an dem Bedarf zu orientieren.

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 wird. 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 BC-Planung auszurichten. Dies bedeutet jedoch auch, dass erst zu einem späteren Zeitpunkt eine allgemeine Reaktionsfähigkeit für Notfälle vorhanden ist.

3 Initiierung des BCMS durch die Institutionsleitung (R+AS)

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 BCMS muss von der Institutionsleitung initiiert werden, weil die zu treffenden Entscheidungen weitreichende Konsequenzen haben. Wie in Abbildung 13 dargestellt, erläutern die nachfolgenden Unterkapitel die Zwischenschritte zur Initiierung des BCMS durch die Institutionsleitung. Alle wesentlichen Inhalte der Initiierung und des nachfolgenden Kapitels 4 *Konzeption und Planung des BCMS (R+AS)* werden in der Leitlinie BCMS dokumentiert. Eine Vorlage hierfür kann den Hilfsmitteln zum Standard entnommen werden.

Abbildung 13: BCM-Prozessschritte zur Initiierung des BCMS durch die Institutionsleitung

3.1 Übernahme der Verantwortung durch die Leitungsebene (R+AS)

Die Institutionsleitung ist für das zielgerichtete und ordnungsgemäße Funktionieren der Institution und damit auch für die Aufrechterhaltung des Geschäftsbetriebs in Notfällen verantwortlich. Sie 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 Vorbild sein. Die Institutionsleitung muss sich zur Etablierung, Aufrechterhaltung und Verbesserung eines BCMS anhand der Vorgehensweise dieses Standards verpflichten. Idealerweise übernimmt hierzu ein Mitglied der Institutionsleitung die Rolle als Prozesseigentümer oder -eigentümerin, der oder die für das BCM verantwortlich ist. Die operativen Aufgaben im Kontext BCM werden an eine Person delegiert, die als der oder die **Business Continuity Beauftragte** (**BCB** oder **BC-Beauftragte**) bezeichnet wird (siehe 3.5 *Benennung des oder der BC-Beauftragten*). Die Institutionsleitung muss darüber hinaus alle Führungskräfte darin unterstützen, sodass die

Führungskräfte in ihren Bereichen effektiv und effizient zur Etablierung, Aufrechterhaltung und Verbesserung beitragen können.

Die Institutionsleitung muss aktiv Informationen über den Status Quo des BCM einfordern (siehe 14.4 *Managementbewertung (AS)*). Zudem muss sie das BCM durch Managemententscheidungen so steuern, dass das BCMS angemessen, wirksam und anforderungsgerecht ist. Darüber hinaus ist es empfehlenswert, dass die Institutionsleitung an ausgewählten Schulungen, Trainings und Übungen teilnimmt und andere Führungskräfte bei der Ausübung ihrer Vorbildfunktion unterstützt.

Synergiepotenzial

Das BCM weist vielfältige Berührungspunkte zu anderen Disziplinen 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 wirtschaftlicher und effektiver umgesetzt wird.

3.2 Zielsetzung (R+AS)

Jede Institution braucht eine individuelle Zielsetzung für ein angemessenes BCM. Diese lässt sich aus den Geschäftsprozessen bzw. Fachaufgaben, den gesetzlichen Rahmenbedingungen und insbesondere den jeweiligen Institutionszielen ableiten. Die Institutionsleitung muss die Ziele für das BCM vorgeben und sie innerhalb der Institution kommunizieren, sodass alle Mitarbeitenden erreicht werden. Es ist empfehlenswert, dies über die Leitlinie BCMS sicherzustellen (siehe 4.8.2 *Veröffentlichung und Aktualisierung der Leitlinie BCMS (R+AS)*). Die Leitung setzt ein klares *Startsignal*, indem sie sämtlichen Interessengruppen der Institution die Ziele des BCM bekannt gibt. Gleichzeitig vergibt die Institutionsleitung den dafür notwendigen Arbeitsauftrag an die taktische und operative Ebene.

Die Ziele des BCM müssen zu den Anforderungen an das BCMS und zu der strategischen Ausrichtung der Institution passen und sollten unmittelbar die Gründe und hier insbesondere die verpflichtenden externen Gründe für ein BCMS berücksichtigen. Darüber hinaus sollten die definierten Ziele messbar sein, sofern dies sinnvoll umsetzbar ist.

Die Zielsetzung geht vorrangig auf drei Fragen ein:

- Warum wird in der Institution ein BCM benötigt? (Motivation für den Aufbau eines BCMS)
- Welche konkreten Ziele werden mit dem BCM verfolgt?
- Wie lange soll durch das BCM ein Ausfall des Normalbetriebs kompensiert werden? (Abzusichernder Zeitraum durch ein BCM)

3.2.1 Motivation für den Aufbau eines BCMS (R+AS)

Die Institution sollte die spezifischen Gründe für ein BCM identifizieren, dokumentieren und das BCMS danach ausrichten. Die Gründe für ein BCM ergeben sich aus bestimmten Rahmenbedingungen der Institution. Solche Rahmenbedingungen sind z. B. gesetzliche Regelungen oder bestimmte Erwartungshaltungen von Kunden und Kundinnen oder Aufsichtsbehörden. Zudem können Erkenntnisse aus aktuellen Umfeld- und Risikoanalysen in die Zielsetzung einfließen, z. B. aus dem (Informationssicherheits-)Risikomanagement. 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 ein BCMS

Ein BCMS liegt insbesondere im Eigeninteresse einer Institution, denn BCM trägt dazu bei, die Überlebensfähigkeit der Institution in Notfällen und Krisen zu erhöhen und erleichtert flexible Reaktionen. 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.

Um wirksam sein zu können, erfordert das BCMS einen gewissen Aufwand an Arbeitszeit und zusätzlichen Ressourcen, d. h. Material und Finanzmittel. Darüber hinaus erfordert BCM, 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.

Externe Gründe für BCMS

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 des Umsetzungsplans Bund dazu verpflichtet, für zeitkritische Geschäftsprozesse Maßnahmen zu entwickeln, um die Arbeitsfähigkeit sicherzustellen.

Zusätzlich erläutert die Konzeption Zivile Verteidigung (siehe [BMI2]) 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 BCMS zu etablieren. Aus gesetzlichen Anforderungen und aus Vorgaben einer Muttergesellschaft kann

sich jedoch die Notwendigkeit ergeben, ein BCMS zu betreiben. Auch andere Verpflichtungen können ein BCMS erfordern, z. B. Verträge mit Kunden und Kundinnen oder Geschäftspartnern und -partnerinnen oder deren Erwartungshaltungen.

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

Z. B. durch die folgenden Gesetze, Verordnungen und Richtlinien (regulatorische Anforderungen) ergeben sich für die betroffenen Unternehmen und Behörden Verpflichtungen zum BCM:

- 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)

Synergiepotenzial

Sofern zuvor ein ISMS nach BSI-Standard 200-2 oder ISO-Norm 27001 etabliert wurde, liegen für das BCM bereits verwendbare Informationen vor, 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.

3.2.2 Entwicklung der Ziele des BCMS (R+AS)

Die Institutionsleitung muss die strategischen Ziele festlegen, die mit dem Aufbau und dem Betrieb des BCMS verfolgt werden. So ist es empfehlenswert, bei den Zielen zu berücksichtigen,

- welche Geschäftsziele geschützt werden sollen,
- welche Arten von Geschäftsunterbrechungen als existenzbedrohend angesehen werden (grobe Vorgaben hinsichtlich Schadenshöhe und zu betrachtenden Schadensszenarien),
- welche Bereitschaft besteht, Risiken einzugehen (Risikobereitschaft),
- in welcher Art und Größenordnung Risiken minimiert werden sollen sowie
- was das primäre Ziel der Bewältigung ist.

Darüber hinaus muss in der Zielsetzung festgelegt werden, dass das BCMS anhand der Vorgaben des BSI-Standard 200-4 etabliert, aufrechterhalten und verbessert wird.

Beispiel

Folgende Ziele könnten beispielsweise auf strategischer Ebene festgelegt werden:

- *Die Abwicklung bestehender Aufträge steht im Vordergrund und es wird kein Neugeschäft angenommen.*
- *Das BCMS wird anhand des BCM-Prozesses aus dem BSI-Standard 200-4 aufgebaut. Nach zwei Jahren wird ein Aufbau-BCMS erreicht und nach insgesamt fünf Jahren ist ein Standard-BCMS etabliert.*
- *Alle Geschäftsprozesse sollen mit mindestens 50 % der Leistungsfähigkeit oder des Durchsatzes auch im Notfall funktionieren.*
- *Das primäre Ziel der Bewältigung ist, die Ausbreitung des Schadens zu verhindern. Dies hat Priorität vor dem schnellstmöglichen Wiederanlauf.*

3.2.3 Abzusichernder Zeitraum durch ein BCMS (R+AS)

Wesentlich für die Zielsetzung ist auch die Frage, wie lange der Geschäftsbetrieb durch das BCMS abgesichert werden soll, d. h. wie lange die Geschäftsfortführung im Schadensfall gewährleistet werden soll (abzusichernder Zeitraum). Tendenziell kann davon

ausgegangen werden, dass die Maßnahmen im BCM umso komplexer und damit auch teurer werden, desto länger ein Ausfall des Geschäftsbetriebs abgesichert und überbrückt werden soll. Im selben Maße steigt jedoch auch die Resilienz der Institution gegen längere Ausfälle, denn je länger der abzusichernde Zeitraum gewählt wird, desto mehr Geschäftsprozesse werden für gewöhnlich abgesichert. Notfälle, die länger als der vom BCMS abgesicherte Zeitraum andauern, führen typischerweise dazu, dass ergänzende Maßnahmen aus dem Krisenmanagement aktiviert werden. Der abzusichernde Zeitraum muss für die Institution individuell festgelegt werden, da dieser stark von unterschiedlichen Gegebenheiten abhängt, z. B. von

- der Risikobereitschaft der Institution (Je kürzer der abzusichernde Zeitraum gewählt wird, desto eher muss das Krisenmanagement aktiviert werden.),
- dem Zeitraum, über den die Institution ohne Umsätze überlebensfähig ist,
- dem Reifegrad des BCMS,
- den 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.

In der Praxis ist ein Zeitraum von 14 bis 30 Tagen üblich. Mehrwöchige Ausfälle bzw. Notfälle sind nicht unrealistisch, sondern kommen in der Praxis durchaus vor. In der Regel ist jedoch auch gleichzeitig eine Wiederherstellung vieler Ressourcen binnen weniger Wochen möglich, abgesehen von Großschadensereignissen wie kompletten Gebäudezerstörungen. Die Institution wird durch ein BCMS in die Lage versetzt, über den abzusichernden Zeitraum grundsätzlich handlungsfähig zu bleiben. Falls absehbar ist, dass ein Ausfall diesen Zeitraum überschreitet, ist es innerhalb der vom BCM häufig abgesicherten 14 bis 30 Tage oft noch möglich, weiterführende Notfallmaßnahmen zu planen und umzusetzen. Der abzusichernde Zeitraum im BCM sollte regelmäßig auf seine Angemessenheit überprüft und falls erforderlich angepasst werden.

Baut eine Institution ihr BCM erst in einem **Reaktiv-BCMS** auf und unterliegt keinen besonderen Anforderungen, dann ist es möglicherweise zunächst akzeptabel, einen kürzeren Zeitraum zu wählen.	**R**

Beispiel

Die Leitung eines mittelständischen Unternehmens ohne Vorerfahrung im BCM legt für sich fest, dass der Ausfall des Geschäftsbetriebs für einen gesamten Monat die finanziellen Rücklagen des Unternehmens aufbrauchen würde. Gleichzeitig wird den agilen Problemlösungsfähigkeiten der Belegschaft und dem guten Netzwerk aus Geschäftspartnern, Geschäftspartnerinnen und Dienstleistungsunternehmen vertraut.

Die Institutionsleitung entscheidet sich daher unter Aufwands- und Risikogesichtspunkten, zunächst den abzusichernden Zeitraum durch das BCMS auf 14 Tage festzulegen und für diesen Zeitraum Notfallvorsorge zu betreiben.

Hinweis

Bei einem falsch gewählten Zeitraum besteht die Gefahr, dass das BCMS die eigenen Geschäftsprozesse nicht angemessen absichert. Deswegen ist es wichtig, den Zeitrahmen nachfolgenden Gesichtspunkten festzulegen:

- *Ist der Zeitraum zu kurz gewählt, werden möglicherweise weniger zeitkritische, aber dennoch relevante Geschäftsprozesse gar nicht identifiziert und sehr zeitkritische Geschäftsprozesse nicht genug abgesichert.*
- *Ist der Zeitraum zu lang gewählt, dann werden die Aufwände für das BCMS zu hoch und die vorhandenen Ressourcen stehen den zeitkritischsten Geschäftsprozessen selbst nicht ausreichend zur Verfügung.*

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

Beispiel

Ein Produktionsunternehmen in der Automobilbranche erwirtschaftet seinen Umsatz hauptsächlich mit zwei Produktionsstraßen. Dabei handelt es sich um einzelne Gebäude mit hochspezialisierter, individueller Ausstattung. Bereits ohne weitreichende Analysen ist dem Unternehmen bewusst, dass beispielsweise nach einem brandbedingten Ausfall dieser Produktionsstraßen die Wiederherstellung aufgrund der Komplexität, Individualität und Lieferzeiten mindestens ein halbes Jahr dauert. Daher wird der abzusichernde Zeitraum durch das BCMS auf sechs Monate festgelegt.

3.3 Geltungsbereich (R+AS)

Vor dem Aufbau eines BCMS muss die Institutionsleitung festlegen, welcher Bereich der Institution abgesichert werden soll. Dabei müssen die Zielsetzung und insbesondere die damit verbundenen regulatorischen Anforderungen und gegebenenfalls weitere Anforderungen an das BCMS berücksichtigt werden. Dieser Bereich, auch Geltungsbereich des BCMS genannt, kann die gesamte Institution umfassen oder nur einzelne Standorte, Teilbereiche, Produkte oder Services. Solche eingeschränkten Geltungsbereiche werden entweder durch organisatorische oder technische Strukturen vorgegeben, z. B. gemeinsame Gebäude oder Produktionsstraßen, oder durch gemeinsame Geschäftsprozesse, z. B. die Produktion. Der Geltungsbereich umfasst die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung dienen. Der Geltungsbereich des BCMS muss zur Zielsetzung des BCMS und den

Anforderungen passen. Zudem sollten die betrachteten Geschäftsprozesse komplett im Geltungsbereich enthalten sein.

Es kann auch sinnvoll sein, mehrere BCMS für mehrere kleinere Geltungsbereiche zu entwickeln. So könnte eine Institution beschließen, zunächst für einen kleinen Bereich mit besonders zeitkritischen oder regulierten Geschäftsprozessen ein Standard-BCMS umzusetzen. In den restlichen Bereichen der Institution kann anschließend ein Reaktiv-BCMS aufgebaut werden, damit auch für diese Bereiche eine grundlegende Geschäftsfortführung möglich ist, die über eine reine Krisenbehandlung im Rahmen der BAO hinausgeht.

Es sollten nicht nur technische, sondern auch organisatorische Aspekte bei der Abgrenzung des Geltungsbereichs berücksichtigt werden, damit die Verantwortung und die Zuständigkeiten eindeutig festgelegt werden können. Die im Geltungsbereich liegenden Geschäftsprozesse sollten explizit benannt werden.

Beispiele

- *Ein Automobilzulieferer mit einem einzigen Standort legt fest, dass der Geltungsbereich des BCMS das gesamte Unternehmen umfasst, da die meisten Geschäftsprozesse zur Produktion von Autoteilen dienen und weil bei Lieferverzug hohe Vertragsstrafen drohen.*
- *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.*
- *Eine Institution mit mehreren Standorten legt fest, dass der Geltungsbereich des BCMS zunächst nur den Hauptstandort umfasst und nicht die Nebenstandorte.*
- *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.*
- *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 anhand nachvollziehbarer Kriterien in sich abgeschlossen sein. Die Grenzen des Geltungsbereichs müssen klar definiert sein. Falls Teile der betrachteten Geschäftsprozesse organisatorisch von externen Institutionen oder Personen abhängig sind, beispielsweise im Rahmen von Outsourcing, sollten diese Schnitt-

stellen ebenfalls klar abgestimmt und beschrieben werden. Falls Einschränkungen und Abgrenzungen für das BCMS vorgenommen wurden, dann müssen diese dokumentiert und Einschränkungen zusätzlich begründet werden.

Synergiepotenzial

Sofern bereits ein ISMS nach BSI-Standard 200-2 etabliert wurde, kann es sinnvoll sein, sich an dem ISMS-Geltungsbereich zu orientieren. Dies hat den entscheidenden Vorteil, 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 auch für den Aufbau des BCMS von Interesse sind. Der übernommene Geltungsbereich muss zur Zielsetzung passen.

3.4 Entscheidung zur Vorgehensweise (R+AS)

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, das keinen schrittweisen Aufbau vorsieht, kann es zu Beginn effizienter sein, ein BCMS in der Linie, d. h. in mehreren kleineren Schritten ohne hohe Investitionskosten, einzuführen, 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 damit verbundene Durchlaufzeit eines PDCA-Zyklus sollte sich grundsätzlich an der Veränderungsgeschwindigkeit der Institution orientieren, wobei die Institution parallel in mehreren Phasen eines PDCA-Zyklus agieren kann. In der Praxis ist es darüber hinaus empfehlenswert, die Durchlaufzeit des PDCA-Zyklus auf ein Geschäftsjahr auszurichten, da dadurch das BCMS besser in das jährliche Berichtswesen und die jährliche Überprüfung der Ziele integriert werden kann. In diesem Zeitrahmen kann insbesondere sichergestellt werden, dass die erreichten Ergebnisse immer aktuell sind. Die Ressourcen sollten darauf ausgerichtet sein, dass die geplanten Ziele in dem aktuellen Zyklus erreicht werden können. Insofern spielt auch die Verfügbarkeit von Ressourcen bei der Festlegung der Durchlaufzeit des PDCA-Zyklus eine Rolle.

Die Institutionsleitung muss entscheiden, wie die weiteren Schritte zum Aufbau eines BCMS aussehen sollen, sodass die kurzfristigen und langfristigen Ziele erreicht werden (siehe 3.1 *Übernahme der Verantwortung durch die Leitungsebene (R+AS)*). Diese Entscheidungen müssen auf der Zielsetzung, den damit zusammenhängenden Rahmenbedingungen des BCMS sowie dem festgelegten Geltungsbereich basieren. Wurde bereits eine für das BCMS zuständige Person benannt, so kann diese die Institutionsleitung durch Erarbeitung von geeigneten Vorschlägen unterstützen. Insbesondere muss die Institutionsleitung eine geeignete Stufe auswählen: Reaktiv-, Aufbau- oder Standard-

BCMS. Anschließend sollte dokumentiert werden, für welchen Bereich mit welchem Zeitplan ein Reaktiv-, Aufbau-, oder Standard-BCMS umgesetzt werden soll.

Falls sich die Institutionsleitung für ein Reaktiv- bzw. Aufbau-BCMS entscheidet, dann muss dies nachvollziehbar begründet und dokumentiert werden, z. B. in der Leitlinie BCMS (siehe 4.8 *Leitlinie BCMS (R+AS)*). Neben den wesentlichen Einflussfaktoren, die zur Auswahl der Stufe geführt haben, sollten darüber hinaus 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 sollte für jede Institution darin liegen, langfristig ein Standard-BCMS zu erreichen.

Die folgende Übersicht fasst die wichtigsten Vor- und Nachteile der einzelnen Vorgehensweisen nochmals zusammen:

Stufe	Pro	Contra
Reaktiv-BCMS	• verhältnismäßig geringer Aufwand • schnellstmöglicher Einstieg, sodass eine rudimentäre Reaktion möglich ist • „Überlebensfähigkeit" der Institution wird rudimentär gesichert.	• ausschließlich für den Einstieg geeignet • Es werden erhebliche Lücken nicht identifiziert oder identifiziert und nicht abgesichert.
Aufbau-BCMS	• Im GP-Umfang betrachtete Prozesse werden angemessen abgesichert. • ermöglicht sehr gute, schrittweise Erweiterung des GP-Umfangs bis hin zum Standard-BCMS. • sehr gute Balance aus Aufwand und Nutzen	• Im nicht betrachteten GP-Umfang können weitere relevante, zeitkritische Geschäftsprozesse verbleiben, sodass weiterhin Lücken in der Absicherung verbleiben.
Standard-BCMS	• angemessene und vollständige Absicherung aller zeitkritischen Geschäftsprozesse ohne Lücken oder Defizite • Ermöglicht ganzheitliche, perfekt abgestimmte BC-Planung von Beginn an.	• höchster Ressourcenaufwand zu Beginn o finanziell o personell o zeitlich

Tabelle 4: Vor- und Nachteile der BCMS-Stufen

Zur Auswahl einer geeigneten Stufe sind ferner die Hinweise im Kapitel 2.6 *BCMS-Stufenmodell* hilfreich.

3.5 Benennung des oder der BC-Beauftragten (R+AS)

Die Institutionsleitung hat in der Regel nicht ausreichend Zeit, das BCM operativ aufzubauen und aufrechtzuerhalten. Um hier die Institutionsleitung zu unterstützen, muss ein **BC-Beauftragter** oder eine **BC-Beauftragte (BCB)** für alle Aspekte rund um das BCM benannt werden. BC-Beauftragte sind die Hauptanlaufstelle für alle BCM-Fragen, koordinieren sämtliche mit BCM zusammenhängenden Aufgaben und treiben diese innerhalb der Institution voran. Zusätzlich sollte für den oder die BCB eine qualifizierte Vertretung benannt werden.

Es steht jeder Institution frei, eine andere Bezeichnung für die Rolle BCB zu wählen. Geläufige Titel sind neben BCB auch der oder die Notfallbeauftragte, Business Continuity Manager sowie Notfall-Manager oder -Managerin. Aus diesen Titeln folgt aber auch manchmal ein anderes Rollenverständnis. Titel wie Notfall-Manager oder -Managerin führen oft dazu, dass fälschlicherweise angenommen wird, die Rolleninhabenden steuerten die Notfallbewältigung, obwohl die Rolle in der Regel innerhalb der Notfallvorsorge tätig ist. In diesem Standard wird daher diese Rolle durchgehend als BCB bezeichnet.

Es ist empfehlenswert, die Position der Rolle BCB 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 oder die BCB 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 ist es wichtig, dass der oder die BCB auch über das Geschehen in der Institution, soweit es einen Bezug zur BCM-Tätigkeit hat, umfassend und frühzeitig unterrichtet wird. Es wird davon abgeraten, die Rolle BCB in einer Organisationseinheit in der Linienorganisation (z. B. IT-Abteilung oder Verwaltung) zu verorten, da hierbei leicht Interessenkonflikte entstehen können.

Zeitliche Ressourcen des oder der BC-Beauftragten

Von hohem Stellenwert ist die Frage, mit welchen zeitlichen Ressourcen ein oder eine BCB den BCM-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. der BCM-Prozessschritt Business-Impact-Analyse (BIA) mehr Zeit in Anspruch nehmen, solange Geschäftsprozesse erstmalig bewertet werden. Weniger Zeit wird die BIA erfordern, sobald es in einem späteren Zyklus nur noch erforderlich ist, die Angaben zu überprüfen. Genauso ist der Aufwand, Geschäftsfortführungspläne (GPs) erstmalig zu erstellen, höher als derjenige Aufwand, in nachfolgenden Zyklen GPs nur noch zu aktualisieren.

Im ersten Schritt kann eine Schätzung der Aufwände durch die Institutionsleitung vorgenommen werden. Diese Schätzung orientiert sich an der Frage: „Wie oft bzw. wie viele

Stunden soll sich der oder die BCB mit dem BCMS auseinandersetzen?“, z. B. drei Tage pro Woche oder kontinuierlich.

BCB müssen grundsätzlich über ausreichend zeitliche Ressourcen verfügen, um ihre Aufgaben erfüllen zu können. Für eher kleine Institutionen kann es nach erfolgreichem Aufbau des BCMS ausreichend sein, eine 50 %-BCB-Stelle für die Aufrechterhaltung und Weiterentwicklung des BCMS einzuplanen. Demgegenüber kann es in großen oder komplexen Institutionen auch erforderlich sein, mehrere Vollzeitstellen zur Unterstützung des oder der BCB, d. h. ein mehrköpfiges BCB-Team, einzusetzen, um das BCMS einzuführen und aufrechtzuerhalten. Es ist daher empfehlenswert, sich bereits frühzeitig intensiv mit der Ressourcenplanung auseinanderzusetzen (siehe 4.4 *Ressourcenplanung*). Dabei sollten die Rahmenbedingungen, die Anforderungen sowie die organisatorischen und finanziellen Möglichkeiten berücksichtigt werden.

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

Hinweis

Es wird ausdrücklich davon abgeraten, die Position der Rolle BCB 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.

Synergiepotenzial

Um die zeitlichen Ressourcen für die Rolle BCB einzuschätzen, können die Mitarbeitendenkapazitäten anderer Managementsysteme zur Orientierung herangezogen werden, z. B. des oder der Informationssicherheitsbeauftragten des ISMS.

Grundsätzlich stellt sich auch die Frage, ob der oder die BCB noch weitere Funktionen oder Rollen anderer Managementsysteme übernehmen kann. Dies muss nicht per se ausgeschlossen werden, wenngleich es weitere Herausforderungen mit sich bringt. Sobald diese Option gewählt wird, ist es wichtig, vorab zu prüfen, ob konfliktträchtige Themen bestehen. Ist dies der Fall, so wird von einer Personalunion dieser Rollen abgeraten.

Insbesondere bei einer Personalunion von ISB und BCB ist es wichtig zu bedenken, dass BCMS und ISMS zwar über eine Schnittmenge verfügen, aber jeweils auch eigene Fragestellungen behandeln. In diesem Fall muss sichergestellt sein, dass der oder die BCB und ISB über ausreichend freie Ressourcen für die Wahrnehmung beider Rollen verfügt. Gegebenenfalls muss er oder sie durch entsprechendes Personal unterstützt werden. Zusätzlich ist es wichtig, zu beachten, dass nicht alle BCM-Anforderungen durch Sicherheitsmaßnahmen in der Informationssicherheit gelöst werden können (z. B. Verfügbarkeit im Notbetrieb vs. im Normalbetrieb). Ziel des

BCMS ist es, insbesondere auch für die Fälle zu greifen, in denen die Maßnahmen des ISMS versagen.

Von einer Personalunion zwischen BCB und ITSC-Manager oder -Managerin wird abgeraten, weil das ITSCM und somit auch ITSC-Manager oder -Managerin in der Regel Auftragnehmende des BCM sind und somit Vorgabe- und Umsetzungsinstanz vermischt würden.

Fachliche und persönliche Eigenschaften des oder der BC-Beauftragten

Um den vielfältigen Aufgaben und Anforderungen im BCM gerecht zu werden, müssen BCB angemessene fachliche und persönliche Eigenschaften inklusive entsprechendem Fachwissen sowie Erfahrungen besitzen. Fehlende fachliche Eigenschaften sollten durch gezielte Maßnahmen aufgebaut werden (siehe 4.6 *Schulung*).

Die Erläuterungen in Kapitel 4.3 *Definition der BC-Aufbauorganisation (R+AS)* decken die in der Praxis üblichen Aufgaben und Zuständigkeiten des oder der BCB ab. Darüber hinaus ist es empfehlenswert, dass BCB über die folgenden fachlichen und persönlichen Fähigkeiten und Kenntnisse verfügen oder dahingehend befähigt werden:

- Fähigkeit zur Führung von Mitarbeitenden (z. B. Kooperations- und Teamfähigkeit, Selbstbewusstsein, Durchsetzungsvermögen)
- sehr gute Kommunikationsfähigkeiten (Es ist wichtig, dass der oder die BCB die Mitarbeitenden und Externen von der Notwendigkeit des BCM und den damit verbundenen Aufgaben überzeugen können. BCB sollten ferner in der Lage sein, Themen des BCMS zielgruppengerecht für die Institutionsleitung aufzubereiten und somit die erforderlichen strategischen Entscheidungen vorzubereiten und voranzutreiben. Es sind umfangreiche Transferleistungen erforderlich, um die jeweiligen Sprachwelten zu verstehen und zu respektieren sowie 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, weiteren Leitlinien
- Kenntnisse zur Bewältigung von Notfällen und Krisen (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
- gute Kenntnisse der Institution (z. B. Prozesse, Produkte, Services, Ziele der Institution)

- Kenntnisse zu Risiken für den Geschäftsbetrieb der Institution und für die spezifischen betrieblichen Auswirkungen von Notfällen
- grundlegendes Wissen und eigene Erfahrungen hinsichtlich möglicher Maßnahmen zum BCM

Hinweis

BCB benötigen kein detailliertes Know-how zu baulichen oder technischen Notfallvorsorgemaßnahmen, wie beispielsweise zu IT-Redundanzkonzepten, Blitzschutz, Backup-Mechanismen und Notstromversorgung. Wenn Expertise zur Erfüllung der Aufgaben erforderlich ist, können BCB Mitarbeitende der AAO oder externe Spezialisten zur Unterstützung heranziehen (siehe 4.3 Definition der BC-Aufbauorganisation).

4 Konzeption und Planung des BCMS (R+AS)

Die Konzeption und Planung des BCMS fällt typischerweise in den Zuständigkeitsbereich des oder der BCB. Dementsprechend ist es empfehlenswert, zuerst eine geeignete Person durch die Institutionsleitung auszuwählen und als BCB zu benennen, bevor mit den nachfolgenden Schritten begonnen wird. Die folgenden Unterkapitel beschreiben die empfohlene Vorgehensweise, mittels derer die Konzeption und Planung des BCMS durchgeführt wird. In Abbildung 14 sind die dazu erforderlichen Schritte in einer Übersicht dargestellt.

Abbildung 14: 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. Dieser Maßnahmenplan sollte bereits in der Konzeption des BCMS berücksichtigt werden, auch wenn er erst für dessen Aufrechterhaltung und Verbesserung relevant ist (siehe Kapitel 15 Aufrechterhaltung und Verbesserung (R+AS)). Wenn bereits identifizierte Korrekturbedarfe und Verbesserungsmöglichkeiten zeitnah dokumentiert werden, dann werden diese nicht vergessen und können zu einem späteren Zeitpunkt behandelt werden. Eine Vorlage für einen Maßnahmenplan kann den Hilfsmitteln zum Standard entnommen werden.

4.1 Definition und Abgrenzung (R+AS)

Ein BCMS besitzt vielfältige Überschneidungen und Berührungspunkte mit gegebenenfalls existierenden anderen Managementsystemen wie dem ISMS, ITSCM, Krisenmanagement oder Risikomanagement. Ferner existieren in 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, abgrenzenden Schritt ist es sinnvoll, zu prüfen, 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 definiert 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 entweder deckungsgleich aufeinander abstimmen oder eindeutig 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. Dazu sollten Kriterien festgelegt werden, wie bei der möglichen Eskalation eines Schadensereignisses die Zuständigkeit von einer Management-Disziplin an eine andere übertragen werden kann (siehe 5.2 *Detektion, Alarmierung und Eskalation (R+AS)*).

4.2 Analyse der erweiterten Rahmenbedingungen (AS)

Als erweiterte Rahmenbedingungen werden sämtliche internen und externen Anforderungen an die Institution sowie interne und externe Einflussfaktoren auf die Institution bezeichnet, die ihr BCMS beeinflussen können. Diese erweiterten Rahmenbedingungen werden in der ISO-Norm 22301 auch als „Kontext der Organisation" bezeichnet. Die nachfolgenden Unterkapitel beschreiben die empfohlene Vorgehensweise, mittels derer die erweiterten Rahmenbedingungen strukturiert analysiert werden können. In Abbildung 15 sind die dazu erforderlichen Schritte dargestellt.

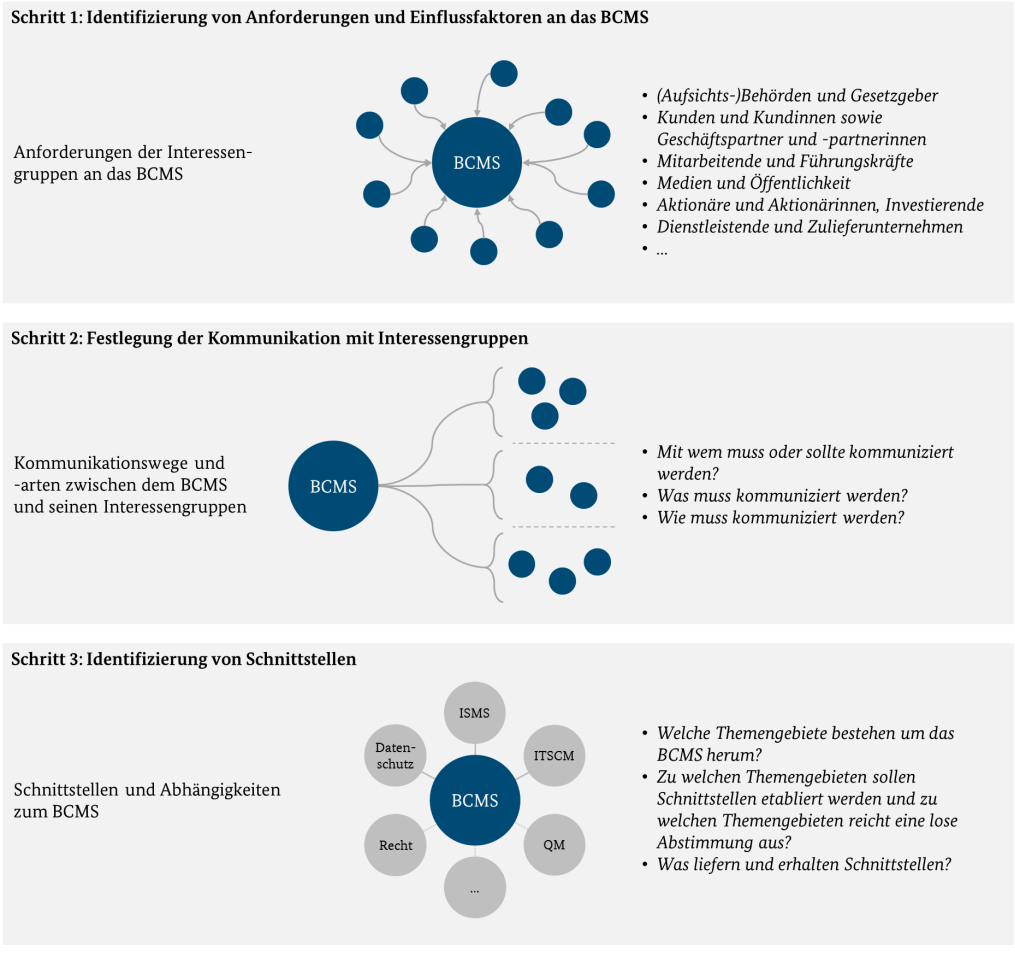

Abbildung 15: Erweiterte Rahmenbedingungen ermitteln

Synergiepotenzial

Liegt bereits ein ISMS nach IT-Grundschutz oder der ISO-Norm 27001 vor, so kann geprüft werden, inwieweit die Interessengruppenanalyse für das BCM übernommen und weitergenutzt werden kann.

4.2.1 Identifizierung von Anforderungen und Einflussfaktoren an das BCMS (AS)

Für die weitere Planung des BCMS müssen die relevanten Interessengruppen und Einflussfaktoren ermittelt werden, die die Rahmenbedingungen und Ziele des BCMS beeinflussen können. Einige Interessengruppen haben ausschließlich Informationsansprüche. Andere Interessengruppen, z. B. Kunden und Kundinnen oder Aufsichtsbehörden, haben klare Erwartungen an das BCMS oder stellen spezifische Anforderungen. Diese Anforderungen und Einflussfaktoren müssen im BCMS angemessen berücksichtigt werden. Dazu

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 Personal- oder Betriebsrat, Mitarbeitende, Beauftragte anderer Managementsysteme, z. B. Informationssicherheitsbeauftragte, 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 Aktionäre und Aktionärinnen, Fachaufsichten, Investierende, Kunden und Kundinnen, Zulieferunternehmen, Geschäftspartner und -partnerinnen, Medien oder auch Versicherungen, Behörden, Branchenverbände, der Gesetzgeber oder die Öffentlichkeit.

Die Abbildung 16 zeigt Beispiele für verschiedene Interessengruppen.

Beispiel

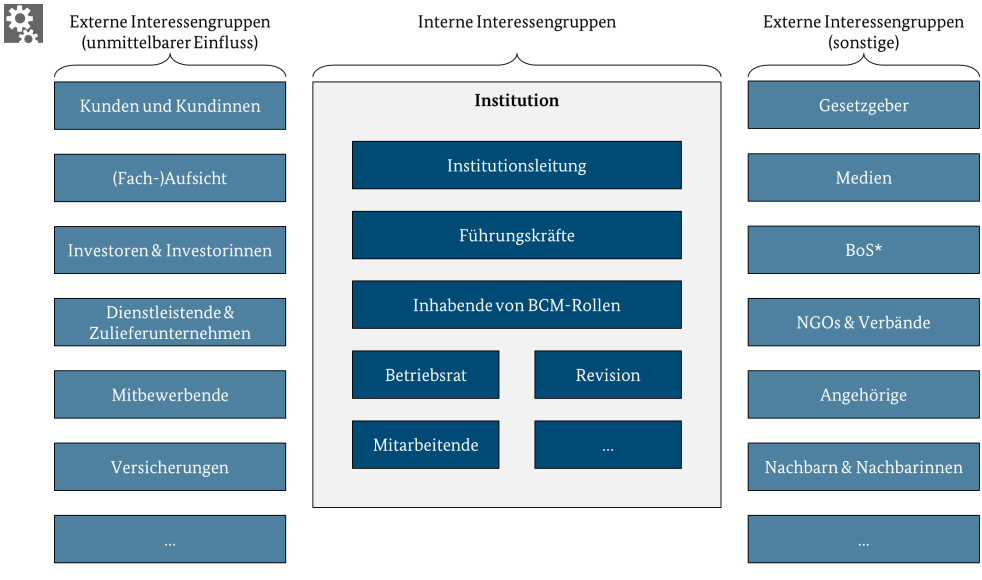

Abbildung 16: Beispiele für Interessengruppen

Bedeutsam sind insbesondere diejenigen Interessengruppen,

- die vertragliche, rechtliche und regulatorische Anforderungen an die Institution stellen,
- auf deren Kooperation die Institution angewiesen ist,
- die einen hohen Einfluss auf das öffentliche Meinungsbild der eigenen Institution haben sowie

- diejenigen, welche die Geschäftstätigkeit der Institution einschränken oder verbessern können.

Die für das BCMS relevanten Interessengruppen und die Arten der Interessen können mittels einer Interessengruppenanalyse (engl. Stakeholder Analysis) ermittelt werden. Anhand der Interessengruppenanalyse werden

- die relevanten Interessengruppen identifiziert sowie
- der Einfluss der relevanten Interessengruppen auf das jeweilige Thema oder Managementsystem analysiert.

Aus der Interessengruppenanalyse müssen die notwendigen Maßnahmen abgeleitet werden, um den Interessen der jeweiligen Gruppe im Sinne der Institution gerecht zu werden. Eine wesentliche Quelle für die Interessengruppenanalyse sind alle Informationen zu internen und externen Gründen für ein BCM, die im Prozess zur Initiierung des BCMS (siehe 3.2.1 *Motivation für den Aufbau eines BCMS (R+AS)*) erhoben wurden. Zu diesen Gründen zählen z. B. die relevanten Gesetze und Verordnungen. Insbesondere für regulatorische, aber auch für alle anderen Anforderungen und Einflussfaktoren muss dokumentiert werden, wo die notwendigen Informationen im Original zu finden sind, z. B. 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 den EBA-Guidelines on ICT and security risk management, Kapitel 3.7. Business continuity management: Financial institutions should establish a sound business continuity management (BCM) process to maximise their abilities to provide services on an ongoing basis and to limit losses in the event of severe business disruption […].

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 und Kundinnen 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. Es ist sinnvoll, dass Interessengruppen mit hohem Einfluss von

der Institution besondere Aufmerksamkeit erhalten, während diejenigen mit niedrigem Einfluss nur im geringen Umfang berücksichtigt werden.

Tabelle 5 und Tabelle 6 zeigen ein vereinfachtes Beispiel für eine Interessengruppenanalyse. Der Grad der Einflussnahme der betrachteten Interessengruppen ist nicht repräsentativ. Sofern die nachstehende Vorgehensweise genutzt wird, ist es wichtig, dass die Institution den Grad der Einflussnahme selbstständig festlegt.

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*
Inhabende 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*
Mitarbeitende	• *Absicherung des oder der Arbeitgebenden (wirtschaftlich, Reputation)* • *Sicherheit der eigenen Handlungen* • *Relevanz oder Bedeutung im Notfall*	*Mittel*
Betriebsrat	• *Schutz und Durchsetzen der Interessen der Mitarbeitenden bei personalrelevanten Entscheidungen* • *Sicherstellung und Aufrechterhaltung der Arbeitsplätze in und nach einem Notfall bzw. einer Krise*	*Hoch*

Tabelle 5: Beispiele interner Interessengruppen

Externe Interessengruppe	*Erwartungen und Anforderungen*	*Grad der Einflussnahme*
Kundschaft	• *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 Anforderungen*	*Mittel*
Angehörige der Mitarbeitenden	• *Wirtschaftliche Absicherung* • *Schutz vor Gefahr für Leib und Leben der Mitarbeitenden*	*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* • *Einhaltung der Obliegenheitspflichten*	*Mittel*
Dienstleistungsunternehmen und Zuliefernde	• *Vereinbarte Leistungsabnahme und Vergütung*	*Niedrig*

Tabelle 6: Beispiele externer Interessengruppen

Hierzu ist es empfehlenswert, jeweils diejenigen Kontaktpersonen innerhalb der Institution einzubeziehen, die aussagefähig zu den Erwartungen und Anforderungen einer Interessengruppe sind. Dies sind üblicherweise Personen aus den Organisationseinheiten (OEs) Kommunikation, Recht, Vertrieb, Dienstleistungsunternehmensteuerung, Betriebsrat, Revision oder vergleichbaren OEs.

Die Interessengruppen sowie deren Anforderungen, Erwartungen und Einflussfaktoren müssen möglichst immer aktuell gehalten werden, z. B. indem ein regelmäßiger Aktualisierungszyklus festgelegt wird. Falls im weiteren Verlauf zur Planung und Umsetzung des BCMS andere bzw. geänderte Interessengruppen oder Anforderungen und Einflussfaktoren bekannt werden, dann sollte die Tabelle überprüft und aktualisiert werden.

4.2.2 Festlegung der Kommunikation mit Interessengruppen (AS)

Der Umgang mit den Interessengruppen erfordert eine adressatengerechte Kommunikation. Gegebenenfalls bestehen jedoch keine direkten Beziehungen vom BCM zu einer

bestimmten Interessengruppe, wie z. B. zu den Aktionären und Aktionärinnen 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 Institution kommuniziert im Normalbetrieb Themen des BCM auf folgenden Wegen:

- *Mitarbeitende werden im Rhythmus von zwei Monaten auf der Intranet-Seite über Neuigkeiten zum BCM informiert. Zudem erhalten die Mitarbeitenden 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 des BCMS informiert.*
- *Kunden und Kundinnen erhalten initial die Information, dass ein BCMS implementiert ist. Weitere Informationen werden nur dann an Kunden und Kundinnen gegeben, wenn ein Notfall eingetreten ist.*

Die Kommunikation mit Interessengruppen in einem Notfall wird in Kapitel 5.7 *NuK-Kommunikation (R+AS)* näher beschrieben.

4.2.3 Identifizierung von Schnittstellen (AS)

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, so können die Qualität der Arbeitsergebnisse verbessert und doppelte Arbeiten vermieden werden. Zudem kann Fehlern vorgebeugt werden, z. B. inkonsistenten oder widersprüchlichen Aussagen.

Die Schnittstellen und Abhängigkeiten des BCM sind in jeder Institution individuell ausgeprägt. Der BSI-Standard 200-4 setzt daher keine konkreten Schnittstellen voraus, son-

dern stellt in diesem Kapitel allgemeine Beispiele für typische Schnittstellen vor, die in vielen Institutionen vorzufinden sind. Ergänzend dazu finden sich in dem gesamten Standard Hinweise auf weitere mögliche Schnittstellen und Synergiepotenziale in entsprechenden Synergiepotenzialboxen.

Das Beispiel in Abbildung 17 zeigt eine Auswahl an typischen Schnittstellen im Überblick.

Beispiel

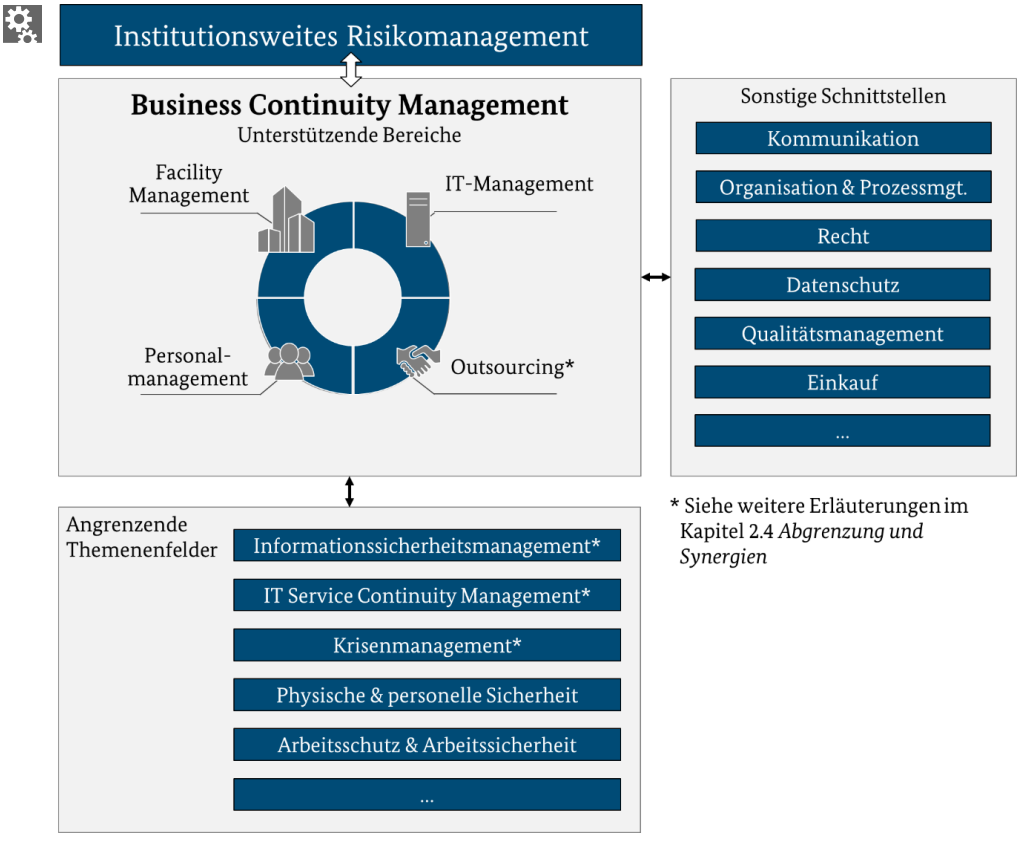

Abbildung 17: Übersicht über mögliche Schnittstellen eines BCMS

Alle für das BCMS relevanten Schnittstellen müssen ermittelt und dokumentiert werden. Jede Schnittstelle des BCMS sollte klar definiert und eindeutig beschrieben werden. Als Ausgangsbasis können die Ergebnisse der Interessengruppenanalyse sowie die Hinweise aus Kapitel 2.4 *Abgrenzung und Synergien* verwendet werden. Es ist empfehlenswert, für jede Schnittstelle des BCMS festzulegen, welche gegenseitigen Informationen oder Leistungen ausgetauscht und welche der angewendeten Methoden und Verfahren der beiden Disziplinen aufeinander abgestimmt werden. Zudem sollten die Art und die Häufigkeit eines Austauschs sowie die abzustimmenden Aspekte festgelegt und dokumen-

tiert werden. In der Praxis hat es sich bewährt, die Schnittstellen zu bedienen, indem gemeinsame Treffen organisiert und hier übergreifende Themen abgestimmt werden.

Hinweis

Im Hinblick auf die erwarteten Aufwände und den Nutzen sollte abgewogen werden, in welcher Intensität eine Schnittstelle genutzt wird. Möglicherweise ist eine der Disziplinen aufgrund fehlender Ressourcen oder Kapazitäten nicht zu einer Zusammenarbeit bereit oder die Schnittstelle weist noch nicht den erforderlichen Reifegrad auf.

Im Folgenden werden einige mögliche wechselseitige Abhängigkeiten und die damit zusammenhängenden Informationsaustausche sowie 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.

Wird von einer Institution gleichzeitig ein ISMS betrieben, so besteht in der Regel dort die Anforderung, dass auch im Notbetrieb die Anforderungen der Informationssicherheit eingehalten werden müssen. Die Aufrechterhaltung eines stabilen Notbetriebs ist jedoch in der Praxis mitunter nur dann erreichbar, wenn andere Schutzziele niedriger priorisiert werden (bspw. Verfügbarkeit versus Vertraulichkeit von Daten). Um diese Zielkonflikte konkurrierender Schutzziele optimal abzustimmen, ist es empfehlenswert, bereits in der Planung und Konzeptionsphase die Schnittstellen zwischen BCMS und ISMS festzulegen, damit dieser Aspekt von Beginn an in die Notfallplanung eingehen kann.

Risikomanagement

Eine der wichtigsten Funktionen in einer Institution stellt das Risikomanagement dar. Dessen Aufgabe ist es, die institutionsspezifischen Risiken zu identifizieren, zu analysieren, zu bewerten, an die verschiedenen Interessengruppen zu kommunizieren und sicherzustellen, dass Risiken adäquat behandelt werden. Die verschiedenen Sicherheitsdisziplinen liefern hierzu häufig detailliertere Informationen zu bestimmten Risikoarten oder übernehmen Aufgaben in der Risikobehandlung.

So setzt sich das BCM aus Sicht des Risikomanagements mit jenen Risiken auseinander, die sich negativ auf die Kontinuität des Geschäftsbetriebs auswirken können und geeignet behandelt werden sollen. Die verschiedenen Präventions- und Notfallmaßnahmen des BCM dienen letztendlich dazu, diese Risiken angemessen zu behandeln.

Im Risikomanagement werden Sicherheitsthemen häufig nach dem sogenannten Three-Lines-of-Defense-Modell betrachtet. Dieses Organisationsmodell stellt die angemessene Steuerung des Risikomanagements sicher, indem es drei Verteidigungslinien bildet:

Die **erste Verteidigungslinie (1st LoD)** besteht aus den Organisationseinheiten, die als **Risikoeigentümer** dafür zuständig sind, ihre Risiken adäquat zu analysieren, zu bewerten, zu steuern, zu überwachen sowie zu vermeiden oder zu reduzieren.

Die **zweite Verteidigungslinie (2nd LoD)** dient dazu, die Risikomanagementfunktionen der ersten „Verteidigungslinie" effektiv zu steuern und zu überwachen. Dazu werden durch die zweite Verteidigungslinie, z. B. das BCM, Vorgaben, Methoden und Verfahren bereitgestellt und überwacht. Im Rahmen des BCMS übernimmt diese Aufgabe in der Regel der oder die BCB.

Die **dritte Verteidigungslinie (3rd LoD)** ist die objektive und unabhängige Prüfinstanz. Sie wird in der Praxis häufig durch die interne Revision ausgeübt. Die dritte Verteidigungslinie überwacht im Auftrag der Institutionsleitung, ob alle Risiken der Institution wirksam und angemessen identifiziert, analysiert, bewertet, gesteuert und überwacht werden. Hierbei werden sowohl die Vorgaben und Methoden der zweiten Verteidigungslinie überprüft, als auch deren angemessene und korrekte Umsetzung durch die erste Verteidigungslinie.

Abbildung 18 beschreibt, wie sich das BCM in das 3LoD-Modell einfügt. Mit dem Risikomanagement sollten vor allem die Methoden zur Identifikation, Analyse, Bewertung und Behandlung von Risiken abgestimmt werden. Zusätzlich können die im Risikomanagement definierten Parameter, z. B. Risikokategorien und Akzeptanzkriterien, als Grundlage dienen, die zeitkritischen Geschäftsprozesse im Rahmen der Business-Impact-Analyse zu identifizieren. Ferner können sowohl die Methode als auch die Parameter, z. B. die Risikokategorien und Akzeptanzkriterien des Risikomanagements, im Rahmen der BCM-Risikoanalyse wiederverwendet werden. Gegebenenfalls können auch bereits vorhandene Ergebnisse genutzt werden. Darüber hinaus ist es möglich, die BCM-Risikoanalyse im Rahmen einer ganzheitlichen Risikoanalyse des Risikomanagements durchzuführen. Dies setzt voraus, dass ein sinnvolles Abstraktionsniveau für alle Gefährdungen und die zu betrachtenden Zielobjekte gefunden werden kann, sodass im Anschluss alle Risikoaspekte, z. B. aus der Informationssicherheit und der Business Continuity, zusammen betrachtet werden können. Umgekehrt unterstützt das BCM das Risikomanagement in der Risikobehandlung, indem Maßnahmen zur Notfallvorsorge und Notfallbewältigung entwickelt und umgesetzt werden. Die Risikobehandlung der potenziellen und tatsächlichen Ausfälle von Geschäftsprozessen obliegt somit dem BCM.

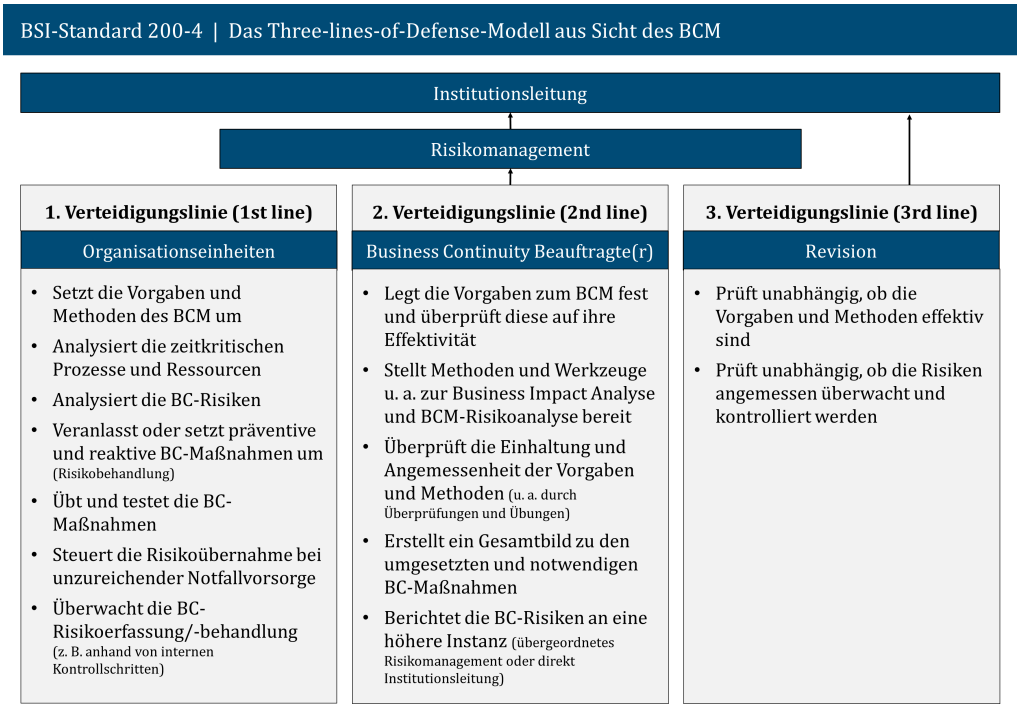

Abbildung 18: BCM-Aspekte im Three-lines-of-Defense-Modell

Facility Management

Die Mitarbeitenden des Facility Managements unterstützen das BCM z. B. bei der Bewertung und Ausgestaltung von Maßnahmen zur physischen Sicherheit sowie zur Verfügbarkeit der Gebäude und der Infrastruktur. Zudem setzt das Facility Management die definierten Maßnahmen um.

Im Notfall kann z. B. die Räumung von Gebäuden erforderlich sein. Gebäudenotfallteams können diese durchführen. Auch den Wiederanlauf und den Notbetrieb können Gebäudenotfallteams unterstützen, indem sie etwa Ausweichstandorte und -arbeitsplätze vorbereiten.

Personalmanagement

Das BCM hat Auswirkungen auf alle Mitarbeitenden. Die Personalabteilung sollte bei allen Entscheidungen und Maßnahmen im Kontext BCM involviert werden, die wesentlichen Einfluss auf die Rechte und Pflichten der Mitarbeitenden haben. Das Personalmanagement kann bei der Planung von Schulungen und Awareness-Maßnahmen unterstützen, damit das BCM ein Teil der „Kultur" der Institution wird.

Betriebs- oder Personalrat

Um Gefahr in Notfällen abzuwehren, sind häufig Maßnahmen nötig, die sich auf die Rechte und Pflichten der Mitarbeitenden auswirken. Hierzu ist üblicherweise die Mitbestimmung des Betriebs- oder Personalrats erforderlich, z. B. vor Anordnung von Über-

stunden, Wochenend- und Nachtarbeit oder Entsendung. Zwar sehen das Betriebsverfassungsgesetz sowie das Bundespersonalvertretungsgesetz explizit vor, dass in Notfällen Maßnahmen zum Schutz der Institution einseitig durch den Arbeitsgeber oder Dienstherrn getroffen werden können, aber im Sinne einer nachhaltigen Zusammenarbeit der verschiedenen Interessenparteien sollte der Betriebs- oder Personalrat frühzeitig eingebunden werden. So können in Abstimmung mit dem Betriebs- oder Personalrat in der BC-Planung u. a. Regelungen zur Rufbereitschaft, abweichende Regelungen zum Personaleinsatz sowie Fragen des Weisungsrechts in einem Not- oder Krisenfall getroffen und dokumentiert werden. Ebenfalls sollte abgestimmt werden, inwieweit der Betriebs- oder Personalrat im Falle eines Not- oder Krisenfalls informiert oder alarmiert werden sollte.

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 in der Regel in der Organisationsabteilung 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. Im Notfall ist es notwendig, Mitarbeitende zu informieren und zu lenken. Zugleich ist es wichtig, die externen Interessengruppen zu betreuen, um 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 Abteilung 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.

Compliance

Die Compliance-Abteilung einer Institution ist dafür zuständig, dass institutionsweit Compliance-Anforderungen eingehalten werden. Dies kann die verschiedensten Anforderungen umfassen, von dem äußeren Erscheinungsbild von Publikationen bis hin zur Einhaltung von vertraglichen Anforderungen, z. B. auch SLAs. Dabei können umfangreiche Berührungspunkte mit dem BCM entstehen, da z. B. auch die Dokumente des BCMS die formalen Anforderungen der Compliance zu erfüllen haben oder die vertraglichen Anforderungen auch für den Notfall oder die Krise relevant sein können.

Datenschutz

Der Datenschutz regelt, wie personenbezogene Daten in einer Institution erhoben, gespeichert, verarbeitet und weitergegeben werden dürfen. Die Anforderungen des Datenschutzes und der Informationssicherheit müssen auch im Notbetrieb eingehalten werden. Die Abstimmung mit dem BCM ist daher bedeutsam.

BCMS und Datenschutz können auch zusammenarbeiten, um gemeinsam technische und organisatorische Maßnahmen des Datenschutzes zu definieren, umzusetzen und zu prüfen.

Qualitätsmanagement

Das Qualitätsmanagement entwickelt Anforderungen, um die Effektivität und Effizienz der Geschäftsprozesse einer Institution systematisch zu verbessern. Dazu gehören auch die Prozesse des BCMS.

Das Qualitätsmanagement erstellt häufig übergreifende Vorgaben für die einzelnen Themenfelder oder stellt Hilfsmittel für diese bereit. Es ist wichtig, dass Vorgaben des Qualitätsmanagements z. B. an die Dokumentation, die Leistungsüberprüfung oder die Korrektur und Verbesserung, vom BCM berücksichtigt werden.

Zudem gibt es im Qualitätsmanagement häufig dokumentierte Geschäftsprozesse oder Ressourcenlisten, auf die das BCMS für die 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 Dienstleistungsunternehmen eingebunden (Outsourcing bzw. Lieferkette), sollten neben den betriebswirtschaftlichen Aspekten auch die Hinweise zu Strategieoptionen bei Outsourcing und deren Folgen für den Einkauf berücksichtigt werden (siehe Hilfsmittel *BC-Strategievorschläge*).

4.3 Definition der BC-Aufbauorganisation (R+AS)

In der Regel benötigt der oder die BCB Unterstützung, um die angestrebten Ziele im BCM erreichen zu können. Die Gesamtheit aller Rollen im BCM wird in der BC-Aufbauorganisation zusammengefasst und beinhaltet zum einen die **BC-Vorsorgeorganisation** sowie zum anderen die **Bewältigungsorganisation für Notfälle und Krisen**.

- Die **BC-Vorsorgeorganisation** umfasst alle Rollen, die das BCMS aufbauen, betreiben und kontinuierlich weiterentwickeln.
- Die **Bewältigungsorganisation für Notfälle und Krisen**, auch **Besondere Aufbauorganisation (BAO)** genannt, umfasst alle Rollen, die dazu dienen ein schwerwiegendes Schadensereignis zu bewältigen. (Die BAO wird erst im Kapitel 4.3 *Definition der BC-Aufbauorganisation (R+AS)*) festgelegt.)

Die Rollen der BC-Vorsorgeorganisation sowie deren Aufgaben, Rechte und Pflichten sowie Zuständigkeiten müssen definiert werden. Anschließend müssen diese Rollen auf geeignete Mitarbeitende übertragen und von diesen erfüllt werden. Nur so ist gewähr-

leistet, dass alle wichtigen Aspekte berücksichtigt und sämtliche anfallenden Aufgaben effektiv und effizient erledigt werden. Die gängigsten Rollen der BC-Vorsorgeorganisation werden in Abbildung 19 beispielhaft dargestellt und in den folgenden Unterkapiteln erläutert.

Beispiel

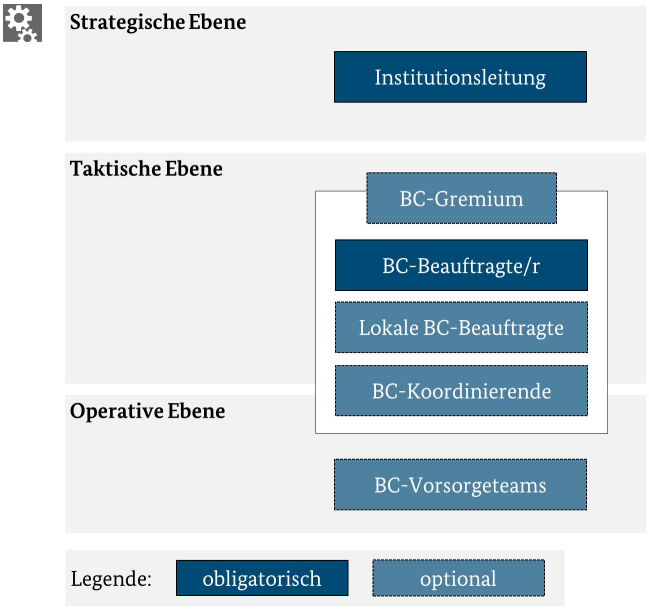

Abbildung 19: Beispiel einer BC-Vorsorgeorganisation

Die nachfolgenden Punkte stellen eine Auswahl relevanter Aspekte dar, nach denen in der Praxis eine BC-Vorsorgeorganisation ausgerichtet werden kann:

- **Größe:** Der oder die BCB begleitet verschiedene Tätigkeiten innerhalb des BCM-Prozesses, die durch die Organisationseinheiten im Geltungsbereich des BCMS umgesetzt werden. Sobald die Anzahl zu unterstützender Organisationseinheiten zu groß wird, kann der oder die BCB 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 oder die BCB nicht mehr allein zusammengetragen und überblickt werden. Um einer hohen Komplexität gerecht zu werden, kann es sinnvoll sein, dass der oder die BCB bestimmte Aufgaben im BCM an weitere Rollen mit entsprechenden Fähigkeiten und Kenntnissen weitergibt.
- **Geografische Verteilung:** Ist eine Institution in mehreren Ländern oder global tätig, dann ist es notwendig, neben sprachlichen und kulturellen Unterschieden auch

verschiedene ortsabhängige Rahmenbedingungen für das BCM zu berücksichtigen, z. B. abweichende, gesetzliche Vorgaben. Falls entschieden wurde, keine separaten BCM-Systeme in den unterschiedlichen Ländern zu etablieren, können die Kenntnisse dieser länderspezifischen Rahmenbedingungen durch getrennte Rollen abgebildet werden, die mit den Gegebenheiten vor Ort vertraut sind (siehe 3.3 *Geltungsbereich (R+AS)*).

Dauerhaft zugewiesene Aufgaben und Zuständigkeiten im BCM sollten im Aufgaben- und Stellenprofil der jeweiligen Mitarbeitenden dokumentiert werden. Bei der Festlegung der Aufgaben und Zuständigkeiten der Rollen kann sich die Institution an den nachfolgenden Unterkapiteln orientieren. Sofern von diesen Unterkapiteln abgewichen wird, muss sichergestellt werden, dass die aufgeführten Aufgaben und Zuständigkeiten über eine der Rollen abgedeckt sind. Die Institution muss in beiden Fällen nachweisen können, dass die Rolleninhabenden über die erforderliche Qualifikation verfügen.

4.3.1 Institutionsleitung (R+AS)

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

- Festlegen der Ziele und Rahmenbedingungen des BCM
- Benennen des oder der BCB
- Bereitstellen der angemessenen personellen, zeitlichen und finanziellen Ressourcen
- Sicherstellen, dass der oder die BCB sein direktes Vorspracherecht wahrnehmen kann
- Sicherstellen, dass BCM in alle relevanten Geschäftsprozesse und Projekte integriert wird
- Informieren des oder der BCB über grundlegende Strategie- oder Organisationsänderungen
- Betonen der Wichtigkeit des BCM allen Mitarbeitenden gegenüber
- Motivation und Aufforderung aller Mitarbeitenden, zu einem effektiven BCMS und dessen Verbesserung beizutragen

4.3.2 Der oder die BC-Beauftragte (R+AS)

Der oder die BCB ist für den Aufbau, den Betrieb und die kontinuierliche Verbesserung des BCMS zuständig. Er oder sie muss die Institutionsleitung bei sämtlichen Aspekten, die für das BCM relevant sind, unterstützen und beraten. Maßgeblich für die Tätigkeit sind die Ziele und Rahmenbedingungen, die der oder die BCB durch die Institutionsleitung erhält. Der oder die BCB 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 und gegebenenfalls weitere Adressaten (z. B. Aufsicht oder Revision) zum Status im BCM

Für geografisch verteilte Institutionen kann es sinnvoll sein, neben einem oder einer globalen BCB weitere lokale BCB einzusetzen, welche die länderspezifischen Anforderungen kennen und die BCM-Vorgaben entsprechend anpassen können. Die Institution muss sicherstellen, dass die globalen und lokalen Vorgaben zum BCM einander nicht widersprechen.

4.3.3 Die BC-Koordinierenden (optional) (R+AS)

BC-Koordinierende (BCKs) fungieren als Kontaktpersonen in fachlichen Dingen und als Multiplikatoren in ihrer Organisationseinheit. Die BCKs stellen die Umsetzung der Vorgaben zum BCM im eigenen Zuständigkeitsbereich sicher. Der oder die BCK 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 BCKs bietet sich insbesondere bei großen oder komplexen Institutionen an, in denen der oder die BCB zeitlich nicht mehr in der Lage ist, die erforderlichen Tätigkeiten in allen Organisationseinheiten zu begleiten. Der oder die BCB kann sich so darauf konzentrieren, die Vorgaben und den BCMS-Prozess zu erstellen, anzupassen und zu überwachen, ob diese eingehalten werden.

4.3.4 BC-Gremium (optional) (R+AS)

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

Synergiepotenzial

Gibt es in der Institution bereits ein Gremium oder mehrere Gremien, die sich mit Sicherheitsfragen oder Fragen der Risikosteuerung in der Institution auseinandersetzen, dann können die Aufgaben dieser Gremien um die BCM-spezifischen Aspekte erweitert werden.

Insbesondere wenn bereits ein ISMS nach BSI-Standard 200-2 vorliegt, kann das BC-Gremium mit dem IS-Koordinierungsausschuss kombiniert werden. Ein gemeinsames Gremium kann gebildet werden, dessen Teilnehmendenkreis situativ um die BCM-Rollen erweitert wird. Die Agenda der Gremiensitzungen kann jeweils entsprechend

angepasst werden. Alternativ kann auch eine gegenseitige Vertretung in den jeweiligen Gremien eingerichtet werden.

4.3.5 BC-Vorsorgeteams (optional) (R+AS)

Bei sehr großen Institutionen mit einer Vielzahl von Geschäftsprozessen kann es erforderlich sein, dass der oder die BCB oder auch die BCKs durch weitere Personen im BCM unterstützt werden. Der oder die BCB oder jeweils ein oder eine BCK bildet in diesem Fall zusammen mit solchen weiteren Personen ein BC-Vorsorgeteam. Die BC-Vorsorgeteams können temporär oder dauerhaft aufgestellt werden.

Die BC-Vorsorgeteams dienen hauptsächlich dazu, Arbeitslast zu verteilen. Dies kann notwendig sein, um priorisierte BCM-Themen zu behandeln, die in der erforderlichen Zeit nur von mehreren Personen parallel abgearbeitet werden können.

4.4 Dokumentation (R+AS)

Eine angemessene Dokumentation ermöglicht es, getroffene Entscheidungen nachzuvollziehen, Handlungen zu wiederholen sowie Managementsysteme zu überprüfen und zu zertifizieren. Zusätzlich können Korrekturbedarfe und Verbesserungsmöglichkeiten besser nachverfolgt werden. Dieser Standard gibt eine grundlegende Dokumentenstruktur für ein BCMS vor. Die geforderten Dokumente werden in den folgenden Unterkapiteln sowie den Kapiteln zu den entsprechenden BCM-Prozessschritten beschrieben, in denen die Dokumente eingesetzt werden. Ferner werden unter den Hilfsmitteln zu diesem Standard entsprechende Dokumentvorlagen mit Beispieltexten zur Verfügung gestellt.

Im **Aufbau- und Standard-BCMS** stellt die Dokumentation sicher, dass den berechtigten Interessengruppen der Zugang zu relevanten Informationen möglich ist. Um diesen Ansprüchen gerecht zu werden, bedarf es im Aufbau- und Standard-BCMS einer Dokumentenlenkung. Die Dokumentenlenkung beinhaltet Vorgaben, wie die Dokumente gestaltet, überarbeitet und freigegeben werden (siehe 4.4.2 *Festlegung von Dokumentinformationen*). Ziel ist es, dass die Inhalte jedes Dokuments für die relevanten Personen verfügbar, aktuell und in angemessener Qualität vorliegen (siehe 4.4.3 *Überprüfung und Aktualisierung von Dokumenten*).

AS

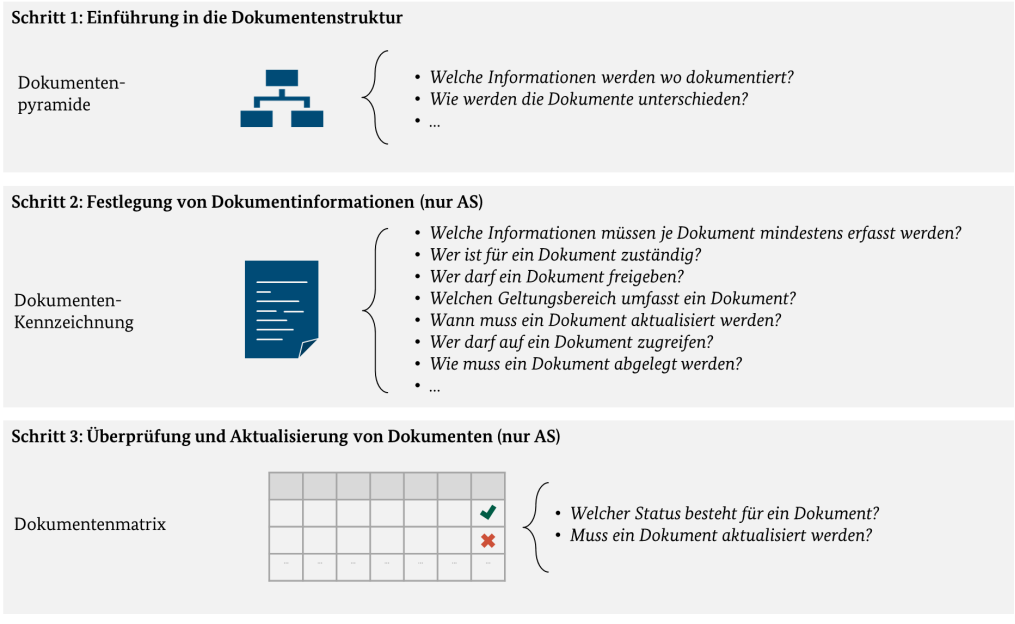

Abbildung 20: BCM-Prozessschritte zur Dokumentation im Standard-BCMS

Synergiepotenzial

Die Dokumentenlenkung ist üblicherweise als Bestandteil des Qualitätsmanagementsystems definiert. Die Vorgaben aus diesem BSI-Standard können mit den institutionsspezifisch geltenden Anforderungen abgestimmt werden. Alternativ kann auf die Regelungen zur Dokumentenlenkung gemäß BSI-Standard 200-2 zurückgegriffen werden. Mitunter müssen auch branchenspezifische, regulatorische Anforderungen an die Dokumentenlenkung berücksichtigt werden, z. B. die „Schriftlich fixierte Ordnung" im Finanzsektor.

4.4.1 Dokumentenstruktur (R+AS)

Im Rahmen dieses Standards werden die verschiedenen Dokumentenarten anhand von zwei Kategorien differenziert:

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

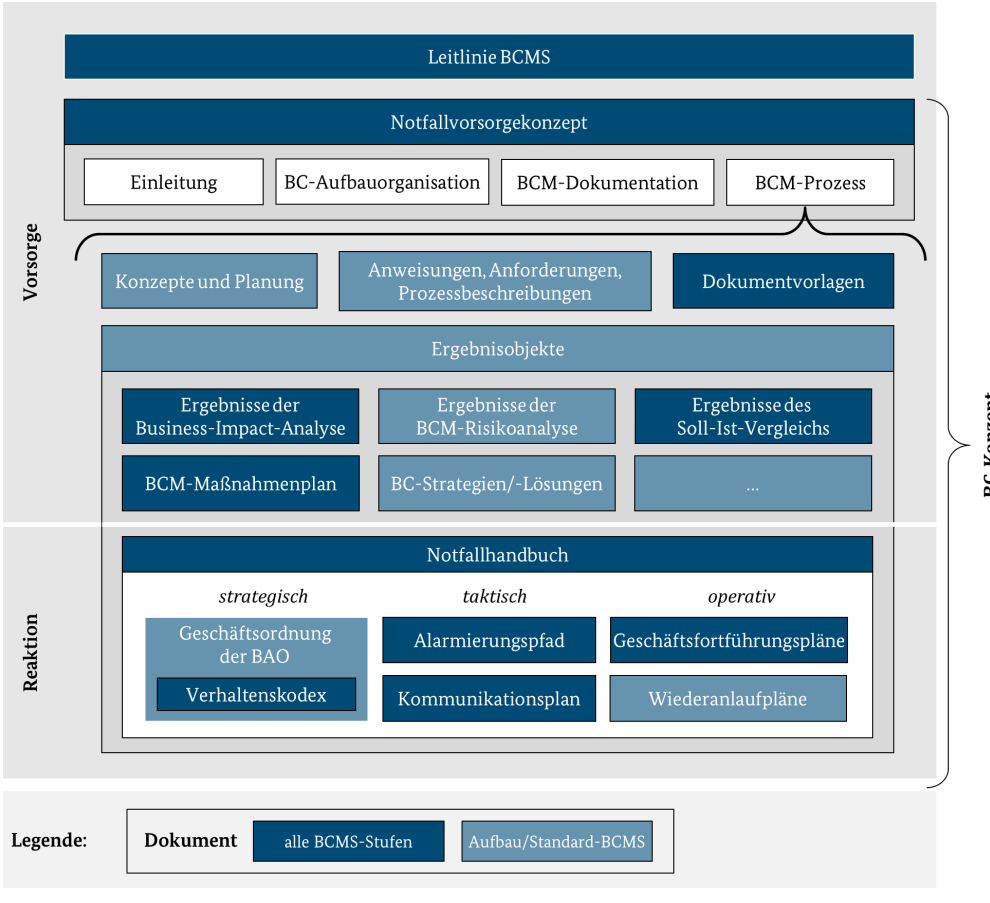

Abbildung 21: Dokumentenstruktur im BCM

In Abbildung 21 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.

Außer der Leitlinie BCMS ist die Dokumentation zur Vorsorge im **Notfallvorsorgekonzept** zusammengefasst. Die Dokumentation zur Reaktion ist im **Notfallhandbuch** (engl. **BC-Plans**) zusammengefasst. Sowohl das Notfallvorsorgekonzept als auch das Notfallhandbuch umfassen oft eine Sammlung von Dokumenten, die aus dem jeweiligen Hauptdokument nur referenziert werden. Beide Hauptdokumente zusammen ergeben das **BC-Konzept** (auch **Notfallkonzept**). Somit ist das BC-Konzept kein eigenständiges Dokument.

Dokumente zur Vorsorge

Die **Leitlinie BCMS** definiert Ziele und allgemeine Vorgaben für das BCMS auf der strategischen Ebene. Damit gibt die Leitlinie BCMS den verbindlichen Rahmen und den Auftrag 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.

Das **Notfallvorsorgekonzept** beinhaltet alle Dokumente des BCMS, die nicht im Notfall benötigt werden. Diese Dokumente legen fest, wie die allgemeinen Ziele und Vorgaben der Leitlinie BCMS 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 Hauptdokument mit Verweisen, sondern es kann auch eine Sammlung aller Dokumente sein, die nicht direkt zur Reaktion dienen.

Es ist empfehlenswert, die Vorgaben aus dem Notfallvorsorgekonzept zu einzelnen BCM-Prozessschritten in **Konzepten und Plänen** sowie in **Prozessbeschreibungen und Anweisungen** zu konkretisieren. **Konzepte und Pläne** regeln übergeordnete Vorgaben und dokumentieren, wie die Umsetzung einzelner Prozessschritte geplant wird. So wird z. B. in einem Übungshandbuch oder in Anweisungen festgelegt und definiert, welche Übungen wie oft durch wen durchgeführt werden sollen.

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 können z. B. für die BIA detaillierte **Anweisungen** vorgegeben werden, wie einzelne Befragungen im Rahmen der BIA durch die zuständigen Rollen durchgeführt werden sollen und welche **Dokumentvorlagen** hierfür genutzt werden sollen.

Dokumentvorlagen sind ergänzende Dokumente, die Anwendende darin unterstützen, Aufgaben innerhalb des BCM-Prozesses umzusetzen. So können insbesondere die Analysen innerhalb des BCMS anhand von 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 Dokumentvorlagen nachvollziehbar dokumentiert. Dadurch werden die gewonnenen Informationen für nachfolgende BCM-Prozessschritte leichter auswertbar und weiterverwendbar.

Dokumente zur Reaktion

Das **Notfallhandbuch** (engl. Business Continuity Plans, bzw. BC-Plans) stellt das zentrale Ergebnisobjekt dar, das alle für einen Not- oder Krisenfall relevanten Ergebnisobjekte aller Prozessschritte bündelt. Es beinhaltet alle Informationen zur Notfallbewältigung. Die Inhalte des Notfallhandbuchs können je nach Größe und Komplexität der Institution in verschiedene Dokumente unterteilt sein. Es ist zielführend, das Notfallhandbuch anhand der Zielgruppen zu unterteilen und so Dokumente auf strategischer, taktischer und ope-

rativer Ebene voneinander zu trennen. So kann bei einem Schadensereignis schneller auf die relevante Information zugegriffen werden.

Ein Notfallhandbuch und die damit einhergehenden Notfallmaßnahmen sowie eine arbeitsfähige BAO sind das zentrale Ergebnis eines BCMS, da sie zusammen eine Institution zur Geschäftsfortführung in einem Schadensfall befähigen.

Hinweis

Die in diesem Standard verwendete Dokumentenstruktur und die Bezeichnungen der Dokumente, beispielsweise Notfallhandbuch oder Notfallvorsorgekonzept, sowie die Dokumentenarten sind nicht bindend und können institutionsspezifisch festgelegt werden. Eine eigenständig entwickelte Dokumentenstruktur sollte jedoch die notwendigen Inhalte aller Dokumente, die in diesem Standard benannt sind, widerspiegeln.

In der BCM-Dokumentation sind zahlreiche schützenswerte Informationen der Institution enthalten. Um einen Verlust oder die unbeabsichtigte Veröffentlichung von schützenswerten Informationen zu verhindern, muss jedes Dokument hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität angemessen geschützt werden. Hierzu sollte in jedem Dokument selbst der Schutzbedarf dokumentiert werden (siehe 4.4.2 *Festlegung von Dokumentinformationen (AS)*). Insbesondere innerhalb des Notfallhandbuchs und der in ihm referenzierten Dokumente werden oftmals interne oder vertrauliche Informationen dokumentiert. Für diese Dokumente sollte die Zielgruppe auf wenige bestimmte Personen begrenzt werden. Zusätzlich muss für alle im Notfall benötigten Dokumente sichergestellt werden, dass diese im Notfall und in der Krise auch für die jeweiligen Zielgruppen verfügbar sind. Dies beinhaltet auch die im Notfallhandbuch referenzierten Dokumente.

Weitere Informationen zur Klassifizierung von Informationen können dem BSI-Standard 200-2, Kapitel 5.1 entnommen werden. Ferner muss für alle Dokumente des BCMS sichergestellt werden, dass keine veralteten Versionen produktiv eingesetzt werden.

4.4.2 Festlegung von Dokumentinformationen (AS)

Die verschiedenen Inhalte und Vorgaben des BCMS werden oft auf verschiedene Einzeldokumente verteilt, um Informationen gezielt steuern, aufbereiten und hierarchisch einordnen zu können.

Die Anzahl und jeweilige Ausprägung der Dokumente sind abhängig von der Größe und Komplexität der Institution, den zu berücksichtigenden Interessengruppen sowie institutionsspezifischen Vorgaben. Die Dokumentenstruktur sowie die Klammerdokumente Notfallvorsorgekonzept und Notfallhandbuch, die im Kapitel 4.4.1 *Dokumentenstruktur (R+AS)* beschrieben wurden, können als Vorlagen zur Orientierung genutzt werden.

Zudem ist es wichtig, Dokumente eindeutig zu kennzeichnen, um sie gezielt zuordnen und nachhalten zu können. Für jede Dokumentenart muss festgelegt werden, wie sie gestaltet und versioniert, wie häufig sie überarbeitet und durch wen sie freigegeben

wird. Diese Kennzeichnungen dienen der **Dokumentenlenkung**. 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 (siehe [820-2]).

Dokumente im BCM sollten mindestens mit den folgenden Eigenschaften gekennzeichnet werden:

- eindeutiger Titel
- eindeutige Versionsnummer (falls relevant)
- Dokumentenart (siehe auch Abbildung 21)
- Autor, Autorin
- Freigabedatum und -person
- Datum der nächsten geplanten Überarbeitung (für Dokumente, die Änderungen unterliegen können)
- Geltungsbereich des Dokuments (sofern für die Dokumentenart erforderlich)
- Klassifizierung
- Zielgruppe
- Ablage
- Aufbewahrungszeitraum (falls erforderlich)
- Änderungshistorie

Darüber hinaus kann es sinnvoll sein, die Funktion der Autorenschaft oder der zuständigen Person zu dokumentieren.

Beispiel

Kennzeichnung	*Erläuterung*
Titel	BCM-Leitlinie
Dokumentenart	Leitlinie BCMS
Version	1.0
Autor, Autorin	Frauke Musterfrau (BCB)
Freigabedatum und -person	31.07.22 durch Erika Mustermann (Institutionsleitung)
Datum der nächsten geplanten Überarbeitung	31.07. (jährliche Überprüfung)
Geltungsbereich des Dokuments	Gesamter BCM-Geltungsbereich
Klassifizierung	Intern
Zielgruppe	Mitarbeitende im Geltungsbereich sowie Externe mit begründetem Interesse

Kennzeichnung	*Erläuterung*
Ablage	https://intranet.institution.de/BCM/Leitlinie BCMS
Aufbewahrungszeitraum	10 Jahre (interne Anforderung)
Änderungshistorie	05.06.: Erster Entwurf, 07.07.: Anpassung der Ziele

Tabelle 7: Beispielkennzeichnung eines Dokuments

Hinweis

Häufig weicht der Notbetrieb erheblich von dem Normalbetrieb ab. In einem Notbetrieb geht es darum, mit eingeschränkten Ressourcen den Geschäftsbetrieb auf einem minimalen Niveau aufrecht zu erhalten, sodass die durch eine Unterbrechung entstehenden Schäden keine kritische Grenze überschreiten. Zu diesem Zweck kann es auch erforderlich werden, dass bei den einzelnen Dokumenten für den Notfall ein abweichender Schutzbedarf (in den Kategorien Vertraulichkeit, Integrität oder Verfügbarkeit) definiert wird.

4.4.3 Überprüfung und Aktualisierung von Dokumenten (AS)

Es muss sichergestellt werden, dass den Dokumenten des BCMS die geforderten Dokumenteigenschaften zugewiesen werden. Die Dokumente des BCMS müssen stets aktuell und den jeweiligen Zielgruppen zugänglich sein. Dies beinhaltet auch, dass die Zielgruppen diese Dokumente verstehen können. Auch sollte überprüft werden, dass sich die Informationen in über- und untergeordneten Dokumenten nicht widersprechen. Daher ist es empfehlenswert, die Überprüfung und Aktualisierung von Dokumenten zentral zu steuern.

So ist für zentrale Dokumente des BCM üblicherweise der oder die BCB selbst zuständig. Er oder sie 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 oder die BCB 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 oder die BCB die Aufgaben und Zuständigkeiten an die BCKs oder die jeweils Zuständigen überträgt. Diese verfügen in der Regel über das detaillierte Fachwissen, das für diese Dokumente relevant ist. Sofern weitere Wissenstragende oder zuständige Personen erforderlich sind, werden diese in den jeweiligen Kapiteln dieses Standards definiert.

Im Rahmen der kontinuierlichen Leistungsüberprüfung muss festgestellt werden, ob die Dokumente ihrem Aktualisierungszyklus entsprechend von den jeweiligen Zuständigen geprüft und, wenn notwendig, aktualisiert wurden (siehe Kapitel 14 *Leistungsüberprüfung und Berichterstattung (AS)*). Insbesondere muss überprüft werden, ob veraltete Dokumente durch neue Versionen an allen Ablageorten ersetzt wurden. So wird sicherge-

stellt, 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 das Notfallhandbuch 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. Abweichend vom Aktualisierungszyklus müssen BCM-Dokumente überprüft werden, sobald sich äußere Rahmenbedingungen oder Regelungen, denen die Institution unterliegt, oder interne Geschäftsziele, Aufgaben oder Strategien ändern.

Es sollte sichergestellt werden, dass relevante Änderungen zeitnah identifiziert und die betroffenen Dokumente umgehend aktualisiert werden. Dazu kann etwa mit den jeweiligen Kontaktpersonen ein Meldeprozess etabliert werden.

Beispiel

Der oder die BCB hat mit der Rechtsverwaltung vereinbart, dass er oder sie informiert wird, wenn sich gesetzliche oder regulatorische Anforderungen ändern, denen die Institution unterliegt. So kann der oder die BCB die Ziele und Ausrichtung des BCMS umgehend überprüfen und gegebenenfalls korrigieren.

Um eine bessere Übersicht der Dokumente zu erhalten und diese leichter steuern zu können, kann der oder die BCB eine Dokumentenmatrix erstellen. Die Dokumentenmatrix ist eine Übersicht, in der die einzelnen Dokumente mit den notwendigen Informationen zur Dokumentenlenkung aufgeführt werden.

Tabelle 8 zeigt beispielhaft auf, wie eine Dokumentenmatrix aufgebaut werden kann. Die dargestellten Informationen zur Dokumentenlenkung werden typischerweise auch in Dokumentenmanagementsystemen angewendet (siehe in dem Hilfsmittel *Tools* zu diesem Standard, Kapitel *Tools*).

Beispiel

Dokument	***Klassifizierung***	***Erstellt durch***	***Freigabe durch***	***Version***	***Aktualisiert am***
BCM-Leitlinie	Intern	BCB	Institutionsleitung	5.0	31.07.2022
GFP (OE Einkauf)	Vertraulich	BCK OE Einkauf	Leitung OE Einkauf	3.2	30.10.2022

Tabelle 8: Beispiel einer Dokumentenmatrix

4.5 Ressourcenplanung (R+AS)

Die Institutionsleitung muss gemäß ihrer Selbstverpflichtung angemessene personelle, zeitliche und finanzielle Ressourcen bereitstellen (siehe 3.1 *Übernahme der Verantwortung durch die Leitungsebene (R+AS)*). Die Ressourcen sollten darauf ausgerichtet sein, dass die geplanten Ziele in dem aktuellen Zyklus erreicht werden können. 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 BC-Aufbauorganisation sowie die Aufgaben und Zuständigkeiten der Rollen

In einer frühen Phase der Etablierung des BCMS kann der finanzielle Ressourcenbedarf nur geschätzt werden. Die konkreten Kosten umzusetzender Maßnahmen ergeben sich erst im weiteren Aufbau des BCMS. Daher ist es empfehlenswert, festzulegen, ob das Budget zentral oder aber dezentral, d. h. auf verschiedene Organisationseinheiten verteilt, verwaltet werden soll. Darüber hinaus ist es empfehlenswert, darauf hinzuweisen, dass im Rahmen der BC-Strategien durchaus noch erhebliche Ausgaben anfallen könnten. Hilfreich ist auch eine frühzeitige Entscheidung, ob das Budget schon auf zukünftige Bedarfe aus den BC-Strategien ausgerichtet werden soll. Die folgenden Posten können z. B. frühzeitig berücksichtigt werden:

- Schulungen und Maßnahmen zur Sensibilisierung
- 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
- Umsetzung und Betrieb von BC-Strategien und -Lösungen (falls das Budget auf zukünftige Bedarfe ausgerichtet wird).

Die Institutionsleitung muss nicht nur über die finanziellen Ressourcenbedarfe, sondern auch über die Organisationsstruktur sowie die personelle und zeitliche Ressourcenplanung entscheiden. Üblicherweise werden für die Institutionsleitung Entscheidungsvorlagen erstellt.

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

Die Ressourcenplanung muss regelmäßig auf ihre Angemessenheit überprüft und bei Bedarf angepasst werden. Damit das BCM seine Ziele erreichen kann, müssen die erforderlichen Ressourcen geplant, bereitgestellt und aufrechterhalten werden.

4.6 Schulung (R+AS)

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

Hinweis

Fähigkeiten und Kenntnisse sind Begriffe, die innerhalb dieses Standards das Wissen und die Erfahrungen zusammenfassen, die erforderlich sind, um die Aufgaben einer Rolle adäquat ausüben zu können.

Für alle Rollen im BCM muss sichergestellt werden, dass diese die benötigten Fähigkeiten und Kenntnisse besitzen oder erlangen. Dies kann durch Schulungsmaßnahmen, z. B. auch in Form von Praktika, erreicht werden. Der Schulungsbedarf richtet sich danach, inwieweit das vorhandene Wissen und die Vorerfahrung der Rolleninhabenden die benötigten Fähigkeiten und Kenntnisse bereits abdecken. Durch Schulungen können die Rolleninhabenden gezielt auf ihre Aufgaben vorbereitet und für diese qualifiziert werden. Die Art der Wissensvermittlung richtet sich nach der Anzahl der Rolleninhabenden, 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 Teilnehmenden nach Schulungsveranstaltungen sichergestellt werden. Falls die Ziele nicht erreicht wurden, sollte dies im Maßnahmenplan dokumentiert und über eine korrektive Maßnahme behandelt werden (siehe 15.2 *Ableitung von Korrektur- und Verbesserungsmaßnahmen (R+AS)*).

4.7 Sensibilisierung (R+AS)

Es ist von entscheidender Bedeutung für den Erfolg des BCMS, dass alle Mitarbeitenden und nicht nur die Rolleninhabenden verstehen, warum ein BCM in der Institution nützlich und notwendig ist. Ziel der Sensibilisierung ist, dass alle Mitarbeitenden ein gewünschtes Verhalten aus eigenem Antrieb und eigener Überzeugung umsetzen und beibehalten.

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

In der kontinuierlichen Verbesserung des BCMS muss jedoch das Bewusstsein für BCM sukzessiv bei allen Mitarbeitenden der Institution angestrebt werden. Dies ist üblicher-

weise am erfolgreichsten, wenn BCM in die bestehende Institutionskultur integriert wird oder die Institutionskultur entsprechend angepasst wird. Die Institution muss alle Mitarbeitenden durch geeignete Maßnahmen zielgruppenorientiert und bedarfsgerecht für das BCM sensibilisieren. Insbesondere muss den Mitarbeitenden bewusst sein, wo sie die für sie relevanten Informationen zur Notfallbewältigung finden und wie sie sich in einem Notfall verhalten sollen. Darüber hinaus sollte sämtlichen Mitarbeitenden bewusst sein,

- dass ein BCMS in der Institution etabliert ist,
- welchen Nutzen und welche Notwendigkeit ein BCMS hat und welche Ziele damit verfolgt werden,
- wie die Mitarbeitenden zum effektiven Betrieb und zur Verbesserung des BCMS beitragen können,
- wie die Mitarbeitenden sich in einem Notfall verhalten sollen sowie
- welche Auswirkungen es haben könnte, wenn Vorgehensweisen und Methoden des BCMS nicht eingehalten werden.

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

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

Synergiepotenzial

Die Bewusstseinsbildung spielt auch für andere Sicherheitsthemen wie die Informationssicherheit, den Datenschutz, die physische und personelle Sicherheit sowie den Arbeitsschutz eine große Rolle. Durch aufeinander abgestimmte Maßnahmen können Ressourcen effizient eingesetzt und eine themenübergreifende Sicherheitskultur geschaffen werden.

4.8 Leitlinie BCMS (R+AS)

Die Leitlinie BCMS (engl. BC Policy) 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 BCMS fixiert die Institutionsleitung ihre Selbstverpflichtung zur Einführung des BCMS und betont damit den Stellenwert des BCM innerhalb der Institution. Üblicherweise bereitet der oder die BCB die Leitlinie BCMS vor. Das Dokument kann anhand der Dokumentvorlage *Leitlinie BCMS* aus den Hilfsmitteln erstellt werden. Die Vorlage beinhaltet bereits mögliche Textbausteine als Vorschläge.

Synergiepotenzial

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

4.8.1 Erstellung der Leitlinie BCMS (R+AS)

Die Leitlinie BCMS hat drei wesentliche Funktionen:

1. Sie dient als dokumentierte Absichtserklärung der Institutionsleitung, ein BCMS aufbauen, betreiben und kontinuierlich verbessern zu wollen. Die Leitlinie ist der Nachweis dafür, dass die Institutionsleitung die Verantwortung für das BCM übernommen hat.
2. Die Leitlinie BCMS dient dazu, die wesentlichen Rahmenbedingungen festzulegen, unter denen ein BCMS etabliert und betrieben werden soll.
3. Die Leitlinie ist ein verbindlicher Auftrag an alle Mitarbeitenden, daran mitzuwirken, dass ein BCMS etabliert, aufgebaut und kontinuierlich weiterentwickelt wird, damit die Institution gegenüber Schadensereignissen selbst und deren Auswirkungen resilienter wird.

Da die Leitlinie BCMS 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 BCMS sollte zu diesem Zweck leicht verständlich und eindeutig formuliert sowie übersichtlich gestaltet werden. Ziel ist es, dass alle Mitarbeitenden die Inhalte der Leitlinie BCMS schnell erfassen und verstehen können.

Hinweis

Je detaillierter die Leitlinie BCMS auf konkrete Inhalte des BCMS eingeht, desto höher wird der Pflege- und Aktualisierungsaufwand. Bei hoher Detailtiefe erfordern bereits kleine Veränderungen im BCMS eine Anpassung der Leitlinie und jede Änderung muss erneut durch die Institutionsleitung freigegeben werden. Ferner kann die Leitlinie BCMS erst dann veröffentlicht werden, wenn die darin beschriebenen Inhalte definiert und etabliert sind. Eine detaillierte Leitlinie steht darum einer schnellen Veröffentlichung entgegen, die sinnvollerweise zeitnah zur Initiierung und Planung des BCMS erfolgt. Da die Leitlinie BCMS 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 ist es daher empfehlenswert, auf zu detaillierte Beschreibungen innerhalb der Leitlinie BCMS zu verzichten.

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

Die folgenden Inhalte, Rahmenbedingungen und Entscheidungen, die aus der Initiierung des BCMS hervorgehen, müssen in der Leitlinie BCMS dokumentiert sein:

- Motivation für den Aufbau des BCMS inklusive der rechtlichen und regulatorischen Anforderungen (siehe 3.2.1 *Motivation für den Aufbau eines BCMS (R+AS)*)
- Ziele für den Aufbau des BCMS und dessen Bedeutung für die Institution (siehe 3.2.2 *Entwicklung der Ziele des BCMS (R+AS)*)
- abzusichernder Zeitraum durch ein BCM (siehe 3.2.3 *Abzusichernder Zeitraum durch ein BCMS (R+AS)*)
- Geltungsbereich des BCMS (siehe 3.3 *Geltungsbereich (R+AS)*)
- Übernahme der Gesamtverantwortung der Institutionsleitung, inklusive der Selbstverpflichtung zur Etablierung, Aufrechterhaltung und kontinuierlichen Verbesserung des BCM nach diesem Standard (siehe 3.1 *Übernahme der Verantwortung durch die Leitungsebene (R+AS)*)
- institutionsspezifische Definition des Begriffs BCM sowie der Eskalationsstufen Störung, Notfall und Krise (siehe 4.1 *Definition und Abgrenzung (R+AS)*)
- Erläuterung der zentralen Rollen der BC-Vorsorgeorganisation, ohne deren Besetzung (siehe 4.3 *Definition der BC-Aufbauorganisation (R+AS)*)
- Dokumentation der Selbstverpflichtung der Institutionsleitung zur Etablierung, Aufrechterhaltung und kontinuierlichen Verbesserung des BCMS sowie Bereitstellung angemessener Ressourcen für das BCMS (siehe 4.5 *Ressourcenplanung (R+AS)*)

Zusätzlich müssen im **Aufbau- und Standard-BCMS** die relevanten Anforderungen der identifizierten Interessengruppen berücksichtigt werden (siehe 4.2.1 *Identifizierung von Anforderungen und Einflussfaktoren an das BCMS* (AS)).	**S**

4.8.2 Veröffentlichung und Aktualisierung der Leitlinie BCMS (R+AS)

Die Institutionsleitung muss die Leitlinie BCMS inhaltlich prüfen, freigeben und gegenüber allen Mitarbeitenden bekannt geben. Um ein Bewusstsein für das BCM bei den Mitarbeitenden zu schaffen und eine BCM-Kultur in der gesamten Institution zu etablieren, sollten alle Mitarbeitenden die Leitlinie BCMS kennen. Die Leitlinie BCMS sollte daher auch allen neuen Mitarbeitenden zur Kenntnis gegeben werden.

Darüber hinaus sollte die Institution prüfen, ob neben den Mitarbeitenden auch weitere Gruppen die Leitlinie BCMS zur Kenntnis nehmen sollen, z. B. Kunden und Kundinnen, zeitkritische Dienstleistungsunternehmen oder anderweitige Geschäftspartner und -partnerinnen. Die Leitlinie BCMS sollte entsprechend hinsichtlich Integrität, Vertraulichkeit und Verfügbarkeit klassifiziert sein. Die Institution muss ermöglichen, dass die Leitlinie BCMS für alle berechtigten Interessengruppen verfügbar ist.

Grundsätzlich sollte bereits bei der Erstellung der Leitlinie BCMS ein Überprüfungszyklus festgelegt und in der Leitlinie BCMS dokumentiert werden.

Falls sich wesentliche Rahmenbedingungen, Geschäftsziele, Aufgaben oder Strategien der Institution verändern, muss die Leitlinie BCMS anlassbezogen aktualisiert werden. Dafür ist es wichtig, die wesentlichen Änderungen zu identifizieren, die Auswirkungen der Änderung für das BCMS zu bewerten und die Leitlinie BCMS entsprechend anzupassen.

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

5 Aufbau und Befähigung der BAO (R+AS)

In Kapitel 2.3 *(zeitlicher) Ablauf* der Bewältigung wurden bereits alle Phasen und Aktivitäten einer Bewältigung schematisch erläutert. Zahlreiche dieser Aktivitäten setzen jedoch voraus, dass die Institution gut vorbereitet ist, indem sie vorab Maßnahmen plant und umsetzt, die im Folgenden beschriebenen werden.

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. Sofern 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 Definition dieses Standards befindet sich die Institution dann 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 verschiedenen Aspekte zum Aufbau und zur Befähigung der BAO werden in den folgenden Unterkapiteln näher erläutert. Die Aspekte überlagern sich zeitlich oder stehen in Wechselwirkung zueinander. In der Praxis bilden z. B. häufig der Aufbau der BAO sowie die Geschäftsordnung des Stabes die Grundlage für die Inhalte der 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 eine von vielen möglichen Ausgestaltungen der BAO 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 dokumentiert werden (siehe 4.4 *Dokumentation (R+AS)*). Das Notfallhandbuch kann anhand der Dokumentvorlage *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 die Institutionslei-

tung in der Vorbereitung zu allen relevanten Punkten eingebunden wird und die beschlossenen Regelungen und Maßnahmen freigibt.

5.1 Aufbau der BAO (R+AS)

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

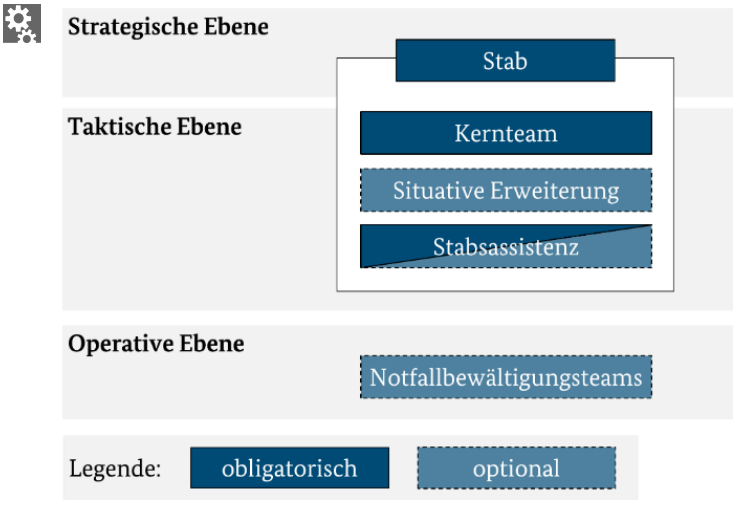

Abbildung 22: Beispiel verschiedener Rollen in einer BAO

Abbildung 22 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 ist es im Zusammenspiel mit anderen Stäben stets empfehlenswert, zu prüfen, wie die Begriffe strategisch, taktisch und operativ 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 im Normalbetrieb etablierten Organisationsform, z. B. der Linien- oder Matrixorganisation. Dadurch kann sichergestellt werden, dass komplexe und damit langwierige Entscheidungs- und Abstimmungswege vermieden werden, die in der Praxis häufig in der AAO vorkommen. Der Stab hat dabei innerhalb eines vorher festgelegten Rahmens Entscheidungsgewalt.

Analog zur Definition der BC-Vorsorgeorganisation müssen die Rollen der BAO, zusammen mit ihren Aufgaben, Rechten und Pflichten im Vorfeld festgelegt werden (siehe 4.3 *Definition der BC-Aufbauorganisation (R+AS)*). Für jede definierte Rolle der BAO kann der oder die BCB eine Besetzung vorschlagen. Für jedes Stabsmitglied sollte mindestens ein oder eine Stellvertretende benannt werden, da der Stab ad hoc und bei Bedarf über einen längeren Zeitraum handlungsfähig sein muss.

5.1.1 Aufbau des Stabs (R+AS)

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 den 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.

Neben der Verantwortung bleibt auch die Zuständigkeit für strategische Entscheidungen in Notfällen bei der Institutionsleitung. Der Stab unterstützt die Institutionsleitung, indem er Lösungen entwickelt und alle Tätigkeiten hierzu koordiniert. Zielsetzungen des Stabes sind, dass

- zeitkritische Geschäftstätigkeiten schnellstmöglich wiederaufgenommen werden,
- weitere Auswirkungen des Schadensereignisses von der Institution abgewendet werden sowie
- eine effektive und effiziente Zusammenarbeit sowie Kommunikation zwischen allen betroffenen Organisationseinheiten, der Institutionsleitung sowie Einsatzkräften, Behörden, Medien und anderen Parteien möglich ist.

Die Institutionsleitung sollte dem Stab angemessene Entscheidungsbefugnisse übertragen, damit er seine Ziele erreichen kann. Ferner ist es empfehlenswert, dem Stab zusätzlich Finanzbefugnisse zu erteilen. Abhängig von seinen Befugnissen kann der Stab auf der strategisch-taktischen oder nur auf der taktischen Ebene agieren.

Es ist empfehlenswert, dass der oder die BCB 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. Bewältigungsteams, erteilen (Aufgabenmanagement)
- umgesetzte Maßnahmen auf deren Wirksamkeit überprüfen und, falls erforderlich, korrigierende Maßnahmen einleiten
- interne und externe NuK-Kommunikation sowie Öffentlichkeitsarbeit (z. B. Pressestelle) steuern
- an die Institutionsleitung oder andere Zuständige eskalieren, falls die Situation die Grenzen der eigenen Zuständigkeit übersteigt

Dieser Vorschlag sollte im **Aufbau und Standard-BCMS** in der Geschäftsordnung konkretisiert werden (siehe 5.5 *Definition der Geschäftsordnung des Stabs (AS)*).	**S**

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 seinerseits 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.

Es ist empfehlenswert, eine grafische Übersicht des Stabsaufbaus zu erstellen. Abbildung 23 zeigt beispielhaft den Aufbau eines Stabes, bestehend aus Kernteam, situativer Erweiterung und Stabsassistenz. Wie eingangs dargestellt, sind die Stabsstrukturen je nach Institution sehr unterschiedlich. Daher ist es wichtig, das Beispiel institutionsspezifisch anzupassen.

Beispiel

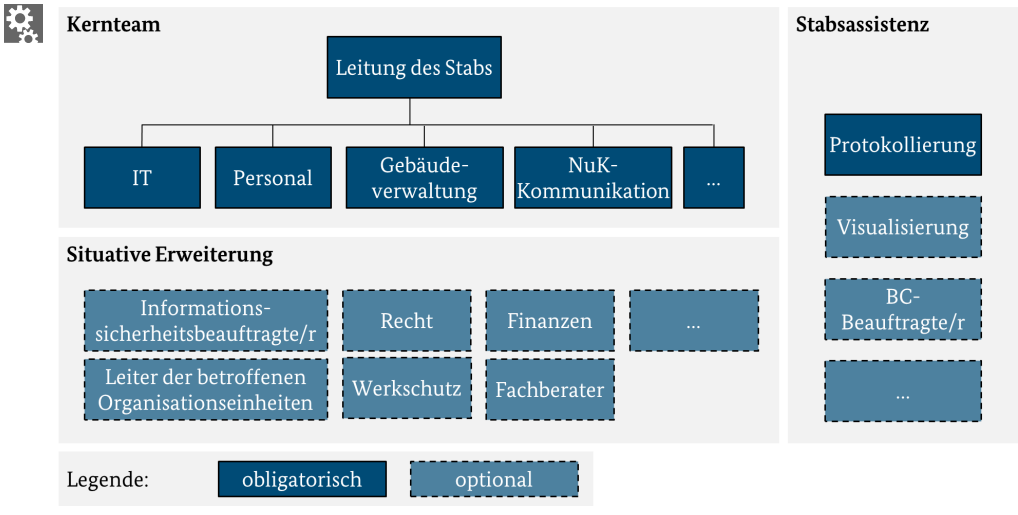

Abbildung 23: Beispiele verschiedener Rollen in einem Stab

Hinweis

Der Informationsaustausch und damit die Entscheidungsfähigkeit des Stabes werden idealerweise nicht durch zu viele Mitglieder ausgebremst. Daher ist es empfehlenswert, die Rollen der situativen Erweiterung sowie bei Bedarf auch die Rollen des Kernteams jeweils nur solange im Stab verbleiben zu lassen, wie es erforderlich ist, um die Lage zu beurteilen oder Maßnahmen abzuleiten.

5.1.2 Aufbau des Kernteams (R+AS)

Der Stab sollte aus einem Kernteam bestehen, dessen Mitglieder Schlüsselpositionen für Entscheidungen im Not- oder Krisenfall abdecken und lageunabhängig für die Bewältigung alarmiert werden. Das Kernteam sollte, neben einem oder einer Leitenden des Stabes, Mitglieder zu folgenden Themen beinhalten:

- IT
- Personal
- Gebäudeverwaltung
- Kommunikation

Der oder die Stabsleitende koordiniert die Aktivitäten aller Stabsmitglieder in der Bewältigung und trifft grundsätzlich die Entscheidungen im Stab. Für den oder die Stabsleitende muss neben den Aufgaben und Zuständigkeiten zusätzlich die Verantwortung im Not- und Krisenfall definiert werden, sobald diese leitende Person bei Ausrufung des Not- oder Krisenfalls über die AAO hinausgehende Entscheidungsbefugnisse oder finanzielle Spielräume erhält. Die Entscheidungsbefugnis kann die leitende Person an das

Kernteam delegieren. Daraufhin kann jede Rolle im Kernteam nach außen in Vertretung und im Auftrag der Stabsleitung Weisungen geben. Für den oder die Stabsleitende sollten mehrere Stellvertretende benannt werden, um sicherstellen zu können, dass diese zentrale Rolle für die Bewältigung besetzt ist.

Die Rollen **IT**, **Personal** und **Gebäudeverwaltung** repräsentieren die Organisationseinheiten, die über die jeweilige Fach- und Sachkenntnis der Ressourcen verfügen. Diese Rollen können in der Notfall- bzw. Krisenbewältigung 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 Dienstleistungsunternehmen steuern, als eigene Rolle im Kernteam ein. Ein Produktionsunternehmen bindet wiederum die Produktionssteuerung als eigene Rolle im Kernteam ein.

Die Rolle **NuK-Kommunikation** ist zuständig für die Informationssammlung sowie adressatengerechte Informationsaufbereitung und -verteilung nach innen und außen. Der NuK-Kommunikation kommt eine sehr hohe Bedeutung für den Erfolg der Notfallbewältigung zu (siehe 5.7.1 *Allgemeine Regelungen zur Kommunikation (R+AS)*).

5.1.3 Aufbau der situativen Erweiterung (R+AS)

Zum erweiterten Stab zählen Rollen, die durch ihre Expertise und Ressourcen zur Bewältigung beitragen können. Der Personenkreis beschränkt sich 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 Dienstleistende und Beratende. In diesem Fall sollten unter anderem die Punkte Vertraulichkeit von Informationen sowie Handlungs- und Entscheidungsbefugnisse explizit geregelt werden.

Beispiel

Typische Beispiele für eine situative Erweiterung:

- *Informationssicherheitsbeauftragte (ISB)*
- *Leitende der betroffenen Organisationseinheiten*
- *Recht*
- *Werkschutz*
- *Finanzen*
- *interne und externe Fachberater*

5.1.4 Aufbau der Stabsassistenz (R+AS)

Der Stab sollte durch eine Stabsassistenz ergänzt werden. Die Rollen der Stabsassistenz entlasten den Stab von organisatorischen Aufgaben und schaffen damit den Freiraum, damit der Stab sich darauf konzentrieren kann, zu handeln und zu entscheiden.

Hinweis

Je nach Arbeitsweise im Stab und den individuellen Fähigkeiten der agierenden Personen kann es möglich sein, dass eine Person gegebenenfalls mehrere Rollen wahrnimmt. So können beispielsweise in der Praxis die Rolle Visualisierung und die Rolle Aufgabenkoordinierung sinnvoll miteinander verbunden werden, wenn die jeweiligen Arbeitsphasen zeitlich auseinanderliegen.

Die Stabsassistenz sollte mindestens aus der Rolle Protokollierung und einer weiteren Person (Backoffice) bestehen. Der oder die Protokollierende 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 Verbesserungs- oder Korrekturbedarfe in der Bewältigung nachzuhalten. Weiterführende Informationen zur Protokollierung sind im Kapitel 5.5.4 *Protokollierung (AS)* beschrieben.

Es ist empfehlenswert, den Stab durch die Rolle **Visualisierung** zu unterstützen. Die Rolle Visualisierung dient dazu, das Ereignis in Schaubildern darzustellen. Mit Hilfe der Schaubilder soll ein möglichst gemeinsames Verständnis der Lage geschaffen werden, auch Lagebild genannt (siehe *5.6.2 Lagebeobachtung und -visualisierung (R+AS)*). So können Lageveränderungen sowie die Maßnahmenumsetzung gut verfolgt werden. 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 **Aufgabenkoordinierung** zu schaffen. Der oder die Aufgabenkoordinierende sammelt die verschiedenen Aufträge aus dem Stab. Dies entlastet andere Rollen des Stabes in komplexen Notfallsituationen.

Der oder die **BCB** ist eine Rolle in der BC-Vorsorgeorganisation. Es ist aber empfehlenswert, diese Rolle auch in die BAO einzubinden. Dies hat den Vorteil, dass das Wissen über die zeitkritischen Geschäftsprozesse und Ressourcen sowie die BC-Dokumentation dem Stab jederzeit direkt zur Verfügung steht und, falls erforderlich, erfragt werden kann. Abbildung 23 zeigt ein mögliches Beispiel, in dem der oder die BCB der Stabsassistenz zugeordnet ist.

5.1.5 Aufbau von Bewältigungsteams (R+AS)

Zur operativen Bewältigung eines Notfalls sollten Notfallbewältigungsteams aufgebaut werden. Da auf diese auch im Krisenfall zurückgegriffen werden kann, werden sie in diesem Standard als Bewältigungsteams bezeichnet.

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 eine einzelne Person für bestimmte Aktivitäten der Notfallbewältigung zuständig ist. Nachfolgend wird jedoch zur besseren Verständlichkeit nur von Bewältigungsteams oder Teams gesprochen.

Die Bewältigungsteams erhalten ihre Arbeitsaufträge aus dem Stab und setzen die technischen, baulichen oder organisatorischen Maßnahmen zur Notfallbewältigung auftragsgemäß um. Im Vorfeld festgelegte Bewältigungsteams 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 Bewältigungsteams können im Vorfeld festgelegt und erprobt werden.

Die Leitenden der Bewältigungsteams berichten üblicherweise während der Notfallbewältigung dem Stab in regelmäßigen Abständen. Dazu sammeln alle Leitenden die jeweiligen Informationen vor Ort und leiten diese an den Stab weiter. Darüber hinaus koordinieren und kontrollieren die Leitenden, ob die vom Stab angeordneten Maßnahmen vor Ort umgesetzt werden und wirksam sind. In der Praxis haben sich die folgenden Bewältigungsteams bewährt:

- IT
- Personal
- Gebäudeverwaltung
- NuK-Kommunikation

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

Falls die BAO vor der Absicherung der Geschäftsprozesse aufgebaut wurde, ist es sehr empfehlenswert, die genaue Zusammenstellung der Bewältigungsteams nochmals an die konkrete Wiederanlauf- und Geschäftsfortführungsplanung anzupassen.

5.1.6 Personelle Besetzung der BAO (R+AS)

Der festgelegte Aufbau der BAO sowie die Rollenbesetzung müssen von der Institutionsleitung freigegeben werden. Um der Institutionsleitung einen Gesamtüberblick über die BAO zu ermöglichen, ist es hilfreich, diese schematisch zu beschreiben. Hierzu kann ein Schaubild, wie in Abbildung 23 dargestellt, erstellt werden. Anhand von Rollenkarten

können zusätzlich die jeweiligen Aufgaben und Zuständigkeiten jeder Rolle im Detail vorgestellt werden.

Im **Reaktiv-BCMS** ist es empfehlenswert, dass jede Rolle des Stabs mit einem oder einer geeigneten Hauptzuständigen sowie einem oder einer Stellvertretenden anhand des festgelegten Aufbaus des Stabes besetzt wird**.**	**R**

Anhand des festgelegten Aufbaus der BAO muss im **Aufbau- und Standard-BCMS** sichergestellt werden, dass jede Rolle der BAO mit einem oder einer geeigneten Hauptzuständigen sowie mindestens einem oder einer Stellvertretenden besetzt wird.	**AS**

Unter anderem durch Schulungen kann sichergestellt werden, dass die Rolleninhabenden fachlich geeignet sind (siehe 5.6.1 *Schulung der BAO (R+AS)*). Gleichzeitig sollte geklärt werden, ob die Personen mental in der Lage sind, in besonderen Stresssituationen zu arbeiten (siehe auch das Hilfsmittel *Weiterführende Aspekte zur Bewältigung*).

Die Rollenbesetzung sollte im **Aufbau- und Standard-BCMS** 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 sollten neben den Aufgaben und Zuständigkeiten jeder Rolle die Entscheidungs- und Weisungsbefugnisse konkretisiert werden.	**AS**

Beispiel

Herr Mustermann wird als Leiter des Krisenstabes benannt. Er ist befugt, 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, bezieht jedoch die Empfehlungen und Einschätzungen der Stabsmitglieder in seine Überlegungen ein. Während die BAO gilt, ist Herr Mustermann von seinen Aufgaben und Pflichten der AAO entbunden.

Auch die Bewältigungsteams sollten mit geeignetem Personal besetzt werden. In der Praxis hat es sich bewährt, dazu auf die fachlich qualifizierten Mitarbeitenden aus den entsprechenden Ressourcenkategorien zurückzugreifen und die Teams mit hinreichenden Vertretungen zu versehen. Auf jeden Fall ist es empfehlenswert, die Mitarbeitenden im Einzelnen und die Personalvertretung im Allgemeinen zu beteiligen, da die Mitgliedschaft in einem Bewältigungsteam meistens mit entsprechenden Verpflichtungen (Bereitschaftszeiten, Arbeit an freien Tagen etc.) einhergeht.

5.2 Detektion, Alarmierung und Eskalation (R+AS)

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 also wichtig, dass dieser möglichst schnell erkannt und an die zuständige Entscheidungsinstanz gemeldet wird. Daher muss die Institution einen Alarmierungs- und Eskalationsprozess definieren und dokumentieren. In diesem Alarmierungs- und Eskalationsprozess sollte vorab festgelegt werden, wie und über welche Kanäle die Meldung von Schadensereignissen mit Notfallpotenzial erfolgt. Zudem sollte die Art der Meldung näher definiert werden. So kann eine Meldung entweder der Information oder der Alarmierung dienen.

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

Die **Alarmierung** führt immer zu einer Handlung von ausgewählten Mitarbeitenden 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 Dienstleistenden oder in der Sicherheitsvorfallbehandlung. Der Alarmierungs- und Eskalationsprozess des BCMS sollte vorhandene Prozesse zur Detektion und Behandlung von Störungen und Sicherheitsvorfällen berücksichtigen. In jedem Fall sollte sichergestellt werden, dass Schadensereignisse und Störungen mit Notfallpotenzial an eine zentrale Entscheidungsinstanz gemeldet werden (siehe Abbildung 24). Der Alarmierungsprozess und die damit verbundenen Reaktionszeiten sollten mit den beteiligten Stellen abgestimmt und dokumentiert sein. Zusätzlich muss für den Alarmierungs- und Eskalationsprozess technisch sichergestellt sein, dass die Kommunikations- und Alarmierungstechnik auch in einem Not- oder Krisenfall zur Verfügung steht. 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 24 stellt verkürzt mögliche Alarmierungspfade dar. Die einzelnen Aktivitäten werden in den nachfolgenden Unterkapiteln näher beschrieben.

Beispiel

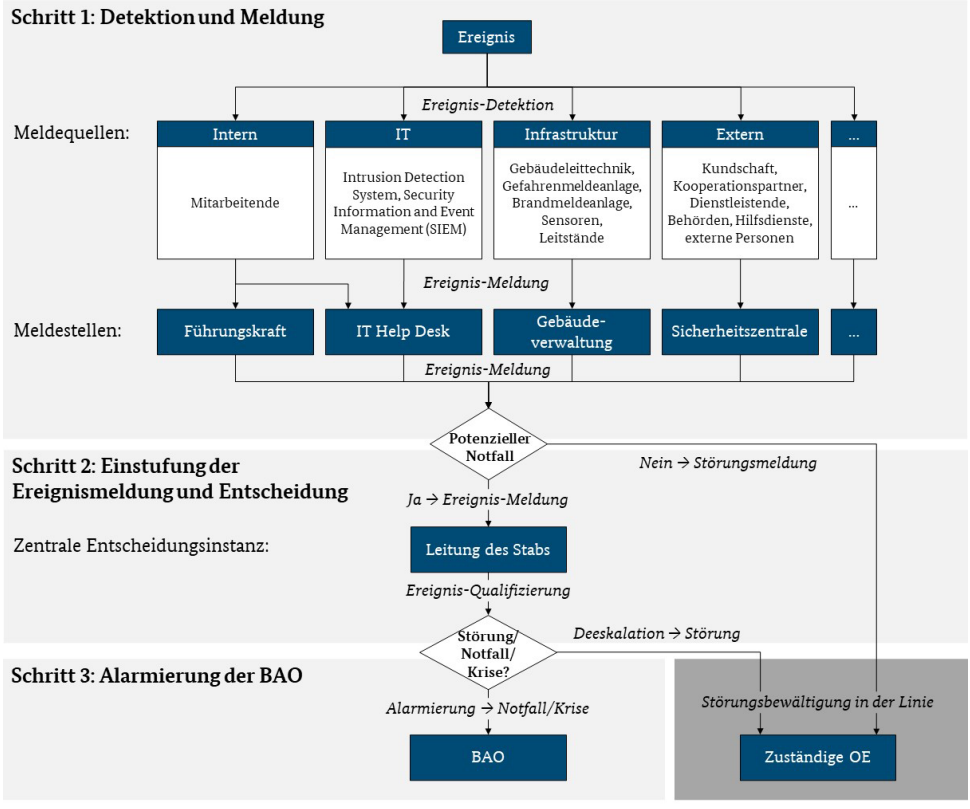

Abbildung 24: Beispiel eines Eskalations- und Alarmierungspfads

5.2.1 Detektion und Meldung (R+AS)

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 Mitarbeitende,*
- *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 Überwa-*

chung der grundlegenden Versorgung (Strom, Wasser, Klimatisierung etc.), Leitstände der Produktion zur Betriebs- bzw. Werkssteuerung sowie

- *externe Personen (z. B. Kunden und Kundinnen, Kooperationspartner und -partnerinnen, Dienstleistungsunternehmen, Behörden, Hilfsdienste, Bürger und Bürgerinnen 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 die 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 ist. 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 24 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 Meldungen zu Elementarschäden laufen meist bei einer Sicherheitsleitstelle oder einem Sicherheitsdienst auf.*
- *Personalausfälle oder Störungen bei Dienstleistungsunternehmen 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 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 muss durch Schulungen und Sensibilisierung für alle Mitarbeitenden 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 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. Falls 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 (Ersteinschätzung). Die Befähigung kann im Rahmen eines gemeinsamen Termins erfolgen, in dem der aktuelle Stand erklärt und gemeinsam Kriterien zur Ersteinschätzung gefunden werden. Da es wichtig ist, dass die Ersteinschätzung möglichst schnell erfolgt und die weiteren Abläufe der Notfallbewältigung so früh wie möglich eingeleitet werden, sollten klare und für alle Beteiligten verständliche Kriterien für eine Ersteinschätzung des Schadensereignisses definiert werden. Daher sollten für jede Meldestelle geeignete Kriterien zur Ersteinschätzung definiert werden. Der 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. Es ist wichtig, dass die Kriterien, um ein Ereignis einschätzen zu können, 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 Beispiel für die Ersteinschätzung eines Schadensereignisses für die häufigsten vier Ressourcenkategorien dargestellt (siehe *Tabelle* 9 bis Tabelle 12). Für jede Institution und Meldestelle muss das Bewertungs- oder Frageschema individuell festgelegt werden. Hierbei kann darauf hingewiesen werden, dass die Meldestellen die Informationen zur Bewertung einer Schadensmeldung auch aktiv von der oder dem Meldenden erfragen können, wenn die Antworten nicht offensichtlich sind.

Beispiel

Meldestelle Facility Management bzw. Sicherheitszentrale bzw. Sicherheitsdienstleistungsunternehmen bzw. 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 (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 Mitarbeitenden am Standort aufgrund eines Ereignisses (Unwetterwarnung, politische Demonstration, Schadensereignis im Umfeld etc.) möglicherweise gefährdet?*	

Sobald mindestens eine Frage mit JA beantwortet werden kann, bitte umgehend an die Stabsleitung melden:

Telefon 1234567890

Tabelle 9: Beispiel einer Ersteinschätzung eines Schadensereignisses am bzw. im Gebäude

Meldestelle IT-Help Desk (1st bzw. 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 Kreis von Benutzenden oder den wesentlichen Geschäftsbetrieb der Institution?* • *Besteht ein dringender Verdacht auf vorsätzliche Daten- oder Systemmanipulationen (Datenabfluss), auf unerlaubte Ausübung von Rechten oder auf einen gezielten Angriff auf IT-Komponenten (physisch oder virtuell)?* • *Ist zu erwarten, dass die Auswirkungen des Ereignisses einen Zeitraum > 8 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, z. B. auf Kundschaft, Medien, Aufsichtsbehörden? Gegebenenfalls die Information beim Anwendenden erfragen.*	

Sobald mindestens eine Frage mit JA beantwortet werden kann, bitte umgehend an die Stabsleitung melden: Telefon 1234567890

Tabelle 10: Beispiel einer Ersteinschätzung eines Schadensereignisses in der IT

Meldestelle Führungskraft Personal

Leitfragen für Schadensereignisse mit Notfallpotenzial – Personal	*Ja/Nein*
• Sind in Ihrem Zuständigkeitsbereich so viele Mitarbeitende nicht arbeitsfähig, dass Sie möglicherweise den Geschäftsbetrieb nicht mehr aufrechterhalten können? • Ist durch die Abwesenheit von Mitarbeitenden mit bestimmten Berechtigungen der normale Geschäftsbetrieb gefährdet oder nicht mehr möglich?	

Sobald mindestens eine Frage mit JA beantwortet werden kann, bitte umgehend an die Stabsleitung melden:

Telefon 1234567890

Tabelle 11: Beispiel einer Ersteinschätzung eines Schadensereignisses beim Personal

Meldestelle Provider Management bzw. Dienstleistungsunternehmen-steuerung

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

Sobald mindestens eine Frage mit JA beantwortet werden kann, bitte umgehend an die Stabsleitung melden: Telefon 1234567890

Tabelle 12: Beispiel einer Ersteinschätzung eines Schadensereignisses bei Dienstleistungsunternehmen

Wenn es sich um ein Schadensereignis mit Notfallpotenzial handelt, muss die zuständige Stelle unverzüglich eine vordefinierte zentrale Entscheidungsinstanz alarmieren. Hierbei müssen folgende Inhalte übermittelt werden:

- alle bekannten Details zum Schadensereignis
- die bisher bekannten Auswirkungen
- bereits eingeleitete Maßnahmen zur Bewältigung des Ereignisses

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 informiert werden. Eventuelle Fehlmeldungen können im Nachgang untersucht werden. Anschließend kann 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, ist es im **Reaktiv-BCMS** empfehlenswert, alternative Techniken vorzuhalten. Es ist ferner empfehlenswert, dass außerdem Kommunikationskanäle zur Verfügung stehen, die unabhängig von der IT der Institution funktionieren.	**R**

Für den Fall, dass die Kommunikations- und Alarmierungstechnik vom Schadensereignis selbst betroffen ist, müssen im **Aufbau- und Standard-BCMS** alternative Techniken vorgesehen werden. Es sollten außerdem Kommunikationskanäle zur Verfügung stehen, die unabhängig von der IT der Institution funktionieren.	**AS**

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.

5.2.2 Einstufung der Ereignismeldung und Entscheidung (R+AS)

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. Im Gegensatz zu dezentralen Entscheidungsinstanzen verhindert eine zentrale Entscheidungsinstanz 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, dass die zentrale Entscheidungsinstanz über die erforderliche Sachkenntnis verfügen muss, z. B. um innerhalb der Institution entscheiden zu können, was eine Störung, was ein Notfall und was eine Krise ist (siehe 4.6 *Schulung (R+AS)*). Zudem muss die zentrale Entscheidungsinstanz den Alarmierungsprozess kennen.

Die zentrale 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 diese Entscheidungsinstanz entscheidungsfreudig sein.

Das Verständnis der zentralen Entscheidungsinstanz kann darüber hinaus erhöht werden, indem sie realitätsnahe, praktische Erfahrungen bei Übungen und Tests sammeln kann. Wenn außerdem die Entscheidungskriterien verbessert werden, begünstigt dies eine korrekte Einschätzung von Schadensereignissen. So werden Fehleinschätzungen durch die kontinuierliche Verbesserung des BCMS gesenkt.

Zusätzlich muss die zentrale 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 oder die Leitende des Stabes oder der oder die BCB geeignete Rollen, um die Ereignismeldung qualifizieren zu können.

Um die Entscheidung zu vereinfachen und sie transparent zu machen, ist es empfehlenswert, der zentralen Entscheidungsinstanz eine Checkliste mit Kriterien zur Verfügung zu stellen. Auf deren Basis kann eine nachvollziehbare und dokumentierte Entscheidung zur Einstufung des Ereignisses getroffen werden. Um Kriterien für einen Notfall (siehe 4.1 *Definition und Abgrenzung (R+AS)*) ableiten zu können, können zunächst folgende Punkte als Grundlage herangezogen werden:

Beispiel

- *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?*

Die Kriterien auf dieser Checkliste können auch vom Stab zu einer ersten Einstufung des Schadensereignisses herangezogen werden, falls es im BCMS noch keine konkreteren Kriterien gibt. Diese kann die Institution dann zu einem späteren Zeitpunkt genauer festlegen.

Das Ergebnis der Ersteinschätzung kann zwei Ausgänge haben:

1. Das Ereignis wird als **Störung** eingestuft.

   Dann sollte 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 zentrale Entscheidungsinstanz über den Verlauf der Störungsbeseitigung durch die zuständige Fachabteilung informieren lassen.

2. Das Ereignis wird als **Notfall** oder **Krise** eingestuft.

Dann muss die zentrale Entscheidungsinstanz die BAO unverzüglich alarmieren.

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

In der Konstituierung der BAO sollte diese Entscheidung durch den Stab anhand weiterer Kriterien überprüft und bestätigt oder deeskaliert werden (siehe 5.8 *Nacharbeiten und Deeskalation (R+AS)*).

5.2.3 Alarmierung der BAO (R+AS)

Um sicherzustellen, dass die BAO unverzüglich alarmiert werden kann, müssen die notwendigen organisatorischen und technischen Voraussetzungen geschaffen und dokumentiert werden. Ein zentraler Punkt, der gemeinsam mit den Rolleninhabenden und der Institutionsleitung abgestimmt werden muss, ist die **Erreichbarkeit der BAO** innerhalb und außerhalb der üblichen Geschäftszeiten. Analog zu dem beschriebenen Vorgehen für die zentrale(n) Meldestelle(n) sollten entsprechende Rufbereitschaften der BAO eingerichtet werden. Für Zeiten, in denen eine Erreichbarkeit der BAO nicht garantiert ist, sollten Risikoübernahmen durch die Institutionsleitung herbeigeführt werden.

Im Ernstfall sollte die Benachrichtigung der Rolleninhabenden der BAO kurz und präzise sein. Diskussionen und längere Ausführungen zur Lage sollten bei der Alarmierung vermieden werden. Zum einen könnten zu viele Informationen die zu alarmierende Person verwirren. Zum anderen würde die Alarmierung unnötig verzögert. Detaillierte Informationen werden in der ersten Lagebesprechung für alle Anwesenden gemeinsam vorgestellt und besprochen. Der Alarmierungs- und Eskalationsprozess sollte organisatorisch regeln,

- 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 die alarmierte Person unternehmen muss, beispielsweise sich im Stabsraum oder in einer virtuellen Arbeitsumgebung, z. B. Telefonkonferenz, einzufinden. Die alarmierte Person muss dem Aufruf zeitnah folgen. Falls weitere Personen die Alarmierung entgegennehmen könnten, z. B. Haushaltsmitglieder, die den Anruf auf dem privaten Telefon entgegennehmen können, so sollten diese für den Umgang mit empfangenen Alarmmeldungen sensibilisiert werden.

Je nach Größe der BAO kann es zeitaufwändig sein, alle Rolleninhabenden einzeln persönlich zu benachrichtigen, z. B. mittels eines manuellen Telefonanrufs. 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. Neben der Alarmauslösung bieten die IT-Anwendungen zur Alarmierung oft wichtige Zusatzfunktionen, z. B.:

- eine Alarmnachverfolgung,

- eine automatische Benachrichtigung der Stellvertretenden bei Nicht-Erreichbarkeit oder
- die Möglichkeit, dass die alarmierten Personen der Stabsleitung den erwarteten Zeitpunkt des Eintreffens im Stabsraum mitteilen können, falls dies der nächste Schritt ist.

Der definierte Eskalations- und Alarmierungsprozess sollte visualisiert und im Notfallhandbuch dokumentiert werden. Dafür kann z. B. die Abbildung 24 angepasst werden (siehe 5.2 *Detektion, Alarmierung und Eskalation (R+AS)*). Diese ist auch in den Hilfsmitteln zum BSI-Standard 200-4 hinterlegt.

Dokumentierte Vorgaben und begleitende Maßnahmen stellen sicher, dass die definierten Meldewege wie vorgesehen eingehalten werden. Als begleitende Maßnahme müssen 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 Mitarbeitenden geplant und veranlasst werden, um eine schnelle Alarmierung und Eskalation zu gewährleisten.

5.3 Definition von Sofortmaßnahmen (R+AS)

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 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. Innerhalb des Notfallhandbuchs MÜSSEN Sofortmaßnahmen dokumentiert werden. Die im Notfallhandbuch definierten Sofortmaßnahmen MÜSSEN Regelungen zum Schutz von Leib und Leben beinhalten.

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, 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 sind entsprechende Anweisungen für Sofortmaßnahmen meist bereits in der Institution vorhanden, z. B. seitens der Fachkraft für Arbeitssicherheit.

Die entsprechenden organisatorischen Maßnahmen können in geeigneter Form in die Ablauforganisation der Notfallbewältigung integriert werden. Entsprechend ist es sinnvoll, die im Notfallhandbuch dokumentierten Sofortmaßnahmen zum Schutz von Leib und Leben mit der Fachkraft für Arbeitssicherheit abzustimmen. Im Notfallhandbuch sollte auf vorhandene Regelungen und Rollen verwiesen werden, z. B. auf die Aufgaben und Zuständigkeiten der Ersthelfenden, Betriebssanitäter und -sanitäterinnen, Brandhelfenden, Evakuierungshelfenden oder Einsatzteams sowie auf entsprechende Aushänge in den Gebäuden. Es ist empfehlenswert, die Sofortmaßnahmen in Form von Checklisten zu dokumentieren. Dies ermöglicht auch unter Zeitdruck eine strukturierte Vorgehensweise.

Hinweis

Häufig wird unter Sofortmaßnahmen die Räumung des Gebäudes verstanden, beispielsweise bei einem Brand. BCM-relevante Sofortmaßnahmen greifen jedoch in der Regel erst ab dem Zeitpunkt, wenn die Mitarbeitenden das Gebäude nach einem Brand verlassen haben und beim Sammelpunkt eingetroffen sind. Deswegen ist es hilfreich, die vorhandenen Regelungen und Sofortmaßnahmen dahingehend zu prüfen, 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 Facility Management (Erstmeldung)	Feststellende Person
2	Fehlersuche und Schadensbegrenzung	Mitarbeitende(r) Facility Management
3	Rufen eines Wartungs- bzw. Reparaturdienstes,	Mitarbeitende(r) Facility Management
4	Ermitteln der konkreten Auswirkungen bzw. betroffenen Gebäude(teile)	Mitarbeitende(r) Facility Management
5	Aktuellen Arbeitsstand der zeitkritischen Geschäftsprozesse prüfen und Aufgaben priorisieren	Führungskräfte der betroffenen OEs
6	Mobile Arbeitsfähigkeit gewährleisten Mitarbeitende des Bewältigungsteams sollen Laptops mitnehmen (Sicherheit geht jedoch vor!) Schlüsselpersonen mit Token ausstatten	Betroffene OE bzw. Führungskräfte
7	Zuständige Meldestelle informieren	Mitarbeitende(r) Facility Management

Tabelle 13: 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 14: Beispiel für Sofortmaßnahmen bei einem Gebäudeausfall

5.4 Festlegung der Grundsätze zur Stabsarbeit (R)

Die Arbeitsweise im Stab unterscheidet sich deutlich von der gewohnten Zusammenarbeit im Normalbetrieb. Für die Stabsmitglieder ist die Stabsarbeit häufig sehr belastend, insbesondere durch die außergewöhnlichen Herausforderungen im Notfall oder in der Krise, z. B. durch hohen Handlungsdruck, gestörte Kommunikationswege oder unvollständige oder widersprüchliche Informationen.

Sind in einer solchen Situation im Stab die Rollen- und Aufgabenverteilung oder die Mitsprache- und Entscheidungsrechte unklar oder ist die Kommunikation zwischen den Mitgliedern unstrukturiert, so 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. So kann eine „Chaosphase" im Notfall weitestgehend vermieden werden. Aus demselben Grund müssen die

Rahmenbedingungen zur Konstituierung und Auflösung der BAO bereits im Vorfeld festgelegt werden.

5.4.1 Festlegung der Methoden und Regeln für die Stabsarbeit (R)

Die grundlegenden Methoden und Regeln zur Stabsarbeit werden in einem sogenannten **Verhaltenskodex** zusammengefasst. Dieser stellt sicher, dass der Stab im Notfall seine Arbeit direkt aufnehmen kann und handlungsfähig ist. Es wird empfohlen, dass der oder die BCB aufgrund der BC-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 in Bezug auf das eigene Aufgabengebiet 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

*Der Stab richtet seine Arbeitsweise anhand der vorliegenden Notfallpläne aus (Geschäftsfortführungspläne GFP). Liegen keine Notfallpläne vor oder greifen diese nicht, wird die Arbeitsweise am **Führungszyklus** FOR-DEC ausgerichtet.*

1. *Der Stab hat Arbeits- und Besprechungsphasen (**Lagebesprechungen**). Diese müssen eindeutig festgelegt und allen Stabsmitgliedern kommuniziert werden.*
2. *Lagebesprechungen*
   - *dauern nie länger als 30 Minuten,*
   - *brauchen immer eine moderierende Person,*
   - *dürfen ihren Fokus nicht durch Einzeldiskussionen zu Spezialthemen verlieren (Diese Diskussionen können im Nachgang geklärt werden.),*
   - *müssen immer eindeutig beendet werden und*
   - *müssen immer zeitlich klar terminiert und angesagt werden.*
3. *Es muss immer ein **Protokoll** geführt werden, in welchem die Meldungen, 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.

4. *Fakten müssen von Gerüchten getrennt und Informationen immer verifiziert werden. In komplexen Lagen sollte dazu ein **Informationsmanagement** aufgebaut werden.*
5. *Die **Visualisierung** sollte regelmäßig genutzt und aktualisiert werden.*
6. *Aufgaben müssen klar benannt, terminiert und delegiert und im **Aufgabenmanagement** festgehalten werden (Zielstellung, Aufgabenstellung, Zuständigkeiten, Umsetzungsfrist bzw. Wiedervorlage).*
7. *Damit allen anwesenden Personen bewusst ist, wer welche Rolle oder Funktion in der BAO einnimmt, muss sich jeder und jede in der ersten Lagebesprechung mit Namen und Rolle oder 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 5.5 Definition der Geschäftsordnung des Stabs (AS) näher beschrieben.

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

Arbeitsbedingungen (R)

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, ist es empfehlenswert, bereits im Vorfeld die Übergabe zwischen den Schichten zu regeln.

Falls die institutionsspezifischen Arbeitszeit- und Überstundenregelungen keine Vorgaben für einen Notfall beinhalten, wird empfohlen, abweichende Regelungen für den Notfall festzulegen. In diesem Fall ist es notwendig, diese vorab mit den relevanten Stellen, wie z. B. der Rechtsabteilung, Personal- oder Betriebsrat sowie der Institutionsleitung abzustimmen.

Protokollierung (R)

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.

Protokolle können in elektronischer Form oder in Papierform erstellt werden. Zur Arbeitserleichterung ist es empfehlenswert, eine Dokumentvorlage oder ein anderes Hilfsmittel für die Protokolle zu entwickeln. 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 oder die BCB sowie die Rolleninhabenden Stabsleitung und Protokollierung abstimmen

Hinweis

In der Praxis hat es sich bewährt, wenn die Rolle Protokollierung 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.

5.4.2 Konstituierung und Auflösung der BAO (R)

Die Konstituierung und Auflösung der BAO markiert den jeweiligen Übergang vom Normal- in den Notbetrieb sowie vom Notbetrieb in den Normalbetrieb. Die Konstituierung der BAO schließt sich dem Alarmierungs- und Eskalationsprozess unmittelbar an (siehe 5.2 *Detektion, Alarmierung und Eskalation (R+AS)*).

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 sind durch das Ereignis selbst gefährdet.

- *Das Leben und die Gesundheit von Personen sind 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.*

- *Ein bedeutsamer Verstoß gegen Gesetze, Vorschriften oder Verträge wurde festgestellt. Der Verstoß kann zu Meldepflichten an Dritte oder zu rechtlichen Konsequenzen führen.*

Über die meisten dieser Kriterien kann in der Regel anhand der Ergebnisse der BIA konkret entschieden werden. Liegen noch keine Ergebnisse der BIA zu den betroffenen Geschäftsprozessen vor, dann müssen die genannten Kriterien ad hoc durch den Stab überprüft werden.

Die Institution muss im Vorhinein standardisierte Abläufe festlegen, sowohl um einen Notfall oder eine Krise auszurufen als auch um diese 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 Person)?
- Wie wird über die erforderlichen Mitglieder im Kernteam sowie 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 aktiviert werden (siehe Kapitel 11 *Geschäftsfortführungsplanung (R+AS)* sowie 12 *Wiederanlauf- und Wiederherstellungsplanung (AS)*)?
- Unter welchen Voraussetzungen wird die Stabsarbeit beendet und die BAO schrittweise aufgelöst?

Beispiel

Fragen für eine Checkliste zum Konstituieren des Stabes:

- *Wie werden die Stabsmitglieder alarmiert?*
- *Wie werden 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?*

Fragen für eine 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 die Nacharbeiten getroffen?*
- *Ist die Maßnahmenverfolgung inklusive der Aufgaben bei den Nacharbeiten vollständig dokumentiert? Durch wen wird diese Maßnahmenverfolgung in der AAO fortgeführt?*
- *Ist das Protokoll der Stabsarbeit vollständig, vertraulich und wiederauffindbar abgelegt?*
- *Wann und durch wen erfolgt der Rückbau des Stabsraums?*

Für den BCM-Prozessschritt BIA wird der zu erwartende Zeitraum benötigt, zwischen Eintreten eines Schadensereignisses bis zur Ausrufung des Notfalls, der in diesem Standard mit **BAO-Reaktionszeit** bezeichnet wird. Die BAO-Reaktionszeit umfasst den Zeitraum vom Erkennen und Alarmieren des Ereignisses, über das Konstituieren der BAO und die Entscheidungsfindung bis zum Ausrufen des Notfalls. Zusätzlich ist es empfehlenswert, in der Reaktionszeit einen zeitlichen Puffer einzuplanen, da insbesondere die Detektion mit Unsicherheiten hinsichtlich des genauen zeitlichen Ablaufs und Umfangs einhergeht.

Diese BAO-Reaktionszeit ist in der Regel unabhängig von den einzelnen Geschäftsprozessen und sollte daher an dieser Stelle zentral festgelegt werden. Anhand von Übungen zur Alarmierung und zur Entscheidungsfindung im Stab kann dieser Zeitraum präzisiert werden (siehe 13.8 *Alarmierungsübung (R+AS)*). Jedoch wird die BAO-Reaktionszeit in der Regel zu einem gewissen Grad variieren, da sie entscheidend von der Detektionszeit abhängig ist, die wiederum von Situation zu Situation variiert. Die BAO-Reaktionszeit stellt somit einen eher groben Richtwert dar.

5.5 Definition der Geschäftsordnung des Stabs (AS)

Die Arbeitsweise im Stab unterscheidet sich deutlich von der gewohnten Zusammenarbeit im Normalbetrieb aufgrund der besonderen Herausforderungen im Notfall. Diese sind 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)?
- Welche Rechte, Pflichten und Zuständigkeiten besitzt der Stab im Not- oder Krisenfall (besondere Befugnisse)?
- 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. Vorab ist es empfehlenswert, dass der oder die BCB aufgrund der BC-Sachkenntnis einen Vorschlag für die Geschäftsordnung erstellt. Gleichzeitig ist es jedoch auch empfehlenswert, die Institutionsleitung 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 erstellt und gepflegt werden.

5.5.1 Konstituierung und Auflösung der BAO (AS)

Die Konstituierung und Auflösung der BAO markiert den jeweiligen Übergang vom Normal- in den Notbetrieb und vom Notbetrieb in den Normalbetrieb. Die Konstituierung der BAO schließt sich dem Alarmierungs- und Eskalationsprozess unmittelbar an (siehe *5.2 Detektion, Alarmierung und Eskalation (R+AS)*).

In der Geschäftsordnung des Stabes sollte daher auf Basis des Alarmierungsprozesses konkret 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 darüber zu entscheiden, ob ein Notfall oder eine Krise vorliegt.

Beispiel

- *Das Leben und die Gesundheit von Personen sind durch das Ereignis selbst gefährdet.*
- *Das Leben und die Gesundheit von Personen sind 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 3.1.4* ***Selbstverpflichtung der Institutionsleitung****).*
- *Ein bedeutsamer Verstoß gegen Gesetze, Vorschriften oder Verträge wurde festgestellt, der zu Meldepflichten an Dritte oder zu rechtlichen Konsequenzen führen kann.*

Über die meisten dieser Kriterien kann in der Regel anhand der Ergebnisse der BIA konkret entschieden werden. Liegen noch keine Ergebnisse der BIA vor, dann ist es notwendig, dass der Stab die genannten Kriterien ad hoc überprüft.

Die Institution sollte im Vorhinein Abläufe und Regeln festlegen, sowohl um einen Notfall auszurufen als auch um diesen 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 sowie 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 Person)?
- Wie wird über die erforderlichen Mitglieder im Kernteam und 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 aktiviert werden (siehe Kapitel 11 *Geschäftsfortführungsplanung (R+AS)*, 12 *Wiederanlauf- und Wiederherstellungsplanung (AS)*)?
- Unter welchen Voraussetzungen wird die Stabsarbeit beendet und die BAO schrittweise aufgelöst?

Beispiel

Fragen für eine Checkliste zum Konstituieren des Stabes:

- *Wie werden die Stabsmitglieder alarmiert?*
- *Wie werden 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?*

Fragen für eine 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 die Nacharbeiten getroffen?*
- *Ist die Maßnahmenverfolgung inklusive der Aufgaben bei den Nacharbeiten vollständig dokumentiert? Durch wen wird diese Maßnahmenverfolgung in der AAO fortgeführt?*
- *Ist das Protokoll der Stabsarbeit vollständig, vertraulich und wiederauffindbar abgelegt?*
- *Wann und durch wen erfolgt der Rückbau des Stabsraums?*

Für den BCM-Prozessschritt BIA wird der zu erwartende Zeitraum benötigt, zwischen Eintreten eines Schadensereignisses bis zur Ausrufung des Notfalls, der in diesem Standard mit **BAO-Reaktionszeit** bezeichnet wird. Die BAO-Reaktionszeit umfasst den Zeitraum vom Erkennen und Alarmieren des Ereignisses, über das Konstituieren der BAO und die Entscheidungsfindung bis zum Ausrufen des Notfalls. Zusätzlich ist es empfehlenswert, in der Reaktionszeit einen zeitlichen Puffer einzuplanen, da insbesondere die Detektion mit Unsicherheiten hinsichtlich des genauen zeitlichen Ablaufs und Umfangs einhergeht.

Diese BAO-Reaktionszeit ist in der Regel unabhängig von den einzelnen Geschäftsprozessen und sollte daher an dieser Stelle zentral festgelegt werden. Anhand von Übungen zur Alarmierung und zur Entscheidungsfindung im Stab kann dieser Zeitraum präzisiert werden (siehe *13.8 Alarmierungsübung (R+AS)*). Jedoch wird die BAO-Reaktionszeit in der Regel zu einem gewissen Grad variieren, da sie entscheidend von der Detektionszeit abhängig ist, die wiederum von Situation zu Situation variiert. Die BAO-Reaktionszeit stellt somit einen eher groben Richtwert dar.

5.5.2 Festlegung eines Zusammenarbeitsmodells (AS)

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 und 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.

5.5.3 Festlegung der Arbeitsbedingungen (AS)

Die Stabsarbeit erfolgt unter Stress und ist physisch wie psychisch belastend. Zudem endet die Stabsarbeit oft nicht zum Ende eines regulären Arbeitstages. Daher sollte die Institution vorab abstimmen und dokumentieren, inwieweit im Not- oder Krisenfall ein Schichtbetrieb für den Stab möglich ist. Hierbei ist es notwendig, die institutionsspezifischen Arbeitszeit- und Überstundenregelungen daraufhin zu prüfen, inwieweit diese im Notfall abweichen oder speziell dafür gesondert geregelt werden können. Zusätzlich ist es wichtig, abweichende Regelungen für den Notfall vorab mit den relevanten Stellen, z. B. mit der Rechtsabteilung, dem Personal- oder Betriebsrat sowie der Institutionsleitung abzustimmen.

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, des Schichtwechsels oder des Bedarfs an Mehrarbeit. Daher 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 Stabs hat eine benannte erste Vertretungsperson, die nach Ende der Schicht oder im Verhinderungsfall die jeweilige Funktion übernimmt. Sind auch erste Vertretende verhindert, so können der oder die Leitende des Stabes oder die Vertretungsperson der Stabsleitung eine Person aus der entsprechenden Organisationeinheit in den Stab berufen. Diese Entscheidung muss schriftlich dokumentiert werden.

Die Übergabephase zwischen zwei Schichten erfolgt zu definierten Zeiten. Sie 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 Mitarbeitenden in der darauffolgenden Schicht benötigt werden.

5.5.4 Protokollierung (AS)

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 formalen Anforderungen an die Dokumentation der Bewältigung, insbesondere an die Protokollierung im Stab sollten in der Geschäftsordnung des Stabes dokumentiert werden.

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

Protokolle können in elektronischer Form oder in Papierform erstellt werden. Zur Arbeitserleichterung ist es empfehlenswert, eine Dokumentvorlage oder ein anderes Hilfsmittel für die Protokolle zu entwickeln. Hierbei sollte ein Kompromiss zwischen den Nachweispflichten der Institution, der Nachvollziehbarkeit von Entscheidungen und der Arbeits- und Entscheidungsfähigkeit des Stabs gefunden werden. Es ist empfehlenswert, dass sich der oder die BCB sowie die Rolleninhabenden Protokollierung und Stabsleitung hierüber abstimmen.

Hinweis

In der Praxis hat es sich bewährt, wenn die Rolle Protokollierung 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.

5.5.5 Festlegung besonderer Befugnisse (AS)

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 oder die Leitende 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 aufgrund der Stabsarbeit in der AAO nicht personalrechtlich belangt. Ausgenommen sind nur Absicht oder grobe Fahrlässigkeit.

Hinweis

In wirtschaftsorientierten Institutionen ist eine Haftungsausschlusserklärung gegenüber dem oder der Leitenden des Stabes dringend anzuraten. Hierbei ist es wichtig, dass die Leitung des Stabes weiterhin für vorsätzliche Handlungen gegen gesetzliche und institutionsinterne Regularien haftbar ist.

5.5.6 Erstellung eines Verhaltenskodexes (AS)

Auch wenn die Geschäftsordnung des Stabes die Rahmenbedingungen festlegt und dokumentiert, ist damit nicht sichergestellt, dass diese „Spielregeln" in der üblichen Hektik der Bewältigung 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. Dieser muss von jeder Institution an die eigenen Bedürfnisse und Anforderungen angepasst werden.

Aufgrund der Bedeutung des Verhaltenskodexes für die Zusammenarbeit während eines Notfalls oder 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 BC-Planung aus. Liegen keine Notfallpläne vor oder greifen diese nicht, so 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 eine moderierende Person, die nicht gleichzeitig den Stab leitet,*
   - *dürfen ihren Fokus nicht durch Einzeldiskussion zu Spezialthemen verlieren (Solche Diskussionen können im Nachgang geklärt werden.),*
   - *müssen immer eindeutig beendet werden und*
   - *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, in welchem die Meldungen, 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 sowie im **Aufgabenmanagement** festgehalten werden (Zielstellung, Aufgabenstellung, Zuständigkeiten, Umsetzungsfrist bzw. Wiedervorlage).*
9. *Damit allen anwesenden Personen bewusst ist, wer welche Rolle oder Funktion in der BAO einnimmt, muss sich jeder und jede in der ersten Lagebesprechung mit Namen und Rolle oder Funktion vorstellen. Dies wird wiederholt, wenn neue Mitglieder hinzustoßen.*

5.6 Herstellung der Fähigkeit zur Stabsarbeit (R+AS)

Für eine funktionierende Bewältigung ist es wichtig, dass die in den vorherigen Schritten geschaffenen organisatorischen Voraussetzungen durch die BAO-Rolleninhabenden verstanden und verinnerlicht werden. Daher muss durch Schulungen und Übungen sicher-

gestellt werden, dass die Stabsmitglieder ihre Aufgaben im Not- und Krisenfall kennen und erworbene Kenntnisse anwenden können.

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.

Die Institution muss einen Stabsraum und dessen Ausstattung festlegen, planen, beschaffen und einrichten, sodass diese Infrastruktur im Notfall verfügbar und einsatzbereit ist.

Die nachfolgenden Unterkapitel beschreiben die wesentlichen Schritte zur

- Schulung der BAO,
- Lagebeobachtung und Visualisierung,
- Festlegung eines Stabsraums,
- Ausstattung des Stabsraums sowie
- Freigabe durch die Institutionsleitung.

Weitere Informationen, wie diese Grundlagen umgesetzt werden können, sind in dem Hilfsmittel *Weiterführende Aspekte zur Bewältigung* beschrieben.

5.6.1 Schulung der BAO (R+AS)

Alle Stabsmitglieder, einschließlich der Stellvertretenden, 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 5.1.6 *Personelle Besetzung der BAO (R+AS)*).

Insbesondere bei unerfahrenen Personen, die ihre Rolle erst verinnerlichen müssen, sollten zunächst die theoretischen Grundlagen der Notfallbewältigung geschult werden. Es ist empfehlenswert, dass die **Grundlagenschulung** folgende Aspekte beinhaltet:

- 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 in der Bewältigung?

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. Visualisierung, Protokollierung)

Das **praktische Training zur Stabsarbeit** kombiniert inhaltliche und methodische Aspekte der Stabsarbeit. Ziel des Trainings ist es, dass die Rolleninhabenden 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 Teilnehmenden praktisch angewendet. Entsprechend ist es wichtig, dass das Training durch einen erfahrenen Trainer für Stabsarbeit moderiert und geleitet wird.

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 Fachleute einzubeziehen oder Seminarangebote zu nutzen.

Es ist empfehlenswert, mögliche weiterführende Schulungen und praktische Trainings, unter anderem zur Protokollierung, zur Visualisierung, zum Aufgabenmanagement sowie zur „Führung im Notfall oder in der Krise", nach Bedarf zusätzlich einzuplanen. Auch ist es empfehlenswert, im Anschluss an diese Schulungen eine Stabsübung durchzuführen, um das erlangte Wissen zu vertiefen und praktische Erfahrungen aufzubauen. Die hierzu erforderlichen Schritte sind im Kapitel 13.6 *Stabsübung (R+AS)* beschrieben.

In der weiteren Entwicklung des BCMS können sich einzelne Aspekte zur Stabsarbeit verändern oder weiter konkretisieren. Daher sollten die Schulungsinhalte für die Stabsmitglieder regelmäßig geprüft und angepasst werden.

Für die weiteren Mitglieder der BAO ist es empfehlenswert, ebenfalls regelmäßig spezifische Schulungen und Awareness-Veranstaltungen durchzuführen, z. B. für die Bewältigungsteams (siehe 4.6 *Schulung (R+AS)* sowie 4.7 *Sensibilisierung (R+AS)*). In der Schulung ist es wichtig, nicht nur allgemein das BCM der Institution, sondern auch die Abläufe und Aufgaben im Notfall zu erläutern.

Ergänzend dazu sollten alle Mitglieder der BAO (inklusive Vertretende) im **Aufbau oder Standard-BCMS** mindestens ein Mal in drei Jahren an einer Übung teilnehmen, in der sie ihre jeweiligen Aufgaben im Fall eines Schadensereignisses trainieren können (siehe Kapitel 13 *Üben und Testen (R+AS)*).	**AS**

5.6.2 Lagebeobachtung und -visualisierung (R+AS)

Notfälle und Krisen sind dadurch gekennzeichnet, dass sich die aktuelle Lage laufend verändert. Es gibt 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 im **Aufbau-** und **Standard-BCMS** die nachfolgenden Punkte vorab festgelegt werden:	**AS**

- zuständige Rollen in der Lagebeobachtung
- mögliche Quellen der Lagebeobachtung, z. B.:
  - Informationen der Stabsmitglieder oder Bewältigungsteams
  - Medienmonitoring (siehe 5.7.3 *Externe Kommunikation*)
- Vorgaben zum Medienmonitoring
- Sicherstellung der Erreichbarkeit der Personen am Ort des Geschehens, z. B.:
  - Personen, die Sofortmaßnahmen ausgeführt haben
  - Bewältigungsteams, welche die Notfallmaßahmen operativ ausführen

Zusätzlich ist es empfehlenswert, für die Lagebeobachtung Schwerpunkte zu setzen, z. B.

- bisher umgesetzte Sofortmaßnahmen
- bekannte Fakten zum Ereignis
- jegliche, bisher ergriffene Maßnahmen und deren Wirksamkeit

Auch wenn es für ein **Reaktiv-BCMS** aufgrund des Aufwandes nicht verbindlich vorgeschrieben wird, ist es für eine effektive **Lagebeobachtung** empfehlenswert, diese Punkte vorab festzulegen.	**R**

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:

- Art und Weise der Visualisierung (Medium und Detailgrad)
- Aktualisierung des Lagebildes möglichst fortlaufend (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 **NuK-Kommunikation**

Abbildung 25 veranschaulicht exemplarisch die Visualisierung eines fortlaufenden Lagebildes anhand eines Zeitstrahls.

Beispiel

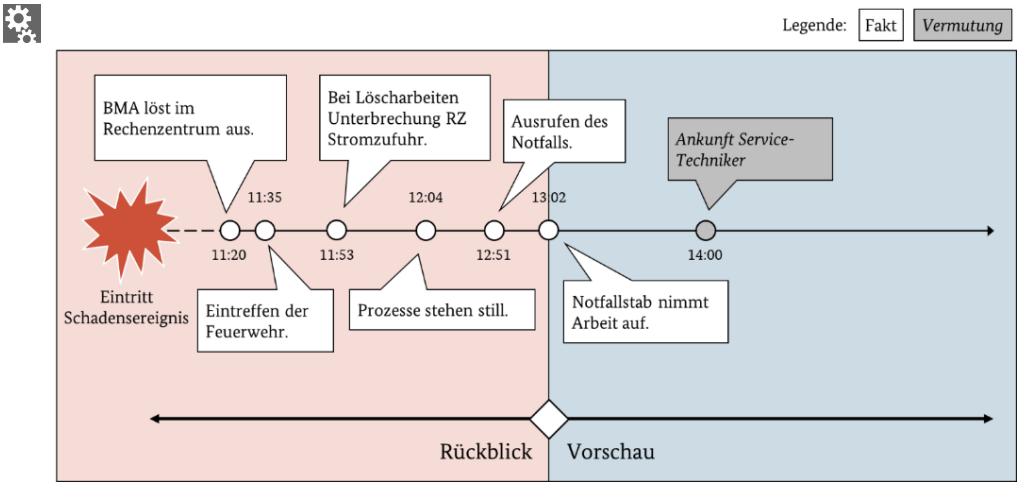

Abbildung 25: Beispiel eines Zeitstrahls zur Visualisierung von Ereignissen

Es sollten bevorzugt gesicherte Informationen visualisiert werden. Vermutungen und Annahmen müssen als solche kenntlich gemacht werden. Falls die Rolle Visualisierung eingesetzt wird, sollte diese für die Elemente zur Lagevisualisierung ausführlich geschult werden. Dabei sollte auch gemeinsam mit dem oder der Leitenden des Stabes festgelegt werden, wie mit dem Stab und der Protokollierung zusammengearbeitet wird. Wird keine separate Rolle Visualisierung eingesetzt, sollten alle Mitglieder des Kernteams mit den Grundsätzen der Lagevisualisierung vertraut gemacht werden.

5.6.3 Festlegung eines Stabsraums (R+AS)

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 einen einzelnen Arbeitsraum handeln, indem alle verschiedenen Phasen der Stabsarbeit stattfinden oder um einen Arbeitsbereich, in dem verschiedene Räume für unterschiedliche Arbeitsphasen und Mitglieder des Stabs zur Verfügung stehen. Verschiedene Bereiche bieten sich an, um die Arbeits-, Ruhe- und Besprechungsphasen örtlich voneinander zu trennen (siehe auch Hilfsmittel Weiterführende Aspekte zur Bewältigung).

Der Begriff Stabsraum differenziert im täglichen Sprachgebrauch nicht zwischen diesen unterschiedlichen räumlichen Situationen. Deswegen wird nachfolgend nur von Stabsraum gesprochen, ohne die Anzahl an Bereichen konkret festzulegen. Wenn gesonderte Bereiche, wie der Raum für Stabsbesprechungen, explizit gemeint sind, wird darauf explizit eingegangen.

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. Die Stabsmitglieder sowie ihre Stellvertretenden 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

Ein Stabsraum sollte so geplant werden, dass er in einem Notfall zeitnah einsatzfähig 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. Für diesen Fall sollte ein alternativer Stabsraum an einem Ausweichstandort definiert werden. Dies können z. B. ähnliche Räumlichkeiten in einem Gebäude mit ausreichen-

dem Abstand sein, aber auch ein Konferenzcenter oder ein Hotelbesprechungsraum. 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 Räumlichkeiten vor oder erlaubt die Lage keine physische Zusammenkunft der Stabsmitglieder, dann kann eine Sekundärlösung auch aus einer virtuellen Arbeitsumgebung bestehen, die z. B. über ein Webkonferenz- oder ein Krisenmanagement-Tool bereitgestellt wird.

Größe und Aufteilung

Es ist empfehlenswert, die Größe des Stabsraums nicht zu knapp zu bemessen, da keine genaue Vorhersage über die Anzahl der Stabsmitglieder gemacht werden kann, die für ein bestimmtes Schadensereignis hinzugezogen werden. Es ist auch empfehlenswert, dass die Räumlichkeiten über ausreichend Arbeitsplätze, über Bereiche für Visualisierungstechnik und über einen abgetrennten Besprechungsraum bzw. Besprechungszonen verfügen.

Einhaltung von Sicherheitsanforderungen

Für alle definierten Stabsräume und zusätzlich geplanten Räume muss sichergestellt werden, dass die geltenden Sicherheitsanforderungen der Institution sowohl bei der Planung als auch im späteren Betrieb eingehalten werden. So ist es zum Beispiel wichtig, dass der Umgang mit vertraulichen Informationen gesichert ist. Die Sicherheitsanforderungen müssen sowohl bei der Planung als auch im späteren Betrieb der Stabsräume eingehalten werden.

5.6.4 Ausstattung des Stabsraums (R+AS)

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. Die Ausstattung aller Stabsräume 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

Es ist empfehlenswert, den Besprechungsraum des Stabs weitgehend frei von Kommunikationsausstattung zu halten oder durch eine gezielte Moderation sicher zu stellen, dass in Besprechungsphasen die Mitglieder nicht durch ihre Kommunikationsmittel abgelenkt

werden. Während Besprechungsphasen ist keine ständige Kommunikation nach außen notwendig und jede Form der externen Kommunikation stört die konzentrierte Arbeit, egal ob in Form von Telefongesprächen oder der Bearbeitung von E-Mails. Es ist jedoch empfehlenswert, ein zentrales Konferenztelefon („Telefonspinne") als Grundausstattung im Besprechungsraum des Stabs vorzuhalten. Hiermit können Mitglieder des Stabes oder Fachleute, 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 im Besprechungsraum des Stabes ist es empfehlenswert, einen zusätzlichen Raum in der Nähe dauerhaft mit allen etablierten Kommunikationsmitteln auszustatten. In diesen zusätzlichen Stabsräumen sollten je nach deren Funktion ausreichend Kommunikationsmittel zur Verfügung stehen. Dazu zählen:

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

Alle zusätzlichen Räumlichkeiten sollten dieselben Anforderungen an die Verfügbarkeit und Sicherheit erfüllen wie der Besprechungsraum des Stabes 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, ist es hilfreich, auch folgende Ausstattung im Vorfeld zu beschaffen

- 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, falls z. B. der Stabsraum, die Dokumentation an sich oder das Notfall-Laptop physisch zerstört sind. Diese doppelte Vorhaltung kann z. B. durch weitere physische oder digitale Kopien erfolgen. Hierbei ist es wichtig, auf Aktualität und die Anforderungen der Informationssicherheit und des Datenschutzes zu achten. 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 die 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, z. B. Maßnahmenverfolgung oder Ereigniszeitstrahl*
- *Tische und Stühle U-förmig in Richtung Visualisierungsflächen aufstellen*
- *Namenskarten entsprechend dem Sitzplan aufstellen*
- *BCM-Dokumentation sortiert nach den Rollen im Raum verteilen*

- *Telefonkonferenzschaltung bereitstellen*
- *Kommunikationsmittel und Technik auf Einsatzfähigkeit testen*
- *Verpflegung und Getränke bereitstellen*

5.6.5 Freigabe durch die Institutionsleitung (R+AS)

Die erarbeiteten, abgestimmten und dokumentierten Entscheidungen und Vorgaben zur Stabsarbeit sowie die zur Alarmierung und Eskalation (siehe 5.2 *Detektion, Alarmierung und Eskalation (R+AS)*) 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. Anschließend müssen die hierfür erforderlichen Maßnahmen umgesetzt und im Maßnahmenplan nachverfolgt werden (siehe 15.1 *Vorbereitung eines BCM-Maßnahmenplans (R+AS)*).

5.7 NuK-Kommunikation (R+AS)

Wie die Institution im Notfall oder der Krise wahrgenommen wird und ob Vertrauen in die NuK-Bewältigung gesetzt wird, hängt im Wesentlichen auch davon ab, wie gut die Notfall- und Krisen-Kommunikation (**NuK-Kommunikation**) gelingt. Daher muss die NuK-Kommunikation im Vorfeld gut vorbereitet, geplant und dokumentiert werden. So ist es wichtig, dass in der Institution präventiv überlegt wird, wann Meldungen an die Mitarbeitenden und an externe Interessengruppen erforderlich sind und wie die externe NuK-Kommunikation kontrolliert werden kann, um Reputationsschäden zu vermeiden.

Zudem ist es beispielsweise wichtig, Geschäftspartnern und -partnerinnen Stornierungen mitzuteilen oder Kundschaft über Zeitverzögerungen bei der Lieferung bestellter Waren zu informieren. Auch die Kommunikation zu Polizei, Feuerwehr und Rettungsdiensten gehört dazu, sofern die Art des Notfalls deren Einsatz verlangt.

5.7.1 Allgemeine Regelungen zur Kommunikation (R+AS)

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

- interne Kommunikation (Was dürfen oder müssen die Mitarbeitenden wann erfahren?)
- externe Kommunikation durch Mitarbeitende (Was dürfen die Mitarbeitenden 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 (siehe 5.7.3 *Externe Kommunikation (R+AS)*)

Die NuK-Kommunikation sollte auf die Meldepflichten der Institution abgestimmt sein.

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. Folgende Anforderungen an die Kommunikation sollten eingehalten werden:

- 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 sowie die zu nutzenden Medienformate, z. B. Pressemitteilung, Pressekonferenz, Stellungnahme auf der Webseite oder Mitteilungen über soziale Medien, vorab festgelegt werden. Sofern innerhalb der Institution mehr als eine Person für die NuK-Kommunikation zuständig ist, müssen die jeweiligen Aufgaben und Zuständigkeiten innerhalb des NuK-Kommunikationsteams festgelegt und dokumentiert werden, damit diese Arbeit effektiv koordiniert werden kann.

5.7.2 Interne Kommunikation (R+AS)

Eine kontinuierliche interne NuK-Kommunikation ist entscheidend, um während eines Notfalls die Unsicherheit unter den Mitarbeitenden so weit wie möglich zu minimieren. Eine sachliche interne NuK-Kommunikation erhöht das allgemeine Vertrauen in die Institutionsleitung und die BAO, dass diese die Situation kontrollieren können. Wenn die Mitarbeitenden 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 Mitarbeitenden jedes Detail des Schadensereignisses kennen. Vielmehr sollte in der NuK-Kommunikation mindestens sichergestellt werden, dass die Mitarbeitenden alle erforderlichen Details des Schadensereignisses kennen, insbesondere wenn diese Details die persönliche Situation oder die persönliche Sicherheit betreffen. Zudem sollten relevante Informationen im Zusammenhang mit dem Status der Notfallbewältigung insbesondere für diejenigen Mitarbeitenden bereitgestellt werden, die in Kontakt mit externen Interessengruppen stehen, z. B. mit Kunden und Kundinnen, Behörden oder Dienstleistungsunternehmen.

Hinweis

In der Praxis hat es sich bewährt, dass alle Mitarbeitenden zeitlich mindestens dieselben Informationen erhalten wie die allgemeine Öffentlichkeit. Das bedeutet, dass die Informationen aus der externen NuK-Kommunikation zeitgleich oder früher intern kommuniziert werden sollten. Somit wird vermieden, dass Mitarbeitende erst durch Medien über das Schadensereignis selbst oder über Neuigkeiten in dessen Zusammenhang erfahren und sich dadurch vernachlässigt fühlen. Außerdem wird Gerüchten und Mutmaßungen vorgebeugt. Gleichzeitig ist es empfehlenswert, Informationen, die auf keinen Fall nach außen kommuniziert werden dürfen, auch nicht intern an alle Mitarbeitenden zu kommunizieren.

5.7.3 Externe Kommunikation (R+AS)

In jedes Notfallszenario sind diverse Interessengruppen direkt oder indirekt involviert. Die Institution muss sämtliche Interessengruppen berücksichtigen. Typische Beispiele hierfür sind Medienvertretende, Kunden und Kundinnen, Dienstleistungsunternehmen, Aufsichtsbehörden, Polizei und Angehörige von Mitarbeitenden.

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 **im Aufbau- und Standard-BCMS** eine intensive Analyse der relevanten Interessengruppen, eine Planung der jeweiligen Kommunikationsstrategie sowie die Erstellung eines Kommunikationskonzeptes. Detailliertere Informationen dazu können im Hilfsmittel *Weiterführende Aspekte zur Bewältigung* nachgeschlagen werden. Tabelle 15 zeigt ein vereinfachtes Beispiel für ein wichtiges Element des Kommunikationskonzeptes: Die adressatenspezifische Information der relevanten Interessengruppen (siehe auch 4.2.1 *Identifizierung von Anforderungen und Einflussfaktoren an das BCMS (AS)*).	**AS**

Beispiel

Priorität	*Interessengruppe*	*Kommunikationsbedarf im Notfall*	*Kommunikationswege*	*Zuständig*
1	*Kundschaft*	*bei direkter Betroffenheit*	*Webseite* *Telefon*	*Kundenservice*
2	*Öffentlichkeit und Medien*	*individuelle Strategie zur NuK-Kommunikation ist abhängig vom jeweiligen Ausfallszenario und dem Interesse der Öffentlichkeit*	*Pressemitteilung* *Webseite* *Soziale Medien* *Interview/Gespräch* *Pressekonferenz*	*Pressesprecher, -sprecherin,* *Leitung Kommunikation*
3	*Versicherungen*	*versicherter Schadensfall*	*Telefon* *E-Mail bzw. Brief*	*Leitung Recht*
4	*Dienstleistungsunternehmen und Zuliefernde*	*bei direkter Betroffenheit*	*Telefon* *E-Mail*	*Leitung Kommunikation*

Tabelle 15: Externe Kommunikation mit Interessengruppen

Für die externe NuK-Kommunikation bieten sich z. B. folgende Kanäle an, sofern verfügbar:

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

Für mögliche Presseanfragen sollten eine Person als Pressesprecher oder -sprecherin sowie ihre stellvertretende Person namentlich benannt und innerhalb der Institution sowie extern veröffentlicht werden. Dies stellt eine einheitliche und offizielle externe Kommunikation sicher.

Die externe NuK-Kommunikation begrenzt sich nicht auf die einseitige Kommunikation der Institution mit Dritten sowie der Öffentlichkeit, sondern betrachtet auch die Kommunikation Dritter untereinander. Dies betrifft vor allem die Medienberichterstattung. Notfälle und Krisen, 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 Not- oder Krisenfall ist es sehr empfehlenswert, Medien zum Schutz der Reputation der Institution stetig zu beobachten (**Medienmonitoring**). Nur wenn die Institution weiß, wie derzeit über sie selbst und das Ereignis kommuniziert wird, kann sie zielstrebig darauf hinarbeiten, ihren Ruf zu wahren. 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. Insbesondere in den sozialen Medien spielt die Schnelllebigkeit der Kommunikation eine wesentliche Rolle. Oftmals ist ein „Shitstorm" innerhalb weniger Stunden vorüber und kann im Nachgang durch die Kommunikatoren der Institution innerhalb der AAO aufgearbeitet werden.

5.8 Nacharbeiten und Deeskalation (R+AS)

Ist das Schadensereignis überwunden, dann sollte der Stab den Notfall offiziell für beendet erklären (**Deeskalation**) 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.

Nacharbeiten

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 Wiederherstellungsmaßnahmen oder Nacharbeiten sind noch nicht abgeschlossen, sodass noch nicht von einem Normalbetrieb gesprochen werden kann.

Beispiele

Ein Gebäude kann je nach Ausfallszenario teilweise, z. B. etagenweise, wiederhergestellt werden. Der Normalbetrieb kann darüber schrittweise erreicht werden.

Für ein IT-System kann der Normalbetrieb erst erreicht werden, wenn das IT-System inklusive der Daten vollständig wiederhergestellt ist. Innerhalb des Notbetriebs wurde auf einem Ersatzsystem gearbeitet. Eine notwendige Maßnahme innerhalb der Nacharbeiten ist es, die Daten vom Ersatzsystem auf das wiederhergestellte Hauptsystem zu transferieren.

Hierzu kann eine Checkliste mit konkreten Prüfpunkten oder zu treffenden Entscheidungen für die Rückführung in den Normalbetrieb entwickelt werden. Neben den direkt ersichtlichen Aspekten, z. B. der Reihenfolge, in der die Geschäftsprozesse wieder in den Normalbetrieb zu versetzen sind, ist es hilfreich, auch die durch den Notbetrieb entstandenen Folgen zu betrachten.

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 der Nacharbeiten?*
- *Wie, durch wen und in welchen zeitlichen Intervallen werden die Mitarbeitenden 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 sowie*
  - *die erwartete Dauer bis zur Rückkehr in den Normalbetrieb.*

In den Geschäftsfortführungsplänen wird näher festgelegt, mit welchen Arbeitsrückständen aufgrund des individuell festgelegten Notbetriebs zu rechnen ist. Welche Optionen genutzt werden können, um diese abzuarbeiten, wird daher individuell in den Geschäftsfortführungsplänen geregelt (siehe 11.2 *Erstellung der GFPs (R+AS)*).

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 der Notfall zu einem spezifischen Zeitpunkt als beendet erklärt werden, um Teile der Berechtigungen der BAO aufzuheben. Dieser Zeitpunkt wird als Deeskalation 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 5.2 *Detektion, Alarmierung und Eskalation (R+AS)*). 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?
- Können die interne und externe Kommunikation wieder vollständig durch die AAO erfolgen?

5.9 Analyse der Bewältigung (R+AS)

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 kann, 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. Jeder Vorfall sollte analysiert werden. Es ist empfehlenswert, dass der oder die BCB jeden Vorfall zentral analysiert, z. B. in Form von Workshops mit den Beteiligten. Es ist empfehlenswert, eine Analyse zeitnah zum Schadensereignis sowie eine weitere Analyse mit einigem zeitlichen Abstand dazu durchzuführen. Weitere Informationen dazu können dem Kapitel Hilfsmittel *Weiterführende Aspekte 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 (insbesondere BAO-Reaktionszeit)?*
- *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 der vorbereiteten Notfallmaßnahmen wurden ergriffen?*
- *Welche Notfallmaßnahmen wurden neu eingeführt?*
- *Wie gut haben die vorbereiteten Notfallpläne funktioniert?*
- *Wurden Notfallpläne neu erstellt oder angepasst?*
- *Wie gut hat die interne NuK-Kommunikation funktioniert? (z. B. Kooperationsbereitschaft der Mitarbeitenden, Einhaltung der Schweigepflichten)*
- *Wie gut hat die externe NuK-Kommunikation funktioniert? (z. B. Effektivität des Medienmonitorings, 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 15.2 *Ableitung von Korrektur- und Verbesserungsmaßnahmen (R+AS)*).

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 und 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, z. B. Einschränkungen zur rationalen Entscheidungsfindung aufgrund einer besonderen Stresssituation (siehe auch das Hilfsmittel Weiterführende Aspekte zur Bewältigung, 2.7.4.4 Psychologische Aspekte bei der Stabsarbeit).

6 BIA-Vorfilter (R+A)

In der Initiierung des BCM hat die Institutionsleitung entschieden, welcher Geltungsbereich und welcher Zeitraum durch das BCM abgesichert werden sollen (siehe 3.3 *Geltungsbereich (R+AS)*). Zu diesem frühen Zeitpunkt konnte jedoch noch keine valide Aussage darüber getroffen werden, wie viele Geschäftsprozesse innerhalb des gewählten Geltungsbereichs liegen und daher im Rahmen einer Business-Impact-Analyse (BIA) untersucht werden müssen (siehe Kapitel 7 *Business-Impact-Analyse (R+AS)*). Da die BIA umfangreiche Analysen beinhaltet, kann eine hohe Anzahl zu berücksichtigender Geschäftsprozesse den weiteren Fortschritt im BCM deutlich verlangsamen. Dies widerspricht dem Ziel eines Reaktiv- oder Aufbau-BCMS, schnellstmöglich eine Reaktionsfähigkeit zu erlangen. Je nachdem wie viele Geschäftsprozesse im Rahmen der BIA als zeitkritisch identifiziert werden, reichen zudem die initial festgelegten Ressourcen unter Umständen nicht aus. In der Folge können nicht alle zeitkritischen Geschäftsprozesse adäquat abgesichert werden. Der BIA-Vorfilter hat daher das Ziel, mit vereinfachten Mitteln bereits vor Beginn der BIA eine Vorauswahl zu treffen und die potenziell zeitkritischsten Geschäftsprozesse einzugrenzen.

Hinweis

Auf Anhieb mag der BIA-Vorfilter 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. In diesem Standard werden folgende Ansätze vorgestellt:

- Vorauswahl von Geschäftsprozessen
  - hierarchisch anhand einer Prozesslandkarte
  - anhand einer groben Vorauswahl durch die Institutionsleitung
- Vorauswahl von Organisationseinheiten anhand eines Organigramms
- Vorauswahl von Produkten oder Services

Je nach Branche sowie institutionsspezifischer Aufbau- und Ablauforganisation eignet sich ein Ansatz besser oder schlechter für eine Institution. Daher ist es empfehlenswert, dass der oder die BCB für die eigene Institution einen geeigneten Ansatz auswählt und für die eigene Institution adaptiert. Der Ansatz für den BIA-Vorfilter sollte möglichst dazu geeignet sein, den Untersuchungsbereich der BIA auf die zeitkritischsten Geschäftsprozesse einzugrenzen.

In den Hilfsmitteln zu diesem Standard steht eine umfangreiche Umsetzungsanleitung für den Ansatz *Vorauswahl von Organisationseinheiten anhand eines Organigramms* zur

Verfügung, der bereits bei der Definition des Begriffs zeitkritisch auf die etablierten BIA-Parameter zurückgreift.

Hinweis

Die Herausforderung besteht darin, einerseits den Aufwand innerhalb der BIA zu reduzieren, indem in dem BIA-Vorfilter möglichst effizient vorgefiltert wird. Andererseits entstehen durch den BIA-Vorfilter Bereiche, die dann in der späteren Absicherung nicht mehr betrachtet werden, da für die als nicht zeitkritisch eingestuften Bereiche keine systematische Schadensbewertung im Rahmen der BIA mehr durchgeführt wird. Infolgedessen könnten zeitkritische Geschäftsprozesse unentdeckt bleiben. Die Ergebnisse des BIA-Vorfilters haben damit weitreichende Konsequenzen für alle weiteren Schritte des BCM. Entsprechend muss die Institutionsleitung in dem BIA-Vorfilter aktiv eingebunden sein, um das damit einhergehende Risiko der unberücksichtigten Bereiche tragen zu können.

Die *Abbildung* 26: *BCM-Prozessschritte des BIA-Vorfilters* verdeutlicht die empfohlenen Schritte, um einen BIA-Vorfilter durchzuführen.

Die einzelnen Schritte werden in den nachfolgenden Unterkapiteln näher erläutert. Nachdem das Ergebnis des BIA-Vorfilters durch die Institutionsleitung freigegeben wurde, kann mit der BIA anhand der getroffenen Vorauswahl begonnen werden.

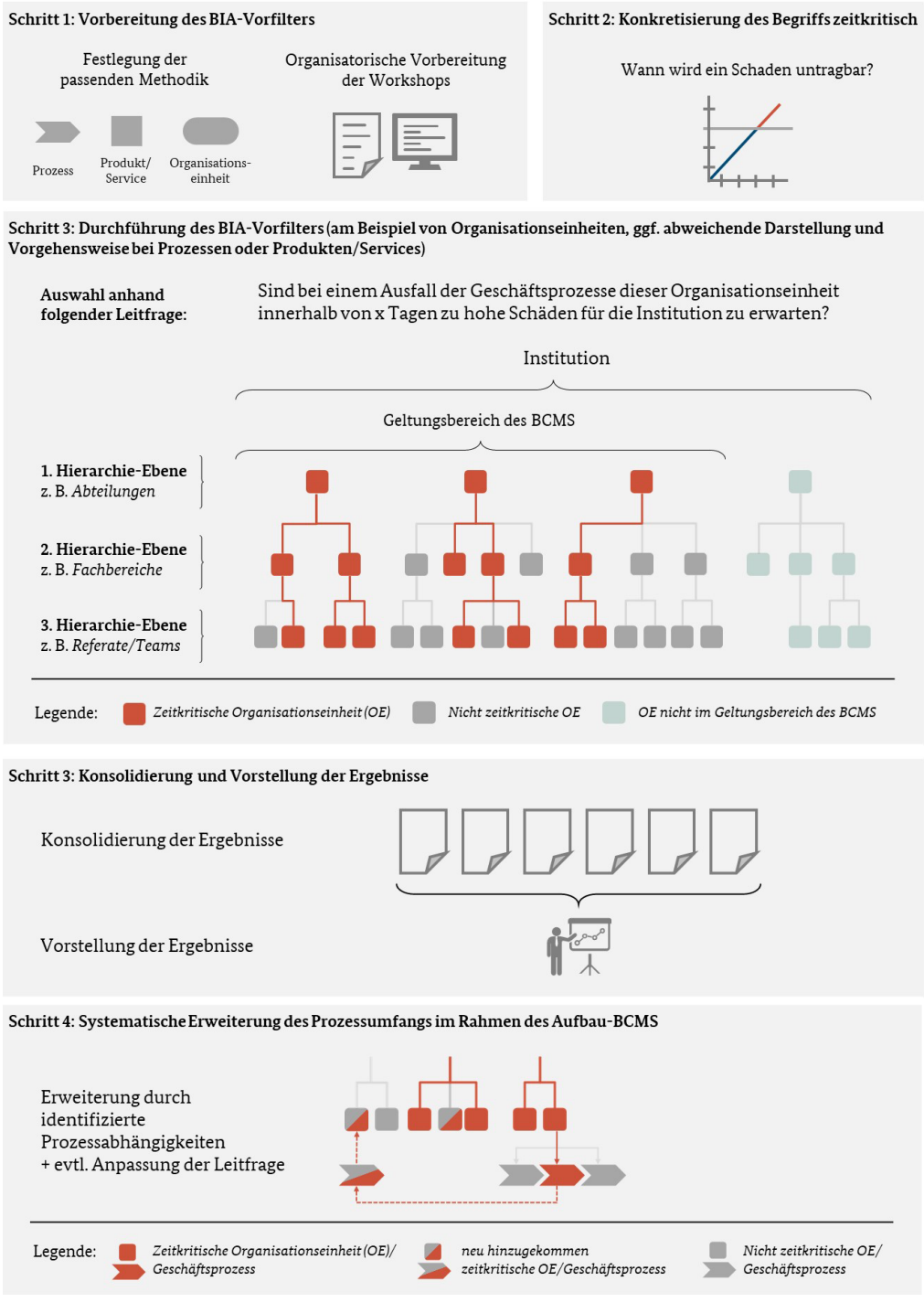

Abbildung 26: BCM-Prozessschritte des BIA-Vorfilters

6.1 Vorbereitung des BIA-Vorfilters (R+A)

Eine effektive **Vorbereitung des BIA-Vorfilters** schafft die Voraussetzungen dafür, dass

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

Ausgehend von der Situation der eigenen Institution wählt der oder die BCB eine passende Methode für den BIA-Vorfilter aus. Liegt z. B. in der Institution keine aktuelle Prozesslandkarte vor und orientiert sich der Geschäftsbetrieb auch nicht an Produkten und Services, dann wird höchstwahrscheinlich ein Ansatz anhand der Organisationseinheiten am erfolgversprechendsten sein. Demgegenüber wäre es naheliegend, den BIA-Vorfilter anhand von Produkten und Services auszurichten, wenn die Institution selbst ihren Geschäftsbetrieb bereits stark an Produkten und Services ausgerichtet hat.

Ferner sollte der BIA-Vorfilter auch organisatorisch vorbereitet werden. Eine gute Vorbereitung beschleunigt den Ablauf und reduziert die Aufwände für alle weiteren Beteiligten. Dazu wird zunächst der Begriff zeitkritisch konkretisiert.

6.2 Konkretisierung des Begriffs zeitkritisch (R+A)

Unabhängig davon, ob Organisationseinheiten, Geschäftsprozesse, Produkte oder Services in dem BIA-Vorfilter untersucht werden, muss die Frage, wann etwas als zeitkritisch gilt, einheitlich in der Institution beantwortet werden können. Daher sollte eine Leitfrage (siehe Abbildung 27) durch den oder die BCB definiert und mit der Institutionsleitung abgestimmt werden, bevor mit dem BIA-Vorfilter begonnen wird.

Beispiel

Abbildung 27: Leitfrage für einen BIA-Vorfilter anhand von Organisationseinheiten

Abbildung 27 stellt eine beispielhafte Leitfrage für eine Vorauswahl anhand von Organisationseinheiten dar. Die Leitfrage kann aber auch für eine Vorauswahl angepasst werden, die anhand von Prozessen oder Produkten oder Services getroffen wird.

Untersuchungszeitraum

Der Untersuchungszeitraum legt fest, für welche mögliche Ausfalldauer ein Schaden für die Institution bewertet werden soll. Den Untersuchungszeitraum repräsentiert die Wortgruppe ***innerhalb von 7 Tagen*** in der eingangs genannten Leitfrage. Er sollte kleiner als der abzusichernde Zeitraum des BCMS von z. B. 14-30 Tage sein gemäß 3.3 *Geltungsbereich (R+AS)*, sowie einen relativ kurzen Zeitraum umfassen, z. B. 7 Tage oder kürzer, um die Vorauswahl auf die zeitkritischsten Einheiten einzuschränken und so den Aufwand in der BIA deutlich zu reduzieren.

Grenze für das Schadenspotenzial

Um die Bewertung in dem BIA-Vorfilter einheitlich durchzuführen, ist es wichtig, mit der Institutionsleitung konkret festzulegen, was im Beispiel ein ***zu hoher Schaden*** wäre. Die so identifizierten Einheiten werden in der BIA näher untersucht, sodass für diese eine angemessene BC-Planung im weiteren PDCA-Zyklus des BCMS entwickelt wird. Um die Einheiten in dem BIA-Vorfilter zu bewerten, werden folgende Aspekte betrachtet:

1. Beeinträchtigung der persönlichen Unversehrtheit
2. Beeinträchtigung der Aufgabenerfüllung
3. Verstoß gegen Gesetze, Vorschriften und Verträge
4. negative Innen- und Außenwirkung (Imageschaden)
5. finanzielle Auswirkungen

Der oder die BCB kann hierzu auf die in der BIA näher zu definierenden Schadenskategorien zurückgreifen (siehe 7.1.2 *Festlegung der BIA-Parameter und betrachteten Zeithorizonte (R+AS)*). Das Hilfsmittel *Vorauswahl von Organisationseinheiten anhand eines Organigramms* zeigt exemplarisch, wie bereits in dem BIA-Vorfilter auf die Parameter der BIA zurückgegriffen werden kann. Dieses Vorgehen hat den Vorteil, dass sowohl in dem BIA-Vorfilter als auch in der BIA ein einheitliches, präzises Verständnis über den Begriff zeitkritisch vorliegt. Darüber hinaus ist es wichtig, dass auch bei allen weiteren an dem BIA-Vorfilter Beteiligten ein einheitliches Verständnis über den Begriff zeitkritisch vorliegt.

6.3 Durchführung des BIA-Vorfilter (R+A)

Idealerweise führt der oder die BCB den BIA-Vorfilter durch, um selbst einen Überblick zu erhalten und die Ergebnisse vergleichbar zu halten. Unabhängig davon, ob als Einheiten Geschäftsprozesse, Organisationseinheiten, Produkte oder Services untersucht werden, ist es sehr empfehlenswert, im Rahmen von Workshops zu analysieren, inwiefern die einzelnen Einheiten entsprechend der Leitfrage aus dem vorigen Kapitel 6.2 im Sinne der Institution zeitkritisch sind. So können Missverständnisse, Unklarheiten oder ein abweichendes Verständnis des Begriffes zeitkritisch direkt behandelt werden, wodurch Nacharbeiten oder Doppelarbeiten vermieden werden können.

6.3.1 Vorauswahl von Geschäftsprozessen (R+A)

Voraussetzung: Die Institution orientiert ihre Arbeitsweise bereits stark anhand von Geschäftsprozessen. Idealerweise liegt eine Prozesslandkarte vor.

Prinzipiell gibt es mehrere Möglichkeiten bei der Vorauswahl von Geschäftsprozessen. Ein relativ simpler, dafür sehr schneller Ansatz besteht darin, die Institutionsleitung grob zu befragen, z. B. mit der Frage:

> „Welche 3-5 Geschäftsprozesse bereiten Ihnen am schnellsten Probleme, falls diese ausfallen?"

Diese Vorgehensweise hat den Vorteil, dass so sehr schnell eine Auswahl vorliegt, besitzt jedoch den Nachteil, dass ein solches Vorgehen nicht dazu geeignet ist, über mehrere PDCA-Zyklen hinweg den Untersuchungsbereich der BIA systematisch zu vergrößern.

Demgegenüber ist es empfehlenswert, einzelne Prozesse systematisch über eine Prozesslandkarte herauszufiltern, falls eine solche existiert. Ausgehend von der Prozesslandkarte der Institution wird von der höchsten Ebene aus jeweils die Frage gestellt:

> „Sind bei einem Ausfall des Geschäftsprozesses innerhalb von x Tagen (z. B. 7 Tagen) zu hohe Schäden zu erwarten?"

Diese Frage sollte somit zuerst im Rahmen eines Workshops von der Institutionsleitung für alle Prozesse der obersten Ebene im Geltungsbereich des BCMS mit Unterstützung des oder der BCB beantwortet werden.

Eine solche Auswahl auf der obersten Prozessebene kann noch sehr grob sein. In diesem Fall ist es empfehlenswert, diese Fragestellung erneut für die nachfolgende Hierarchieebene zu wiederholen, deren übergeordneter Prozess zeitkritisch ist. Diese Fragestellung kann erneut entweder von der Institutionsleitung selbst im Rahmen eines Workshops geklärt werden oder mit den jeweiligen Prozessverantwortlichen.

Dieser Schritt kann prinzipiell so oft wiederholt werden, bis der BIA-Vorfilter bei einer Hierarchieebene der Geschäftsprozesse angekommen ist, auf der eine hinreichende Filterwirkung erreicht ist. Es ist empfehlenswert, in dem BIA-Vorfilter Geschäftsprozesse gebündelter auf einer abstrakteren, höheren Ebene als in der BIA zu betrachten (siehe 7.1.1 *Erhebung der Geschäftsprozesse (R+AS)*). Der oder die BCB sollte in Abstimmung mit der Institutionsleitung festlegen, wie viele Hierarchieebenen im Rahmen des BIA-Vorfilters berücksichtigt werden.

Beispiel

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

Abbildung 28: Beispiel für ein Ergebnis des BIA-Vorfilters anhand von Geschäftsprozessen

Vorteile: In dem BIA-Vorfilter ausgewählte Einheiten können sehr leicht weiter in die Untersuchungsgegenstände der BIA aufgeteilt werden, es ist kein Transfer mehr nötig. Eine sehr präzise Filterung ist möglich.

Nachteile: Bei zu detaillierter Betrachtung in dem BIA-Vorfilter wird nur eine sehr geringe Filterwirkung für die BIA erzielt, bei erheblichem Aufwand.

6.3.2 Vorauswahl von Organisationseinheiten anhand eines Organigramms (R+A)

Voraussetzung: Ein Organigramm liegt vor und die Organisation ist möglichst hierarchisch gegliedert.

Auf Basis des Organigramms der Institution wird von der höchsten Ebene aus jeweils die Frage gestellt:

„Welche der untergeordneten Organisationseinheiten ist zeitkritisch?"

Diese Frage sollte somit zuerst im Rahmen eines Workshops von der Institutionsleitung für alle hierarchisch obersten Organisationseinheiten im Geltungsbereich des BCMS mit Unterstützung des oder der BCB beantwortet werden.

Da diese Auswahl in der Regel noch sehr grob sein wird, ist es empfehlenswert, diese Fragestellung erneut für die nachfolgende Hierarchieebene zu wiederholen, deren übergeordnete Organisationseinheit zeitkritisch ist. Diese Fragestellung kann erneut von der Institutionsleitung selbst im Rahmen eines Workshops geklärt werden oder von den jeweiligen verantwortlichen Leitenden der Organisationseinheiten in Abstimmung mit ihren Vorgesetzen.

Dieser Schritt könnte so oft wiederholt werden, bis der BIA-Vorfilter bei der untersten Hierarchieebene des Organigramms angekommen ist, was jedoch den Aufwand erhöht und nicht unbedingt eine effektive weitere Einschränkung der Organisationseinheiten bedeutet. Der oder die BCB sollte in Abstimmung mit der Institutionsleitung vorab festlegen, wie viele Hierarchieebenen im Rahmen des BIA-Vorfilters berücksichtigt werden.

Das nachfolgende Beispiel zeigt einen BIA-Vorfilter über alle Hierarchieebenen für eine Organisation mit drei Hierarchieebenen:

Beispiel

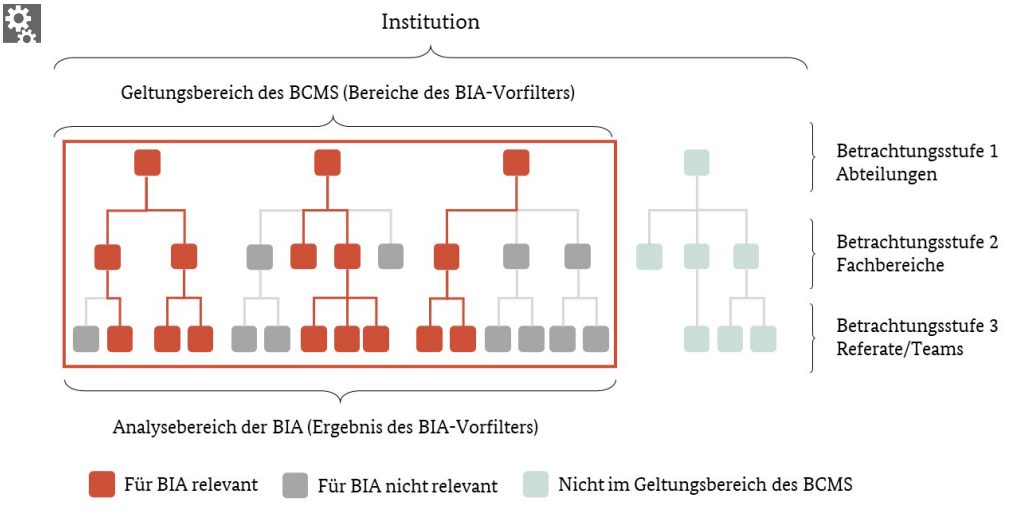

Abbildung 29: Beispiel für ein Ergebnis des BIA-Vorfilters anhand eines Organigramms

Vorteile: Diese Vorgehensweise ist nahezu universell einsetzbar, da die meisten Institutionen eine entsprechende hierarchische Organisation haben. Der Untersuchungsbereich für die BIA kann systematisch und sukzessive über mehrere PDCA-Zyklen hinweg vergrößert werden. Je mehr Betrachtungsstufen untersucht werden, umso genauer wirkt dieser Filter, sodass er gut für kleine und große Institutionen geeignet ist.

Nachteile: Je genauer zwischen Organisationseinheiten differenziert werden soll, umso mehr steigt der Aufwand. Nicht immer lassen sich zeitlich kritische Geschäftsprozesse ideal auf Organisationseinheiten abbilden.

6.3.3 Vorauswahl von Produkten oder Services (R+A)

Voraussetzung: Ein Produkt- oder Service-Katalog liegt vor.

Ausgehend von einer Übersicht aller Produkte oder Services entscheidet die Institutionsleitung in einem Workshop anhand der Frage:

„Welche Produkte und Services sind zeitkritisch?"

Beispiel

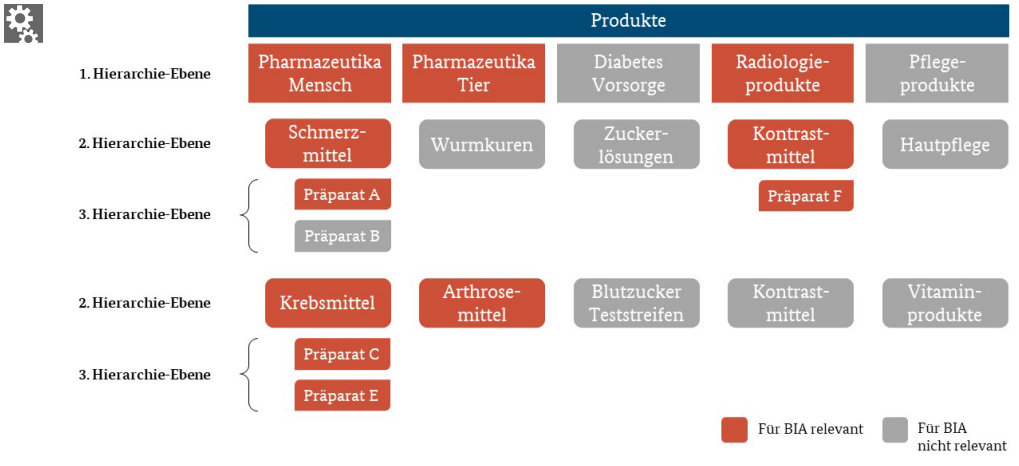

Abbildung 30: Beispiel für ein Ergebnis des BIA-Vorfilters anhand von Produkten oder Services

Vorteile: Diese Vorgehensweise ermöglicht eine sehr schnelle Entscheidung mit wenigen Workshops. Die Entscheidungsgrundlage, d. h. die Zeitkritikalität von Produkten und Services, ist aus fachlicher Sicht ideal dazu geeignet, um bei Ausfall einen möglichen Schaden z. B. im produzierenden Gewerbe und im Dienstleistungssektor zu bewerten. Die Vorauswahl enthält primär Wertschöpfungsprozesse. Management- und Supportprozesse können hierüber sehr gut herausgefiltert werden.

Nachteile: Ein zusätzlicher Aufwand ist erforderlich, um die erforderlichen Geschäftsprozesse für die ausgewählten Produkte und Services im Rahmen der BIA zu identifizieren. Dies kann insbesondere zu einer zu schwachen Filterwirkung führen, wenn unterschiedlich zeitkritische Produkte und Services durch dieselben Geschäftsprozesse erbracht werden. Management- und Supportprozesse können häufig nicht exakt einem bestimmten Produkt oder Service zugeordnet werden, sondern dienen übergreifend bzw. allgemein dem Fortbestehen der Institution.

6.4 Konsolidierung und Vorstellung der Ergebnisse (R+A)

Da in dem BIA-Vorfilter verschiedene Personen mitwirken, kann die Aussagekraft der Informationen schwanken. Dies trifft umso mehr zu, wenn der BIA-Vorfilter nicht wie

empfohlen im Rahmen von moderierten Workshops durchgeführt wird, sondern beispielsweise per Selbstauskunft der Teilnehmenden abgefragt wird. Der oder die BCB sollte daher überprüfen, ob die Ergebnisse des BIA-Vorfilters plausibel sind. Anschließend sollte der oder die BCB die als zeitkritisch ausgewählten Einheiten, d. h. Geschäftsprozesse, Organisationseinheiten oder Produkte und Services, in einer Gesamtübersicht zusammenfassen.

Es ist sinnvoll, dass der oder die BCB der Institutionsleitung die Ergebnisse des BIA-Vorfilters vorstellt. So kann sichergestellt werden, dass die Institutionsleitung darüber entscheidet, ob der Analysebereich in der BIA, abweichend vom Geltungsbereich des BCMS, anhand der Ergebnisse des BIA-Vorfilters 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, d. h. ob beispielsweise ein zu geringer oder ein sehr hoher Prozentsatz der im Geltungsbereich des BCMS liegenden Organisationseinheiten, Geschäftsprozesse oder Produkte und Services als potenziell zeitkritisch ermittelt wurde. Falls durch die Institutionsleitung entschieden wird, dass die Eingrenzung des Analysebereichs nicht angemessen ist, sollten die Parameter überarbeitet oder eine alternative Methode zur Vorauswahl gewählt und der BIA-Vorfilter wiederholt werden. Der BIA-Vorfilter ist abgeschlossen, wenn die Institutionsleitung die Ergebnisse freigegeben hat.

6.5 Systematische Erweiterung des GP-Umfangs im Rahmen des Aufbau-BCMS (A)

Grundsätzlich werden in einem Aufbau-BCMS im Rahmen der BIA auch die Geschäftsprozessabhängigkeiten der zeitkritischen Geschäftsprozesse untersucht (siehe 7.2.2 *Identifizierung der Prozessabhängigkeiten (AS)*). Hierbei kann die Situation auftreten, dass abhängige Geschäftsprozesse identifiziert werden, die selbst im Rahmen der BIA nicht als zeitkritisch eingestuft wurden oder die selbst gar nicht Teil des Untersuchungsgegenstands der BIA waren. Genau diese neu identifizierten, abhängigen zeitkritischen Geschäftsprozesse erweitern den GP-Umfang automatisch.

Falls der GP-Umfang darüber hinaus erweitert werden soll, kann der BIA-Vorfilter auch erneut als eine systematische Vorgehensweise herangezogen werden, um im Rahmen eines Aufbau-BCMS den GP-Umfang der BIA systematisch zu vergrößern, bis der gesamte Geltungsbereich erreicht ist.

Der GP-Umfang der BIA kann z. B. vergrößert werden, indem die Filterwirkung des BIA-Vorfilters reduziert wird. Dies kann sehr einfach erreicht werden, indem in der Leitfrage der Untersuchungszeitraum angepasst wird mit der Formulierung ***innerhalb von x Tagen***. Wird ein längerer Zeitraum betrachtet, werden voraussichtlich weniger Einheiten ausgefiltert werden.

Dieser Parameter kann über verschiedene PDCA-Zyklen hinweg systematisch angepasst werden, sodass nach jeder Anpassung eine angemessene Verringerung der Filterwirkung des BIA-Vorfilters zu erwarten ist. Die Einheiten, die bereits in der BIA untersucht wur-

den, müssen nicht erneut in dem BIA-Vorfilter betrachtet werden, da diese automatisch in der BIA wieder betrachtet werden. So kann der GP-Umfang systematisch erweitert werden, bis in einem finalen Schritt im Rahmen eines Standard-BCMS gänzlich auf den BIA-Vorfilter verzichtet wird.

Alternativ kann der GP-Umfang der BIA auch einfach durch eine Leitungsentscheidung erweitert werden, z. B. indem der GP-Umfang der BIA um 20 % der noch fehlenden Organisationseinheiten im nächsten PDCA-Zyklus ergänzt wird. Dieses Vorgehen hat den erheblichen Vorteil, dass es deutlich weniger Aufwand erzeugt als eine systematische Vorgehensweise anhand der Hierarchien im Rahmen des BIA-Vorfilters. In diesem Vorgehen nach Leitungsentscheidung wird jedoch nicht automatisch sichergestellt, dass die im nächsten PDCA-Zyklus zusätzlich zu untersuchenden Einheiten auch tatsächlich zeitkritische Aktivitäten und Prozesse bearbeiten.

7 Business-Impact-Analyse (R+AS)

In der BIA wird untersucht, welche Geschäftsprozesse zeitkritisch sind und ab wann deren Ausfälle nicht tolerierbare Auswirkungen haben. Daraus werden die Wiederanlaufanforderungen abgeleitet, d. h. ob und ab wann für diese Geschäftsprozesse ein Notbetrieb zur Verfügung stehen sollte und welche Ressourcen dafür benötigt werden.

Zusätzlich werden im **Standard- und Aufbau-BCMS** für zeitkritische Geschäftsprozesse die Prozessabhängigkeiten ermittelt.	**AS**

Die BIA betrachtet nur die potenziellen **Auswirkungen** eines Geschäftsprozessausfalls, nicht dessen 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 BIA und die Identifizierung zeitkritischer Geschäftsprozesse keine Rolle. Innerhalb der BIA muss vom Totalausfall des Geschäftsprozesses (Worst Case) ausgegangen werden und die in Folge zu erwartenden Schäden bewertet werden.

In einer BIA wird nicht nur bewertet, welche Auswirkungen ein Ausfall eines Geschäftsprozesses für die Institution hat, sondern auch, wie sich der potenzielle Schaden zeitlich entwickelt. Das Ergebnis der BIA zeigt, 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 BC-Planung benötigt werden. Abbildung 31 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.

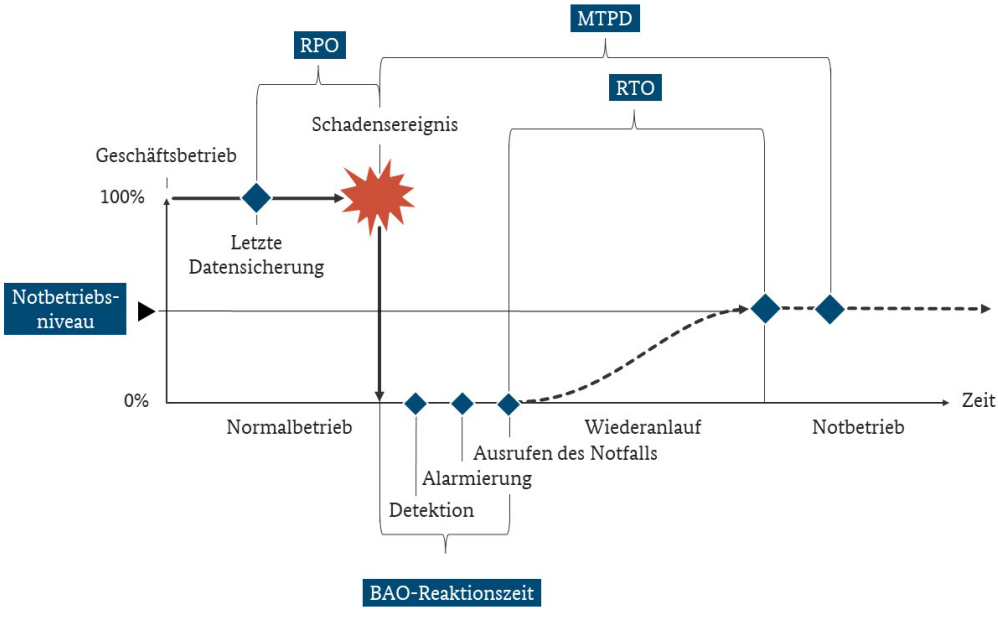

Abbildung 31: Erläuterung der Kenngrößen MTPD, RTO, RPO sowie Notbetriebsniveau

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. Die MTPD wird anhand einer Bewertung des Schadenspotenzials je Geschäftsprozess ermittelt.
2. Die **Recovery Time Objective** (**RTO**, deutsch: Geforderte Wiederanlaufzeit, WAZ) wird aus der MTPD abgeleitet und sowohl den zeitkritischen Geschäftsprozessen als auch den Ressourcen zugeordnet, die relevant sind für die Aufrechterhaltung der zeitkritischen Geschäftsprozesse. Die RTO umfasst den Zeitraum vom Ausrufen des Notfalls bis zum Zeitpunkt der geforderten Inbetriebnahme der BC-Lösung. Im Falle von IT-Ressourcen wäre das z. B. der Schwenk auf eine Ausweich- oder Ersatzressource oder das Zurücksetzen eines IT-Systems auf den letzten gesicherten Zustand. Die RTO muss zwingend kürzer sein als die MTPD des relevanten Geschäftsprozesses, denn die Reaktionszeit wird von der MTPD abgezogen, um mit der RTO die MTPD noch erreichen zu können. Zusätzlich ist es empfehlenswert, einen weiteren zeitlichen Puffer einzuplanen, da insbesondere die Detektion mit Unsicherheiten hinsichtlich des genauen zeitlichen Ablaufs einhergeht.
3. Die **Recovery Point Objective** (**RPO**, deutsch: maximal zulässiger Datenverlust) legt fest, welcher Datenverlust akzeptiert wird, d. h. wie alt verfügbare Daten maximal sein dürfen, um im Notbetrieb sinnvoll damit arbeiten zu können. Diese Kenngröße dient auch dazu, um den notwendigen Datensicherungszyklus daraus abzuleiten. (Theoretisch kann die RPO auch für analoge Informationen erhoben werden. Da die-

se analogen Informationen in der Praxis aber nicht in sinnvoller Art und Weise versioniert werden können, ist es in der Regel zielführender, benötigte analoge Informationen allein über die Ressourcenkategorie *Informationen* zu erheben, ohne RPO zu erheben und immer vom aktuellen Stand auszugehen.)

4. Das **Notbetriebsniveau** (englisch: Minimum Business Continuity Objective oder **MBCO**) 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 können Aktivitäten priorisiert werden. In Abbildung 31 wird das Notbetriebsniveau nur schematisch dargestellt.

Die Vorgehensweise und Methodik sowie die benötigten Rollen und Hilfsmittel der BIA sollten im **Standard**- und **Aufbau-BCMS** schriftlich dokumentiert werden, um nachvollziehbare Ergebnisse mit einer angemessenen Qualität zu erhalten. Hierzu kann auf die erläuternden Texte aus diesem Kapitel zurückgegriffen werden.	**AS**

Um eine BIA durchzuführen, kann die Dokumentvorlage *BIA-Auswertungsbogen* aus den Hilfsmitteln verwendet werden. Anhand dieser Dokumentvorlage werden einige der nachfolgend aufgeführten Beispiele und Hinweise dargestellt.

Die nachfolgenden Unterkapitel beschreiben die empfohlene Vorgehensweise, mittels derer die BIA vorbereitet, durchgeführt und ausgewertet werden kann. In Abbildung 32 sind die hierfür erforderlichen Schritte in einer Übersicht dargestellt.

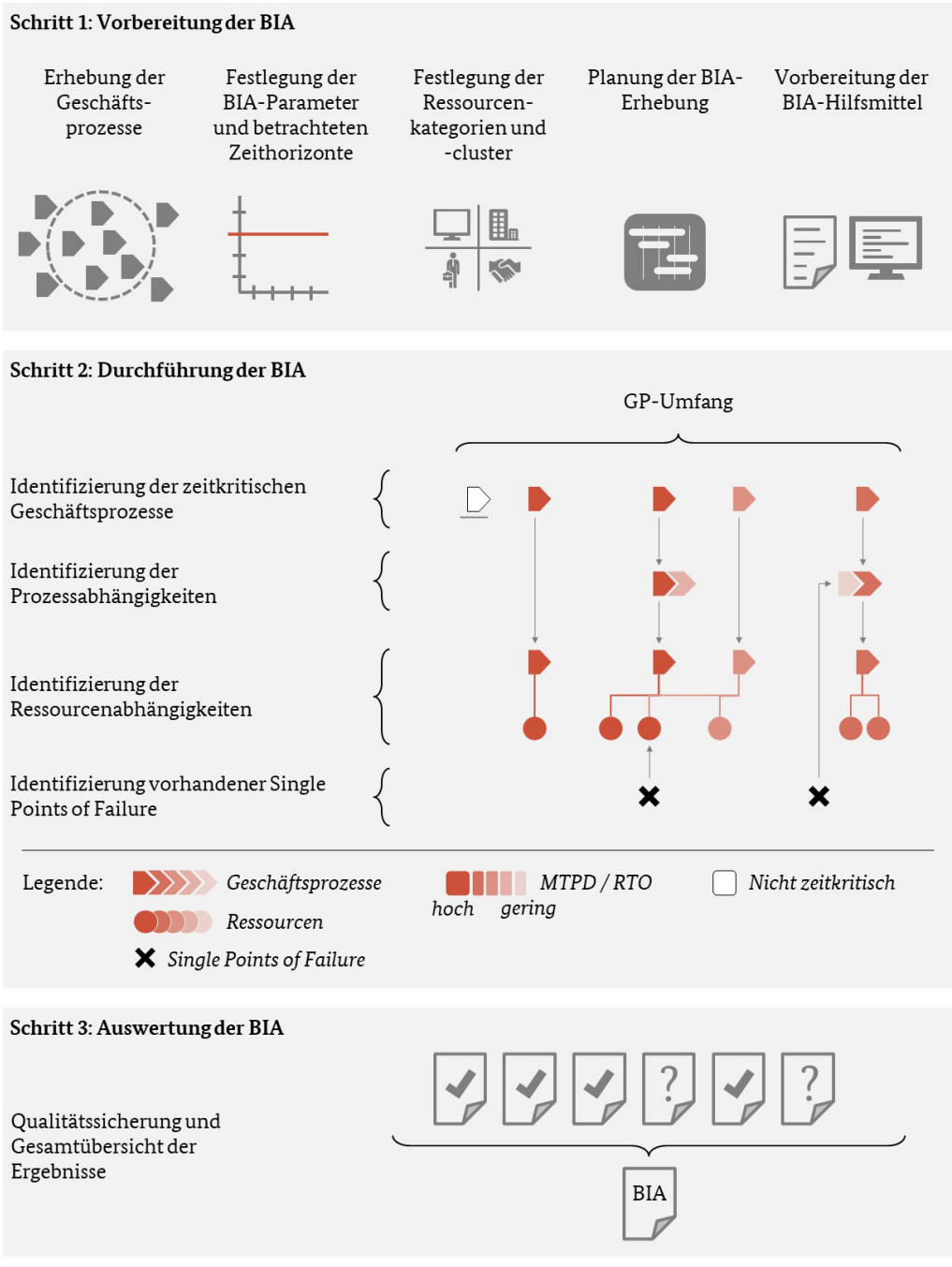

Abbildung 32: BCM-Prozessschritte der Business-Impact-Analyse

7.1 Vorbereitung der BIA (R+AS)

Die Vorgehensweise und Methodik der BIA sollte einheitlich sein. Daher ist es empfehlenswert, dass der oder die BCB die Methodik und Vorgehensweise festlegt und die BIA organisatorisch vorbereit, denn der oder die BCB verfügt über das notwendige Fachwissen und steuert den BCM-Prozess zeitlich. Vorbereitende Tätigkeiten können ganz oder teilweise an weitere Rollen im BCM delegiert werden. Die Aufgaben in der Vorbereitung der BIA werden in den nachfolgenden Unterkapiteln näher erläutert. Die Unterkapitel folgen einer logischen Reihenfolge, jedoch können sich verschiedene beschriebene Aufgaben in der Praxis zeitlich überlagern.

7.1.1 Erhebung der Geschäftsprozesse (R+AS)

Innerhalb des aktuellen GP-Umfangs 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, ob sie vollständig den aktuellen GP-Umfang 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 Reaktiv- und Aufbau-BCMS als auch das Standard-BCMS in diesem Kapitel abgebildet werden, wird hier allgemein vom GP-Umfang gesprochen. Für ein Standard-BCMS entspricht der aktuelle GP-Umfang dem Geltungsbereich des BCMS. Im Reaktiv- und Aufbau-BCMS kann der GP-Umfang anhand des BIA-Vorfilters festgelegt werden.

Liegt keine aktuelle Übersicht der Geschäftsprozesse und ihrer Abhängigkeiten vor, so muss diese im Rahmen der BIA erhoben oder aktualisiert werden. Eine solche Übersicht zu erstellen ist jedoch keine originäre Aufgabe des BCM, sondern das BCM erhebt diese Übersicht nur, soweit die Inhalte für den Notbetrieb relevant sind. Hierzu können Geschäftsverteilungspläne, Aufgabenbeschreibungen oder andere organisationsbeschreibende Dokumente der Institution zu Hilfe genommen werden. Zudem ist es empfehlenswert, die BIA an den Organisationseinheiten auszurichten, die für den GP-Umfang relevant sind. So kann auf Kontaktpersonen zurückgegriffen werden.

Während bei einer Organisationsanalyse häufig eine sehr große Anzahl an Informationen erhoben wird, 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 Bewertung des Schadenspotenzials hilfreich sein.

Synergiepotenzial

Liegt ein ISMS nach BSI-Standard 200-2 oder nach ISO-Norm 27001 vor, können die dort identifizierten Geschäftsprozesse als Grundlage verwendet werden.

*Das **Verzeichnis von Verarbeitungstätigkeiten** für den Datenschutz kann möglicherweise ebenfalls als Grundlage genutzt werden. Es fasst alle Verfahrenstätigkeiten zusammen, in denen personenbezogene Daten verarbeitet werden. Verfahrenstätigkeiten können gegebenenfalls auch als Geschäftsprozesse verstanden werden oder diese können daraus abgeleitet werden.*

Wird auf vorhandene Prozessübersichten zurückgegriffen, so sollte sichergestellt sein, dass alle Geschäftsprozesse im GP-Umfang in den Übersichten dokumentiert sind.

Je nach Größe und Komplexität der Institution kann es unterschiedliche Detailebenen der Geschäftsprozesse geben. Bevor die BIA durchgeführt wird, ist es empfehlenswert, festzulegen, auf welcher Abstraktionsebene der Geschäftsprozesse die BIA durchgeführt werden soll. Dies dient zum einen 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 der Geschäftsprozesse. Zum anderen kann über die Abstraktionsebene gesteuert werden, wie detailliert die Bewertung des Schadenspotenzials erfolgen soll.

Es ist weder empfehlenswert, Geschäftsprozesse zu stark zusammenzufassen, z. B. auf der Ebene von Produkten, noch Geschäftsprozesse zu detailliert in der BIA zu betrachten (z. B. auf Aktivitätenebene). Es ist empfehlenswert, den Detailgrad der Geschäftsprozesse an den Strukturen der eigenen Institution auszurichten. 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. Der optimale Mittelweg wird beschritten, wenn die Planung des Notbetriebs und die Erstellung von geeigneten Geschäftsfortführungsplänen mit den Ergebnissen der BIA ausreichend gut möglich sind.

Synergiepotenzial

Häufig ist es sinnvoll, denselben Detailierungsgrad der Geschäftsprozesse aus dem ISMS oder dem Datenschutz auch für die BIA zu wählen.

Eine Bewertung des Schadenspotenzials der in Abbildung 33 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

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

Abbildung 33: Beispiele hierarchisch angeordneter Geschäftsprozesse

Die BIA sollte alle Hierarchieebenen der Organisationseinheiten berücksichtigen, nicht nur die unterste Ebene. Nur so kann sichergestellt werden, dass anhand der jeweiligen Kontaktpersonen eine Aussage zu allen Geschäftsprozessen möglich wird.

Beispiel

Für die Geschäftsprozesse IT-Strategie und IT-Ressourcenmanagement ist die Organisationseinheit IT-Abteilung zuständig. Der Unterstützungsprozess IT Incident Management wird hingegen durch eine untergeordnete Organisationseinheit IT-Betrieb durchgeführt. Um alle Geschäftsprozesse in der BIA zu berücksichtigen, ist es empfehlenswert, die BIA mit je einer Kontaktperson sowohl aus der übergeordneten als auch aus der untergeordneten Organisationseinheit durchzuführen oder diese beiden Personen gemeinsam in einem Termin zu befragen.

7.1.2 Festlegung der BIA-Parameter und betrachteten Zeithorizonte (R+AS)

Ziel der BIA ist es, einheitlich festzustellen, ob ein Geschäftsprozess zeitkritisch ist und wie lange dieser ausfallen darf, bevor nicht mehr tolerierbare Schäden entstehen. In der BIA wird betrachtet, welche Schäden durch den ausgefallenen Geschäftsprozess über einen definierten Zeitverlauf entstehen. Dafür müssen sogenannte Zeithorizonte festgelegt werden. Die BIA stellt zur Bewertung des Schadenspotenzials die folgende Leitfrage:

> „Wenn ein Geschäftsprozess ausfällt, mit welchem Schadenspotenzial ist im jeweiligen Zeithorizont zu rechnen?"

Um die Bewertung des Schadenspotenzials 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 sollte ein Untragbarkeitsniveau anhand der definierten Parameter festgelegt werden, um festzustellen, zu welchem Zeitpunkt ein Ausfall eines Geschäftsprozesses aufgrund der Höhe seines Schadenspotenzials nicht länger akzeptiert werden kann.

Die nachfolgende Abbildung 34 stellt beispielhaft die **Bewertung des Schadenspotenzials** für einen Geschäftsprozess grafisch dar und fasst die relevanten BIA-Parameter zusammen:

Beispiel

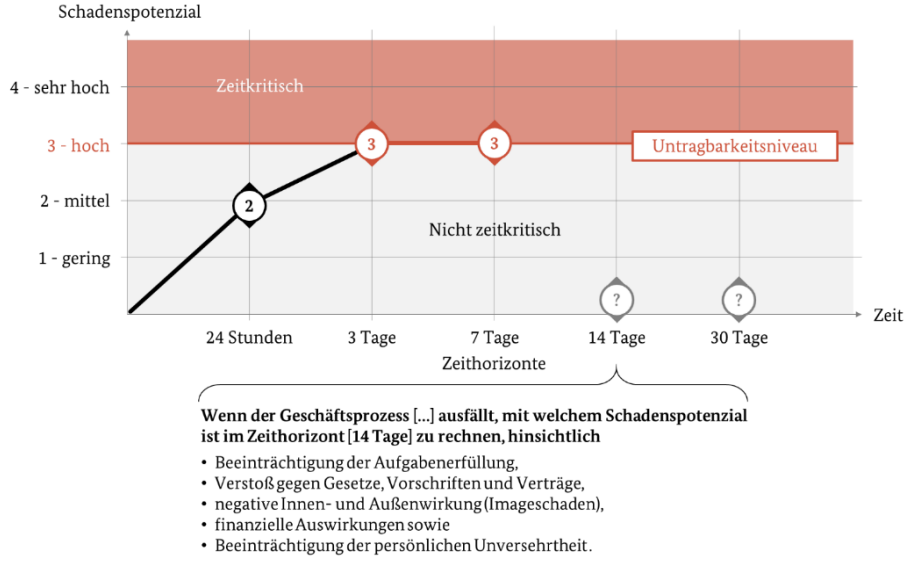

Abbildung 34: Beispiel einer Bewertung des Schadenspotenzials je Zeithorizont

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 der größten erreichten Schadenskategorie 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 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

Die Anzahl und Unterteilung der Zeithorizonte müssen nachvollziehbar gewählt werden und sich an den Gegebenheiten der Institution ausrichten. Deswegen ist es empfehlenswert, Zeithorizonte festzulegen, 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, Prozesse durchgeführt oder Services bereitgestellt werden,*
- *die Erwartungshaltung an Ausfallzeiten (unter anderem von Interessengruppen),*
- *interne Vorgaben und Geschäftsziele,*
- *branchenübliche Standards,*
- *gesetzliche Vorgaben sowie*
- *die Risikobereitschaft 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 festgelegt wurde (siehe 3.2.3 *Abzusichernder Zeitraum durch ein BCMS (R+AS)*).

Beispiel

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

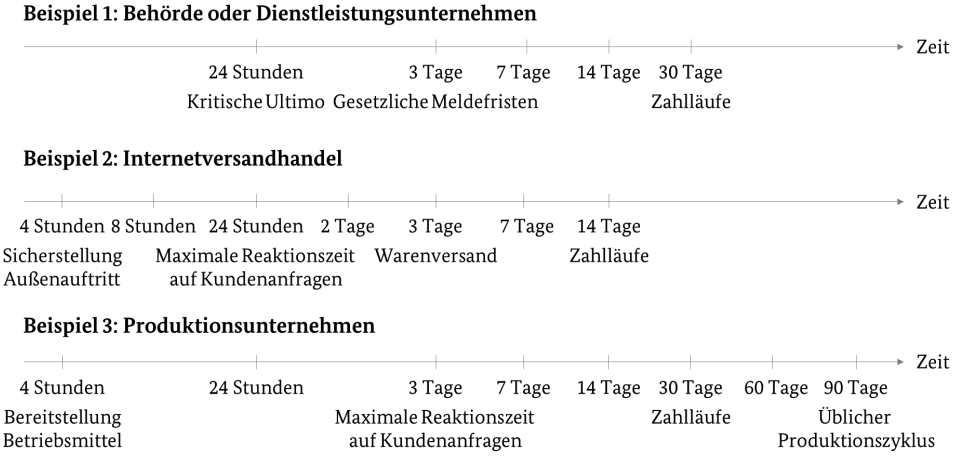

Abbildung 35: Beispiele für Zeithorizonte

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 mindestens die folgenden Schadensszenarien berücksichtigt werden:

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

Die beiden Begriffe Ausfall- und Schadensszenarien werden in der Praxis leicht verwechselt. Der BSI-Standard 200-4 unterscheidet die beiden Begriffe jedoch eindeutig hinsichtlich ihrer Bedeutung:

- Mit **Schadensszenarien** sind verschiedene Auswirkungskategorien der Unterbrechung eines Geschäftsprozesses gemeint.
- Unter **Ausfallszenarien** werden die möglichen Ausfälle der Ressourcen verstanden (z. B. Ausfall des Gebäudes, von Personal, von Dienstleistungsunternehmen oder IT).

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 haben diese finanziellen Schäden für Behörden keine existenzbedrohenden oder nicht tolerierbaren Auswirkungen. Um mögliche Ausnahmefälle zu identifizieren, wird empfohlen, die finanziellen Auswirkungen in der Bewertung des Schadenspotenzials dennoch mit zu berücksichtigen und unter Umständen als nicht relevant zu markieren.

Schadenskategorien

Die festgelegten Schadensszenarien erlauben noch keine Bewertung des Schadenspotenzials, da hierbei für Anwendende nicht klar ersichtlich ist, wonach sie den potenziellen Schaden bewerten sollen. Zu diesem Zweck muss für alle Schadensszenarien das Schadenspotenzial anhand verschiedener Schadenskategorien definiert werden. Die Anzahl an Schadenskategorien sollte 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 16 erläutert beispielhaft, wie die Schadenskategorien je Schadensszenario konkretisiert werden können. Die Definitionen sollten individuell für die Institution angepasst werden. Die angepasste Tabelle 16 kann gleichzeitig als Hilfsmittel eingesetzt werden, um bei der Durchführung der BIA die Bewertung des Schadenspotenzials zu unterstützen.

Es bietet sich an, wie in der Tabelle 16 aufgezeigt, die Bewertung des Schadenspotenzials 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 7.2.1 *Identifizierung zeitkritischer Geschäftsprozesse (R+AS)*).

Beispiel

Schadenskategorie	*Erläuterung je Schadensszenario*
1 (Gering)	• ***Allgemeine Beschreibung:*** *Ausfall hat geringe, kaum spürbare Auswirkungen.* • ***Beeinträchtigung der persönlichen Unversehrtheit:*** *Eine Beeinträchtigung ist ausgeschlossen.* • ***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.*
2 (Mittel)	***Allgemeine Beschreibung:*** *Ausfall hat spürbare Auswirkungen.* • ***Beeinträchtigung der persönlichen Unversehrtheit:*** *Eine Beeinträchtigung ist unwahrscheinlich.* • ***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.*
3 (Hoch)	***Allgemeine Beschreibung:*** *Ausfall hat nicht tolerierbare Auswirkungen.* • ***Beeinträchtigung der persönlichen Unversehrtheit:*** *Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden.* • ***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.*

4 (Sehr hoch)	***Allgemeine Beschreibung:*** *Ausfall führt zu existentiell bedrohlichen Auswirkungen.* • ***Beeinträchtigung der persönlichen Unversehrtheit:*** *Es besteht akut Gefahr für Leib und Leben oder gravierende Beeinträchtigungen der persönlichen Unversehrtheit.* • ***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.*

Tabelle 16: 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 34). Die Entscheidung darüber, ab welcher Höhe Schäden nicht länger toleriert werden, sollte aufgrund der Tragweite für die weitere BC-Planung 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.

7.1.3 Festlegung der Ressourcenkategorien und -cluster (R+AS)

Innerhalb der BIA müssen die Ressourcenabhängigkeiten der zeitkritischen Geschäftsprozesse erhoben werden (siehe 7.2.3 *Identifizierung der Ressourcenabhängigkeiten (R+AS)*), denn der Ausfall eines Geschäftsprozesses kann üblicherweise auf den Ausfall einer notwendigen Ressource zurückgeführt werden. 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 sollten für alle definierten Ressourcenkategorien die dazugehörigen Ressourcen der Institution festgelegt 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 werden, sodass nach der BIA unmittelbar mit dem Soll-Ist-Vergleich begonnen werden kann (siehe Kapitel 8 *Soll-Ist-Vergleich (R+AS)*).

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 17 beschriebenen Ressourcenkategorien berücksichtigt werden:

- IT
- Personal
- Infrastruktur
- Dienstleistungen (Services und Lieferungen)

Für das produzierende Gewerbe sollten zusätzlich die folgenden in Tabelle 17 beschriebenen Ressourcenkategorien verwendet werden:

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

Es ist empfehlenswert, die Anzahl und Beschreibung der Ressourcenkategorien an die Bedürfnisse der Institution anzupassen.

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 Mitarbeitende benötigt, die Entscheidungen treffen, Aufgaben ausführen, Maschinen bedienen oder sonstige Arbeitsschritte durchführen. Die jeweiligen Aufgaben und Pflichten werden in Form von Rollen und Funktionen definiert. Ferner sind an Rollen Berechtigungen für Zugang, Zutritt und Zugriff sowie Stellvertretungsregelungen geknüpft.*
Dienstleistungen (Services und Zuliefernde)	*Unter dem Begriff Dienstleistungen werden alle intern und extern bezogenen Leistungen zusammengefasst, die einen Input liefern oder benötigte Ressourcen (z. B. Betriebsmittel) für einen Geschäftsprozess bereitstellen.*
Informationen	*Für gewöhnlich werden aus Sicht von Endanwendenden 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.* *Achtung: Informationen, die in den Köpfen der Mitarbeitenden 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 und Kommunikationsverbindungen (z. B. 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 (z. B. PKW, LKW, Zug, Flugzeug, Schiff). Auch spezielle Bürogeräte können unter dieser Kategorie zusammengefasst werden.*
Betriebsmittel (Sonstige)	*Unter Betriebsmitteln sind alle weiteren Ressourcen zu verstehen, die in keiner vorherigen Ressourcenkategorie erfasst wurden. Diese können auch Rohstoffe für eine Produktion oder Kleinmaterial umfassen (z. B. Büromaterial, Büroausstattung, Zugangstoken).*

Tabelle 17: Beispiele verschiedener Ressourcenkategorien

Ressourcencluster

Innerhalb bestimmter Ressourcenkategorien, z. B. der IT, können mitunter sehr viele einzelne Ressourcen vorhanden sein, die für die BIA relevant sind. Wenn alle Ressourcen einzeln erfasst werden, besteht jedoch die Gefahr, dass diese aufgrund der Menge und der Komplexität nicht handhabbar sind. Es ist daher sinnvoll, Ressourcen sinnvoll zu Clustern zusammenzufassen. 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 Standardarbeitsplatz 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 einem Telefon. Der Standardarbeitsplatz wird mit den Medien Strom und Internet versorgt. Auf dem PC sind die gängigen Anwendungen der Institution installiert, z. B. E-Mail und Textverarbeitung, wie mit der IT-Abteilung abgestimmt. Weitere Ausstattung muss rollen- oder funktionsspezifisch definiert werden.*

*In einer Bank wird ein **Handelsarbeitsplatz** definiert, der zusätzlich zu einem Standardarbeitsplatz 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 Standardarbeitsplatz 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.*

Cluster dienen nicht nur dazu, Ressourcen unterschiedlicher Ressourcenkategorien zu bündeln, sondern können auch genutzt werden, um eine Vielzahl an Ressourcen mit gleichen Eigenschaften innerhalb einer Ressourcenkategorie zu bündeln. Z. B. können unterschiedliche Postdienstleistungsunternehmen in einem Ressourcencluster abgebildet werden, anstatt alle Dienstleistungsunternehmen einzeln zu erfassen.

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 vo-*

raussichtlich 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.*
- *Aufgrund 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.*

7.1.4 Planung der BIA-Erhebung (R+AS)

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 Prozesseigentümer oder die -eigentümerin anhand eines papierbasierten, elektronischen oder toolgestützten Fragebogens,
- Einzelinterviews mit verschiedenen Personen (z. B. Leitenden der Organisationseinheiten, Prozesszuständigen oder sonstigen Prozessfachleuten, die Auskunft geben können) oder
- Workshops, mit mehreren Personen.

Wird die BIA zum ersten Mal durchgeführt, ist es empfehlenswert, diese anhand von Workshops durchzuführen. Der Workshop bietet verschiedene Vorteile gegenüber Formaten, in denen die Kontaktpersonen die Informationen selbstständig erheben, z. B. folgende:

- 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.
- Der Workshop lässt Raum für Fragen und gestattet, mögliche Unsicherheiten und Bedenken der Teilnehmenden auszuräumen.
- Es kann sichergestellt werden, dass die Ergebnisse anhand der Dokumentvorlage BIA einheitlich erhoben werden.

- Fehlerhafte oder fehlende Angaben 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 Prozesszuständigen teil sowie eventuell weitere Prozessfachleute, die den Geschäftsprozess im Detail kennen. Die Anzahl der BIA-Workshops kann sich an der Anzahl zu berücksichtigender Geschäftsprozesse ausrichten.

Wurde die BIA bereits häufiger durchgeführt oder sind die Kontaktpersonen mit der BIA-Methodik vertraut, können diese Kontaktpersonen die BIA auch selbstständig durchführen. Der oder die BCB oder die BCKs können in diesem Fall für Rückfragen zur Verfügung stehen. Dann ist es empfehlenswert, dass der oder die BCB oder die BCKs die BIA zwecks Qualitätssicherung auswerten (siehe 7.3 *Auswertung (R+AS)*).

Darüber hinaus ist es empfehlenswert, den maximal erwünschten Gesamtzeitraum der BIA inklusive Nachbereitung und Auswertung festzulegen, damit die personellen und zeitlichen Ressourcen darauf ausgerichtet werden können (siehe 4.5 *Ressourcenplanung (R+AS)*).

7.1.5 Vorbereitung der BIA-Hilfsmittel (R+AS)

Es muss sichergestellt werden, dass die Ergebnisse des BIA-Durchlaufs einheitlich und nachvollziehbar dokumentiert werden. Hierzu sollten Hilfsmittel vorbereitet werden, die den Kontaktpersonen die Bewertung des Schadenspotenzials vereinfachen. Insbesondere ist es empfehlenswert, eine Übersicht aus Schadensszenarien und Schadenskategorien zur Verfügung zu stellen (siehe Tabelle 16*: Beispiele von Schadenskategorien und Erläuterung je Schadensszenario*).

Präsentation zur Erläuterung der BIA

Mit der Präsentation zur Erläuterung der BIA können die Kontaktpersonen thematisch auf die Bewertung des Schadenspotenzials vorbereitet werden. Dazu ist es empfehlenswert, das Ziel der BIA und die Vorgehensweise zur Bewertung des Schadenspotenzials vorzustellen (siehe Abbildung 34). 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 *BIA-Vorfilter/BIA* aus den Hilfsmitteln verwendet werden.

Liste der Geschäftsprozesse

Als Ergebnis der Identifizierung der Geschäftsprozesse (siehe 7.1.1 *Erhebung der Geschäftsprozesse (R+AS)*) liegt eine Liste aller Geschäftsprozesse innerhalb des aktuellen GP-Umfangs vor. Da alle Geschäftsprozesse anhand dieser Liste in der BIA untersucht werden, 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 Dokumentvorlage 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 eigene Methoden und Vorgehensmodelle zur Business-Impact-Analyse vor, an denen sich die Benutzenden orientieren können. Bei der Auswahl eines Software-Tools ist es empfehlenswert, neben dem Preis und den Leistungsmerkmalen, darauf zu achten, 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 Kontaktpersonen, die BIA durchzuführen und Fehleingaben zu vermeiden. Ferner müssen die Daten in der Auswertung nicht mehr auf Dubletten oder Schreibfehler untersucht werden. Die Dokumentvorlage *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 bereits Hilfsmittel erstellt worden sein, die für die BIA adaptiert werden können. Werden in der BIA und Schutzbedarfsfeststellung 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 im ISMS und der Kontinuität im BCM leichter identifiziert werden können.

Ferner können aus der Strukturanalyse mögliche Zuordnungen zwischen Geschäftsprozessen und Ressourcen übernommen werden. Jedoch kann eine solche gemeinsame Erhebung der Schutzbedarfsfeststellung und BIA nicht in allen Fällen vorteilhaft sein, da gerade die Schutzbedarfsfeststellung aus Effizienzgründen sehr häufig zu Maximalgruppierungen neigt, die durchaus erheblich von der Clusterbildung in der BIA und den Anforderungen für den Notbetrieb abweichen kann. Ferner betrachtet die Schutzbedarfsfeststellung alle Ressourcen für den Normalbetrieb, während die BIA die Ressourcen für den Notbetrieb betrachtet. Auch dies kann zu erheblich abweichenden Ergebnissen beziehungsweise Fragestellungen und damit verbundenen Analyseergebnissen führen.

Übersicht zu Schadenskategorien und Schadensszenarien

Um eine vergleichbare Bewertung des Schadenspotenzials zu erhalten, ist es empfehlenswert, die Schadensszenarien und Ausprägungen je Schadenskategorie den Kontaktpersonen vorzulegen. Wie in Tabelle 16 dargestellt, sollte den Kontaktpersonen ein entsprechendes Hilfsmittel schriftlich zur Verfügung gestellt werden, z. B. in Form einer BIA-Anweisung oder einer Präsentation.

7.2 Durchführung der BIA (R+AS)

Sind die notwendigen Vorbereitungen abgeschlossen, kann mit der BIA begonnen werden. Abhängig von der organisatorischen Planung erfolgt die Durchführung der BIA entweder in Form von Workshops oder eigenständig durch die zuständigen Kontaktpersonen.

7.2.1 Identifizierung zeitkritischer Geschäftsprozesse (R+AS)

In der Identifizierung zeitkritischer Geschäftsprozesse wird der potenzielle Schaden für die Institution untersucht, den der Ausfall von Geschäftsprozessen verursachen könnte. Daraus wird anhand der eingeführten Parameter abgeleitet, wie zeitkritisch die Geschäftsprozesse sind.

Bewertung des Schadenspotenzials von Geschäftsprozessen

Das Schadenspotenzial jedes Geschäftsprozesses im GP-Umfang muss anhand der definierten Schadensszenarien und Schadenskategorien über verschiedene Zeithorizonte hinweg bewertet werden. Dies sollte von den Kontaktpersonen für die Geschäftsprozesse, d. h. von Prozesszuständigen oder Prozessfachleuten durchgeführt werden, da diese den Prozess am besten bewerten können und auch die nötige Information bezüglich eines Notbetriebs kennen. Je nach Bedarf können weitere Wissenstragende hinzugezogen werden, um das finanzielle Schadenspotenzial zu bewerten, z. B. das Controlling. Für die Bewertung kann auf die Leitfrage der BIA zurückgegriffen werden, die z. B. in der Workshop-Präsentation oder in der BIA-Anweisung dokumentiert wurde (siehe 7.1.5 *Vorbereitung der BIA-Hilfsmittel (R+AS)*).

Tabelle 18 zeigt beispielhaft eine Bewertung des Schadenspotenzials für einen Geschäftsprozess anhand der verschiedenen Schadensszenarien. Hierzu werden die BIA-Parameter zugrunde gelegt, die in der Vorbereitung der BIA im Kapitel 7.1.2 *Festlegung der BIA-Parameter und betrachteten Zeithorizonte (R+AS)* erläutert wurden.

Beispiel: Bewertung des Schadenspotenzials des Geschäftsprozesses „Kundschaftsanfragen bearbeiten" anhand verschiedener Schadensszenarien

Leitfrage: *Wenn der Geschäftsprozess „Kundschaftsanfragen bearbeiten" 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 18: Beispiel einer Bewertung des Schadenspotenzials anhand der verschiedenen Schadensszenarien

Es gibt unterschiedliche Möglichkeiten aus dieser Bewertung die MTPD abzuleiten. In diesem Standard wird nur die einfachste Variante beschrieben und schon bei der Schadensbewertung vereinfacht. Dazu ist es nicht notwendig, die Einzelbewertungen je Schadensszenario in jedem Fall gesondert zu dokumentieren, 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 dieses die Worst-Case-Betrachtung erleichtert (siehe Tabelle 16). Tabelle 19 greift das Beispiel von Tabelle 18 auf, reduziert jedoch die Bewertung des Schadenspotenzials auf eine Worst-Case-Sicht, die alle Schadensszenarien beinhaltet. Neben dem Vorteil, dass die Bewertung des Schadenspotenzials beschleunigt wird, ermöglicht diese Sicht einen besseren Gesamtüberblick über die Geschäftsprozesse und deren Schadenspotenzial.

Beispiel: Worst-Case-Bewertung des Schadenspotenzials des Geschäftsprozesses „Kundschaftsanfragen bearbeiten"

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***
Kundschaftsanfragen bearbeiten	*2 (mittel)*	*3 (hoch)*	*4 (sehr hoch)*	*4 (sehr hoch)*	*4 (sehr hoch)*

Tabelle 19: Beispielhafte Bewertung des Schadenspotenzials nach dem Worst-Case-Prinzip

Hinweis

Mitunter kann ein ausgefallener Geschäftsprozess zu bestimmten Ereignissen und Terminen zu höheren Schäden als gewöhnlich führen. Dies kann etwa im Rahmen des Endjahresgeschäftes, von Rechnungsabschlüssen oder von Vergleichbarem der Fall sein. Um diesen Umstand in der weiteren BC-Planung zu berücksichtigen, können die Geschäftsprozesse grundsätzlich unter der Prämisse bewertet werden, dass diese zum ungünstigsten Zeitpunkt (engl. Worst Case) im Jahr ausfallen. Grundsätzlich ist es auch möglich, die Zeiträume getrennt zu betrachten und in der weiteren BC-Planung auch getrennt zu behandeln. Erfahrungsgemäß führt dies jedoch zu einer hohen Komplexität und damit verbunden zu 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.

In der Bewertung des Schadenspotenzials muss berücksichtigt werden, dass ein einmal eingetretener Schaden nur gleichbleiben oder weiter steigen, nicht jedoch im Laufe der Zeit wieder abnehmen kann. Tabelle 20 zeigt hierzu beispielhaft ein korrektes Ergebnis („Geschäftsprozess RICHTIG") und ein fehlerhaftes Ergebnis („Geschäftsprozess FALSCH"). Die fehlerhafte Angabe ist 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 20: Beispiel einer korrekten und fehlerhaften Bewertung des Schadenspotenzials

Festlegung der MTPD

Um die MTPD eines Geschäftsprozesses zu bestimmen, sollte der kleinste Zeithorizont gewählt werden, bei dem das Untragbarkeitsniveau erreicht wird, da hier der Zeitraum erreicht wird, zu dem der Ausfall nicht mehr toleriert werden kann. Bei dem Worst-Case-Ansatz genügt es hierbei, wenn bei einem Schadensszenario das Untragbarkeitsniveau überschritten wird. Dem gegenüber gibt es andere Ansätze, wie z. B. die gewichtete Summe, wo jedes Schadensszenario eine Gewichtung erhält und über alle Schadensszenarien hinweg die Bewertung mit der Gewichtung multipliziert und das Ergebnis aller Schadensszenarien summiert wird. Hier wird das Untragbarkeitsniveau mit dieser Summe verglichen.

Tabelle 21 zeigt einige Beispiele, wie die MTPD anhand des Schadenspotenzials festgelegt wird. Die relevanten Zeithorizonte, zu denen das Untragbarkeitsniveau erreicht wird, sind hervorgehoben. Der daraus jeweils kleinste Zeithorizont liefert die MTPD (umrandet). Für die nachfolgenden Beispiele wird die Schadenskategorie 3 (hoch) als Untragbarkeitsniveau zugrunde gelegt. Das erste Beispiel in Tabelle 21 (Geschäftsprozess Kundschaftsanfragen bearbeiten) greift das Geschäftsprozessbeispiel aus der Abbildung 33 und Tabelle 19 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*
Kundschaftsanfragen bearbeiten	*2 (mittel)*	*3 (hoch)*	*4 (sehr hoch)*	*4 (sehr hoch*	*4 (sehr hoch*	*3 Tage*
Schlüsselkundschaft betreuen	*1 (gering)*	*2 (mittel)*	*3 (hoch)*	*3 (hoch)*	*3 (hoch)*	*7 Tage*
Kundschaftsanfragen im Kundencenter entgegennehmen	*3 (hoch)*	*3 (hoch)*	*3 (hoch)*	*4 (sehr hoch*	*4 (sehr hoch*	*24 Stunden*
Kundschaftszufriedenheitsumfragen	*1 (gering)*	*1 (gering)*	*1 (gering)*	*1 (gering)*	*1 (gering)*	*Keine*

Tabelle 21: Beispiele für die Festlegung der MTPD (Erreichen des Untragbarkeitsniveaus 3 (hoch) hervorgehoben)

Begründung zur Bewertung des Schadenspotenzials

Die Bewertung des Schadenspotenzials 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 Bewertung des Schadenspotenzials auch zu einem späteren Zeitpunkt nachvollziehbar ist, sollte diese begründet werden.
- Regulatoren setzen eine Begründung voraus, um auch als außenstehende Dritte die Schadensanalyse 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 zur Bewertung des Schadenspotenzials und somit zur MTPD beigetragen haben, sollten in der Begründung benannt werden. Wird die BIA aktualisiert, dann kann so besser überprüft werden, ob die für die Schadensanalyse getroffenen Annahmen noch aktuell sind. Ferner ist es empfehlenswert, die grundsätzlichen Annahmen, die der Bewertung zu Grunde lagen, mit in der Begründung anzuführen. So sind z. B. gewisse Grundannahmen wie Mengengerüste oder Kurse zielführend, um die Höhe der finanziellen Auswirkungen zu berechnen. *Tabelle* 22 greift das Beispiel

aus *Tabelle* 21 auf und erweitert dieses um die Begründung. Aus Platzgründen ist die Bewertung des Schadenspotenzials ausgeblendet.

Beispiel

Geschäftsprozess	~	MTPD	Begründung des Schadenspotenzials
Kundschaftsanfrage im Kundencenter entgegennehmen	~	*24 Stunden*	*Bei einem Gesamtausfall des Prozesses können keine Kundschaftsanfragen angenommen und priorisiert werden. Es werden ca. 500 Telefonate und E-Mails pro Tag entgegengenommen. Ein kurzfristiger Ausfall des Prozesses bis 24 h führt zu hohen Arbeitsrückständen und wird bereits extern bemerkt. Fällt der Prozess bis zu 3 Tage aus, ist zusätzlich von einem hohen Reputationsschaden auszugehen, da dies in erheblicher Weise extern bemerkt werden würde. Das Vertrauen in die Institution wird beschädigt, da vertraglich vereinbarte SLAs nicht eingehalten werden können. Interne Leistungskennzahlen, z. B. Servicequalität und durchschnittliche Fallbearbeitungszeit, werden negativ beeinflusst. Sowohl die Arbeitsrückstände als auch die negativen Außenwirkungen nehmen mit jedem weiteren Ausfalltag zu.*

Tabelle 22: Beispielhafte Begründung eines Schadenspotenzials

Festlegung der RTO für zeitkritische Geschäftsprozesse

Für die zeitkritischen Geschäftsprozesse muss zusätzlich die geforderte Wiederanlaufzeit RTO festgelegt werden. Sie beschreibt, wie lange der reine Wiederanlauf dauern darf, bevor es zu nicht tolerablen Schäden kommt. Daher wird von der MTPD die BAO-Reaktionszeit abgezogen (siehe 5.5.1 *Konstituierung und Auflösung der BAO (AS)*). Die BAO-Reaktionszeit verstreicht in der Regel unabhängig von einzelnen Geschäftsprozessen, bis der Notfall ausgerufen und die relevanten BC-Pläne gestartet werden.

Die RTO nimmt eine zentrale Rolle in der Notfallplanung und -behandlung ein. Sie wird in Übungen verifiziert, sodass ein realistischeres Bild für die Notfallbehandlung entsteht. Für die BAO ist dann sichtbar, wie lange der Wiederanlauf vermutlich dauern wird, sodass dort bei dem Auftrag zum Wiederanlauf gut abgeschätzt werden kann, ob die MTPD noch eingehalten werden kann. Auch für die Notfallteams ist die RTO eine klare Zielvorgabe.

Zwischen der Bestimmung der RTO und der BAO-Reaktionszeit besteht eine Wechselwirkung: Einerseits bietet es sich an, diese Reaktionszeit einfach von der MTPD abzuziehen, um an die RTO zu gelangen. Hierbei kann ein zusätzlicher Puffer berücksichtigt werden, z. B. für den Fall, dass beim Wiederanlauf Schwierigkeiten auftreten.

Andererseits wird hier sehr deutlich, dass längere Reaktionszeiten z. B. bei der Detektion oder Alarmierung alle Zeiträume für RTOs verkürzen. Dadurch können sich auch die Kos-

ten erhöhen, um diese RTOs einzuhalten. Letzten Endes ist auch die BAO-Reaktionszeit eine Sollvorgabe, die sich aus den Anforderungen der Institution an die MTPDs ergibt.

Zudem ist es bei der Festlegung der RTO hilfreich, schon Teile der BC-Planung, z. B. das angestrebte Notbetriebsniveau, konzeptionell vorzubereiten, sodass die RTO konkretisiert werden kann.

Beispiel

In vielen Institutionen gibt es einen Prozess, um bestimmte Ereignisse oder Informationen unter Einhaltung von Fristen an Aufsichtsbehörden zu melden. Unter diesen Prozess fällt beispielsweise die gesetzlich verbindliche Meldung von Datenschutzvorfällen und Datenpannen gemäß Datenschutzgrundverordnung (DSGVO). Aufgrund der massiven Auswirkungen hinsichtlich der Einhaltung von Gesetzen ist dieser Prozess häufig als sehr zeitkritisch eingestuft. Die gesetzlich vorgegebenen Fristen stellen hierbei die maximal tolerierbare Ausfallzeit dar, d. h. zu diesem Zeitpunkt muss der Prozess bereits durchlaufen und eine Meldung abgegeben worden sein. Entsprechend leitet sich die geforderte Wiederanlaufzeit des Prozesses (Prozess-RTO) so ab, dass neben der Reaktionszeit auch die Prozessausführungszeit von der MTPD abgezogen und idealerweise um einen zeitlichen Puffer ergänzt wird. So wird sichergestellt, dass nach dem rechtzeitigen Wiederanlauf des Prozesses die Meldung in jedem Fall fristgerecht, d. h. innerhalb der gesetzlichen Frist, erfolgen kann.

Für nicht zeitkritische Geschäftsprozesse entfallen die nachfolgenden Schritte, da diese im Rahmen des BCM nicht weiter betrachtet werden.

Festlegung des Notbetriebsniveaus (MBCO)

Um im folgenden Schritt die für einen Notbetrieb zwingend erforderlichen Prozess- und Ressourcenabhängigkeiten ermitteln zu können, muss vorab festgelegt werden, welches Notbetriebsniveau ein zeitkritischer Geschäftsprozess erreichen soll. Hierzu genügt eine stichpunktartige Beschreibung, welche Aktivitäten des Geschäftsprozesses innerhalb des Notbetriebs aufrechterhalten werden sollen und welche Aktivitäten zurückgestellt werden können (Priorisierung). Je nach Aufgaben- oder Geschäftszweck ist auch eine prozentuale Angabe des Notbetriebsniveaus möglich, z. B. im produzierenden Gewerbe.

Tabelle 23 greift das Beispiel aus Tabelle 22 auf und erweitert dieses um das Notbetriebsniveau zu den einzelnen Prozessen. Aus Platzgründen ist die Bewertung und Begründung des Schadenspotenzials ausgeblendet.

Beispiel

Geschäftsprozess	~	*Notbetriebsniveau*
Kundschaftsanfragen beantworten	~	*Im Notbetrieb werden nur Prio-1- und Prio-2-Fragen innerhalb der üblichen Frist beantwortet. Alle anderen Fragen werden zurückgestellt.*
Kundschaftsanfrage im Kundencenter entgegennehmen	~	*Im Notbetrieb werden nur Anfragen per E-Mail entgegengenommen. Es wird eine längere Reaktionszeit von einem Tag gewährt. Die Telefonhotline wird über eine Bandansage bedient, die über die längere Reaktionszeit und die Möglichkeit des E-Mail-Supports informiert.*

Tabelle 23: Beispiel eines dokumentierten Notbetriebsniveaus

Zudem kann es hilfreich sein, nicht nur den Zielzustand des Notbetriebsniveaus zu beschreiben, sondern auch mögliche kurz- und langfristige Ziele, beispielsweise: „Was soll in den ersten Stunden, Tagen oder 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.

Dieser Prozessschritt der BIA ist abgeschlossen, wenn

- die Geschäftsprozesse im GP-Umfang hinsichtlich ihres Schadenspotenzials bewertet wurden,
- die Geschäftsprozesse im GP-Umfang anhand der Kriterien mit einer MTPD versehen sind,
- die MTPD je zeitkritischem Geschäftsprozess begründet wurde,
- für zeitkritische Geschäftsprozesse die jeweilige RTO definiert ist sowie
- für zeitkritische Geschäftsprozesse das erforderliche Notbetriebsniveau definiert wurde.

7.2.2 Identifizierung der Prozessabhängigkeiten (AS)

In der Identifizierung zeitkritischer Geschäftsprozesse 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, gegebenenfalls auch parallel aufeinander aufbauende Tätigkeiten.

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 Ge-

schäftsprozesse bereits Prozessabhängigkeiten erfasst wurden, können diese als Grundlage zum weiteren Vorgehen verwendet werden.

Falls eine für den Notbetrieb unverzichtbare Prozessabhängigkeit identifiziert wurde, sollte die RTO des benötigten Geschäftsprozesses so zwischen den Kontaktpersonen abgestimmt werden, dass die RTO des abhängigen Geschäftsprozesses eingehalten wird, sofern der benötigte Geschäftsprozess nicht bereits über die gleiche oder eine geringere RTO verfügt. Der benötigte Prozess wird damit automatisch auch zeitkritisch und somit muss auch hierfür das Notbetriebsniveau festgelegt werden. Darüber hinaus sollte, analog zur Begründung des Schadenspotenzials, die RTO begründet werden, damit ersichtlich ist, woraus sie sich ergibt. Abhängigkeiten zwischen Geschäftsprozessen können individuell eingeschätzt werden, da diese von den individuellen Anforderungen an den Notbetrieb eines Geschäftsprozesses sowie vom Grad der Abhängigkeit beeinflusst werden. So kann z. B. berücksichtigt werden, ob der benötigte Geschäftsprozess nur wiederangelaufen oder bereits abgeschlossen sein muss, bevor der abhängige Geschäftsprozess startet.

Um hierbei jedoch Zirkelbezüge zu vermeiden, ist es sehr empfehlenswert, die Prozessabhängigkeiten nur in eine Richtung zu betrachten, entweder vor- oder nachgelagert. Parallele Prozessabhängigkeiten sollten hiervon unabhängig immer betrachtet werden. Welche Richtung die Institution wählt, ist von ihrem Geschäftszweck abhängig. Üblicherweise werden die vorgelagerten Prozesse betrachtet. In bestimmten Fällen kann es jedoch auch sinnvoll sein, die nachgelagerten Prozessabhängigkeiten zu betrachten, z. B. Aufrechterhaltung einer zeitkritischen Kühlkette.

Über diesen BCM-Prozessschritt wird iterativ in jedem BIA-Zyklus eine weitere Stufe der Prozessabhängigkeiten erfasst. So werden über mehrere Zyklen zeitkritische Prozessketten identifiziert. Die Erkenntnisse aus für den Notbetrieb unverzichtbaren Prozessabhängigkeiten können im nächsten BIA-Zyklus zur Identifizierung weiterer Prozessabhängigkeiten führen. 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.

Hinweis

Bei der Abstimmung der RTO sollte darauf geachtet werden, dass die RTO eines abhängigen Geschäftsprozesses sich nicht automatisch auf alle weiteren Prozessabhängigkeiten der benötigten Geschäftsprozesse minimierend auswirken (Kaskadeneffekt). Nachfolgend sind einige Beispiele dargestellt, wie unverzichtbare Prozessabhängigkeiten identifiziert werden können.

Beispiel

***Antragsbearbeitung**: Der Geschäftsprozess „Antragsbearbeitung", mit einer RTO von 3 Tagen, ist vom Geschäftsprozess „Antragsprüfung" abhängig. Die Antragsprüfung hat eine geringere Prozessausführungszeit. Zudem sind erfahrungsgemäß im-*

mer mehr Anträge bereits geprüft als in Bearbeitung (Arbeitsvorrat von einigen Tagen). 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 Prozesszuständigen vereinbart, dass die RTO des benötigten Geschäftsprozesses „Antragsprüfung" mit 7 Tagen deutlich größer sein kann als die RTO des abhängigen Geschäftsprozesses „Antragsbearbeitung".

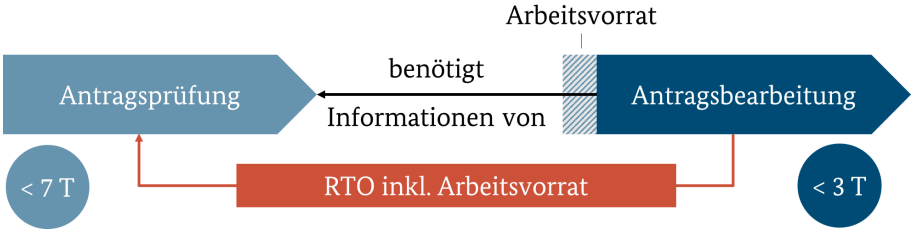

Abbildung 36: Beispiel einer vorgelagerten Prozessabhängigkeit

„Kundschaftsbetreuung": *Der Geschäftsprozess „Kundschaftsbetreuung" mit einer RTO 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 „Kundschaftsbetreuung" weitergeleitet werden. Da der benötigte Geschäftsprozess „Telefon-Hotline-Dienst" parallel zum abhängigen Geschäftsprozess „Kundschaftsbetreuung" ausgeführt werden muss, wird entschieden, dass die RTO des abhängigen Geschäftsprozesses übernommen wird.*

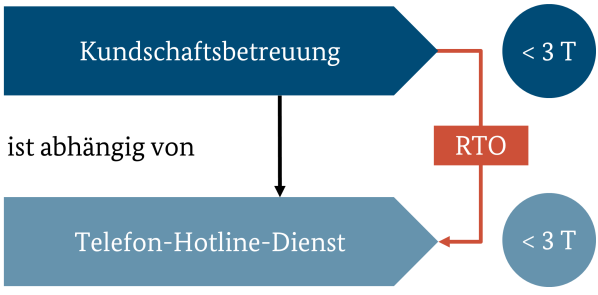

Abbildung 37: Beispiel einer parallelen Abhängigkeit zweier Geschäftsprozesse

Produktion: *Der Geschäftsprozess „Produktion" in einer Milchfabrik, mit einer RTO von drei Tagen, ist vom nachgelagerten Geschäftsprozess „Distribution" abhängig. Da nur begrenzte Lagermöglichkeiten für die produzierten Güter bestehen, können diese maximal zwei weitere Tage aufbewahrt werden, bevor das Lagervolumen ausgeschöpft ist. Um einen kontinuierlichen Produktionsfluss zu gewährleisten, wird beschlossen, die RTO des benötigten Geschäftsprozesses „Distribution" auf fünf Tage festzulegen.*

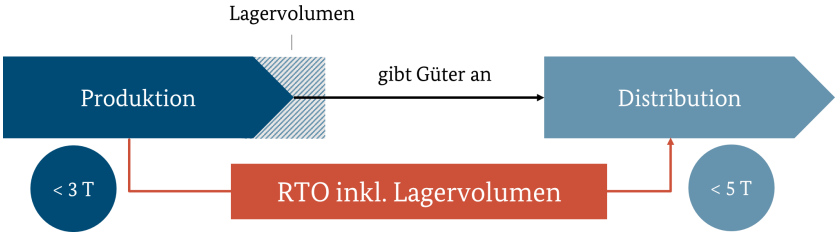

Abbildung 38: Beispiel einer nachgelagerten Prozessabhängigkeit

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 unverzichtbare Abhängigkeit, wenn zwei Geschäftsprozesse im Normalbetrieb in einer bestimmten Reihenfolge ablaufen oder Informationen austauschen. Unverzichtbare Abhängigkeiten bestehen nur dann, wenn für den Wiederanlauf und den Notbetrieb des untersuchten Geschäftsprozesses weitere Geschäftsprozesse zwingend benötigt werden, um das definierte Notbetriebsniveau zu erreichen und aufrecht zu erhalten.

7.2.3 Identifizierung der Ressourcenabhängigkeiten (R+AS)

Für alle zeitkritischen Geschäftsprozesse müssen anhand der festgelegten Ressourcenkategorien (siehe *7.1.3 Festlegung der Ressourcenkategorien und -cluster (R+AS)*) 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 BC-Planung berücksichtigt werden sollen, kann auf die Angabe von Ressourcen, die nur im Normalbetrieb eingesetzt werden, bewusst verzichtet werden.

Beispiel

Mitarbeitende können 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 BC-Planung oder ad hoc im Notfall berücksichtigt werden. Die Mitarbeitenden haben so die Möglichkeit gewonnen, den Geschäftsprozess im Notbetrieb effizienter als notwendig durchzuführen und somit nicht nur das Notbetriebsniveau zu erreichen, sondern dieses zu übertreffen und die Nacharbeiten zu reduzieren.

Mit steigender Reife des BCMS und sofern ausreichend Ressourcen hierzu bestehen, können auch die im Normalbetrieb genutzten Ressourcen miterfasst werden. Zwar erhöht die Erfassung der im Normalbetrieb genutzten Ressourcen den Umfang der BIA deutlich, aber sie bietet Dritten die Chance, die BIA-Ergebnisse nachzuvollziehen. Z. B. ändern sich in größeren Institutionen sehr oft BIA-Kontaktpersonen oder im Nachgang wird die Ressourcenliste von Dritten gesichtet und bewertet. Möglicherweise sind ungewöhnliche Konstellationen schon im Normalbetrieb vorhanden. Dritte sehen ohne die Ressourcen des Normalbetriebs z. B. nicht, ob eine Ressource bewusst nicht für den Notbetrieb ausgewählt wurde oder ob die Ressource schlicht vergessen wurde.

Es ist empfehlenswert, die Ressourcen(cluster) anhand vorgegebener Listen zu ermitteln und zu dokumentieren. 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 BC-Planung der Ressourcen sind die folgenden BIA-Kenngrößen für Ressourcen:

- Geforderte Wiederanlaufzeit (RTO)
- Ressourcenbedarf in Abhängigkeit zur Dauer des Notbetriebs
- Im Falle von Daten und IT-Ressourcen: maximal zulässiger Datenverlust (RPO)

RTO der benötigten Ressourcen

Anhand der RTO des zeitkritischen Geschäftsprozesses muss die RTO der prozessnotwendigen Ressourcen(cluster) so abgeleitet werden, dass der Notbetrieb rechtzeitig erreicht wird. Ähnlich wie die RTO in den Prozessabhängigkeiten kann auch die RTO der Ressourcen(cluster) individuell abgestimmt werden. Falls mehrere Geschäftsprozesse auf dieselbe(n) Ressourcen(cluster) zurückgreifen, muss die kleinste RTO für diese Ressource gewählt werden.

Tabelle 24 greift die Beispiele der Geschäftsprozesse aus Tabelle 21 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 (siehe Zeile 3 und 4). In Zeile 2 hat die Ressource E-Mail bewusst eine deutlich geringere RTO erhalten. So steht ein hinreichender Puffer zur Verfügung, um die angefallenen Anfragen per E-Mail innerhalb der Tagesfrist entgegenzunehmen, nachdem das Tool selbst wieder bereitgestellt wurde.

Beispiel (sortiert nach Ressource)

Ressourcen, deren RTO aufgrund des Minimalprinzips ermittelt wurden, sind hervorgehoben.

Ressourcen-kategorie	Ressource	RTO der Ressource	Geschäftsprozess	RTO des Geschäftsprozesses
IT	Telefonie	20 Stunden	Kundschaftsanfrage im Kundencenter entgegennehmen	< 24 Stunden
IT	E-Mail	20 Stunden	Kundschaftsanfrage im Kundencenter entgegennehmen	< 24 Stunden
IT	Tickettool TT	< 24 Stunden	Kundschaftsanfrage im Kundencenter entgegennehmen	< 24 Stunden
IT	Tickettool TT	< 24 Stunden	Kundschaftsanfragen bearbeiten	< 3 Tage
IT	Customer Relationship Management Tool CRM	2 Tage	Kundschaftsanfragen bearbeiten	< 3 Tage
Dienstleistungen	Call-24h	< 24 Stunden	Kundschaftsanfrage im Kundencenter entgegennehmen	< 24 Stunden
Dienstleistungen	Call-24h	< 24 Stunden	Kundschaftsanfragen bearbeiten	< 3 Tage
Informationen	Kundschaftsdaten	n/a	Kundschaftsanfragen bearbeiten	< 3 Tage
Informationen	FAQ-Liste	n/a	Kundschaftsanfragen bearbeiten	< 3 Tage

Tabelle 24: Beispiele für Ressourcenabhängigkeiten verschiedener Geschäftsprozesse

Ressourcenbedarf in Abhängigkeit zur Dauer des Notbetriebs

Für viele Ressourcenkategorien wie z. B. Personal und Arbeitsplätze, aber auch Maschinen oder Arbeitsmittel kann sich die Anzahl der benötigten Ressourcen mit der Dauer des Notbetriebs verändern. Dies kann aus unterschiedlichen Gründen erforderlich werden, z. B.

- um das ansteigende Arbeitsvolumen aufzufangen (z. B. durch ein steigendes Notbetriebsniveau),
- um zu berücksichtigen, dass noch nicht die volle Kapazität (z. B. an Personal) von Beginn des Notbetriebs zur Verfügung steht oder

- um die Arbeitslast so zu verteilen, dass auch die weiteren, zeitkritischen Geschäftsprozesse bedient werden 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 zusätzlich 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 25 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 Kundenmanagement

Ressourcenkategorie	*Ressource*	*Anmerkungen*	*24 Stunden*	*3 Tage*	*7 Tage*	*14 Tage*	*30 Tage*
Arbeitsplatz vor Ort	*Standard-Arbeitsplatz*		*3*	*5*	*5*	*5*	*5*
Personal	*Kundencenter (KC) Teamleitende*	*arbeiten mobil*	*1*	*2*	*2*	*2*	*2*
Personal	*Kundencenter (KC) Mitarbeitende*		*3*	*5*	*5*	*5*	*5*
Personal	*Technisch Beratende*	*arbeiten mobil*	*1*	*2*	*3*	*3*	*3*

Tabelle 25: Beispiel für Arbeitsplatz- und Personalabhängigkeiten

Im Beispiel wird angenommen, dass die Organisationseinheit über zwei Teamleitende und fünf Mitarbeitende im Kundencenter sowie drei technisch Beratende zur Beantwortung der Kundschaftsanfragen verfügt. Jede dieser Personen verfügt im Normalbetrieb über einen eigenen Arbeitsplatz. Während eines eingeschränkten Notbetriebs werden innerhalb der ersten 24 Stunden zunächst nur ein Teamleiter oder eine Teamleiterin, drei Mitarbeitende und eine technisch beratende Person benötigt, da die Kundschaftsanfragen entsprechend kurzfristig quittiert und klassifiziert werden müssen. Die technisch beratende Person hat dann Zeit, die dringendsten Anfragen zu bearbeiten, sodass diese fristgerecht beantwortet werden können. Hierbei werden genauso viele Arbeitsplätze wie Kundencenter-Mitarbeitende benötigt, da diese nicht mobil arbeiten können. Teamleitende und technisch beratende Personen können mobil arbeiten und benötigen daher keine dedizierten Arbeitsplätze vor Ort.

RPO

Bei informationsbasierten Ressourcenkategorien, d. h. beispielsweise die Ressourcenkategorien Informationen und IT (Daten), muss zusätzlich die RPO bestimmt werden. Die RPO stellt in diesem Zusammenhang eine fachliche Anforderung des Prozesseigentümers oder der -eigentümerin dar, bis zu welchem Datenstand er oder sie eine Datensicherung voraussetzt, um mit geeigneten Informationen (Daten) im Notbetrieb arbeiten zu können. Die RPO ist **unabhängig** von der MTPD oder der RTO 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 26 greift die Beispiele der Geschäftsprozesse aus Tabelle 21 auf, analog zu Tabelle 24.

Beispiel

Ressourcenkategorie	Ressource	Konsolidierte RPO	Geschäftsprozess	RPO
Informationen	*Kundschaftsdaten*	*transaktionsgenau*	*Kundschaftsanfragen bearbeiten*	*transaktionsgenau*
Informationen	*Kundschaftsdaten*	*transaktionsgenau*	*Schlüsselkundschaftsbetreuung*	*2 Tage*

Tabelle 26: Beispiele für informationsbasierte Ressourcenabhängigkeiten verschiedener Geschäftsprozesse

Synergiepotenzial

Oft genügt das Datensicherungsintervall des Normalbetriebs als RPO. 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.

7.2.4 Identifizierung vorhandener Single Points of Failure (AS)

Wenn viele (sehr) zeitkritische Geschäftsprozesse eine einzelne Ressource benötigen, stellt diese ein erhöhtes Risiko für eine Geschäftsunterbrechung dar. Üblicherweise werden solche Ressourcen als **Single Point of Failure** bezeichnet. Es gibt verschiedene Arten von Single Points 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 Dienstleistungsunternehmen 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 die alleinige Kontaktperson ist, oder eine Schnittstelle, die die alleinige Kommunikationsstelle für einen bestimmten Sachverhalt ist.*
- *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 identifiziert und risikoorientiert abgesichert werden. SpoFs sollten unbedingt in der BCM-Risikoanalyse (siehe Kapitel 9 *BCM-Risikoanalyse (AS)*) untersucht und je nach Ergebnis in den BC-Strategien berücksichtigt werden.

7.3 Auswertung (R+AS)

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, ob diese vollständig, korrekt und nachvollziehbar sind. Es ist empfehlenswert, zu überprüfen, ob sämtliche notwendigen Informationen erhoben sowie die Schadensanalyse formal korrekt vorgenommen wurde und ob die Begründung der Schadensanalyse 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 Kontaktpersonen 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 zugehörigen Kontaktpersonen,
- Übersicht der Prozessabhängigkeiten sowie
- Übersicht der abhängigen Ressourcen und SpoFs 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. Anschließend kann mit dem Soll-Ist-Vergleich begonnen werden.

8 Soll-Ist-Vergleich (R+AS)

Als Ergebnis der BIA liegen für alle betrachteten zeitkritischen Ressourcen die RTOs (geforderte Wiederanlaufzeit) sowie gegebenenfalls die RPO (maximal zulässiger Datenverlust) vor. RTO und RPO stellen gewünschte Soll-Werte dar. Die Ressourcenzuständigen müssen im Rahmen des Soll-Ist-Vergleichs die Frage beantworten, ob die RTO der Ressource mit vorhandenen technischen und organisatorischen Maßnahmen erreicht werden kann. Hierzu muss der RTO die **Recovery Time Actual** (**RTA**, deutsch: tatsächliche Wiederanlaufzeit) gegenübergestellt und die Zeitwerte müssen miteinander verglichen werden. Die RTA einer zeitkritischen Ressource bezeichnet den real erreichbaren Zeitraum ab dem Ausruf des Notfalls bis zu dem Zeitpunkt, an dem eine BC-Lösung für diese Ressource produktiv gesetzt wird. Analog muss für informationsbasierte Ressourcen auch die RPO mit dem Recovery Point Actual (RPA, deutsch: tatsächlicher Datenverlust) verglichen werden. Aus Vereinfachungsgründen wird nachfolgend nur bei Abweichungen im Vorgehen auf die RPO eingegangen. Ansonsten gilt das Vorgehen analog zum Soll-Ist-Vergleich der RTO.

Die nachfolgenden Unterkapitel beschreiben die empfohlene Vorgehensweise, mittels derer der Soll-Ist-Vergleich durchgeführt wird. In Abbildung 39 sind die hierfür erforderlichen Schritte in einer Übersicht dargestellt.

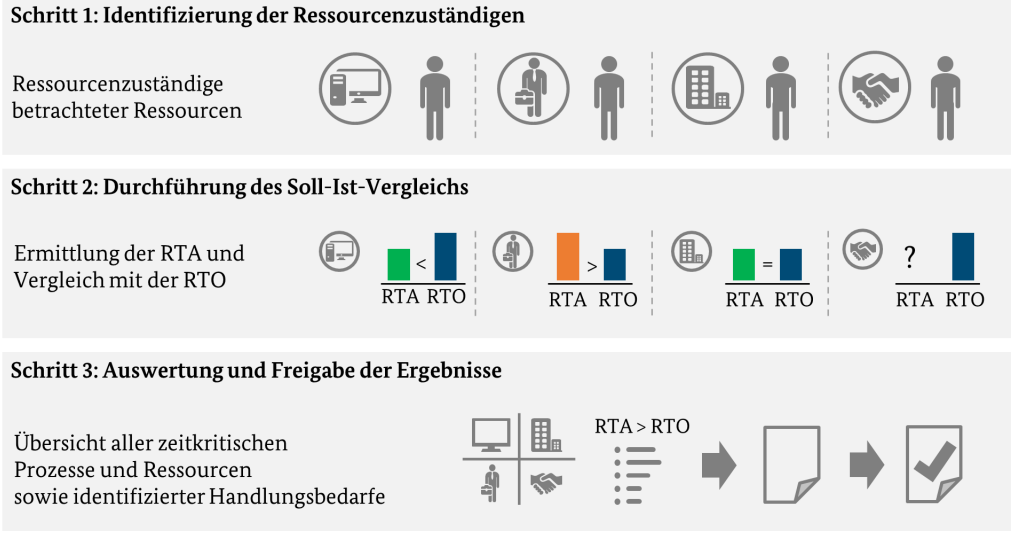

Abbildung 39: BCM-Prozessschritte des Soll-Ist-Vergleichs

8.1 Identifizierung der Ressourcenzuständigen (R+AS)

Vor dem Soll-Ist-Vergleich ist es notwendig, die Ressourcenzuständigen zu identifizieren. Da der oder die BCB in der Regel über den besten Gesamtüberblick über die BIA-Ergebnisse verfügt, ist es empfehlenswert, dass er oder sie diese Aufgabe übernimmt.

Dabei kann er oder sie anhand der Ressourcenkategorien vorgehen. Tabelle 27 gibt beispielhaft die typischen Kontaktpersonen je Ressourcenkategorie wieder. Falls die Institution abweichende Ressourcenkategorien benannt hat, dann ist es wichtig, dass diese entsprechend berücksichtigt werden.

Beispiel

Ressourcenkategorie	Geschäftsprozess- bzw. Ressourcenzuständige
IT	*ITSC-Manager (ITSCM)*
Personal	*Leitung Personal*
Arbeitsplätze	*Leitung Gebäudeverwaltung, Haustechnik*
Dienstleistungen	*Leitung Einkauf (Provider Management) oder dezentrale Provider (Supplier Manager)*
Informationen	• *zentrale physische Daten: Leitung Aktensammelstelle/Archiv* • *dezentrale physische Daten: Leitung der jeweiligen Organisationseinheit (gemäß BIA)* • *Bei elektronischen Daten: ITSC-Manager*
Infrastruktur	*Leitung Infrastruktur, Werksleitung, Technische Betriebsleitung*
Maschinen, Geräte, Anlagen, Fahrzeuge	*Leitung Infrastruktur, Werksleitung, Technische Betriebsleitung*
Betriebsmittel (Sonstige)	*Leitung Infrastruktur, Werksleitung, Technische Betriebsleitung*

Tabelle 27: Beispiele für Ressourcenzuständige

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

Zur Sensibilisierung der oben aufgeführten Leitenden kann die **BIA-Workshop-Präsentation** dienen (siehe 7.1.5 *Vorbereitung der BIA-Hilfsmittel (R+AS)*). 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.

8.2 Durchführung des Soll-Ist-Vergleichs (R+AS)

Die Ressourcenzuständigen müssen im Rahmen des Soll-Ist-Vergleichs die Frage beantworten, ob die RTO der Ressource mit vorhandenen technischen und organisatorischen Maßnahmen erreicht werden kann. Dazu wird der RTO die RTA gegenübergestellt und die Zeitwerte werden miteinander verglichen.

Die RTA kann im Rahmen von Übungen und Tests (siehe Kapitel 13 *Üben und Testen (R+AS)*) ermittelt und nachgewiesen werden. Für die Ressourcenkategorie **Dienstleistungen** sollte in den bestehenden Verträgen oder Service Level Agreements geprüft werden, ob darin Aussagen zur Realisierbarkeit der RTO vorliegen. Ferner sollte untersucht werden, inwiefern die bestehenden Dienstleistungsunternehmen bereits allgemeine Anforderungen an ein BCM erfüllen oder aber ob die bestehenden Dienstleistungen in einer anderen Art und Weise unmittelbar in einem Schadensfall erbracht werden können. Weiterführende Informationen zu möglichen BC-Strategien zur Absicherung von Dienstleistungsunternehmen können dem Hilfsmittel *Vorschläge zu BC-Strategien* entnommen werden.

Wird der PDCA-Lebenszyklus z. B. in einem Reaktiv-BCMS erstmalig durchlaufen, dann liegen im Regelfall noch keine Ergebnisse zu Übungen und Tests vor. In diesem Fall kann die RTA von einer fachlich kundigen Person realistisch geschätzt werden. Weder sollten einfach zu bewältigende Ausfallszenarien zu Grunde gelegt werden noch unlösbare Worst-Case-Szenarien, die die präventiven Planungsmöglichkeiten eines BCMS erschöpfen. Beispiele für Worst-Case-Szenarien sind z. B. Cyberattacken oder höhere Gewalt. 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. Hierbei ist es empfehlenswert, dass der oder die BCB kommuniziert, unter welchen Bedingungen die RTA betrachtet werden soll, z. B. unter Ausschluss von höherer Gewalt. Falls keine realistische 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, über ein Tool oder in Einzelgesprächen abgefragt werden. Es 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 28 zeigt dies am Beispiel von IT-Ressourcen.

Beispiel

Ressourcen-kategorie	**Ressource**	**RTO**	**RTA**	**Nachweis**	**RTA ≤ RTO**	**Getestet?**
IT	*Standard-IT-Ausstattung*	*< 3 Tage*	*2 Tage*	*Schätzung anhand ausgewerteter IT-Service-Requests*	*Ja*	*Nein*
IT	*E-Mail-Service*	*< 1 Tag*	*05:45 h*	*Funktionstest*	*Ja*	*Ja*
IT	*Fileserver*	*< 1 Tag*	*unbekannt*	*nicht vorhanden*	*unbekannt*	*Nein*
Dienstleistungsunternehmen	*Cloud Services*	*< 1 Tag*	*6h*	*RTA vertraglich zugesichert laut SLA mit dem Cloudanbieter overCloud*	*Ja*	*Nein*

Tabelle 28: Beispiel eines Soll-Ist-Vergleichs der RTO anhand der Ressourcenkategorie IT

Für die Ressourcenkategorien, für die eine RPO festgelegt wurde, muss diese mit dem vom IT-Betrieb festgelegten Datensicherungszyklus abgeglichen werden (siehe Tabelle 29).

Beispiel

Ressource	**RPO**	**Datensicherungs-zyklus**	**Nachweis**	**Datensicherung ≤RPO**
Kundschaftsdaten	*Vortag*	*12 Stunden*	*Betriebshandbuch*	*Ja*

Tabelle 29: Beispiel eines Soll-Ist-Vergleichs der RPO

Synergiepotenzial

Falls ein ITSCM vorhanden ist, wurden die RTA und RPA voraussichtlich bereits dort in der Gap-Analyse erhoben.

8.3 Auswertung und Freigabe der Ergebnisse (R+AS)

Eine Übersicht aller zeitkritischen Ressourcen, insbesondere jedoch der unzureichend abgesicherten Ressourcen, muss erstellt und mit der Institutionsleitung 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 im **Reaktiv-BCMS** anhand der Geschäftsfortführungsplanung abgeleitet (siehe 11.2 *Erstellung der GFPs (R+AS)*).	**R**
Der weitere Handlungsbedarf wird im **Aufbau- und Standard-BCMS** anhand der BCM-Risikoanalyse abgeleitet.	**AS**

9 BCM-Risikoanalyse (AS)

Während die BIA die möglichen Auswirkungen von Geschäftsunterbrechungen auf den Geschäftsbetrieb untersucht, betrachtet die BCM-Risikoanalyse die möglichen Ursachen für den Ausfall des Geschäftsbetriebs, um bei der Entwicklung von BC-Strategien und -Lösungen die Auswirkungen dieser Ursachen zu minimieren oder zu reduzieren. In der BCM-Risikoanalyse wird dazu untersucht, gegen welche Gefährdungen der Geschäftsbetrieb abgesichert werden soll, d. h. bei welchen Gefährdungen das Risiko einer Unterbrechung so hoch ist, dass abgesichert werden soll. Als **Zielobjekte** in der BCM-Risikoanalyse müssen alle zeitkritischen Geschäftsprozesse und Ressourcen systematisch betrachtet werden, die vorab in der BIA identifiziert wurden. Die Risiken, die sich auf die zeitkritischen Geschäftsprozesse auswirken, werden aus den Risiken der benötigten zeitkritischen Ressourcen abgeleitet, sodass die BCM-Risikoanalyse in diesem Standard nachfolgend nur die zeitkritischen Ressourcen betrachtet.

Die Ergebnisse der BCM-Risikoanalyse schaffen die Voraussetzung dafür, dass in den Folgeschritten des BCMS gezielte BC-Strategien und BC-Lösungen und hieraus wiederum konkrete Vorsorge- und Notfallmaßnahmen sowie Notfallpläne unter Kosten-Nutzen-Risiko-Gesichtspunkten abgeleitet werden können.

Hinweis

Dieses Kapitel beschreibt die BCM-spezifischen Aspekte am Beispiel des Vorgehens nach BSI-Standard 200-3. Entsprechend werden hier auch die dort verwendeten Begriffe und Schritte der Risikoanalyse vorausgesetzt. 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. Daher ist es wichtig, die Angaben entsprechend institutionsspezifisch anzupassen.

Abbildung 40 fasst die wesentlichen Schritte zusammen, wie eine BCM-Risikoanalyse nach BSI-Standard 200-3 durchgeführt wird. Abweichend davon könnte in der Praxis auch auf vorhandene Ergebnisse einer Risikoanalyse zurückgegriffen werden oder die BCM-relevanten Risiken könnten im Rahmen 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 Egebnisse aus der Risikoanalyse ableiten zu können, sollte die Risikoanalyse möglichst zeitnah im Anschluss an die BIA und 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

inzwischen verändert haben. Zudem sollte die Risikoanalyse ebenso häufig wie die BIA und der Soll-Ist-Vergleich stattfinden, z. B. jährlich. So kann sichergestellt werden, dass die betrachteten Zielobjekte stets vollständig und aktuell analysiert werden.

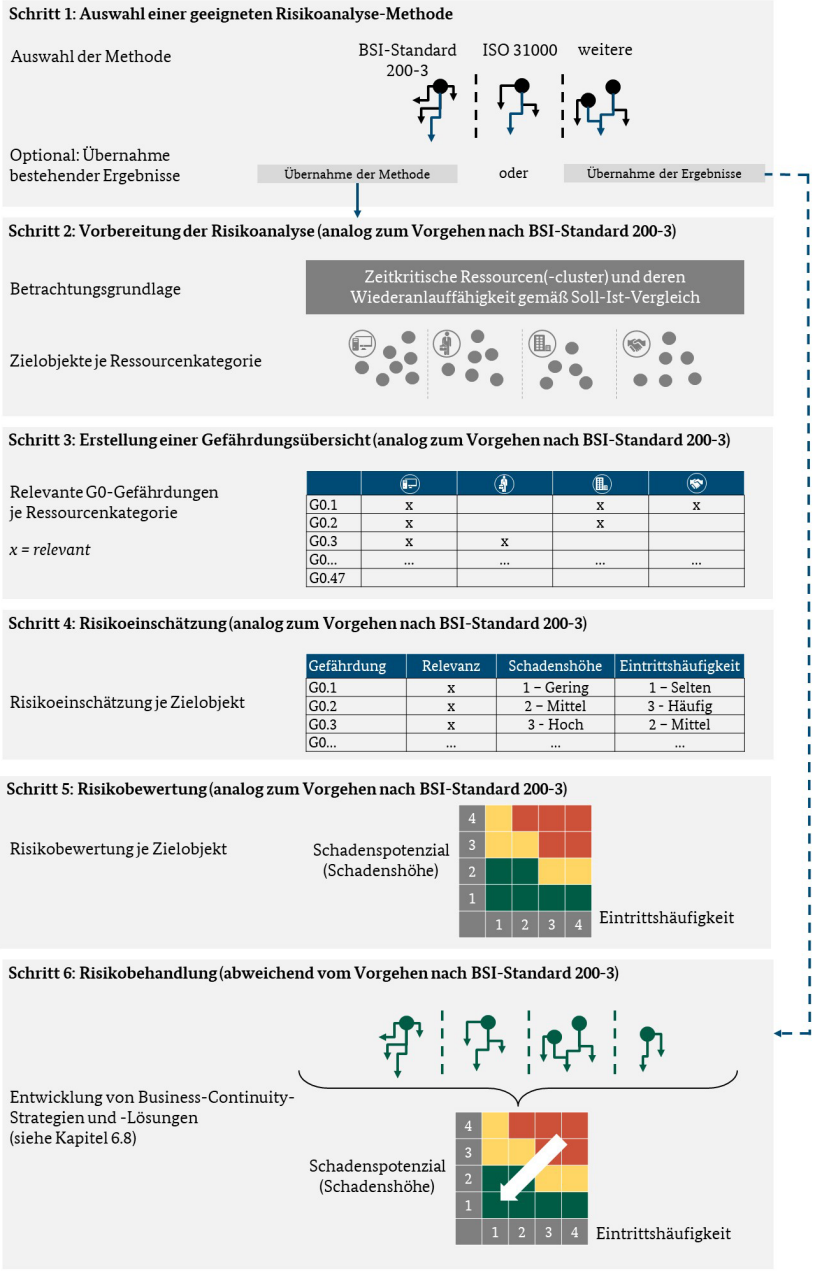

Abbildung 40: BCM-Prozessschritte der BCM-Risikoanalyse

9.1 Auswahl einer geeigneten Risikoanalyse-Methode (AS)

Eine BCM-Risikoanalyse unterscheidet sich methodisch nicht von Risikoanalysen aus anderen Managementdisziplinen, wie z. B. dem Informationssicherheitsmanagement, dem (IT-)Risikomanagement oder dem Facility Management. Üblicherweise fließen die Ergebnisse aller themenspezifischen Risikoanalysen in ein institutionsübergreifendes Risikomanagement ein und werden darin konsolidiert.

Der BSI-Standard 200-4 beschreibt keine eigenständige Methodik für eine BCM-Risikoanalyse. Vielmehr kann hierzu auf etablierte Risikomanagement-Standards zurückgegriffen werden. Diese Methoden müssen die BCM-relevanten Risiken für alle zeitkritischen Ressourcen, insbesondere SpoFs, sowie für alle zeitkritischen Geschäftsprozesse systematisch untersuchen. Unter BCM-relevanten Risiken werden dabei in der Regel Risiken verstanden, die sich unmittelbar auf die Verfügbarkeit der zeitkritischen Ressourcen auswirken. Im Gegensatz hierzu betrachten Risikoanalysen in anderen Bereichen, z. B. in einem ISMS, auch weitere Gefährdungen gleichwertig, beispielsweise den Verlust der Integrität oder der Vertraulichkeit von relevanten Ressourcen. Insbesondere wenn kein ISMS vorliegt, kann der Verlust der Integrität oder der Vertraulichkeit einer zeitkritischen Ressource in seiner Konsequenz auch zu einer nicht tolerierbaren Geschäftsunterbrechung führen, da nicht mehr im Normalbetrieb weitergearbeitet werden kann. Sofern kein hinreichendes ISMS vorliegt, sollten die Grundwerte Integrität und Vertraulichkeit in einer BCM-Risikoanalyse berücksichtigt werden, sodass zumindest die hieraus resultierenden Auswirkungen auf die Verfügbarkeit in den BC-Strategien behandelt werden können.

Die BCM-Risikoanalyse muss die folgenden Anforderungen erfüllen:

- Die Risikoanalyse sollte die Risikokriterien Eintrittshäufigkeit und Schadenshöhe berücksichtigen.
- Die Risikoeinschätzung sollte alle vorhandenen risikoreduzierenden Maßnahmen berücksichtigen. (Netto-Risikoeinschätzung)
- Der Detailgrad der betrachteten Ressourcen(cluster), der Gefährdungen und der resultierenden Risiken sollte so gewählt werden, dass geeignete BC-Strategien und -Lösungen dafür identifiziert werden können.
- Die Institution muss die identifizierten Risiken auf den weiteren Handlungsbedarf hin bewerten.
- Die Institution muss sicherstellen, dass vor der Risikoakzeptanz alle anderen Risikobehandlungsoptionen angemessen geprüft wurden.
- Die Ergebnisse der BCM-Risikoanalyse, insbesondere bestehende Restrisiken, sollten durch die Institutionsleitung zur Kenntnis genommen werden.
- Die bestehenden Restrisiken müssen durch die Institutionsleitung akzeptiert werden.

Unter anderem erfüllen die Risikomanagement-Standards BSI-Standard 200-3 *Risikomanagement* sowie die Norm DIN ISO 31000:2018 *Risikomanagement – Grundsätze und 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 oder der Informationssicherheitsbeauftragten oder dem Risikomanager oder der Risikomanagerin.

Zudem können Risiken, die zu einem Ausfall zeitkritischer Ressourcen führen, bereits anhand bestehender Risikoanalysen aus anderen Managementsystemen 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.*
- *Die Sortierung oder Gruppierung der Zielobjekte aus anderen Managementsystemen sollte dahingehend überprüft werden, ob sie auch zu den Ressourcen und deren Clustern im BCMS passt.*

Während im Risikomanagement häufig sehr abstrakte Risikoszenarien strategisch betrachtet werden, z. B. die Ausfallwahrscheinlichkeit eines Rechenzentrums, können andere Risikoanalysen wiederum zu detailliert sein, z. B. eine IT-Risikoanalyse, die den Ausfall eines E-Mail-Servers aufgrund von Schadsoftware analysiert. Um im BCM angewendet werden zu können, ist es gegebenenfalls notwendig, diese Informationen zu präzisieren oder zu verdichten. Das Ergebnis der Risikoanalyse sollte somit einen Detailgrad besitzen, der es gestattet, daraus konkrete BC-Lösungen im BCM 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 und -Lösungen entwickeln zu können.

9.2 Vorbereitung der Risikoanalyse (AS)

Durch die BIA liegt bereits die Liste der zeitkritischen Ressourcen und damit der relevanten Zielobjekte für die BCM-Risikoanalyse vor. Die Vorbereitung zur Risikoanalyse gemäß BSI-Standard 200-3 beschränkt sich daher auf eine geeignete Gruppenbildung dieser relevanten Zielobjekte. In der BCM-Risikoanalyse kann auch auf die bereits definierten Ressourcen(cluster) gemäß BIA zurückgegriffen werden. Aufgrund ihrer hohen Bedeutung sollten zusätzlich die in der BIA identifizierten SPoFs als eigenständige Zielobjekte in der BCM-Risikoanalyse betrachtet werden.

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 7.1.4 *Planung der BIA-Erhebung (*R+AS*)*). Auch der Einsatz von vorgegeben Hilfsmitteln bietet sich in der BCM-Risikoanalyse an (siehe 7.1.5 *Vorbereitung der BIA-Hilfsmittel (R+AS)*). Insbesondere kann es hilfreich sein, eine Workshop-Präsentation vorzubereiten, in der auf die spezifischen Eigenschaften der BCM-Risikoanalyse eingegangen wird.

9.3 Erstellung einer Gefährdungsübersicht (AS)

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 als relevant betrachtet werden, die sich auf das Schutzziel Verfügbarkeit beziehen. Gefährdungen, die sich nur auf andere Schutzziele auswirken, wie z. B. Gefährdungen, die die Vertraulichkeit oder Integrität beeinträchtigen, werden innerhalb des BCM nicht direkt behandelt. Das BCM wird in der Regel beispielsweise keine Vorkehrungen treffen, um den Verlust der Vertraulichkeit oder Integrität präventiv zu verhindern. Dies gehört in der Regel zu den Aufgabengebieten des ISMS. Demgegenüber kann aber ein Verlust der Vertraulichkeit oder Integrität auch zu einem Verlust der Verfügbarkeit führen, sodass zumindest diese Form der Auswirkung auch im Rahmen der Risikoanalyse betrachtet werden sollte, wenn noch kein ISMS erfolgreich etabliert wurde.

Tabelle 30 gibt am Beispiel ausgewählter, elementarer Gefährdungen ein mögliches Beispiel wieder, wie für das BCM relevante Gefährdungen selektiert werden können, falls ein ISMS etabliert ist.

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 30: Ausgewählte elementare Gefährdungen des BSI mit Bezug auf das Schutzziel Verfügbarkeit (Beispiel)

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 (siehe 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 31 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***	***Dienstleis-tung***	***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 Dienstleistungsunternehmen	*Indirekt relevant*	*Direkt relevant*	*Nicht relevant*	*Nicht relevant*	…
…	…	…	…	…	…
G0.33 Personalausfall	*Indirekt relevant*	*Nicht relevant*	*Nicht relevant*	*Direkt relevant*	…
…	…	…	…	…	…

Tabelle 31: Zuordnung der Gefährdungen zu den Ressourcenkategorien (Beispiele)

Darüber hinaus ist es empfehlenswert, dass die Risikofachleute für die (gruppierten) Zielobjekte anhand der tatsächlichen Bedrohungen und Schwachstellen mögliche weitere Gefährdungen identifizieren, beispielsweise mit der Delphi-Methode.

9.4 Risikoeinschätzung (AS)

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 im BSI-Standard 200-3 beschriebenen Vorgehen. In der Praxis sind die Ressourcenzuständigen üblicherweise auch die **Risikofachleute**, die am besten Aussagen über die möglichen Risiken für ihre Ressource treffen können. Da die Ressourcenzuständigen bereits aus dem Soll-Ist-Vergleich bekannt sind, ist es empfehlenswert, dass diese Kontaktpersonen auch in der BCM-Risikoanalyse berücksichtigt werden.

Für die Risikoeinschätzung sollte die Eintrittshäufigkeit und potenzielle Schadenshöhe berücksichtigt werden. Wie hoch das Risiko ist, wird im BSI-Standard 200-3 und in vielen weiteren Methoden von zwei Parametern bestimmt:

- Die **Eintrittshäufigkeit** bezeichnet, wie häufig sich eine Gefährdung auf eine zeitkritische Ressource schätzungsweise auswirkt.
- Die **Schadenshöhe** bezeichnet die zu erwartende Höhe des Schadens, der bei Eintritt des Schadensereignisses entsteht.

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* entnommen 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 ausschließlich einzeln dahingehend analysiert, welche potenziellen Schäden entstehen können, falls der Prozess ausfällt. Dies umfasst z. B. keine Kumulation der potenziellen Schäden über mehrere Geschäftsprozesse hinweg. Für bestimmte Ressourcen(cluster), beispielsweise ein Gebäude oder einen zentralen Server, von deren Verfügbarkeit mehrere Geschäftsprozesse abhängig sind, wird das Schadenspotenzial in der Risikoanalyse dementsprechend höher eingeschätzt werden. Ferner werden, anders als in der BIA, in der Risikoanalyse 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 Eintrittshäufigkeit oder Schadenshöhe der Risiken auswirken.*

Beispiel

Durch die Risikofachleute 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 Risikofachleute sowohl bestehende risikoreduzierende Maßnahmen als auch die Wiederanlauffähigkeit berücksichtigt.

Folgende risikoreduzierende Maßnahmen werden berücksichtigt:

- *Es finden regelmäßige Brandschutz-Übungen und -Schulungen für alle Mitarbeitenden statt.*
- *Eine automatische Brandmeldeanlage und eine Brandlöschanlage sind installiert.*
- *Das Gebäude wird regelmäßig auf Brandlasten untersucht, die jeweils zeitnah beseitigt werden.*

Die Eintrittshäufigkeit wird daher durch die zuständige Risikoexpertin 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, sodass RTA < RTO gilt.*

Unter Abwägung des maximal möglichen Schadens und der hohen Wiederanlauffähigkeit wird das Schadenspotenzial durch die Risikoexpertin als mittel eingestuft.

9.5 Risikobewertung (AS)

Durch die Institution müssen die identifizierten Risiken hinsichtlich ihres weiteren Handlungsbedarfs bewertet werden. Wie in Abbildung 41 dargestellt, können verschiedene Risikokategorien anhand einer Risikomatrix festgelegt werden (siehe BSI-Standard 200-3, Kapitel 5.2 *Risikobewertung*). In diesem Standard wurde bewusst ein vom BSI-Standard 200-3 abweichendes Beispiel gewählt, um eine weitere Möglichkeit darzustellen. Es ist jedoch sehr sinnvoll, beim ISMS und BCM die gleichen Kategorien zugrunde zu legen.

Beispiel

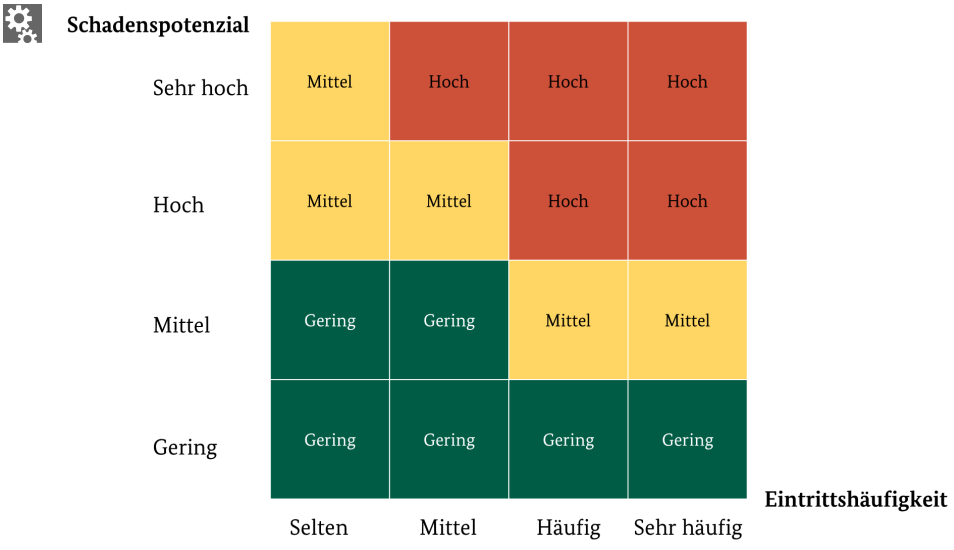

Abbildung 41: Beispiel einer Risikomatrix

Tabelle 32 enthält einen BCM-spezifischen Vorschlag zur Definition der verschiedenen Risikokategorien aus Abbildung 41 angelehnt an den BSI-Standard 200-3.

Beispiel

Risikokategorien	***Erläuterung***
gering	*Die Vorsorge- und Notfallmaßnahmen sowie die bereits umgesetzten BC-Lösungen 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 sowie die bereits umgesetzten BC-Lösungen reichen **möglicherweise nicht aus**.*
hoch	*Die Vorsorge- und Notfallmaßnahmen sowie die bereits umgesetzten BC-Lösungen bieten **keinen ausreichenden Schutz** vor der jeweiligen Gefährdung, z. B. weil die RTA nicht ausreichend ist.*

Tabelle 32: Definition der Risikokategorien

Hinweis

*Es ist empfehlenswert, die Risikobewertung anhand einer Risikomatrix in Kategorien einzuteilen, z. B. in die drei Kategorien geringe, mittlere und hohe Risiken. Daraus kann die weitere Behandlung von Risiken abgeleitet werden. 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 zu unterziehen, z. B. durch risikoreduzierende Maßnahmen.*

9.6 Risikobehandlung (AS)

Die Risikobehandlung im BCMS orientiert sich grundlegend an den vier Risikobehandlungsoptionen des BSI-Standard 200-3 (siehe BSI-Standard 200-3, Kapitel *6.1 Risikobehandlungsoptionen*). Jedoch ist die Risikobehandlungsoption *Transfer von Risiken* im BCM nur bedingt geeignet. Zum einen können aus dieser Option keine Maßnahmen zur Sicherstellung eines kontinuierlichen Geschäftsbetriebs abgeleitet werden. Zum anderen bleibt die Erfüllung von gesetzlichen oder vertraglichen Vorgaben von dieser Risikobehandlungsoption unberührt. Aus denselben Gründen muss auch genau geprüft werden, ob eine Risikoakzeptanz möglich ist. Insbesondere Institutionen, die eine Versorgungssicherheit zu garantieren haben, z. B. im KRITIS-Umfeld, legen daher den Fokus darauf, Risiken, die die kritischen Dienstleistungen betreffen, zu **vermeiden** oder zu **reduzieren,** sofern Sicherheitsvorkehrungen nach Stand der Technik möglich und angemessen sind.

Die weitere Risikobehandlung erfolgt im BCM anhand von Business-Continuity-Strategien und -Lösungen, die im nachfolgenden Kapitel 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-Risikoaspekten 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 11 Geschäftsfortführungsplanung (R+AS)).

10 Business-Continuity-Strategien und -Lösungen (AS)

Die BCM-Risikoanalyse liefert die relevanten Risiken, die durch die zu entwickelnden BC-Strategien vermieden oder reduziert werden sollen. Mithilfe von BC-Strategien muss die Institutionsleitung für den gesamten Geltungsbereich des BCMS strategisch festlegen, wie sie die BC-Planung der zeitkritischen Ressourcen und Geschäftsprozesse gestalten und umsetzen lassen möchte. Die Institution muss geeignete BC-Strategien definieren, die den Handlungsbedarf aus der BCM-Risikoanalyse und der BIA abdecken. Sie kann zu diesem Zweck für jede in der BIA identifizierte Ressourcenkategorie Schwerpunkte vorgeben.

Aufgrund dieser BC-Strategien wird später die BC-Planung der zeitkritischen Ressourcen und Geschäftsprozesse entwickelt. Die BC-Planung kann auf unterschiedliche Art und Weise erfolgen. Findet die BC-Planung je Organisationseinheit separat statt, sind erfahrungsgemäß höhere Koordinationsaufwände, höhere Gesamtkosten oder gar widersprüchliche BC-Planungen zu erwarten. Insofern ist es wichtig, übergreifend nach Lösungen zu suchen, die zudem zu der Ausrichtung der Institution passen.

Hinweis

Für mögliche Beispiele von BC-Strategien kann das Hilfsmittel BC-Strategievorschläge genutzt werden. Zusätzlich kann der oder die BCB weitere Geschäftsprozess- und Ressourcenzuständige der Institution hinzuziehen.

Welche BC-Strategien für die Institution am besten geeignet sind, hängt jedoch nicht ausschließlich von den Anforderungen an die BC-Planung 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 BC-Planung 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 BC-Planung effektiver und effizienter zu gestalten sowie die individuelle Risikosituation zu berücksichtigen.

Synergiepotenzial

Falls es in der Institution bereits Verfahren oder Management-Prozesse gibt, um strategische Entscheidungen vorzubereiten und zu treffen, kann auf diese Prozesse zurückgegriffen werden, 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 42 sind die erforderlichen Schritte in einer Übersicht dargestellt.

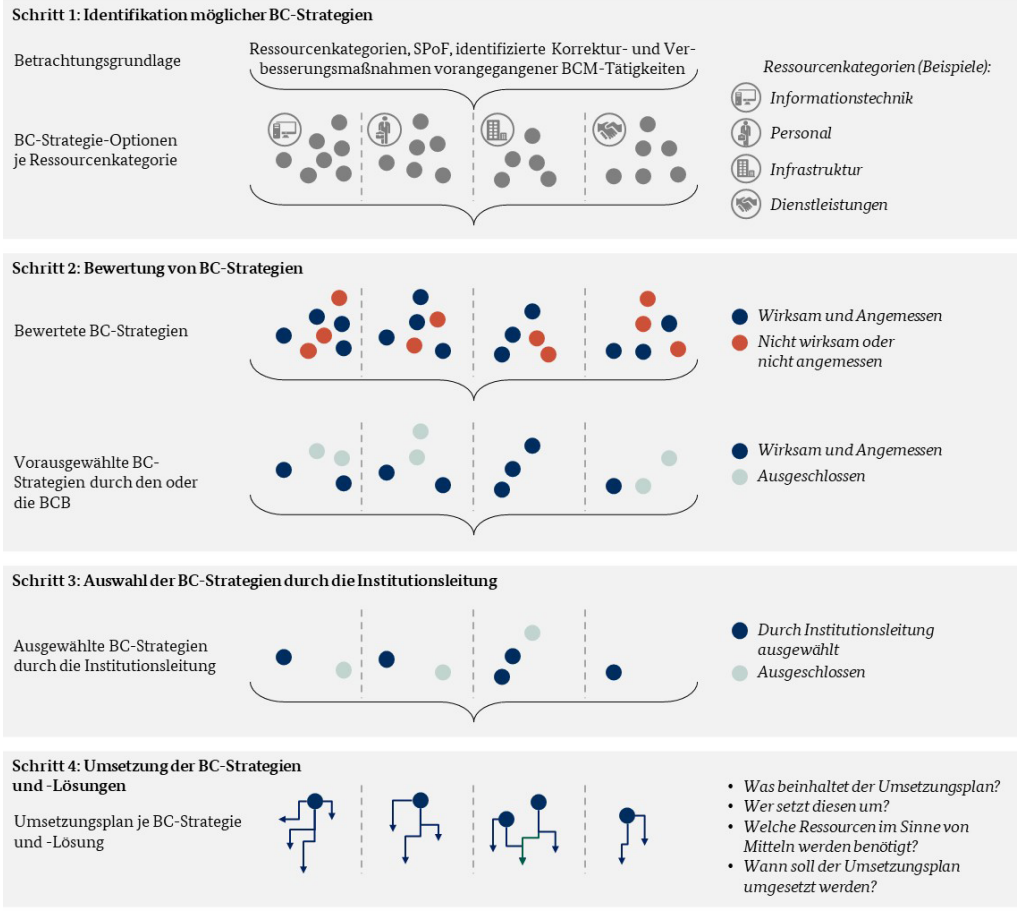

Abbildung 42: BCMS-Prozessschritte zur Entwicklung von BC-Strategien und -Lösungen

Hinweis

Werden BC-Strategien explizit für die Ressourcenkategorie Dienstleistungsunternehmen entwickelt oder sollen Dienstleistungsunternehmen Teil einer BC-Strategie sein, so müssen Besonderheiten wie etwa Verträge oder allgemeine Vorgaben an

Dienstleistungsunternehmen berücksichtigt werden. Die zu beachtenden Besonderheiten werden im Kapitel 14.2 Bewertung und Überwachung von externen Dienstleistungsunternehmen (AS) gesondert erläutert.

Um BC-Strategien zu entwickeln und zu dokumentieren, kann die Dokumentvorlage *Bewertungstabelle für BC-Strategien* aus den Hilfsmitteln verwendet werden. Die einzelnen Schritte werden nachfolgend anhand der Ressourcenkategorien Gebäude und Infrastruktur beispielhaft erläutert.

10.1 Identifikation möglicher BC-Strategien (AS)

Die Institution muss geeignete BC-Strategien definieren, die den Handlungsbedarf aus der BCM-Risikoanalyse abdecken. Üblicherweise übernimmt diese Tätigkeit der oder die BCB.

Hierzu kann sich der oder die BCB 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 Eintrittshäufigkeit eines Ressourcen- oder Geschäftsprozessausfalls durch Vorsorgemaßnahmen zu senken, als auch einen Notbetrieb durch BC-Lösungen sowie Notfallmaßnahmen zu ermöglichen. Sie sollte geeignet sein, den Geschäftsbetrieb mindestens über den abzusichernden Zeitraum mit einem angemessenen Notbetrieb abzudecken.

Liegt bereits eine Wiederherstellungsplanung vor, z. B. aus einem ITSCM oder einem früheren BCM-Zyklus, dann können aus dieser Planung Rückschlüsse gezogen werden, wie lange eine vollständige Wiederherstellung der Ressource voraussichtlich zeitlich in Anspruch nehmen wird. Diese Information kann im BCM genutzt werden, um in der Auswahl von BC-Strategien und -Lösungen die **maximal mögliche Notbetriebsdauer** mit der voraussichtlich notwendigen **Notbetriebsdauer** vergleichen zu können. Die Wiederherstellungsplanung unterstützt somit bei der Identifikation bedarfsgerechter und wirtschaftlicher BC-Strategien und -Lösungen.

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 in der Regel sinnvoll, einen Standort mittels Vorsorgemaßnahmen präventiv soweit abzusichern, dass die Eintrittshäufigkeit 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 Ressourcenkategorie 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.

Die BC-Strategien sollten die noch nicht adressierten Korrekturbedarfe und Verbesserungsmöglichkeiten aus vorangegangenen BCMS-Zyklen angemessen 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.

Beispiel

Bei einem Gebäude- und Infrastrukturausfall könnte innerhalb des Reaktiv-BCMS als Notfallmaßnahme definiert worden sein, dass Organisationseinheiten ohne zeitkritische Tätigkeiten von 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

Das BCM und das ITSCM zielen darauf ab, die Kontinuität des Geschäftsbetriebs sicherzustellen. In der Praxis können bestimmte Schadensereignisse eintreten, die zunächst andere Schutzziele der Institution beeinträchtigen und sich erst in der Folgewirkung negativ auf die Verfügbarkeit auswirken. Dies kann etwa der Fall sein, wenn der IT-Betrieb heruntergefahren werden muss, um zu verhindern, dass sich ein Cyberangriff weiter auswirkt oder die Organisationseinheiten die korrumpierten Daten weiter nutzen können.

Obwohl Cyberangriffe nicht in der BC-Planung des BCM oder ITSCM vollumfänglich abgedeckt werden können, kann es sinnvoll sein, diese themenübergreifenden Aspekte in der Identifikation von BC-Strategien mit zu berücksichtigen und dazu das ISMS mit einzubinden. 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. Jedoch können RTO und RPO bei einem Cyberangriff meist nicht eingehalten werden.

Hinweis

Für die Ressourcenkategorie Dienstleistungsunternehmen sollten die Hinweise zu den unterschiedlichen BC-Strategien aus dem Hilfsmittel Vorschläge zu BC-Strategien *berücksichtigt werden. Insbesondere die BC-Strategie* Ausreichende BC-Fähigkeit des Dienstleistungsunternehmens *geht mit einer umfangreichen Vorgehensweise einher, die normalerweise Grundlage für die Vertragsgestaltung sein sollte und daher bereits bei der Auswahl des Dienstleistungsunternehmens beachtet werden sollte. Darüber hinaus genügt es für Zuliefernde nicht nur, dass diese selbst abgesichert sind, sondern es sollte geprüft werden, ob und wie die Lieferung über die gesamte Lieferkette hinweg sichergestellt werden kann. Alternativ sollte für die BC-Strategie „Redundante Zuliefernde" sichergestellt sein, dass die redundanten Zuliefernden ihre Leistungen aus tatsächlich unabhängigen Lieferketten beziehen.*

Als Ergebnis dieses Abschnitts verfügt der oder die BCB je Ressourcenkategorie über eine Liste möglicher BC-Strategien.

10.2 Bewertung von BC-Strategien (AS)

Nachdem der oder die BCB die grundsätzlich möglichen BC-Strategien identifiziert hat, muss er oder sie bewerten, ob diese für die Institution **wirksam** und **angemessen** sind. Eine BC-Strategie ist dann **wirksam**, wenn durch die umgesetzte BC-Strategie die Eintrittshäufigkeit eines Ausfalls auf ein akzeptables Maß gesenkt werden kann oder die zeitkritischen Geschäftsprozesse innerhalb der RTO 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 wenn der Nutzen die Kosten überwiegt. Um die BC-Strategien bewerten zu können, ist es empfehlenswert, dass der oder die BCB verschiedene Bewertungskriterien festlegt. Anhand der Bewertungskriterien können die BC-Strategien qualitativ und quantitativ bewertet und gegeneinander abgewogen werden. Falls sich frühzeitig herausstellt, dass eine BC-Strategie nicht wirksam oder angemessen ist, ist es nicht notwendig, diese weiter zu bewerten. Im Folgenden werden einige Bewertungskriterien benannt, die bei der Bewertung 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 je nach Risikobereitschaft der Institution nicht hinreichend geeignet oder muss um weitere Maßnahmen ergänzt werden.

Restrisiken: Es muss geprüft werden, welches Restrisiko eines Ressourcenausfalls trotz umgesetzter BC-Strategie bestehen bleibt. Wird etwa ein Ausweichstandort geplant, der

gleichen regionalen Bedrohungen ausgesetzt ist wie der primäre Standort, dann verbleibt ein mögliches Restrisiko, dass beide Standorte durch dasselbe Ereignis betroffen sind. Dies kann z. B. der Fall sein durch eine Bombenentschärfung bei Standorten in derselben Region oder durch Hochwasser eines Flusses bei Standorten im gleichen Hochwassergebiet oder durch ein Erdbeben im selben Erdbebengebiet etc. Hierzu zählt unter anderem auch das Restrisiko bei der BC-Strategie „Redundante Zuliefernde", falls z. B. in beiden Lieferketten der gleiche Zuliefernde auftaucht oder die Lieferketten durch gleiche Bedrohungen gefährdet sind. Ziel der BC-Strategien ist es, die Bedrohungen nach Möglichkeit auszuschließen und daher im Vorhinein die Tätigkeiten auf unterschiedliche Standorte und Services zu verteilen, die ausreichend voneinander getrennt sind. So 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. Entsprechende Aussagen kann beispielsweise das (Risiko-)Controlling treffen. Finanzielle Aufwände beinhalten die Anschaffungskosten, die notwendigen Kosten während und nach einem Notfall sowie die erforderlichen Kosten, um die BC-Strategien aufrechtzuerhalten, z. B. die laufenden Kosten eines Ausweichstandortes oder zusätzliche Kontroll- und Steuerungsaufwände.

Beispiel

Im Falle der BC-Strategie „Ausreichende BC-Fähigkeit des Dienstleistungsunternehmens" wird das Dienstleistungsunternehmen vertraglich daran gebunden, ein für die Institution akzeptables Notbetriebsniveau für vorab definierte Notfälle sicherzustellen. Dies ist mit einem Aufwand auf Seiten des Dienstleistungsunternehmens verbunden und wird daher in der Regel als zusätzliche Kostenposition mit in die Leistung einberechnet. Als Folge erhöhen sich die Kosten für die beauftragende Institution. Für diese entsteht zudem ein Kontroll- und Steuerungsaufwand, um die vertraglich festgelegte BCM-Fähigkeit des Dienstleistungsunternehmens fortlaufend zu bewerten und zu überwachen.

Hinweis

Im Rahmen der Ressourcenplanung des BCMS (siehe 4.5 Ressourcenplanung (R+AS)) hat die Institutionsleitung den oder die BCB 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. Es ist daher wichtig, BC-Strategien, die das vorhandene Budget des BCMS übersteigen, nicht bereits im Vorhinein auszuschließen. Sofern der Nutzen der BC-Strategie die entsprechenden

finanziellen Ressourcen rechtfertigt, ist es sinnvoll, diese stattdessen auch weiterhin in der Auswahl der BC-Strategien zu berücksichtigen.

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 die allgemeine Risikobereitschaft der Institutionsleitung berücksichtigen. Mögliche interne und externe Anforderungen wurden bereits mit den erweiterten Rahmenbedingungen zum BCMS erfasst (siehe 4.2 *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 sind oder der Normalbetrieb wiederhergestellt ist. Die maximal mögliche Notbetriebsdauer sollte mindestens den abzusichernden Zeitraum abdecken (siehe 3.2.3 *Abzusichernder Zeitraum durch ein BCMS (R+AS)*).

Die maximal mögliche Notbetriebsdauer ist darüber hinaus von Bedeutung, weil 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 infolgedessen Nachteile in der Kommunikation im Normalbetrieb zu erzeugen.

Die BC-Strategie „Mobiles Arbeiten" kann möglicherweise nur umgesetzt werden, wenn die damit verbundenen rechtlichen Gegebenheiten mit den jeweiligen Arbeitnehmervertretenden 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, so könnte dies in der Folge zu Effizienzverlusten oder einem mangelnden Wissensaustausch der beteiligten Mitarbeitenden führen, Aber es können auch neue Risiken entstehen, die unabhängig von einem zweiten Standort sind, beispielsweise Abweichungen zu Vorgaben an den Arbeitsschutz oder Verletzungen der Schutzziele der Informationssicherheit. Solche Risiken werden empfehlenswerter Weise mittels einer übergreifenden Risikoanalyse gegeneinander abgewogen.

Entstehender Zusatznutzen: Es wird empfohlen, zu prüfen, ob die betrachteten BC-Strategien auch im Normalbetrieb zu Verbesserungen führen oder positive Seiteneffekte auf Schnittstellen und andere Aspekte haben, z. B Einkaufsvorteile. So kann der oder die BCB 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, z. B. um flexibel von unterschiedlichen Standorten aus arbeiten zu können. Infolgedessen könnte die BC-Strategie 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 sich die Möglichkeit, zukünftig flexibel arbeiten zu können, positiv auf das jeweilige Geschäftsmodell auswirken. Die BC-Strategie wäre somit nicht nur im Rahmen der BC-Planung sinnvollerweise weiter zu betrachten, sondern könnte auch in weiteren Themenbereichen der Institution zu strategischen Vorteilen führen.

Einschätzung Verhältnis Kosten-Nutzen-Risiko: Die Entscheidung für oder gegen eine BC-Strategie ergibt sich aus der Abwägung der entstehenden Kosten im Verhältnis dazu, wie sehr die Eintrittshäufigkeit oder das Schadenspotenzial des Risikos einer Geschäftsunterbrechung reduziert werden können. Eine BC-Strategie kann dann als sinnvoll betrachtet werden, wenn die Kosten für ihre Umsetzung und ihren Betrieb gerechtfertigt sind, um das Risiko zu minimieren. Ferner ist es empfehlenswert, einen möglichen zusätzlichen Nutzen in der Kosten-Nutzen-Risiko Abwägung zu berücksichtigen.

Um die notwendigen Informationen zu erheben, kann der oder die BCB beispielsweise auf die Ressourcen- und Prozesszuständigen zugehen, in deren Zuständigkeitsbereich die

BC-Strategien umgesetzt werden. Auch kann er oder sie mit Anbietern entsprechender Lösungen in Kontakt treten.

Die Bewertung der BC-Strategien kann in der Dokumentvorlage *Bewertungstabelle BC-Strategien* aus den Hilfsmitteln dokumentiert werden. Tabelle 33 zeigt beispielhaft die bewertete BC-Strategie für „Mobiles Arbeiten“:

Beispiel

Bewertungskriterium	***Bewertung der BC-Strategie „Mobiles Arbeiten“***
Einhalten der RTO	*Mitarbeitende 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.*
Restrisiken	*Diese BC-Strategie greift nicht bei Feuer. Fällt der Standort etwa durch Feuer tagsüber aus, so stehen Ressourcen, die aktuell im Gebäude verwendet werden, im Notfall nicht zur Verfügung und werden gegebenenfalls zerstört.* *Falls Mitarbeitende ihre Laptops nicht immer über Nacht oder am Wochenende mit nach Hause nehmen, dann werden diese auch bei einem Feuer in der Nacht oder am Wochenende zerstört werden.* *Siehe BC-Strategie „Feuer“ für den Umgang mit diesem Risiko.*
Finanzielle Aufwände	*Alle in zeitkritische Geschäftsprozesse eingebundenen Mitarbeitenden benötigen entsprechendes Equipment. Für die Arbeit außerhalb der Organisation müssen die technischen Voraussetzungen geschaffen werden. Schätzung:* *Erstbeschaffung: 100.000€* *Aufrechterhaltung der Infrastruktur: 10.000€ pro Jahr*
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 Arbeitnehmendenvertretungen abgestimmt werden, die auch die gesetzlichen Anforderungen berücksichtigt.*
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.*

Bewertungskriterium	***Bewertung der BC-Strategie „Mobiles Arbeiten“***
Entstehender Zusatznutzen	*Mitarbeitenden könnte es ermöglicht werden, auch im Normalbetrieb „Mobiles Arbeiten“ zu nutzen. So würden die vorhandenen Arbeitsflächen des Unternehmens selbst bei einer wachsenden Zahl an Mitarbeitenden ausreichend bleiben.*
Einschätzung Verhältnis Kosten-Nutzen-Risiko	*Die Auswirkungen auf den Geschäftsbetrieb bei Ausfall des Bürogebäudes sinken auf nahezu null. Gleichzeitig erhöht sich die Arbeitsflexibilität. Die Kosten der Lösung zum mobilen Arbeiten fallen gering aus, da parallel Kosten zum Betrieb des Bürogebäudes reduziert werden, u. a. geringere Strom-, Heiz- und Wasserkosten. Feste Arbeitsplätze können teilweise eingespart werden.*

Tabelle 33: Beispiel für die Bewertung der BC-Strategie „Mobiles Arbeiten“

Als Ergebnis erhält der oder die BCB eine Übersicht prinzipiell sinnvoller BC-Strategien und kann ersehen, inwieweit diese sowohl wirksam als auch angemessen sind. Es ist empfehlenswert, dass die Rolle BCB die aus ihrer Sicht passendsten BC-Strategien vorauswählt. Dies erleichtert es der Institutionsleitung, die bestmöglich geeignete BC-Strategie festzulegen. Dazu ist es hilfreich, dass der oder die BCB prüft, welche der BC-Strategien die Anforderungen an die BC-Planung sowie die Rahmenbedingungen der Institution bestmöglich vereinen.

Nachdem der oder die BCB die BC-Strategien geprüft hat, kann er oder sie je Ressourcenkategorie eine oder mehrere BC-Strategien vorauswählen. Insbesondere wenn die BC-Strategien nicht von allen Organisationseinheiten gleichermaßen genutzt werden können, kann es sinnvoll sein, mehrere prinzipiell mögliche BC-Strategien vorzuschlagen.

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 Eintrittshäufigkeit zu senken, dass eine kritische Menge an Mitarbeitenden 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, z. B. 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 oder die BCB für jede Ressourcenkategorie über mindestens eine mögliche BC-Strategie, die der Institutionsleitung im folgenden Schritt vorgestellt werden muss.

10.3 Auswahl der BC-Strategien durch die Institutionsleitung (AS)

Nachdem der oder die BCB 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 beziehungsweise den Nutzen der BC-Strategien sowie die erwarteten Kosten und die eigene Risikobereitschaft gegeneinander abwägen.

Es ist empfehlenswert, die BC-Strategien im Rahmen einer Entscheidungspräsentation vorzustellen und abzustimmen. Die Entscheidungspräsentation ermöglicht es dem oder der BCB, 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 an bestimmten Stellen zum Thema BC-Strategien mit einbezogen wird, ist es empfehlenswert, dass der oder die BCB zu Beginn der Entscheidungspräsentation auf die Ziele der BC-Strategien eingeht. Er oder sie 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 BC-Planung durch die BC-Strategien abgesichert werden muss, kann der oder die BCB die betrachteten Ressourcenkategorien und Teilkategorien vorstellen. Er oder sie 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 oder die BCB die empfohlenen BC-Strategien vorstellen sowie die jeweiligen Vor- und Nachteile erläutern. Hierbei kann er oder sie 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 BC-Planung 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 zu übernehmen bereit ist.

Sofern zeitkritische Prozesse durch Dienstleistungsunternehmen oder in Lieferketten erbracht werden, müssen BC-Strategien ausgewählt werden, die eine angemessene Leistungserbringung im Notfall sicherstellen. Hierzu ist es empfehlenswert, die weitreichenden Erläuterungen in dem Hilfsmittel *Vorschläge zu BC-Strategien* zu berücksichtigen. Dort wird näher erläutert, welche Auswirkungen je nach gewählter BC-Strategie auf unterschiedliche Phasen des PDCA-Zyklus im BCMS bestehen.

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 Institutionsleitung entscheidet sich, die Bürogebäude durch folgende BC-Strategien abzusichern:

- *Mitarbeitende, die mobil arbeiten können, sollen mit entsprechender Technik ausgestattet werden, um im Falle eines Gebäudeausfalls zu Hause arbeiten zu können.*
- *Falls kein „Mobiles Arbeiten" möglich ist, verdrängen Mitarbeitende mit zeitkritischen Aufgaben andere Mitarbeitende 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 Eintrittshäufigkeit eines Ausfalls auf ein akzeptables Niveau gesenkt und das verbleibende Restrisiko durch die Institutionsleitung übernommen wird. Als Vorsorgemaßmaßnahmen werden zusätzlich zu den rechtlich verbindlichen Maßnahmen, z. B. Brandschutz, weitere Maßnahmen, z. B. 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 oder die BCB, einen Umsetzungsplan zu erstellen. Sollte aus Sicht der Institutionsleitung keine der vorgeschlagenen BC-Strategien ausreichend wirksam oder angemessen erscheinen, kann sie den oder die BCB 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 9 *BCM-Risikoanalyse (AS)*).

10.4 Umsetzung der BC-Strategien und -Lösungen (AS)

Nachdem die Institutionsleitung die BC-Strategien freigegeben hat, muss festgelegt werden, wer für die Umsetzung zuständig ist und wer das hierzu notwendige Fachwissen beisteuern kann. Gemeinsam mit dem oder der BCB können diese Personen abstimmen, wie die BC-Strategien umgesetzt werden. Hierzu ist es empfehlenswert, zunächst zu prüfen, aus welchen Vorsorgemaßnahmen, BC-Lösungen und Notfallmaßnahmen sich die ausgewählten BC-Strategien zusammensetzen. 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 Kontaktpersonen betreffen. Falls im Falle von Outsourcing die BC-Strategie *Ausreichende BC-Fähigkeit des Dienstleistungsunternehmens* gewählt wird, muss die Institution zusätzlich die erwarteten BC-Fähigkeiten der relevanten, zeitkritischen Dienstleistungsunternehmen anhand von BC-Anforderungen definieren und bewerten (siehe Hilfsmittel *BC-Strategievorschläge*).

Beispiel

Eine Institution möchte die BC-Strategie eines Ausweichstandortes im Rahmen eines Projektes umsetzen. Als beteiligte Projektkontaktpersonen 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 sowie*
- *das Projektmanagement-Büro, um das Projekt mit dem oder der BCB übergreifend zu steuern.*

Nachdem der oder die BCB die jeweiligen Ressourcenzuständigen ermittelt hat, muss ein Umsetzungsplan erstellt werden. Erfahrungsgemäß wird dieser von den Ressourcenzuständigen erstellt. Der Umsetzungsplan muss die konkret benötigten Ressourcen und Tätigkeiten dokumentieren, die benötigt werden, um die ausgewählten BC-Strategien umzusetzen. Zu diesem Plan gehören mindestens die folgenden Inhalte:

- 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 inklusive der benötigten Dienstleistungsunternehmen

- 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 beschlossenen Maßnahmen durch die Zuständigen umgesetzt werden. Sie sollten im festgelegten Zeitraum umgesetzt werden.

Der oder die BCB sollte die Umsetzung dieser Maßnahmen steuern und kontrollieren. Hierzu ist der Maßnahmenplan ein sehr geeignetes Mittel (siehe 15.1 *Vorbereitung eines BCM-Maßnahmenplans (R+AS)*). Die Notfallmaßnahmen werden im Rahmen der Geschäftsfortführungsplanung sowie Wiederanlaufplanung behandelt (siehe Kapitel 11 *Geschäftsfortführungsplanung (R+AS)* und Kapitel 12 *Wiederanlauf- und Wiederherstellungsplanung (AS)*).

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 auf einem abgestimmten Notbetriebsniveau wieder in Betrieb nimmt, beispielsweise durch umgesetzte BC-Lösungen oder Ersatzlösungen.

Innerhalb von **Wiederherstellungsplänen (WHP)** wird dokumentiert, wie bei Ressourcenausfall der Normalzustand auf Ressourcenebene wieder erreicht werden kann.

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 43 verdeutlich die Beziehung der Dokumente untereinander.

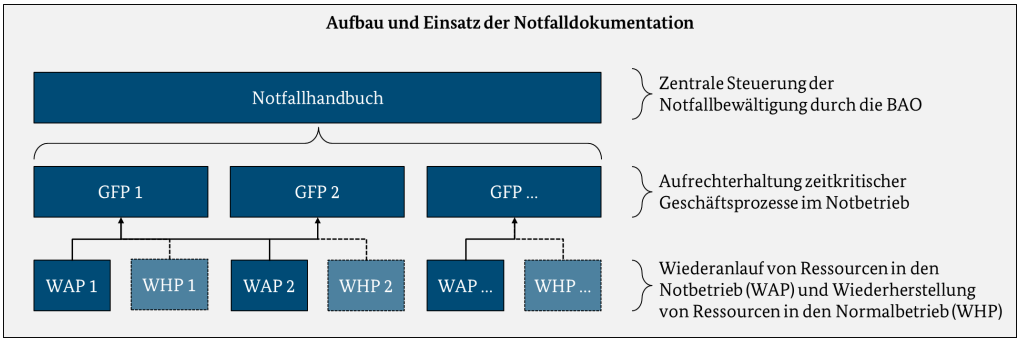

Abbildung 43: Aufbau und Einsatz des Notfallhandbuchs

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.

11 Geschäftsfortführungsplanung (R+AS)

Innerhalb der Geschäftsfortführungspläne (GFPs) wird dokumentiert, wie, d. h. mit welchen Notfallmaßnahmen, die Institution auf der Prozessebene auf eine Geschäftsunterbrechung reagiert. Für alle zeitkritischen Geschäftsprozesse muss eine Geschäftsfortführungsplanung dokumentiert werden.

Die Geschäftsfortführungsplanung im **Reaktiv-BCMS** strebt an, konkrete Notfallmaßnahmen zu beschreiben, mit denen zeitkritische Geschäftsprozesse innerhalb der jeweiligen RTO auf dem in der BIA definierten Notbetriebsniveau wiederaufgenommen oder fortgeführt werden können. Das Reaktiv-BCMS beschränkt sich jedoch auf Notfallmaßnahmen, die mit den vorhandenen Mitteln und Ressourcen der Institution möglich sind oder durch kurzfristig umsetzbare Investitionen realisiert werden können.

R

Im Rahmen der Geschäftsfortführungsplanung im **Aufbau- und Standard-BCMS** beschreibt die Institution, wie sie im Notfall die festgelegten BC-Strategien und -Lösungen auf Prozessebene anwenden wird. Dies gilt auch unabhängig davon, ob gemäß der Risikoanalyse nur ein geringes Risiko besteht, dass der Geschäftsprozess oder auch die zugrundeliegenden Ressourcen ausfallen könnten.

Sofern die Institution bereits über GFPs verfügt, die etwa im Rahmen des Reaktiv-BCMS erstellt wurden, müssen die bestehenden Notfallmaßnahmen überprüft werden. Die Notfallmaßnahmen müssen den im Aufbau- oder Standard-BCMS festgelegten BC-Strategien und -Lösungen entsprechen und angepasst werden, falls dies erforderlich ist.

AS

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

Um die GFPs zu dokumentieren, kann die Dokumentvorlage *Geschäftsfortführungsplan* aus den Hilfsmitteln verwendet werden. Anhand dieser Dokumentvorlage werden einige in diesem Kapitel aufgeführten Beispiele und Hinweise dargestellt.

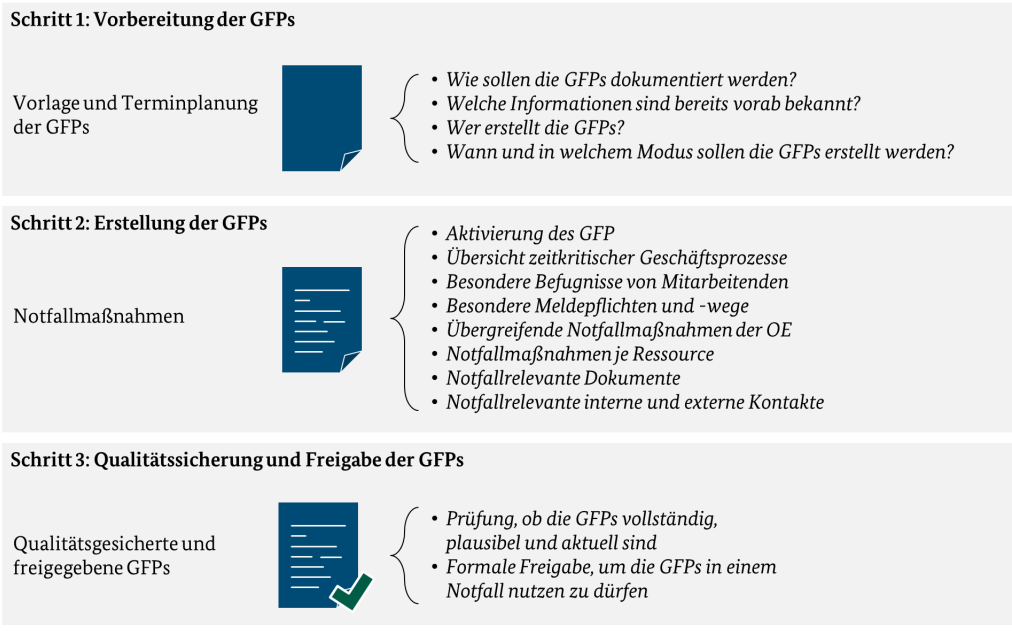

Abbildung 44: BCM-Prozessschritte zur Geschäftsfortführungsplanung

Die Abbildung 44 gibt einen Überblick über die notwendigen Schritte zur Vorbereitung, Erstellung sowie Qualitätssicherung und Freigabe der GFPs. Diese werden in den folgenden Kapiteln näher beschrieben.

11.1 Vorbereitung der GFPs (R+AS)

Eine effektive Vorbereitung der GFPs ist die Voraussetzung dafür, dass

- die GFPs effizient, vergleichbar und valide erstellt werden können,
- die Teilnehmenden optimal auf die Fragestellungen vorbereitet werden,
- die Verfügbarkeit der Pläne im Notfall gewährleistet ist sowie
- im Notfall die Leser die GFPs gut lesen und schnell anwenden können.

Es ist empfehlenswert, dass die Vorbereitung durch die Rolle BCB erfolgt, da diese über das notwendige Fachwissen zum BCM-Prozess verfügt und diesen zeitlich steuert. Der oder die BCB kann vorbereitende Tätigkeiten ganz oder teilweise an weitere Rollen im BCM delegieren, z. B. an lokale BCBs, BCKs oder ein BC-Vorsorgeteam (siehe 4.3 *Definition der BC-Aufbauorganisation (R+AS)*). Die Aufgaben in der Vorbereitung der GFPs werden in den nachfolgenden Unterkapiteln näher erläutert.

11.1.1 Aufteilung der GFPs

Es ist wichtig, dass der oder die BCB festlegt, 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 oder Organisationseinheit erstellt werden. Ferner könnten GFPs auch weiter anhand von Ausfallszenarien aufgeteilt werden. Entscheidend für eine schnelle Reaktion 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 Kontaktpersonen, 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 oder die BCB sollte daher die Aufteilung der GFPs im Rahmen der Erstellung der GFPs mit den entsprechenden Kontaktpersonen diskutieren und gegebenenfalls den Geltungsbereich des GFP anpassen oder in mehrere GFPs aufteilen.

Um die Erläuterungen in den folgenden Kapiteln zu vereinfachen, wird davon ausgegangen, dass die GFPs entsprechend den Organisationseinheiten aufgeteilt wurden. Werden die GFPs in der Institution anderweitig aufgeteilt, so sollten die Inhalte dieses Standards angepasst auf die eigene Vorgehensweise angewendet werden.

11.1.2 Erstellung einer GFP-Dokumentvorlage

Um die Geschäftsfortführung im Notfall zu erleichtern, sollte der oder die BCB sicherstellen, dass die GFPs einheitlich aufgebaut und nachvollziehbar dokumentiert sind. Hierzu sollte eine GFP-Dokumentvorlage 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 oder 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 Normalbetriebs zweckentfremdet oder mit anderen Themen vermischt wird.

Der **Aktivierungsprozess,** die **gesonderten Rechte und Pflichten der Mitarbeitenden** sowie die **besonderen Melde- und Berichtspflichten** werden in Kapitel 11.2.1 *Festlegung übergreifender Maßnahmen (R+AS)* näher erläutert.

Innerhalb des GFP müssen alle **zeitkritischen Geschäftsprozesse** einer Organisationseinheit sowie deren MTPD und RTO dokumentiert werden. Die Dokumentation hat zum Ziel, dem Stab im Notfall eine Übersicht über die zeitkritischen Geschäftsprozesse im Geltungsbereich sowie deren MTPD und RTO 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 und RTOs sowie die RPOs und RPAs müssen innerhalb des GFP dokumentiert werden. Aufgeteilt nach möglichem Ressourcenausfall 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, vor allem im Notfall erreichbare Telefonnummern. Dies sind z. B. die Kontaktdaten von Mitarbeitenden aus anderen Fachbereichen, von internen oder externen Fachleuten sowie von innerhalb der Organisationseinheit benötigten Dienstleistungsunternehmen. 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 ausfall-

sicher 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. In einem Notfall kann durch die zielgerichteten 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 sichergestellt werden, dass die Ablageorte entsprechend dem Schutzbedarf 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.

11.1.3 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, die RTO und das Notbetriebsniveau jedes gelisteten Geschäftsprozesses sowie
- die zeitkritischen Ressourcen mit ihrer jeweiligen RTA, RTO sowie RPA und 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.

11.1.4 Planung der GFP-Erstellung

Die Geschäftsfortführungsplanung kann weitestgehend analog zum Vorgehen in der BIA organisiert werden (siehe 7.1.4 *Planung der BIA-Erhebung (*R+AS*)*). Insbesondere, wenn GFPs erstmalig erstellt werden, ist es empfehlenswert, dass der oder die BCB dies im Rahmen von Workshops durchführt. Er oder sie 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 Teilnehmendenkreis bleibt so überschaubar, kann jedoch bei Bedarf durch weitere Prozess- und Ressourcenfachleute ergänzt werden.

11.2 Erstellung der GFPs (R+AS)

In diesem Kapitel wird beschrieben, wie die Inhalte der GFPs erarbeitet werden. Insbesondere müssen folgende Inhalte im GFP dokumentiert werden:

- Geltungsbereich des GFP
- Zweck und Zielsetzung des GFP
- Aktivierungsprozess des GFP
- die gesonderten Rechte, Berechtigungen und Pflichten der Mitarbeitenden im Geltungsbereich des GFP im Notfall
- alle zeitkritischen Geschäftsprozesse und deren RTO im Geltungsbereich des GFP
- die identifizierten Abhängigkeiten zu den zeitkritischen Geschäftsprozessen des GFP
- die für die zeitkritischen Geschäftsprozesse des GFP benötigten Ressourcen und deren RTO/RPO
- organisatorische Notfallmaßnahmen zur Geschäftsfortführung
- die im Notfall relevanten Kontakte oder Referenzen auf diese

Zusätzlich ist es empfehlenswert, die Melde- und Berichtspflichten im Notfall im GFP zu dokumentieren:

Falls auf Informationen in anderen Dokumenten verwiesen wird, müssen diese Dokumente im GFP nachvollziehbar referenziert werden. Im GFP muss beschrieben werden, wie die relevanten Mitarbeitenden im Notfall alarmiert und informiert werden.

11.2.1 Festlegung übergreifender Maßnahmen (R+AS)

Die Festlegung übergreifender 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 **Mitarbeitenden 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 5.2.3 *Alarmierung der BAO (R+AS)* 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 Bewältigungsteams, weitere Mitarbeitende, externe Fachleute 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 5.5.1 *Konstituierung und Auflösung der BAO (AS)* 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 Mitarbeitenden im Geltungsbereich des GFP **besondere Rechte und Pflichten** zuzuteilen. Diese beschreiben etwa, welche gesonderten Zuständigkeiten und Zugangs-, Zutritts- und Zugriffs-Rechte Mitarbeitenden 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 GFPs aus, können **besondere Melde- und Berichtspflichten an interne und externe Stellen** bestehen. Diese Meldepflichten sollten innerhalb des GFP dokumentiert werden, sofern sie 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 und Kundinnen sowie dienstleistende und zuliefernde Institutionen, die für die Dauer des Notfalls gesondert informiert werden. Dies kann beispielsweise häufigere Meldungen oder Berichte umfassen oder gesonderte Inhalte der Meldungen. Es ist empfehlenswert, folgende Informationen zu beschreiben:

- Stelle, an die gemeldet oder berichtet werden soll
- Rolle, die melden oder berichten soll
- Medium, über das gemeldet oder berichtet werden soll
- Inhalt, der gemeldet oder berichtet werden soll
- Zeitpunkt oder Häufigkeit, zu dem oder in der gemeldet oder berichtet werden soll

Anhand der BIA wurden im **Aufbau- und Standard-BCMS** bereits zeitkritische Prozessabhängigkeiten identifiziert. Falls es wichtig ist, zeitliche Reihenfolgen einzuhalten, in denen voneinander abhängige Geschäftsprozesse in einem Notbetrieb anlaufen, sollten diese im GFP dokumentiert oder referenziert werden.	**AS**

11.2.2 Entwicklung von Notfallmaßnahmen im Reaktiv-BCMS (R)

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. Einfache 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 einer Umsetzungsfrist aufgenommen und innerhalb dieses Zeitrahmens umgesetzt werden (siehe 11.3 *Qualitätssicherung und Freigabe der GFPs (R+AS)*). Ferner sollte in den GFPs selbst beschrieben werden, wie die BC-Lösungen im Notfall konkret angewendet werden. 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 wird die Durchführung der Notfallmaßnahmen dauern?
- Welche Voraussetzungen müssten gegeben sein, um die Notfallmaßnahmen durchführen zu können?
- Welche Reaktionen werden von anderen erwartet?

Hinweis

Obwohl im Reaktiv-BCMS keine BC-Strategien als solche entwickelt werden, kann es hilfreich sein, sich im Hilfsmittel Vorschläge zu BC-Strategien einen Überblick über mögliche BC-Lösungen und Maßnahmen zu verschaffen. Dort sind einige Beispiele für BC-Strategien und Lösungen, die möglicherweise keine Investitionen erfordern.

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

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

- In manchen Fällen kann möglicherweise durch Ausweich- oder Ersatzressourcen dieselbe Funktionalität und Leistungsfähigkeit wie im Normalbetrieb erreicht werden, z. B. anhand von Redundanzkonzepten für die IT.
- In anderen Fällen 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:

- In manchen Fällen können möglicherweise Ausweich- oder Ersatzressourcen innerhalb der geforderten RTO tatsächlich zur Verfügung gestellt werden.
- In anderen Fällen 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 zwei 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 in dieser Zeit das Notbetriebsniveau.

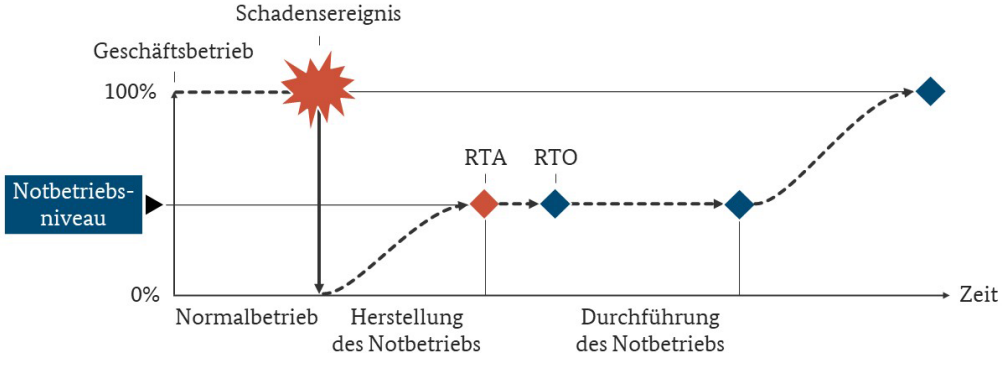

Abbildung 45: Fall 1: RTA ≤ RTO und das Notbetriebsniveau wird erreicht

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 dazu weitere Schritte im Notfall durch die Organisationseinheit erforderlich sind, müssen diese im GFP dokumentiert werden. Wird im Notbetrieb eine Ersatzressource bereitgestellt, z. B. durch das Facility Management oder das ITSCM, dann muss die Organisationseinheit zusätzlich beschreiben, wie diese aus Sicht der Organisationseinheit eingebunden und genutzt werden kann. Sie muss 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, ist es empfehlenswert, dass die Organisationseinheit zusätzlich Maßnahmen beschreibt, die diese Nacharbeiten identifizieren und behandeln.

Beispiel 1: 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 zum Wiederanlauf des IT-Systems 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 Organisations-

einheit auf einer Annahme. Beides wird dokumentiert und die Annahme wird überprüft, sobald die Erkenntnisse aus dem durchgeführten Funktionstest vorliegen.

Beispiel 2: Ausfall eines Gebäudes

Für einen Gebäudeausfall wird der Organisationseinheit eine gleichwertige Ausweichlokation zur Verfügung gestellt. Für alle Mitarbeitenden mit zeitkritischen Aufgaben stehen ausreichend Arbeitsplätze mit den benötigten Arbeitsmaterialien zur Verfügung. Die Organisationseinheit definiert dazu innerhalb ihrer Notfallmaßnahmen, wie sie diese Mitarbeitenden an die Ausweichlokation entsendet und dort die Arbeit wiederaufnimmt. Dies entspricht der „Herstellung des Notbetriebs" und umfasst z. B. Transportmöglichkeiten abzustimmen, notwendige Zutrittsberechtigungen zu erhalten oder die Mitarbeitenden 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 und*
- *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 beispielsweise Mitarbeitende 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: Die vorgegebenen Parameter werden nicht erreicht

In diesem Fall ist die zugesicherte Wiederanlaufzeit länger als die RTO oder das geforderte Notbetriebsniveau wird nicht erreicht. Im ungünstigsten Fall werden beide Parameter gleichzeitig nicht erfüllt.

Abbildung 46 zeigt den Fall, dass zwar die **RTA erreicht** wird, jedoch **nicht das geforderte Notbetriebsniveau**. Dies tritt bei Ersatzressourcen auf, die gegenüber der ausgefallenen Originalressource über einen stark eingeschränkten Funktions- und Leistungsumfang verfügen, der auch nicht im zeitlichen Verlauf auf das geforderte Notbetriebsniveau gesteigert werden kann:

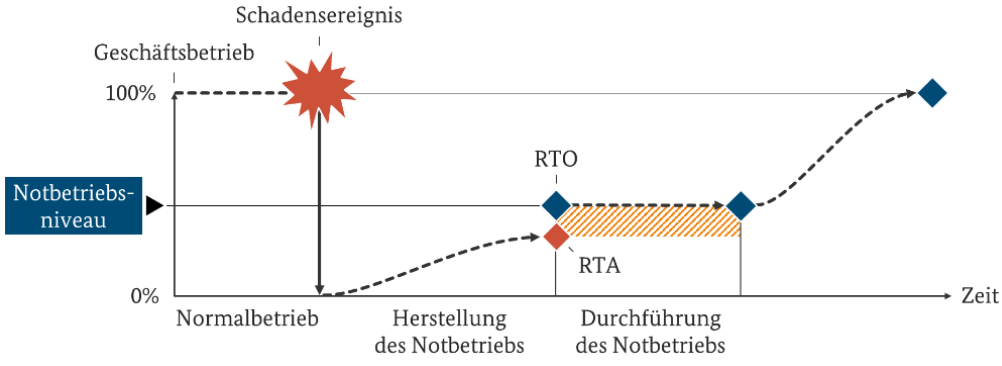

Abbildung 46: Fall 2a: RTA ≤ RTO, jedoch wird das Notbetriebsniveau nicht erreicht

Beispiel: Nichterreichen des Notbetriebsniveaus

Im Falle eines Gebäudeausfalls wurde der Organisationseinheit zugesichert, innerhalb der RTO eine Ausweichlokation zu erhalten. In der Ausweichlokation stehen jedoch nicht genügend Arbeitsplätze für alle Mitarbeitenden mit zeitkritischen Aufgaben zur Verfügung.

Abbildung 47 zeigt den Fall, dass zwar **das Notbetriebsniveau erreicht** wird, jedoch die zugesicherte Wiederanlaufzeit länger ist als die RTO. Dies tritt bei Ersatzressourcen ein, die zwar grundsätzlich über das nötige Notbetriebsniveau verfügen, die jedoch länger für den Wiederanlauf benötigen als gefordert.

Beispiel: RTA > RTO

Im Falle eines Gebäudeausfalls wurde der Organisationseinheit eine Ausweichlokation zugesichert. Die Ausweichlokation steht jedoch erst einen Tag nach Ablauf der RTO zur Verfügung.

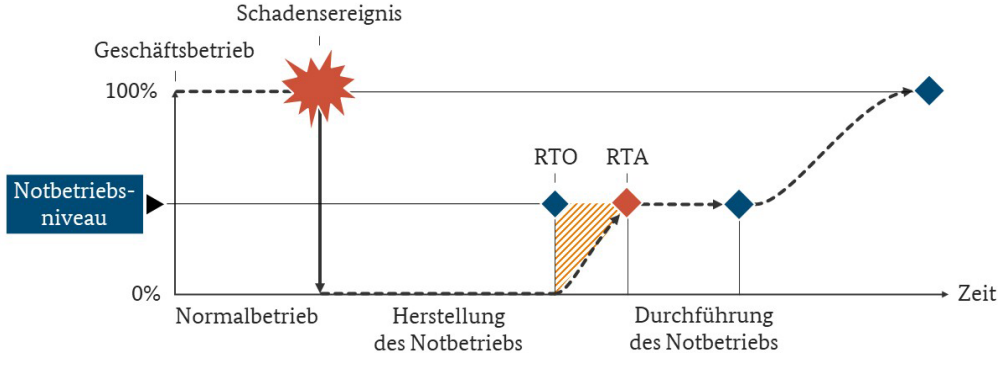

Abbildung 47: Fall 2b: RTA > RTO

Darüber hinaus existieren auch **Mischformen**, wie die folgende Abbildung 48 darstellt:

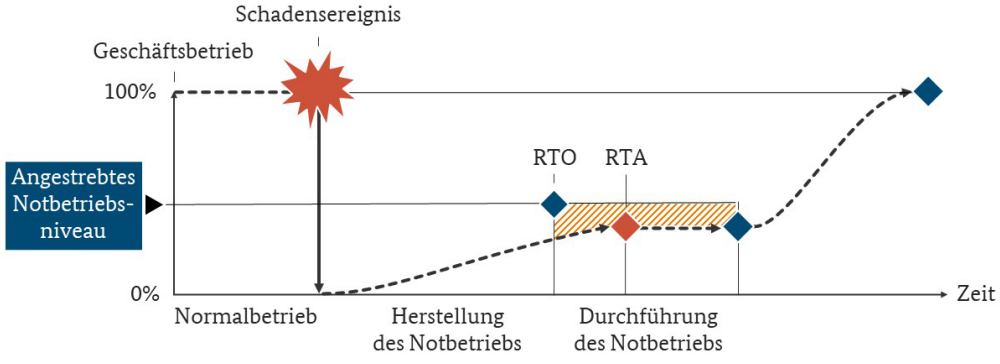

Abbildung 48: Fall 2c: Mischform: Unzureichende RTA + Notbetriebsniveau.

Beispiel: RTA > RTO und Nichterreichen des Notbetriebsniveaus

Im Falle eines Produktionsausfalls wurde der Organisationseinheit zugesichert, dass eine der beiden für das Notbetriebsniveau erforderlichen Produktionsstraßen nach einem Zeitraum, der länger als die RTO ist, zur Verfügung steht.

In allen Ausprägungen des Falls 2 existiert ein erhöhter Schaden, falls die betrachtete Ressource und damit der Geschäftsprozess ausfällt. Die Anforderungen des BCMS werden an dieser Stelle nicht erfüllt. Grundsätzlich gibt es folgende Möglichkeiten, mit dieser Situation umzugehen:

1. Behebung durch Workarounds und Quickfixes
2. Risikoakzeptanz mit Behebung im Aufbau- oder Standard-BCMS

Behebung durch Workarounds und Quickfixes

In vielen Fällen lassen sich das Notbetriebsniveau und die geforderte Wiederanlaufzeit durch überschaubare Investitionen oder schnelle Workarounds erreichen, die nicht vollständig auf den vorhandenen Mitteln aufbauen, jedoch auch nicht einen solchen Umfang wie vollumfängliche BC-Strategien umfassen:

Beispiele

Nichterreichen des Notbetriebsniveaus

Der Ausfall eines Gebäudes wird durch eine Verlagerung der Bürotätigkeiten der Organisationseinheit ins Homeoffice kompensiert. Hierbei wird auch die RTA erreicht. Jedoch wird nicht das geforderte Notbetriebsniveau erreicht, da nicht für alle Mitarbeitenden genügend Lizenzen für die benötigte Webkonferenzplattform zur Verfügung stehen. Diese werden für eine überschaubare Summe zusätzlich erworben, sodass alle Mitarbeitenden im Notbetrieb die Webkonferenzplattform benutzen

können. Diese zusätzliche Maßnahme ermöglicht es, das Notbetriebsniveau zu erreichen.

RTA > RTO

Der Ausfall einer Werkstatt wird durch die Organisationseinheit kompensiert, indem von einem etablierten Dienstleistungsunternehmen eine entsprechende Ausstattung geleast und mit firmeneigenen Werkzeugen an einen firmeneigenen Ausweichstandort transportiert wird. Anschließend wird dort die Ersatzwerkstatt in Betrieb genommen. Hierbei wird die RTA nicht erreicht, weil nicht genügend Transporter zur Verfügung stehen. Diese Lücke wird kompensiert, indem der Vertrag mit dem Dienstleistungsunternehmen um die fehlenden Transporter erweitert wird. Diese Maßnahme ermöglicht es, die RTO zu erreichen.

Hierbei ist es grundsätzlich empfehlenswert, Typ-2-Fälle möglichst durch Workarounds und Quickfixes zu behandeln und somit zu Typ-1-Fällen zu transformieren, die die Anforderungen des BCMS erfüllen. Die dazu erforderlichen Vorsorgemaßnahmen sollten im BCM-Maßnahmenplan (siehe 15.2 *Ableitung von Korrektur- und Verbesserungsmaßnahmen (R+AS)*) beschrieben werden.

Risikoakzeptanz mit Behebung im Aufbau- oder Standard-BCMS

In der Praxis werden in der Regel im Reaktiv-BCMS eine Reihe von Fällen bestehen, in denen die Anforderungen nicht in der geforderten Zeit oder auf dem geforderten Niveau erreicht werden können und gleichzeitig auch keine einfachen Möglichkeiten für Workarounds bestehen. Alternativ kann die Situation eintreten, dass zwar Workarounds möglich sind und auch angewendet werden, aber die die Anforderungen dennoch nicht vollständig erfüllt werden können.

Beispiel

Wie in Abbildung 46: Fall 2a: RTA ≤ RTO, jedoch wird das Notbetriebsniveau nicht erreicht dargestellt und im dazugehörigen Beispiel beschrieben, wurde bei Gebäudeausfall der Organisationseinheit zugesichert, innerhalb der RTO eine Ausweichlokation bereitzustellen. In der Ausweichlokation stehen jedoch nicht genügend Arbeitsplätze für alle Mitarbeitenden mit zeitkritischen Aufgaben zur Verfügung.

Um dies zu kompensieren, entscheidet sich die Organisationseinheit dafür, die vorhandenen Arbeitsplätze in mehreren Schichten zu nutzen. Darüber hinaus werden bestimmte Tätigkeiten für die Dauer des Notbetriebs ausgelassen. Es wird dokumentiert, dass das geforderte Notbetriebsniveau nicht erreicht werden kann. Die notwendigen Nacharbeiten werden durch temporäre Mehrarbeit der Mitarbeitenden kompensiert.

Hinweis

Unter Umständen können mit den vorhandenen Mitteln sowie den Möglichkeiten des Reaktiv-BCMS keine Notfallmaßnahmen konzipiert werden, die ausreichen, um 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. Hierzu muss eine Gesamtübersicht erstellt werden, die alle Lücken des Reaktiv-BCMS und die darin betroffenen Geschäftsprozesse und Ressourcen umfasst. Die Institutionsleitung muss entscheiden, ob sie das Risiko eines potenziellen Prozessausfalls über die MTPD hinaus zum gegenwärtigen Zeitpunkt akzeptiert oder Ad-hoc-Maßnahmen ergreift.

Die Defizite sollten je Ressource als Verbesserungsbedarf im Maßnahmenplan dokumentiert werden (siehe 15.2 Ableitung von Korrektur- und Verbesserungsmaßnahmen (R+AS)). Zusätzlich sollte im GFP selbst dokumentiert werden, dass in diesem Fall die fachlichen Anforderungen nicht erfüllt werden, sodass in einem Notfall die BAO dieses Defizit direkt erfasst.

Fallunterscheidung für unterschiedlich 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 lediglich einzelner Gebäudeteile bedeuten.

Je nach Schweregrad des Ereignisses kann es sinnvoll sein, unterschiedliche Notfallmaßnahmen zu treffen. Bei dem gesamten Ausfall eines Standortes könnte es z. B. 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 ausreichen.

Nicht alle Notfallmaßnahmen müssen neu dokumentiert werden, falls diese bereits leicht verständlich in anderen Dokumenten beschrieben sind. Wenn bereits zutreffende Prozessbeschreibungen oder Arbeitsanweisungen der AAO existieren, kann auf die entsprechenden Textstellen in den bestehenden Dokumenten verwiesen werden. Um schnell auf diese Textstellen zugreifen zu können, sollten alle im GFP aufgeführten Dokumente am Ende des GFP noch einmal in einer Gesamtliste namentlich aufgeführt werden. Zusätzlich sollten 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 die Dokumente gleichzeitig im Notfall zugänglich sind.

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 die Rolle BCB gemeldet werden. Diese muss die identifizierten Lücken und Schwachstellen sowie Annahmen und Verbesserungsbedarfe in einem Maßnahmenplan vorhalten (siehe 15.2 *Ableitung von Korrektur- und Verbesserungsmaßnahmen (R+AS)*). Dadurch kann sichergestellt werden, dass keine Aspekte verloren gehen und alle in einem Aufbau- oder Standard-BCMS wieder aufgegriffen und behandelt werden.

11.2.3 Entwicklung von Notfallmaßnahmen im Standard-BCMS (AS)

Innerhalb der Erstellung der GFPs müssen Notfallmaßnahmen entwickelt und dokumentiert werden, um ausgefallene Geschäftsprozesse in einem definierten Notbetrieb wiederaufzunehmen. Diese werden üblicherweise von den zuständigen Kontaktpersonen 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. Im GFP sollten der Ablauf und die konkreten Tätigkeiten zur Wiederaufnahme der relevanten Geschäftsprozesse sowie die entsprechenden Zuständigkeiten dokumentiert werden. Die Notfallmaßnahmen sollten geeignet sein, die Geschäftsprozesse auf Notbetriebsniveau für die Dauer fortführen zu können, die in den BC-Strategien definiert ist.

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 der Ressourcen abgestimmt werden. Abschließend sollte beschrieben werden, wie die Geschäftsprozesse vom Notbetrieb in den Normalbetrieb überführt werden sollen und wie mit notwendigen Nacharbeiten, beispielsweise 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 (Arbeiten im Notbetrieb)
- Maßnahmen zur Rückführung in den Normalbetrieb (inklusive Nacharbeiten)

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 Mitarbeitenden an den Ausweichstandort entsenden und diese dort die Arbeit wiederaufnehmen. Die Erstellung der GFPs umfasst z. B. Transportmöglichkeiten abzustimmen, notwendige Zutrittsberechtigungen zu erteilen oder zu planen, wie die Mitarbeitenden auf die vorhandenen Notfallarbeitsplätze im Notfall verteilt werden. Darüber hinaus wird festgelegt, welche Maßnahmen für die Dauer des Notbetriebs am Ausweichstandort wichtig sind, z. B. Regelungen dazu,

- *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 z. B. Mitarbeitende 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 mit in den GFP zu übernehmen. So können neben den hauptsächlich anzuwenden Maßnahmen auch alternative Varianten aufgeführt werden.

Der Detailgrad der beschriebenen Maßnahmen sollte 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, ist es empfehlenswert, diese anhand von Checklisten zu dokumentieren.

Werden Notfallmaßnahmen definiert, so 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 lediglich einzelner Gebäudeteile bedeuten. Bei einem gesamten Standortausfall könnte es notwendig sein, sämtliche Tätigkeiten oder eine vorhandene Produktion an einen Ausweichstandort zu verlagern. Fallen hingegen nur einzelne Gebäude-

teile aus, kann die Verlagerung der Arbeitsplätze oder der Produktion innerhalb des Gebäudes oder Standortes ausreichend sein.

Beispiel

Für die Ressource Gebäude besteht in einer Institution die BC-Strategie, Mitarbeitende an eine Aufweichlokation oder in das 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 Mitarbeitenden an den Ausweichstandort. Für den Fall, dass das gesamte Gebäude ausfällt, verlagert sie Mitarbeitende, die mobil arbeiten können, in Home-Offices, da die Kapazität des Ausweichstandorts begrenzt ist. Mitarbeitende, 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. Wenn bereits zutreffende Prozessbeschreibungen oder Arbeitsanweisungen der AAO existieren, kann auf die jeweiligen Textstellen in den bestehenden Dokumenten verwiesen werden. Um schnell auf die entsprechenden Textstellen zugreifen zu können, sollten alle im GFP aufgeführten Dokumente am Ende des GFP noch einmal in einer Gesamtliste namentlich aufgeführt werden. Zusätzlich sollten 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 gleichzeitig die Dokumente auch im Notfall zugänglich sind.

11.3 Qualitätssicherung und Freigabe der GFPs (R+AS)

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-Dokumentvorlage verwendet und bilden die Inhalte alle vorgegebenen Punkte ab? Wurden alle relevanten Inhalte der BIA innerhalb des GFP erfasst und sind Notfallmaßnahmen dazu beschrieben? Sind die Inhalte des GFP aktuell? Unvollständige oder nicht aktuelle 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 sowohl die Angaben innerhalb des GFP als auch die beschriebenen Abhängigkeiten zu anderen GFPs oder WAPs plausibel dargestellt?
- **Aktualität**: Sind die referenzierten Dokumente in der jeweils aktuellen Version hinterlegt? Wurden die relevanten Kontaktpersonen auf Basis einer aktuellen Kontakt-

liste 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 können durch die Qualitätssicherung der Detailgrad und die sprachliche Verständlichkeit 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 13 Üben und Testen (R+AS)).

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 erstellt, qualitätsgesichert und freigegeben sind, ist es 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 oder die BCB die aktualisierten Informationen der Institutionsleitung und dem Risikomanagement mitteilt. Hierdurch kann der Institutionsleitung ein realistischeres Bild über die Risikosituation vermittelt werden als es zu einem früheren Zeitpunkt möglich war.

12 Wiederanlauf- und Wiederherstellungsplanung (AS)

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. Gegebenenfalls wird dies durch ITSCM, Facility Management etc. bereits abgedeckt.

Die **Wiederherstellungsplanung** hat zum Ziel, 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, z. B. von der Art der Ressource, welche Schäden an den Ressourcen entstanden sind und welche Mittel zu ihrer Wiederherstellung zur Verfügung stehen.

Abbildung 49 stellt den Wiederanlauf und die Wiederherstellung anhand einer stark vereinfachten, schematischen Darstellung der Notfallbewältigung gegenüber. Die Wiederherstellung kann prinzipiell parallel oder nach dem Wiederanlauf starten. In der Praxis ist es auch möglich, dass die vollständige Wiederherstellung aus dem Wiederanlauf heraus erfolgt, z. B. wenn eine Ersatzressource die Hauptressource vollständig ersetzt und anschließend im Normalbetrieb weiter eingesetzt wird.

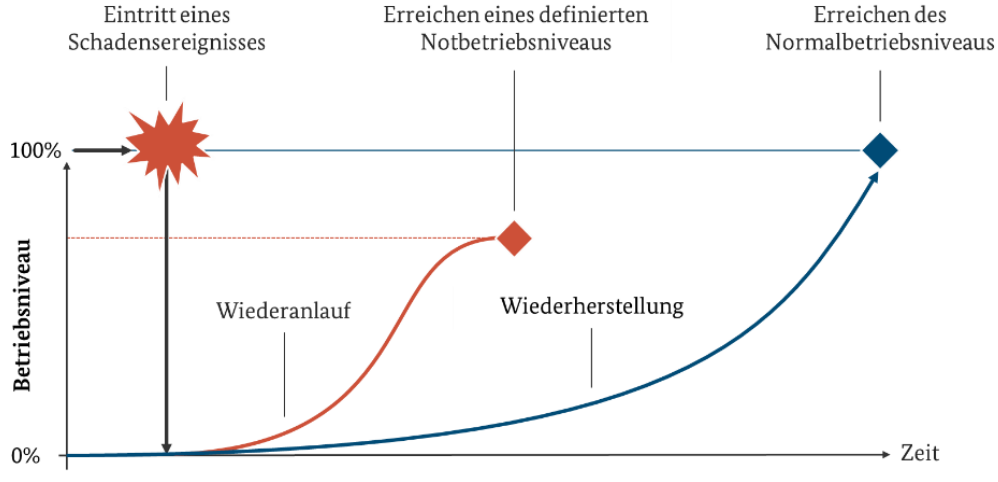

Abbildung 49: Darstellung der Phasen für den Wiederanlauf und die Wiederherstellung

Hinweis

Der englische Begriff „Recovery" wird im deutschsprachigen Raum häufig mit „Wiederherstellung" und im technischen Umfeld gelegentlich mit „Wiederanlauf" übersetzt. Je nach Informationsquelle definiert der festgelegte Begriff die Wiederaufnahme unterbrochener Tätigkeiten entweder mit einer festgelegten Mindestkapazi-

tät oder mit den vereinbarten Minimalanforderungen, wobei letzten Endes immer der Normalbetriebszustand zurückerlangt werden soll. Um sprachlich präziser zwischen einer vollständigen Wiederherstellung des ursprünglichen oder verbesserten Normalbetriebs-Zustands und einem eingeschränkten Notbetrieb unterscheiden zu können, wird im gesamten Standard konsequent zwischen den Begriffen Wiederanlauf und Wiederherstellung unterschieden. Der Wiederanlauf umfasst das Erreichen eines definierten Notbetriebsniveaus. Die Wiederherstellung umfasst das Erreichen des Normalbetriebsniveaus.

Um die Wiederanlaufplanung zu erstellen, kann die Dokumentvorlage *Wiederanlaufplan* aus den Hilfsmitteln verwendet werden. Anhand dieser Dokumentvorlage 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 und jede Mitarbeitende 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 50 einen Überblick über die notwendigen Schritte zur Vorbereitung, Erstellung sowie Qualitätssicherung und Freigabe der Wiederanlaufpläne (WAPs) sowie Hilfestellung für die optionale Wiederherstellungsplanung durch Wiederherstellungspläne (WHPs).

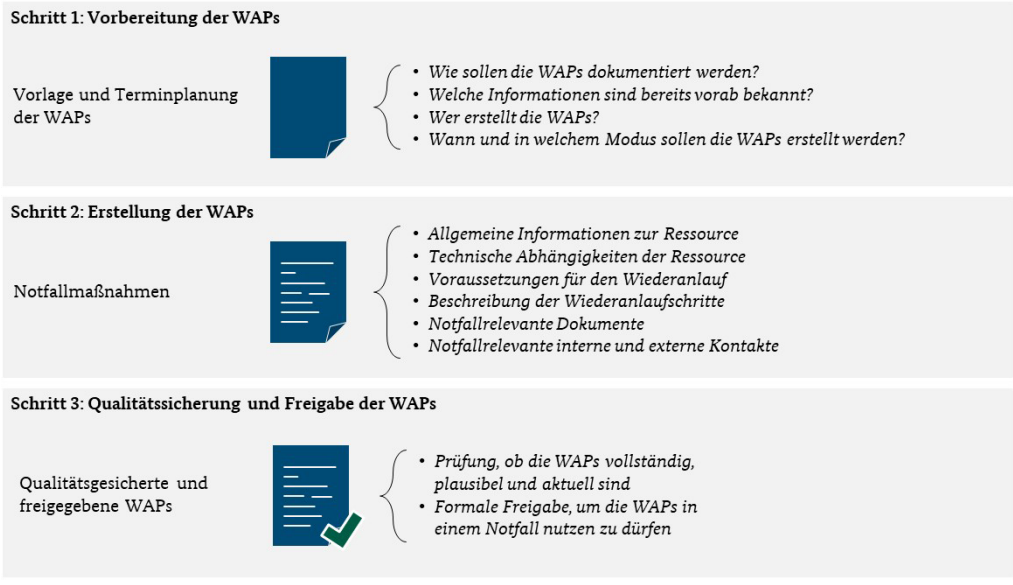

Abbildung 50: BCM-Prozessschritte zur Wiederanlauf- und Wiederherstellungsplanung

12.1 Vorbereitung der WAPs (AS)

Die Vorbereitungsphase ist von großer Bedeutung, um die WAPs effektiv und effizient erstellen zu können. Es ist empfehlenswert, dass die Vorbereitung durch den oder die BCB in Abstimmung mit den Ressourcenzuständigen erfolgt. Falls die Ressourcenzuständigen bereits Vorlagen oder Pläne haben, wie z. B. im ITSCM, können diese übernommen werden, solange die Anforderungen aus dem BCM erfüllt sind. Die Aufgaben in der Vorbereitung der WAPs 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.

12.1.1 Aufteilung der WAPs (AS)

Es ist wichtig, dass der oder die BCB festlegt, wie die WAPs im Hinblick auf die zugrundeliegende Struktur der Ressourcen aufgeteilt werden sollen. Es gibt viele Möglichkeiten, wie WAPs organisatorisch aufgeteilt werden könnten. So könnte ein Plan je einzelner Ressource erstellt werden oder ein Plan kann umfangreichere Ressourcencluster umfassen. Entscheidend für eine schnelle Reaktion ist jedoch, dass

- die zuständigen Stellen die jeweils für ihren Bereich relevanten Informationen erhalten,
- die Verfügbarkeit der Pläne im Notfall gewährleistet ist sowie
- die Übergabepunkte zwischen den Plänen klar geregelt sind.

Hierbei hat es sich in der Praxis bewährt, zunächst einen Plan je Ressource zu erstellen, die von einer zuständigen Stelle bearbeitet wird. Dieses Vorgehen bietet folgende Vorteile:

- Die zuständigen Kontaktpersonen, die den Plan erstellen und aktualisieren, können eindeutig einer abgegrenzten Ressource zugeordnet werden.
- Die Pläne spiegeln die vertraute Umgebung und 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. Es ist daher empfehlenswert, die Aufteilung der Pläne im Rahmen der Erstellung mit den entsprechenden Kontaktpersonen zu diskutieren und gegebenenfalls anzupassen, in mehrere Pläne aufzuteilen oder in verschiedene Pläne zusammenzufassen.

12.1.2 Erstellung einer WAP -Dokumentvorlage (AS)

Um den Wiederanlauf im Notfall zu erleichtern, sollte der oder die BCB sicherstellen, dass die WAPs einheitlich aufgebaut und nachvollziehbar dokumentiert sind. Hierzu kann es hilfreich sein, eine WAP-Dokumentvorlage zu erstellen. Die nachfolgenden Aspekte müssen darin berücksichtigt werden:

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

Zusätzlich müssen auch der **Geltungsbereich und** die **betrachteten Ressourcen** klar dokumentiert werden, sodass der WAP eindeutig gegenüber den weiteren WAPs abgegrenzt werden kann.

Der **Aktivierungsprozess** des WAP muss dokumentiert werden. Dieser beschreibt, wie der WAP offiziell aktiviert wird. Die Definition eines eindeutigen Aktivierungsprozesses ist notwendig, da die Maßnahmen des WAP häufig nicht ohne Weiteres rückgängig gemacht werden können und ein frühzeitiges Auslösen des WAP verhindert werden soll.

Innerhalb des WAP 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 **Voraussetzungen zum Wiederanlauf der Ressource** führen die organisatorischen sowie technischen Bedingungen auf, um die beschriebenen Notfallmaßnahmen initiieren zu können.

Die **Notfallmaßnahmen** stellen den Hauptteil des WAP dar und beschreiben konkreter die notwendigen Schritte, um die spezifische Ressource wiederanlaufen zu lassen und im Notbetrieb fortzuführen.

Hinweis

Damit der Aufwand für die Autoren und Autorinnen 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 und Notbetriebsniveau, sowie möglicherweise benötigte Dokumente, auf die in der Wiederanlaufplanung referenziert wird.

12.1.3 Planung der WAP-Erstellung (AS)

Für die Erstellung der WAPs wird ein hoher Grad an technischem Detailwissen benötigt. Idealerweise wird der WAP daher durch die gleichen Mitarbeitenden erstellt, die im Rahmen eines Notfalls auch die beschriebenen Maßnahmen durchführen.

Abhängig von dem notwendigen Fachwissen kann es erforderlich sein, weitere Fachleute unterstützend hinzuziehen. Dies ist dann erforderlich, wenn für den Wiederanlauf oder die Wiederherstellung der Ressource weitere (Infrastruktur-)Ressourcen oder -Komponenten benötigt werden, die nicht in den Zuständigkeitsbereich des Ressourcenzuständigen fallen oder durch dessen Fachwissen abgedeckt sind.

Ferner sollte gewährleistet werden, dass die verschiedenen WAPs einheitlich strukturiert sind, damit sich im Notfall auch andere Mitarbeitende 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 Dokumentvorlage hinterlegt werden. Alternativ kann der Erstellungsprozess auch im Rahmen eines Workshops durch einen BCM-Experten oder eine BCM-Expertin und die Ressourcenfachleute gemeinsam erarbeitet werden.

Darüber hinaus ist es empfehlenswert, dass bereits an anderer Stelle dokumentierte Inhalte, z. B. in Betriebsdokumentationen, nicht wiederholt, sondern stattdessen referenziert werden. Dies setzt eine Kenntnis dieser Dokumentationen voraus. Wichtig ist, dass die referenzierten Stellen leicht gefunden werden und auch im Notfall für einen sachkundigen Dritten verständlich sind. Auch für referenzierte Dokumente sollte sichergestellt werden, dass diese im Notfall verfügbar und zugänglich und entsprechend des Schutzbedarfs abgelegt sind (siehe 4.4 *Dokumentation (R+AS)*).

12.2 Erstellung der WAPs (AS)

Es ist wichtig, innerhalb der Wiederanlaufplanung alle erforderlichen Rollen und Rolleninhabenden, ihre jeweiligen Vertretenden sowie die benötigten Dienstleistungsunternehmen zu benennen. Dieser Personenkreis kann auch in der Alarmierung und Eskalation berücksichtigt werden, z. B. als definiertes Bewältigungsteam.

Folgende Aspekte müssen in einem WAP oder in aus dem WAP heraus referenzierten Dokumenten möglichst detailliert und konkret beschrieben sein:

- Geltungsbereich des WAP (abgedeckte Ressourcen)
- Zweck und Zielsetzung des WAP
- Aktivierungsprozess des WAP
- die zuständigen Rollen, Rolleninhabende und deren Stellvertretende sowie alternative Wissenstragende jeweils mit ihren aktuellen Kontaktdaten im Geltungsbereich des WAP
- alle für den Wiederanlauf benötigten Ressourcen und deren RTO sowie die benötigten Dokumentationen
- Ablauf und konkrete Tätigkeiten zum Wiederanlauf der Ressource oder relevante Referenzen

Falls auf Informationen in anderen Dokumenten verwiesen wird, MÜSSEN diese Dokumente im WAP nachvollziehbar referenziert werden.

Folgende Aspekte sollten in einem WAP auch möglichst detailliert und konkret beschrieben sein:

- Voraussetzungen zum Wiederanlauf der Ressource (insbesondere die benötigten Rechte und Berechtigungen)
- Weitere Abhängigkeiten zu anderen Ressourcen
- Liste der erforderlichen Dienstleistungsunternehmen
- Funktionstest, ob der Wiederanlauf erfolgreich war und Übergabe in den Notbetrieb

Der Detailgrad der beschriebenen Maßnahmen sollte so gewählt sein, dass eine fachkundige dritte Person in der Lage wäre, den Wiederanlauf anhand des WAP umzusetzen. Die Notfallmaßnahmen müssen geeignet sein, ausgefallene Ressourcen innerhalb der erforderlichen Zeit und auf dem definierten Notbetriebsniveau wiederanlaufen zu lassen. Um die erforderlichen Notfallmaßnahmen zu ermitteln, können die Leitfragen aus Kapitel 11.2.3 *Entwicklung von Notfallmaßnahmen im Standard-BCMS (AS)* als Grundlage verwendet werden.

Synergiepotenzial

Nicht in jedem Fall müssen die Maßnahmen zum Wiederanlauf in einem WAP beschrieben sein. Häufig sind solche Angaben bereits in vorhandenen Dokumentationen zu finden, z. B.

- *ITSCM-Pläne oder IT-Betriebskonzepte (IT-Recovery, Datenwiederherstellung, Failover-Konzept),*
- *eine Pandemieplanung (Maßnahmen zum Umgang mit massivem Personalausfall) sowie*
- *Notfallpläne von Dienstleistungsunternehmen oder Exit-Strategien.*

In diesem Fall können die vorhandenen Dokumente weiter genutzt werden, sofern diese im Notfallhandbuch referenziert und im Notfall verfügbar sind. Es ist wichtig, dabei sicherzustellen, dass alle beschriebenen Anforderungen an WAPs auch in den bestehenden Dokumenten erfüllt werden.

Voraussetzungen zum Wiederanlauf der Ressource

Bevor der Wiederanlauf einer Ressource initiiert werden kann, ist es notwendig, dass die erforderlichen Voraussetzungen und Abhängigkeiten technischer oder organisatorischer Art von anderen Ressourcen erfüllt sind. 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 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

Es ist empfehlenswert, die für den Wiederanlauf der Ressource durchzuführenden Schritte in Form von Handlungsanweisungen zu beschreiben. Es ist auch empfehlenswert, zusätzlich die Schritte mit Abhängigkeiten untereinander sowie parallel ausführbare Schritte zu kennzeichnen, z. B. anhand nummerierter Einträge innerhalb einer Checkliste. Um die WAPs leicht anwenden zu können, ist es darüber hinaus hilfreich, wenn die Beschreibung möglichst eindeutig und nur so ausführlich wie unbedingt notwendig gestaltet ist. Auch Screenshots können dort 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 oder genau referenziert werden, sodass die Information auch leicht in einer Stresssituation wie einem Notfall auffindbar und erfassbar ist.

Alle für den Wiederanlauf benötigten Ressourcen, Dokumentationen und Abläufe sollten in den Plänen aufgeführt werden.

Darüber hinaus sollten die aus dem Notbetrieb der Ressource resultierenden Einschränkungen dokumentiert werden. Dies kann etwa eine eingeschränkte Kapazität der Ressource oder einen reduzierten Funktionsumfang bedeuten.

Erstellung der übergeordneten Wiederanlaufplanung

Über die Abhängigkeiten und Reihenfolgen der WAPs kann sichergestellt werden, dass die jeweiligen Voraussetzungen für den Wiederanlauf jeder Ressource erfüllt sind. Anhand dessen sollten die Abhängigkeiten der verschiedenen WAPs in einer übergeordneten Wiederanlaufplanung dokumentiert werden, z. B. innerhalb des Notfallhandbuchs. An dieser Stelle werden zudem die durchzuführenden Maßnahmen für den Wiederanlauf priorisiert. Die Priorisierung richtet sich üblicherweise an der logischen Abhängigkeit von Ressourcen aus. Falls der Wiederanlauf von Ressourcen vom Wiederanlauf weiterer Ressourcen abhängig ist, sollte eine übergeordnete Wiederanlaufplanung dokumentiert werden, die eine geeignete Wiederanlaufreihenfolge festlegt.

Abbildung 51 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 im Beispiel auf Abhängigkeiten zwischen Komponenten innerhalb einer Ebene verzichtet.

Beispiel (aus dem ITSCM)

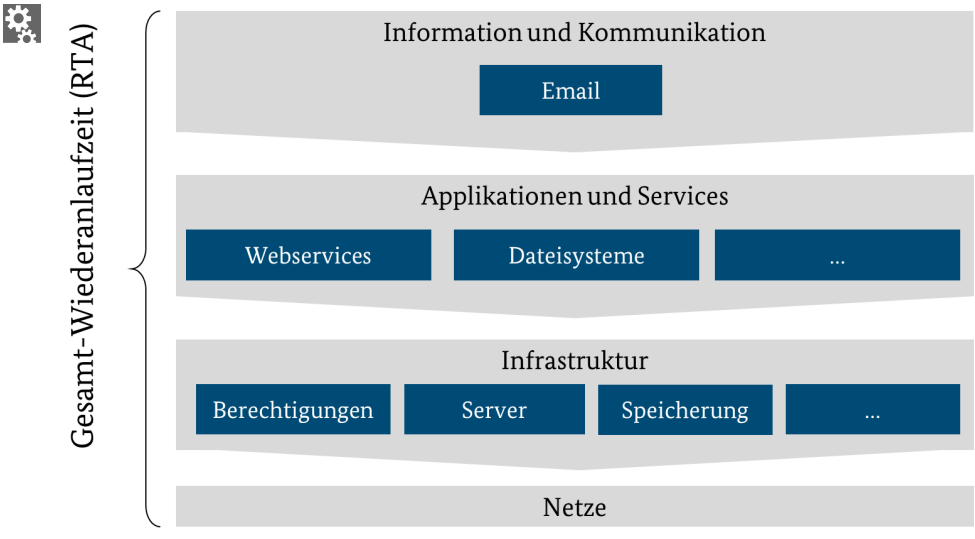

Abbildung 51: Beispiel einer übergeordneten IT-Wiederanlaufplanung

Die übergeordnete Wiederanlaufplanung muss sicherstellen, dass die Gesamt-RTA für eine zeitkritische Ressource auch unter Berücksichtigung der abhängigen Ressourcen die RTO nicht übersteigt.

12.3 Qualitätssicherung und Freigabe der WAPs (AS)

Um sicherzustellen, dass alle Vorgaben zur Wiederanlaufplanung eingehalten wurden, sollten die erstellten WAPs formal qualitätsgesichert werden. Dabei sollten die folgenden Aspekte berücksichtigt werden:

- **Vollständigkeit:** Bilden die Inhalte der erstellten WAPs alle vorgegebenen Punkte ab? Wurden alle relevanten Inhalte der BIA innerhalb der WAPs erfasst und sind diese aktuell? Wurden Maßnahmen über alle Phasen beschrieben? Unvollständige WAPs 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 Kontaktpersonen auf Basis einer aktuellen Kontaktliste dokumentiert?

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 13 Üben und Testen (R+AS)).

Nachdem die WAPs qualitätsgesichert wurden, müssen diese offiziell freigegeben werden. Dies kann beispielsweise durch die Leitungen der für die Ressourcen zuständigen Organisationseinheiten erfolgen. Dieser Schritt signalisiert, dass der Plan offiziell in einem Notfall verwendet werden kann.

Nachdem die WAPs 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 oder die BCB die aktualisierten Informationen der Institutionsleitung und dem Risikomanagement 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, dann ist es empfehlenswert, diese im Maßnahmenplan aufzunehmen und zeitnah umzusetzen.

12.4 Wiederherstellungsplanung im Rahmen des BCM (AS)

Abweichend zur Wiederanlaufplanung besteht für die vollständige Wiederherstellung der meisten Ressourcen eine andere, meistens deutlich längere Zeitvorgabe, die maximal mögliche Notbetriebsdauer aus der BC-Strategie. Gleichzeitig ist es in vielen Situationen nur sehr eingeschränkt sinnvoll möglich, eine vollständige, belastbare Wiederherstel-

lungsplanung bereits vorab zu erstellen, z. B. den Neubau eines Firmensitzes für den Fall eines Totalverlustes des alten. Daher hat die Wiederherstellungsplanung eine untergeordnete Rolle und wird in diesem Standard nicht zwingend gefordert. Infolgedessen wird hier der mögliche Inhalt auch nur grob beschrieben, denn die Inhalte können sehr unterschiedlich sinnvoll dokumentiert werden.

Um das Normalbetriebsniveau zu erreichen, muss nicht zwangsläufig exakt die Ressource wiederhergestellt werden, die ausgefallen ist. Mitunter kann eine Wiederherstellung auch bedeuten, dass ein verbesserter Zustand erreicht wird, weil z. B. eine Maschine neu beschafft statt repariert wird oder ein IT-System in einer aktuelleren Version neu aufgesetzt wird. Aus diesen Gründen ist es sinnvoll, die notwendigen konkreten Schritte zur Wiederherstellung der ausgefallenen Ressource erst bei deren Ausfall zu planen.

Es ist jedoch in den meisten Fällen hilfreich, sinnvolle Vorüberlegungen zu treffen, um in der stressigen Notfallsituation alle nötigen Informationen auch für die Wiederherstellung zur Verfügung zu haben. Diese können in Wiederherstellungsplänen selbst oder dort als Referenz dokumentiert werden. Dazu können folgende Punkte gehören, die im Detailgrad stark variieren können, je nachdem, wie konkret die Wiederherstellungsplanung vorbereitet wird:

- Übersicht zu Möglichkeiten der Beschaffung neuer Ressourcen, inklusive einer gewählten Präferenz und gegebenenfalls schon im Vorfeld geregelter Aspekte wie Vorverträge etc.
- Anleitung zur Inbetriebnahme, Integration der Ressource und entsprechende Funktionstests vor Inbetriebnahme (Häufig bereits in Betriebshandbüchern abgedeckt, worauf referenziert werden kann)
- Technischer Wechsel von der Ersatzlösung auf die neue Lösung
- Abgleich wiederhergestellter Datenstände mit dem im Notbetrieb abweichend erstellten Datenbestand oder Migration
- Ergänzende organisatorische Maßnahmen (z. B. Erstellung von Migrationshilfen, notwendige Schulungen oder Trainings, Anpassung von Prozessaktivitäten und Prozessdokumentation)

In Einzelfällen kann es auch sinnvoll sein, die Wiederherstellungsplanung auf dem Wiederanlauf aufzubauen. Folglich ist es sinnvoll, dies dann im Wiederherstellungsplan zu dokumentieren.

13 Üben und Testen (R+AS)

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 BC-Lösungen, die Rollen der BAO und die erstellten Pläne kontinuierlich anhand von Übungen 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 schwerwiegende 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 Mitarbeitenden auf den Notfall vorbereitet sind, indem sie eigene Erfahrungen sammeln und so im Notfall überlegt handeln können.

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 allgemeiner 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-Normen der 22300-Reihe. Der Begriff Übung wird daher als Oberbegriff verwendet. Tests stellen eine spezielle Form von Übungen dar. Aus Gründen der besseren Lesbarkeit wird nachfolgend primär der Begriff Übungen verwendet, die Tests miteinschließen.

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 34 aufgeführten Übungsarten. Die Bezeichnungen und Definitionen der jeweiligen Übungsarten können institutionsspezi-

fisch angepasst werden, sofern sichergestellt wird, dass der jeweilige Inhalt der Übungsart berücksichtigt wird.

Übungsart	Inhalt und Ziel	Beispiele	Relevant für
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 Rolleninhabenden durchsprechen, ohne dass Handlungsschritte real ausgeführt werden (GFP, Alarmierungsplan, Rechenzentrumsumschaltung, Vertragsklauseln in SLAs etc.).	Aufbau- und Standard-BCMS
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.	Alle Stufen

Übungsart	Inhalt und Ziel	Beispiele	Relevant für
Stabsrahmenübung	Erweiterte Form der Stabsübung, bei der weitere Stellen der Institution eingebunden werden Ziel: Die übergreifende Kommunikation und Zusammenarbeit zwischen dem Stab und ausgewählten Stellen der Notfallbewältigung üben. Neben dem Stab und seinen Unterstützungsrollen sind auch operative Teams an der Übung beteiligt, z. B. das Kommunikationsteam oder Organisationseinheiten mit zeitkritischen Geschäftsprozessen. Eine besondere Form der Stabsrahmenübung ist eine Vollübung, die sich an der Wirklichkeit orientiert und alle Hierarchieebenen von der Leitungsebene bis zu den einzelnen Mitarbeitenden mit einbezieht.	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.	Aufbau- und Standard-BCMS
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.	Alle Stufen
Funktionstest	Reale Ausführung eines Notfallplans Ziel: Einsatzbereitschaft und Funktionsfähigkeit von einzelnen oder mehreren baulichen, technischen oder organisatorischen Maßnahmen oder Ressourcen prüfen, die für die Notfallbewältigung benötigt werden.	Test eines Notfallarbeitsplatzes durch Mitarbeitende, 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.	Aufbau- und Standard-BCMS

Tabelle 34: Übungsarten gemäß BSI-Standard 200-4

Die folgende Abbildung zeigt die Schritte, die zum Üben notwendig sind:

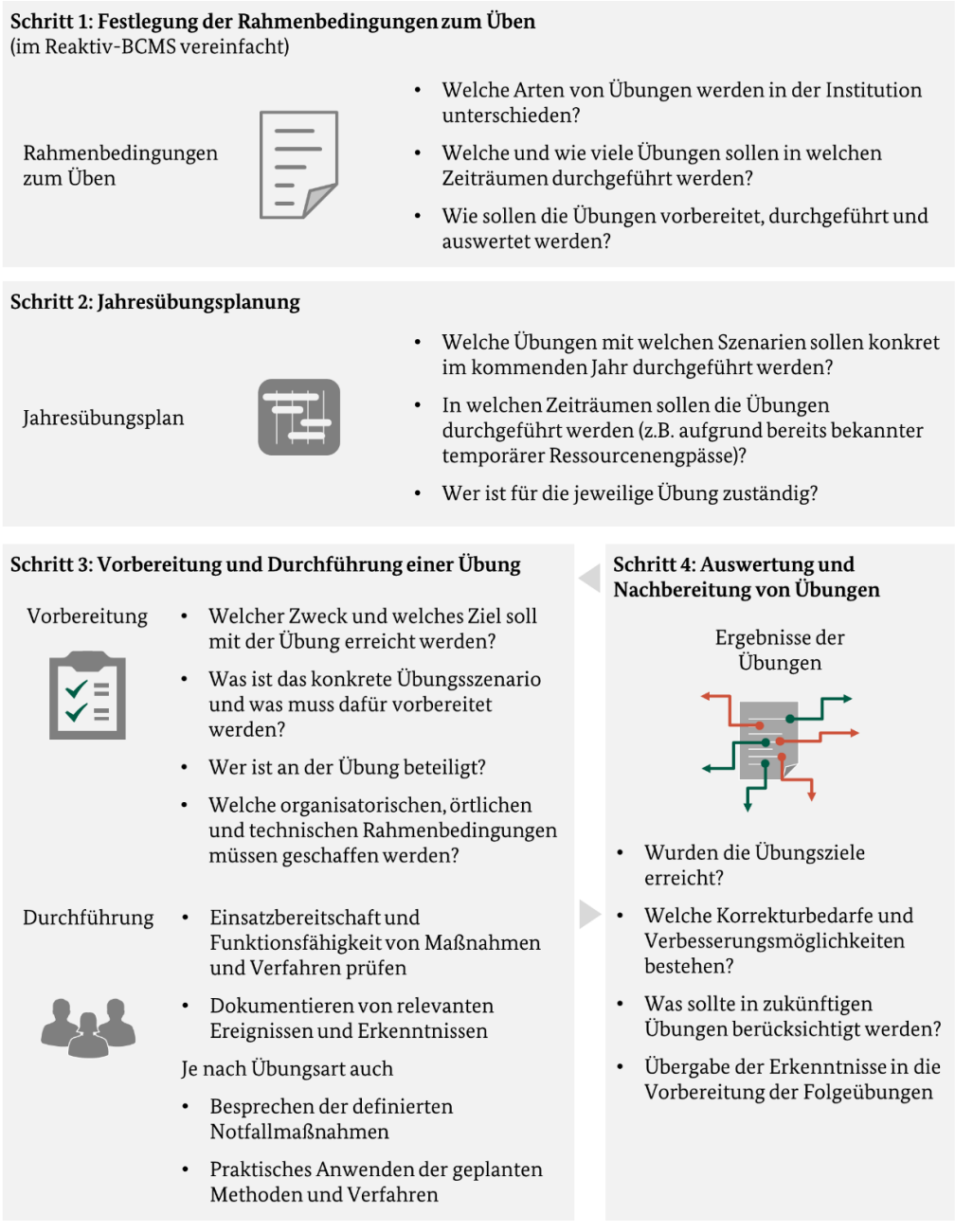

Abbildung 52: BCM-Prozessschritte zum Üben

Synergiepotenzial

Wenn in anderen Themenfeldern wie dem ITSCM oder dem Krisenmanagement bereits Übungen durchgeführt werden und eigenständige Übungsarten definiert sind, sollte dies bei der Jahresübungsplanung und den Rahmenbedingungen berücksichtigt werden. Es wird empfohlen, die Begriffe einheitlich zu definieren, z. B. zwischen dem BCM, dem Krisenmanagement, dem ITSCM sowie weiteren Stellen, die Übungen durchführen. Werden diese Begriffe nicht einheitlich definiert, wird empfohlen, die Begriffe namentlich klar voneinander abzugrenzen.

13.1 Rahmenbedingungen zum Üben im Reaktiv-BCMS (R)

Für das Reaktiv-BCMS müssen die Übungsarten **Stabsübung** und **Alarmierungsübung** regelmäßig durchgeführt werden. Ferner ist es empfehlenswert, auch die Übungsarten **Planbesprechung** („Schreibtischtest") sowie **Funktionstest** regelmäßig im Reaktiv-BCMS durchzuführen.

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. Aus diesem Grund ist es empfehlenswert, frühzeitig **Planbesprechungen** für GFPs einzuplanen, auch wenn diese noch nicht im ersten BCMS-Zyklus vollständig umgesetzt werden können.*

13.2 Festlegung der Rahmenbedingungen zum Üben (AS)

Alle Übungen des BCM sollten geplant und vorbereitet werden. Um dies zu erreichen und um störende Auswirkungen auf den Geschäftsbetrieb so gering wie möglich zu halten, muss der oder die BCB die Rahmenbedingungen zum systematischen Üben festlegen und dokumentieren. 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 konkret beantwortet und dokumentiert werden, z. B. in einem Übungshandbuch oder Anweisungen:

- Welche Arten von Übungen werden in der Institution unterschieden?
  - Wie sind diese Übungen definiert?
- Welche übergreifenden, Übungsziele sollen mit welchen Übungsarten erreicht werden?
  - Sind diese messbar?
- Welche regulatorischen, rechtlichen und vertraglichen Anforderungen bestehen an das Üben?
- Wie viele Übungen sollten in welchen Zeiträumen durchgeführt werden?

- Welche Zielgruppen sollen mit welcher Übungsart adressiert werden? An wie vielen Übungen sollen Mitglieder jeder Zielgruppe jährlich oder 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, ob und wie sich Übungen auf den Geschäftsbetrieb auswirken können?
- Wie sollen die verschiedenen Übungsarten 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 Rollen?

Ferner ist es empfehlenswert, die mit den Übungsarten verbundenen Aufwände vorab zu schätzen.

Die Institution sollte sicherstellen, dass die Rahmenbedingungen zum Üben geeignet sind, um die Ziele des BCMS zu erreichen. Da Übungen mit Aufwand und Kosten verbunden sind, sollte der oder die BCB 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.

Zunächst ist es empfehlenswert, die wesentlichen Merkmale der einzelnen Übungsarten zu benennen, z. B. Zielgruppe (Übende), Voraussetzungen und Zuständigkeiten. Ein Beispiel zeigt Tabelle 35:

Beispiel

Übungsart	***Übungsziel***	***Übende***	***Voraussetzung***	***Zuständig für Vorbereitung***
Planbesprechung	…	*Rollen im Notfallplan*	*Plan liegt vor*	*Dokumenteigentümer*
Funktionstest	…	*Bewältigungsteam*	*Planbesprechung wurde durchgeführt*	*Ressourcenzuständige*
Stabsübung	…	*Stabsmitglieder*	*Geschäftsordnung des Stabs liegt vor*	*BCB*
…	…	…		…

Tabelle 35: Übungsarten und wesentliche Merkmale

Synergiepotenzial

Übungsarten, die in anderen Managementsystemen wie z. B. dem Krisenmanagement, ITSCM oder dem Facility Management 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 mit den in diesem Standard definierten Übungsarten abgestimmt werden.

Vorgaben zu Ausfallszenarien

Grundsätzlich wird empfohlen, dass über einen Mehrjahreszeitraum alle für die Institution relevanten Ausfallszenarien berücksichtigt werden. Typische Szenarien sind Ausfälle bestimmter Ressourcenkategorien oder die Bewältigung eines Cyberangriffs, z. B. mit Datenverlust oder -manipulation. Hierzu sollte festgelegt und dokumentiert werden, welche Ausfallszenarien in welchem Zeitraum anhand von Übungen berücksichtigt werden sollen.

Bei Ausfallszenarien wird zwischen Ursachen- und Wirkungsszenarien unterschieden:

- Ein **Wirkungsszenario** geht von definierten Ausfällen oder Beeinträchtigungen aus, ohne die Ursachen zu berücksichtigen (z. B. Ausfall eines Rechenzentrums).
- 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. Es ist wichtig, dass der Übungsautor oder die -autorin je nach Übungsziel entscheidet, 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 funktioniert, z. B. weil die Datenbestände und die Datensicherungen der letzten vier Wochen kompromittiert wurden. In diesem Fall wird meist die Krise ausgerufen (siehe Hilfsmittel Weiterführende Aspekte zur Bewältigung) und die RTOs der betroffenen Geschäftsprozesse sowie Ressourcen werden in der Regel nicht erreicht. Beim Szenario Cyberangriff steht daher eher die Zusammenarbeit der einzelnen Themenfelder, wie z. B. Informationssicherheit, ITSCM und (IT-)Krisenmanagement im Vordergrund. Für das Üben der Zusammenarbeit bieten sich Übungsarten wie eine Planbesprechung, Stabsübung oder Stabsrahmenübung an.

Vorgaben zur Vollständigkeit und kontinuierlichen Verbesserung des Übens

Es muss sichergestellt werden, dass anhand des Jahresübungsplans über einen festgelegten Zeitraum alle BC-Strategien und -Lösungen und die damit verbundenen BC-Pläne durch Übungen validiert werden (siehe 13.3 *Erstellung einer Jahresübungsplanung (R+AS)*). Alle in Tabelle 34 genannten Übungsarten müssen berücksichtigt und regelmäßig durchgeführt werden. Nur so können alle Maßnahmen, organisatorischen Strukturen und Pläne anhand von Übungen überprüft werden. Zusätzlich kann durch wechselnde Szenarien eine Fehlsteuerung vermieden werden. Wenn die Teilnehmenden ihre Aufgaben nur noch routinemäßig in derselben Übungssituation bearbeiten, steigt die Gefahr von „Betriebsblindheit". Diese 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.

Die Komplexität und die Herausforderung der Übungen müssen kontinuierlich gesteigert werden. Hierzu sollte die Institution risikoorientiert vorgehen, d. h. die Übungen müssen realistischer und handlungsorientierter werden, ohne jedoch unzumutbare Auswirkungen auf den Geschäftsbetrieb auszulösen. Zudem genügt es nicht, über Jahre hinweg nur einseitig entweder technisch oder organisatorisch zu üben. Es ist empfehlenswert, die technischen sowie organisatorischen Aspekte der Notfallbewältigung schrittweise im Zusammenspiel zu üben. Dies kann z. B. dadurch erreicht werden, dass korrespondierende Wiederanlaufpläne und Geschäftsfortführungspläne kombiniert getestet werden. Auch sollte sichergestellt werden, dass nicht nur die Erstbesetzungen der BAO an Übungen eingesetzt werden, sondern auch die Stellvertretenden üben.

Ankündigung von Übungen

Für jede Übung muss entschieden werden, ob diese in der Institution angekündigt wird oder nicht. Wenn Übungen im Voraus angekündigt werden, können sich alle Teilnehmenden 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 fordern.

Vorgaben zur Dokumentation

Der oder die BCB sollte anhand von Mindestanforderungen sowie über entsprechende Vorlagen und Anweisungen sicherstellen, dass die Dokumentation der Übungen innerhalb einer Übungsart möglichst einheitlich erfolgt und möglichst zielführend ausgerichtet

ist. Je einfacher eine Übungsart ist, desto einfacher kann die Dokumentation ausgestaltet sein.

Die folgende Abbildung zeigt eine Übersicht über die Dokumentation bei Übungen:

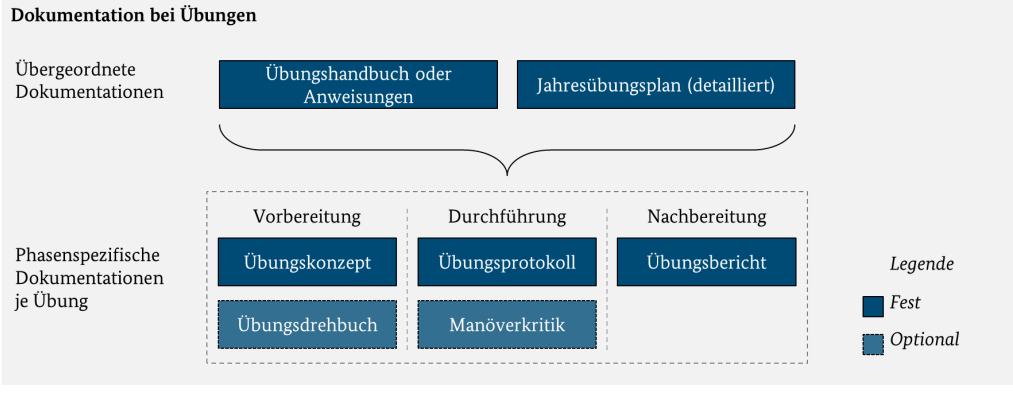

Abbildung 53: Dokumentation bei Übungen

Die Jahresübungsplanung sollte übergreifend durch den oder die BCB erstellt werden, da sie zusammen mit den Rahmenbedingungen den notwendigen Rahmen für alle Übungen bildet.

Für jede Übung muss in der Vorbereitungsphase ein **Übungskonzept** (siehe 13.4 *Vorbereitung und Durchführung einer Übung (R+AS)*) erstellt werden, das die Rahmendaten aus der Jahresübungsplanung präzisiert und weiter detailliert. Im Übungskonzept 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. Das Übungsprotokoll sollte die Ergebnisse, Korrekturbedarfe und Verbesserungsmöglichkeiten dokumentieren. Die Inhalte des Protokolls sollten prägnant und für sachverständige Dritte verständlich formuliert sein. Bei komplexeren Übungen, z. B. Stabsübungen, mit einer umfangreicheren Zielgruppe sollten direkt im Anschluss der Durchführung die unmittelbaren Eindrücke und Verbesserungsvorschläge der Teilnehmenden gesammelt und dokumentiert werden. Diese Tätigkeit wird auch **Manöverkritik** oder „**hot wash up“** genannt. Für jede Übung muss ein **Übungsbericht** erstellt werden, der die wesentlichen Ergebnisse der Übung, wie Zielerreichungsgrad, Änderungsbedarfe und Verbesserungspotenziale, zusammenfasst.

Die vorgestellten phasenspezifischen Dokumente können auch in einem einzigen Dokument je Übung gesammelt werden. Welche Informationen in diesen Dokumenten erfasst werden sollen, wird in den nachfolgenden Kapiteln je Übungsart individuell beschrieben.

Rollen bei Übungen

Neben der Rolle BCB, die 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 13.4 *Vorbereitung und Durchführung einer Übung (R+AS)* erläutert.

Sofern erforderlich oder sinnvoll können Personen auch mehrere Rollen einnehmen. So wäre es etwa möglich, dass der oder die Übungsleitende auch die Tätigkeiten der Übungsautorenschaft übernimmt oder eine Person gleichzeitig die Rolle Übungsprotokollierung übernimmt. Das folgende Beispiel zeigt typische Rollen und deren Aufgaben bei Übungen.

Beispiel

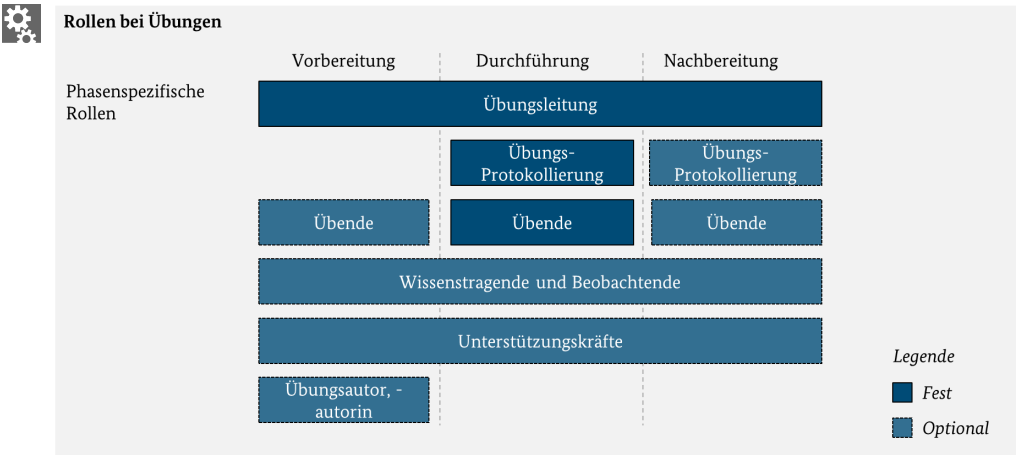

Abbildung 54: Beispiele verschiedener Rollen bei Übungen

Rolle	***Typische Aufgaben***
Übungsleitung	***Vorbereitung:*** • *Mit dem Übungsautor oder der -autorin 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*

Rolle	***Typische Aufgaben***
Übungsautor, -autorin	***Vorbereitung:*** • *Übungskonzept erstellen inklusive Übungsziele, organisatorischer Ablauf, Zielgruppen, Vorbereitungsmaßnahmen, Abbruchkriterien etc.* • *Weitere Übungsdokumente und -materialien erstellen und vorbereiten, wie z. B. das Übungsdrehbuch, die Szenario-Einlagen oder die Übungsumgebung (abhängig von Übungsart)* • *Übende auswählen* • *Unterstützungskräfte koordinieren*
Übungsprotokollierung	***Durchführung:*** • *Übungsablauf detailliert im Protokoll erfassen* ***Nachbereitung:*** • *Beobachtungen in die Auswertung einbringen*
Übende	***Vorbereitung:*** • *Einlesen in Materialien, die zur Vorbereitung bereitgestellt oder als Übungsvoraussetzung genannt wurden* ***Durchführung:*** • *Übende Personen reagieren entsprechend ihrer vorgesehenen Funktionen oder Rollen auf die Szenarien, Einlagen und Anforderungen gemäß dem geplanten Übungsverlauf* ***Nachbereitung:*** • *An Nachbesprechung oder Debriefing teilnehmen, Fragebogen beantworten, Rückmeldung zur Übung geben*
Beobachtende	***Vorbereitung:*** • *Sich vertraut machen mit der Übung gemäß Übungskonzept und weiteren Dokumenten* ***Durchführung:*** • *Übung aus neutraler Sicht beobachten* ***Nachbereitung:*** • *Beobachtungen in die Auswertung einbringen*
Wissenstragende	***In allen Phasen:*** • *Andere Übungsrollen fachlich beraten* ***Durchführung:*** • *Anfragen der Teilnehmenden aus fachlicher Sicht beantworten*

Rolle	*Typische Aufgaben*
Unterstützungskräfte	***Vorbereitung:*** • *Übungsautor oder -autorin unterstützen, z. B. das Drehbuch erstellen oder logistische Aufgaben erledigen* • *Aufbau der Übungsumgebung* ***Durchführung:*** • *Übungsleitung unterstützen, wie z. B. die Einlagen gemäß Drehbuch einspielen* ***Nachbereitung:*** • *Beobachtungen in die Auswertung einbringen* • *Abbau der Übungsumgebung inklusive Herrichtung des Ursprungszustandes*

Tabelle 36: 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. Es ist daher wichtig, dass jede Institution genau abwägt, 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 37).

Beispiel

Übungsart	*Geschätzter Übungsumfang*	*Häufigkeit*	*Detailtiefe*
Planbesprechung	*niedrig*	• *zeitnah nach Planerstellung* • *zeitnah nach wesentlichen Änderungen betroffener Pläne*	*alle Kapitel (möglicherweise verteilt über mehrere Planbesprechungen)*

Übungsart	*Geschätzter Übungs-umfang*	*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* *ressourcenübergreifend*
Stabsübung	*niedrig – mittel*	• *mindestens jährlich*	*alle Stabsmitglieder (Kernteam) und stabsnahe Unterstützungsfunktionen sowie alle Stellvertretenden*

Tabelle 37: Beispiel für differenzierte Angaben zum Übungsumfang

13.3 Erstellung einer Jahresübungsplanung (R+AS)

Die Institution muss eine Jahresübungsplanung erstellen, die gewährleistet, dass die definierten Prozesse, Ressourcen, Verfahren und Abläufe der Notfallbewältigung über einen längeren Zeitraum, gegebenenfalls über mehrere Jahre, vollständig geübt werden. 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)
- regulatorische, rechtliche und vertragliche Anforderungen
- die zeitlichen und personellen Ressourcen der beteiligten Rollen
- aktuelle Ergebnisse der anderen BCMS-Prozessschritte, insbesondere der Folgenden:
  - Ergebnisse der BIA
  - Ergebnisse des Soll-Ist-Vergleichs
  - Geschäftsfortführungsplanung
  - Rollen der BAO
- die vorherigen Jahresübungspläne sowie die Übungserfahrung der Übenden (sofern vorhanden)
- die gewonnenen Erkenntnisse aus den letzten Jahren (sofern vorhanden)

Zusätzliche Aspekte sollten im **Aufbau-** und **Standard-BCMS** berücksichtigt werden:

- die Erwartungen von Interessengruppen gemäß 4.2.1 *Identifizierung von Anforderungen und Einflussfaktoren an* das BCMS
- die Reife des BCMS

AS

Pro Übung sollten mindestens folgende Punkte festgelegt und im Jahresübungsplan dokumentiert werden:

- konkretes Datum oder geplanter Zeitraum der Übung
- Übungsart
- übergreifendes Übungsziel und Umfang (gegebenenfalls inklusive Ausfallszenario und zu übenden Geschäftsprozessen oder Ressourcen)
- zuständige Personen, welche die Übung vorbereiten
- zuständige Personen, welche die Übung durchführen
- Zielgruppe oder -gruppen und geplante Übende
- Abschätzung der erforderlichen personellen, materiellen und finanziellen Ressourcen
- Abschätzung des zu erwartenden Einflusses der Übung auf den Normalbetrieb

Es ist sinnvoll, das festgelegte **Datum bzw. den geplanten Zeitraum** der Übung mit den zuständigen Personen abzustimmen, die die Übung vorbereiten und durchführen. Zusätzlich ist es empfehlenswert, die Verfügbarkeit aller Übungsteilnehmenden zu berücksichtigen. Bei der Terminplanung ist es daher wichtig zu beachten, 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 richtet sich an der Reife des BCMS aus, bestimmt das allgemeinere Übungsziel der Übungsart näher und berücksichtigt die Übungserfahrung der Institution. Übungen sollten so geplant werden, dass sie einerseits herausfordernd für die Übenden sind, andererseits aber auch Erfolgserlebnisse und einen Erkenntnisgewinn für die Teilnehmenden 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.

Übungsziele sollten idealerweise messbar sein. Da die Messbarkeit erheblich zwischen Übungsarten variieren kann, sollte im Vorfeld je Übung und Übungsart grob definiert werden, wie gemessen werden kann, ob oder in welchem Grad das Übungsziel erreicht wurde. Bei Funktionstests oder Alarmierungsübungen sind häufig quantitative Auswertungen möglich, z. B. in Form einer Bewertung („bestanden" oder „nicht bestanden") oder als Abgleich mit einer zeitlichen Vorgabe (RTO). Demgegenüber sind für eine Stabsübung eher qualitative Ziele angemessen, die sich auf die Qualität der Zusammenarbeit im Stab beziehen.

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, dass 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 in einem weiteren Schritt kann die Kombination aus beiden geübt werden kann.

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.

Ankündigung von Übungen

Für jede Übung muss entschieden werden, ob diese in der Institution angekündigt wird oder nicht. Wenn Übungen im Voraus angekündigt werden, können sich alle Teilnehmenden besser darauf vorbereiten. So können Terminkonflikte vermieden werden. Auf der anderen Seite kann dies auch Nachteile mit sich bringen, beispielsweise einen niedriger wahrgenommenen Realitätsgrad oder eine künstliche Vorbereitung. Für Institutionen ohne Übungserfahrung ist es sinnvoll, zu Beginn alle Übungen anzukündigen, z. B. im Reaktiv-BCMS. Die Beteiligten haben dann die Möglichkeit, sich auf die Übungen 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 fordern.

Hinweis

Nicht angekündigte Stabsübungen und Stabsrahmenübungen können gut mit Alarmierungsübungen kombiniert werden (siehe 13.6 Stabsübung, 13.7 Stabsrahmenübung, 13.8 Alarmierungsübung). 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- oder Stabsrahmenübung.

Der erstellte Jahresübungsplan sollte mit der Institutionsleitung abgestimmt und durch diese freigegeben werden. Einer der Gründe hierfür ist, dass die Institutionsleitung in der Praxis häufig die notwendigen personellen, materiellen und finanziellen Ressourcen freigibt. 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 Stäbe, die auf strategischer Ebene arbeiten, üben. In Tabelle 38 wird ein vereinfachtes Beispiel für einen Jahresübungsplan dargestellt.

Beispiel

Nr.	Übungsart	Datum/ Zeitraum	Ziel und Umfang der Übung	Zuständig	Ressourcen
2023-01	*Planbesprechung*	*14.04.2023, 09 – 11 Uhr*	*GFP der IT-Abteilung im Szenario „Standortausfall" prüfen*	*Hr. Meier (IT)*	*2 – 3 IT-Mitarbeitende, ca. 2 h je Person*
2023-02	*Funktionstest*	*22.09.2023, 13 – 16 Uhr*	*Arbeitsfähigkeit ausgewählter IT-Mitarbeitender an den definierten Notfallarbeitsplätzen überprüfen*	*Hr. Meier (IT)*	*2 – 3 IT-Mitarbeitende, ca. 1 Tag je Person*
2023-03	*Alarmierungstest*	*13.11.2023, 08:30 Uhr*	*Meldewege und Alarmierung der Stabsmitglieder prüfen*	*BCB*	*Mitglieder des Stabs, ca. 1 h je Person*
2023-04	*Stabsübung*	*13.11.2023, 09 – 11 Uhr*	*Abläufe des Szenarios „Brand im RZ" im Stab üben*	*BCB*	*Mitglieder des Krisenstabs, Drehbuch und Einlagen, ca. 15 Tage zur Vorbereitung, Durchführung, Nachbereitung + 0,5 Tage je Person*

Tabelle 38: Beispiel für einen Jahresübungsplan

Der oder die BCB 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 oder die BCB prüfen, ob eine Wiederholung der Übung erforderlich ist, nachdem die Mängel behoben wurden.

Synergiepotenzial

Vielfach werden bereits zu anderen Sicherheitsthemen Übungen geplant und durchgeführt. So finden aufgrund gesetzlicher Vorgaben regelmäßig Brandschutz- und Räumungsübungen statt, für deren Planung der oder die 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 oder Vorfallsmanagement im Rahmen des ISMS 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 und doppelte Übungen zu vermeiden. 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.

13.4 Vorbereitung und Durchführung einer Übung (R+AS)

Jede Übung sollte gemäß der Jahresübungsplanung vorbereitet und durchgeführt 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 richtet sich am gesetzten Übungsziel aus. Der Umfang der Vorbereitung hängt von der Art und Komplexität der Übung ab.
- Die **Durchführung der Übung** beinhaltet, dass die Beteiligten einen vorgegebenen Übungsablauf bewältigen 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 jede Übungsart in den nachfolgenden Kapiteln beschrieben.

Um einen klaren Rahmen zur Konzeption und Durchführung für alle beteiligten Personen vorzugeben, ist es wichtig, die organisatorischen Eckpunkte für jede Übung in einem **Übungskonzept** zusammenzufassen. Das Übungskonzept sollte folgende Punkte beinhalten:

- Datum der Übung
- Standort und Raum (Buchung)
- Übungsbeginn (Uhrzeit)

- Übungsende (Uhrzeit)
- Übungsziele (Konkretisieren der Ziele aus der Jahresübungsplanung)
- Teilnehmende (jeweils Rolle und Name)
- Ankündigung der Übung (Ja/Nein)

Abweichungen zu dieser Liste sind in den einzelnen Kapiteln zu jeder Übungsart beschrieben.

13.5 Planbesprechung (R optional +AS)

In Planbesprechungen werden einzelne Pläne der Notfallbewältigung, insbesondere die Geschäftsfortführungspläne, gemeinsam mit den Anwendenden 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 Teilnehmenden greifbarer zu gestalten, können die Problemstellungen auch anhand fiktiver Lagen erörtert werden. Die beschriebenen Maßnahmen sollten in der Planbesprechung durch die Anwendenden dahingehend beurteilt werden, ob diese auch in einer Stresssituation verständlich, plausibel, vollständig und aktuell sind. Planbesprechungen sind vor allem dazu geeignet, Abhängigkeiten aufzudecken oder notwendige Voraussetzungen von Maßnahmen zu erkennen und bewusst zu machen. Darüber hinaus können Planbesprechungen eingesetzt werden, um die Teilnehmenden zu sensibilisieren.

13.5.1 Vorbereitung einer Planbesprechung

Die Vorbereitung einer Planbesprechung kann der oder die BCB prinzipiell selbst übernehmen. Deutlich zielführender ist es jedoch, wenn die Übung durch eine Person aus derjenigen Organisationseinheit vorbereitet wird, in deren Zuständigkeitsbereich der Plan erstellt wurde. Diese Person kann besser die Arbeitsbelastung und Terminsituation in der jeweiligen Organisationseinheit einschätzen und so geeignete Zeiträume festlegen, um die Planbesprechung durchzuführen. Zudem sind dieser Person geeignete weitere Mitarbeitende 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 umgesetzt. Daher ist es empfehlenswert, einen Plan gleich nach seiner Erstellung im Rahmen einer Planbesprechung weiter zu plausibilisieren und zu vervollständigen. Ein validierter Plan kann dann auch Grundlage einer Planbesprechung zur Sensibilisierung sein, z. B. von neuen Mitarbeitenden.

Es ist sinnvoll, eine Planbesprechung anzukündigen. Die Übungsdauer beträgt typischerweise zwei bis vier Stunden, abhängig vom Umfang des besprochenen Plans. Diese Details werden, wie beschrieben, im Übungskonzept dokumentiert. Die Übungsziele von Planbesprechungen werden oft „weich" formuliert.

Beispiel

- Sensibilisierung und Schaffung eines gemeinsamen Verständnisses bei allen Stellen, die in diesen Plan involviert sind
- Klärung von Zuständigkeiten
- Aufdeckung von internen und externen Abhängigkeiten
- Überprüfung eines Notfallplans auf Schwachstellen, bevor dieser mit großem Aufwand realisiert oder geübt wird

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 die Abstimmung der eigenen Geschäftsfortführungspläne mit der BC-Planung zeitkritischer Dienstleistungsunternehmen. Hierbei steht im Fokus, Zielkonflikte zu identifizieren, z. B. ob die verschiedenen Aktivitäten in der Alarmierung sowie Geschäftsfortführung konsistent und aufeinander abgestimmt sind und für alle Parteien nachvollziehbar dokumentiert sind.

13.5.2 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 den 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 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 Kontaktpersonen auf Basis einer aktuellen Kontaktliste dokumentiert?

13.6 Stabsübung (R+AS)

Ziel der Stabsübung ist es, die Zusammenarbeit innerhalb der BAO sowie die Methoden zur Stabsarbeit zu üben. Im Gegensatz zur Stabsrahmenübung (siehe 13.7 *Stabsrahmenübung (AS)*) wird die Stabsübung im BCM in einem „geschützten Raum" durchgeführt, ohne Externe zu beteiligen. Eine Stabsübung sollte so gestaltet sein, dass der Stab die Grundelemente der Stabsarbeit praktisch anwendet. Bei Stabsübungen nimmt dabei die Vorbereitung aufgrund der Komplexität den größten Umfang im Gegensatz zu den anderen Übungsphasen ein.

Folgende Vorlagen und Hilfsmittel werden in der Regel innerhalb der Vorbereitung und Durchführung der Stabsübung erstellt:

- Übungskonzept
- Übungsdrehbuch und Einlagen
- Übungsprotokoll

Auf die wesentlichen Vorlagen sowie Hilfsmittel wird im weiteren Verlauf detailliert eingegangen.

13.6.1 Vorbereitung einer Stabsübung

Die Vorbereitung wird in der Regel von einem benannten Übungsautor oder einer -autorin wahrgenommen. Diese Rolle kann durch den oder die BCB, durch die für die Übung zuständige Person oder weitere beauftragte Personen übernommen werden. Da Stabsübungen deutlich komplexer als die meisten anderen Übungsarten sind, sollten neben den bereits beschriebenen organisatorischen Eckpunkten im Übungskonzept die nachfolgenden Aspekte festgelegt und dokumentiert werden (siehe 13.4 *Vorbereitung und Durchführung einer Übung (R+AS)*):

Übungsziele

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

- *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 oder die -autorin den Rahmenablauf der Stabsübung planen. Hierbei sollten folgende Fragestellungen beantwortet werden:

- Soll die Übung den Teilnehmenden vorab angekündigt werden und falls ja, wann und mit welchen Detailinformationen (z. B. Termin, Übungsdauer, Ort etc.)?
- Soll vor der Stabsübung eine Alarmierung der Teilnehmenden erfolgen (z. B. anhand einer vorgeschalteten Alarmierungsübung)?

Darüber hinaus ist es auch hilfreich, festzulegen,

- in welcher Form eine direkte Rückmeldung über die Übungsergebnisse gegeben wird und wie viel Zeit dafür eingeplant wird sowie
- ob und wie die Rückmeldungen der Übenden erfasst werden sollen.

Eine Auswertungsrunde erfolgt idealerweise möglichst direkt im Anschluss an die Stabsübung, um die erste Resonanz der Teilnehmenden direkt und ungefiltert aufnehmen zu können. Zudem wird empfohlen, eine zweite Auswertungsrunde mit den Teilnehmenden vorzusehen, um ein strukturiertes und konsolidiertes Feedback zu erhalten. Es ist empfehlenswert, diesen Termin mit etwas zeitlichem Abstand zur Übung festzulegen, 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 oder die -autorin Regeln für die Übung festlegen. Die Regeln für die Übung sollten besondere Sicherheitsvorkehrungen dokumentieren, die verhindern, dass sich eine Übung auf den Normalbetrieb auswirkt. Dazu gehören folgende Aspekte:

- Welche Abbruchbedingungen führen zu einem vorzeitigen Ende der Übung?
- Gibt es besondere Sicherheitsvorkehrungen als Bestandteil der Übung (z. B. eine bestimmte Kennzeichnung von Dokumenten)?
- Ist den Teilnehmenden eine Kommunikation mit Personen außerhalb des Übungsraums gestattet und falls ja, mit wem und wie?

Abbruchbedingungen für eine Stabsübung sind z. B. der Eintritt eines realen Notfalls, eine deutliche Überschreitung der Übungszeit oder wenn Personen mit Schlüsselfunktionen die Übung ungeplant verlassen müssen.

Es ist sehr empfehlenswert, während der Übung die Kommunikation außerhalb des Übungsraums nur in Ausnahmefällen zu gestatten, wenn z. B. eine Auskunft durch Fachleute 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 Teilnehmende 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 Teilnehmenden reagieren müssen. Das Szenario kann reale oder fiktive realitätsnahe Vorfälle enthalten und liefert die für die Übung relevanten Grundinformationen oder Annahmen.

Das Übungsszenario sollte dafür geeignet sein, die Zielsetzung der Stabsübung zu erreichen. Es ist darüber hinaus empfehlenswert, dass die Übenden sich sowohl mit den Grundelementen der Stabsarbeit als auch mit den Notfallplänen und vorgesehenen Notfallmaßnahmen auseinandersetzen können.

Hinweis

Für die ersten Stabsübungen reichen einfache Notfallszenarien vollkommen aus, um die Grundlagen der Stabsarbeit zu überprüfen.

Mit steigender Übungserfahrung sollten Stabsübungen einen immer stärkeren realen Bezug erhalten. Der reale Bezug kann auch gesteigert werden, indem vermehrt Stabsrahmenübungen durchgeführt werden.

Übungsdrehbuch

Damit die Übungsleitung den Übungsablauf koordinieren und steuern kann, ist es empfehlenswert, aus der Gesamtheit der Einlagen ein Übungsdrehbuch mit dem gedachten Verlauf zu erstellen. Tabelle 39 zeigt beispielhaft den Aufbau eines Übungsdrehbuchs.

Beispiel

Nr.	Zeit	Sender	Empfänger	Information bzw. Ereignis	Erwartete Handlung
…	…	…	…	…	…
2	09:15	Leitung RZ	Hr. Lorenz	Löscharbeiten im Rechenzentrum wurden durch die Feuerwehr abgeschlossen.	Funktionsfähigkeit des RZ prüfen und Erstmaßnahmen aus dem GFP initiieren
3	09:22	mitarbeitende Person 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 39: Beispiel des Aufbaus eines Übungsdrehbuchs

Einlagen

Sogenannte **Ausgangslagen** beschreiben anhand des Szenarios die Übungsumgebung zur Ausgangssituation. **Einlagen** sind geplante eingehende fiktive Informationen oder Unterbrechungen während der Übung. Damit können Informationen im Szenario ergänzt, erweitert oder verändert und der Verlauf der Übung etwas gesteuert werden. Durch Einlagen sollen die Teilnehmenden 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, die während der Übung neue Informationen zum Szenario beitragen.

Je nach hierfür notwendiger Fachexpertise oder anderen Einflussfaktoren kann es erforderlich sein, weitere Personen hinzuzuziehen, die selbst Einlagen entwickeln oder den Übungsautor oder die -autorin fachlich beraten.

Hinweis

Der Übungsautor oder die -autorin 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, keine Funktion so zu überlasten, dass ein „Flaschenhals-Effekt" entsteht. Es sei denn, genau dies soll geübt werden.

Übungsrollen

In einem nächsten Schritt muss der Übungsautor oder die -autorin die für die Übungsdurchführung relevanten Teilnehmenden festlegen und mit konkreten Personen besetzen:

Übungsleitung: Eine Person wird benannt, welche die Übung insgesamt steuert.

Unterstützungskräfte: Für mehr Realitätsnähe ist es hilfreich, dass die Übungsleitung abhängig von der Komplexität des Szenarios durch weitere Personen unterstützt wird, 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.

Übungsprotokollierung: Eine oder mehrere Personen werden benannt, die den Verlauf der Übung nachvollziehbar im Übungsprotokoll erfassen. Die Rolle Übungsprotokollierung erfüllt nicht die Rolle des oder der Protokollierenden des Stabs. Der oder die Protokollierende des Stabs wirkt ebenfalls innerhalb des Übungsszenarios mit, aber protokolliert nur die Aktivitäten und Entscheidungen des Stabs.

Beobachtung (optional): Eine oder mehrere Personen werden benannt, welche die Übung neutral „aus der zweiten Reihe" beobachten und hinsichtlich möglicher Verbesserungspotenziale bewerten.

Letzte Vorbereitungen

Die Vorbereitungsphase ist dann abgeschlossen, wenn sichergestellt ist, dass die gesteckten Übungsziele realistisch erreicht werden können und die Übung damit ermöglicht wird. 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

- *Frühzeitig alle Beteiligten einladen (bei angekündigten Übungen)*
- *Prüfung der Aktualität von Dokumenten des Notfallhandbuchs, die während der Übung verwendet werden sollen*
- *Vorbereitung einer Kurzpräsentation, um in die Besonderheiten der Übung einzuführen (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 E-Mails, als Skript zum Vorlesen oder als gedruckte Handouts)*

- *Prüfung, ob die eingesetzte Technik funktionsfähig ist (z. B. Beamer, Telefone etc.)*
- *Logistische Vorbereitung der Übung (z. B. die Verpflegung während der Übung oder die Unterbringung von Teilnehmenden)*
- *Durchführung von Briefings mit allen Teilnehmenden der Übung*

Es ist empfehlenswert, dass der Übungsautor oder die -autorin bis zum Übungstag wiederkehrend prüft, ob eventuell andere Ereignisse die Durchführung der Übung beeinflussen oder sogar verhindern können.

13.6.2 Durchführung einer Stabsübung

Auch bei einer guten Vorbereitung können oft nicht alle Eventualitäten vorhergesehen werden. Daher können Stabsübungen auch für die Übungsleitung herausfordernd sein. Es ist die Aufgabe der Übungsleitung, das Übungsszenario unter Beachtung der Ziele und der Zeitplanung zu steuern. Insbesondere ist es hilfreich, darauf zu achten, dass die vorbereiteten Einlagen durch die Unterstützungsrollen geeignet in den Übungsverlauf eingespielt werden. Die Übungsleitung kann jederzeit entscheiden, dass eine Einlage früher, später oder überhaupt nicht eingespielt wird, wenn sich dies positiv auf den Übungsverlauf auswirkt.

In der Regel beginnen Stabsübungen mit einer Ausgangslage und einer damit verbundenen Lagefeststellung des Stabes (auch Konstituierung in 5.5.1 *Konstituierung und Auflösung der BAO (AS)* genannt). In dieser Lagefeststellung verschafft sich der Stab ein erstes Lagebild und stellt in der Regel fest, dass sich die Institution in einem Notfall oder einer Krise befindet und ruft diesen bzw. diese aus. Diese Zeit, die bis zum Ausrufen des Notfalls oder der Krise vergeht, ist ein essenzieller Bestandteil der BAO-Reaktionszeit neben der Detektions- und Alarmierungszeit (siehe 7 *Business-Impact-Analyse (R+AS)*). Daher wird empfohlen, diese Zeit zu messen und in Kombination mit der Alarmierungszeit mit der BAO-Reaktionszeit zu vergleichen (siehe 13.10.2 *Zusätzliche Aspekte zur Auswertung einer Alarmierungsübung*).

Die Übungsleitung sollte den Übungsablauf koordinieren. Hierfür ist es empfehlenswert, dass die Übungsleitung das Recht besitzt, von der Zeitplanung abzuweichen oder die Übung abzubrechen. Es ist hilfreich, wenn sich alle Teilnehmenden während der Übung stets an die geltenden Übungsregeln und -künstlichkeiten halten, ohne jedoch ihren kreativen Handlungsraum zu beschränken.

Der oder die Übungsprotokollierende muss den Übungsverlauf und die Übungsergebnisse dokumentieren. Hilfestellungen zu Inhalten des Protokolls geben die folgenden Beispiele. Die Rolle Übungsprotokollierung unterscheidet sich von der Rolle des oder der Protokollierenden des Stabes.

Beispiele für Inhalte des Protokolls zum Übungsverlauf

- *Notizen zum beobachteten Ablauf der Übung*
- *Hinweise von Teilnehmenden als Input für die Übungsauswertung*
- *Erreichung oder Nicht-Erreichung von Übungszielen*
- *verwendete Dokumente, Werkzeuge, Ressourcen*
- *erkannte Korrekturbedarfe oder Verbesserungsmöglichkeiten*

Werden Beobachtende eingesetzt, können diese notieren, was gut funktioniert hat und was noch optimierbar ist. Dabei wird empfohlen, Personen als Beobachtende einzusetzen, die viel Wissen zum BCM der Institution besitzen. Die Übungsprotokollierenden und Übungsbeobachtenden müssen sich während der Übungsdurchführung neutral verhalten und dürfen nicht in das Geschehen eingreifen. Erst in der Auswertung der Übung sollten die Übungsprotokollierenden und Übungsbeobachtenden 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 Teilnehmenden können sich stark in das Szenario hineinversetzen. Ein klares Übungsende trägt dazu bei, dass Emotionen abflauen und alle Teilnehmenden das durchlebte Szenario abschließen können.

13.7 Stabsrahmenübung (AS)

Stabsrahmenübungen im BCM stellen eine erweiterte Form der Stabsübung dar (siehe 13.6 *Stabsübung (R+AS)*). Alle Anforderungen an Stabsübungen müssen daher auch für Stabsrahmenübungen erfüllt sein. Stabsrahmenübungen 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 handeln, z. B. zur NuK-Kommunikation. Es kann auch gemeinsam mit operativen Einheiten der Institution geübt werden, wie etwa mit einer zeitkritischen Organisationseinheit, mit der IT-Abteilung oder mit dem Facility Management. Gleiches gilt für mögliche extern Beteiligte oder Fachleute, welche die Übung beispielsweise als neutrale Beobachtende 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 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, die 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 erhalten. So können Stabsrahmenübungen z. B. mit Funktionstests (siehe 13.9 *Funktionstest (R optional +AS)*) kombiniert werden, um realitätsnah zu üben und damit Erkenntnisse zu gewinnen, die mit Simulationen alleine nicht erlangt werden können.

Synergiepotenzial

In Stabsrahmenübungen können insbesondere komplexe Szenarien geübt werden, die einen fließenden Übergang der Zuständigkeiten beinhalten oder es erforderlich machen, dass unterschiedliche (Sicherheits-)Disziplinen zusammen agieren. Dies ist zum Beispiel bei Cyberangriffen der Fall, die zunächst vom Incident Management der IT behandelt und wahrgenommen werden, bevor sie als schwerwiegender Sicherheitsvorfall durch die Informationssicherheit koordiniert werden. Wenn der Geschäftsbetrieb durch den Cyberangriff massiv beeinträchtigt wird, ist zusätzlich dazu eine Abstimmung zwischen der Informationssicherheit, der IT und dem sich konstituierenden Stab erforderlich, sobald der Not- oder Krisenfall ausgerufen wird. Auch wenn Cybersicherheitsvorfälle nicht per se durch BCM abgedeckt werden, kann es daher sinnvoll sein, ein solches Szenario im Stab zu üben. Stabsrahmenübungen können dann sachdienliche Hinweise über die Entscheidungshierarchien geben und die Zuständigkeiten oder Lücken in Zuständigkeitsbereichen transparent machen.

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.

13.7.1 Vorbereitung einer Stabsrahmenübung

Die Stabsrahmenübung wird wie die Stabsübung vorbereitet. Der zentrale Unterschied zwischen den beiden Übungsarten besteht darin, dass die Kommunikation der Teilnehmenden nicht auf den Stabsraum beschränkt ist. Es übt somit nicht nur der Stab, sondern auch darüberhinausgehende Teile der BAO, wie z. B. Notfallteams. Wie in einem realen Notfall üben die Teilnehmenden einer Stabsrahmenübung somit ihre Funktion an ihren jeweiligen Standorten. Sie nutzen hierzu auch die vorgesehenen Kommunikations-

kanäle dazwischen. Dies erfordert entsprechende Sicherheitsvorkehrungen. Es ist wichtig, diese Sicherheitsvorkehrungen bereits im Vorfeld zu klären und zu treffen. An jedem Übungsort sollte ein Mitglied des Übungsteams oder eine beobachtende Person anwesend sein oder per Videokonferenz zugeschaltet sein, um im Bedarfsfall eingreifen zu können. Im Folgenden werden einige Beispiele für weitere solcher Sicherheitsvorkehrungen genannt:

Beispiel

- *Einlagen und sonstige schriftliche Unterlagen müssen unter Angabe des Übungsdatums und der Bezeichnung eindeutig und auffällig als Übungselemente oder -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 geregelt sein, wie sich die Übungsteilnehmenden verhalten sollen, falls eine Abbruchbedingung oder ein realer Notfall eintritt.*
- *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 Medien, 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 Teilnehmenden 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 oder die BCB erwägen, den Ablauf zuvor mindestens einmal mit geeigneten Vertretenden der Teilnehmenden durchzuspielen („dry run"). 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 es empfehlenswert, die Teilnehmenden darauf hinzuweisen, dass die Übungsinhalte und -abläufe vertraulich behandelt werden sollen, damit die Geschehnisse und das Verhalten Einzelner nicht innerhalb der Institution weiter kommuniziert werden.*

Wenn die Stabsrahmenübung mit anderen Übungsarten, wie z. B. Funktionstests, kombiniert wird, dann beinhaltet die Vorbereitungsphase auch deren Aspekte und Schritte.

Ein wesentlicher Bestandteil einer Stabsrahmenübung ist die Simulation der Außenwelt durch Personen, die nicht zur BAO gehören. Diese Personen unterstützen den Ablauf indem sie während der Übung z. B.

- Szenario-Elemente wie einzuspielende Einlagen spielen
- 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 aufzubauen, die den Übungsablauf inklusive der Simulation der Außenwelt gesamthaft steuert (vgl. LÜKEX-Glossar des BBK, siehe [BBK2]).

13.7.2 Durchführung einer Stabsrahmenübung

Stabsrahmenübungen werden weitestgehend mit den gleichen Schritten wie Stabsübungen durchgeführt. Jedoch gehen Stabsrahmenübungen in der Regel mit einer größeren Beteiligung unterschiedlicher Übungsteilnehmender einher, die sich nicht nur auf den Stab selbst begrenzen.

13.8 Alarmierungsübung (R+AS)

Die Alarmierungsübung zielt darauf ab, Fehlerquellen und Schwächen in der Alarmierung der BAO zu identifizieren, die Wirksamkeit von Alarmierungsverfahren festzustellen und die BAO-Reaktionszeit konkreter verifizieren zu können. Eine erfolgreiche Alarmierung ist Grundlage für die weitere Bewältigung und es ist daher empfehlenswert, diese schnellstmöglich zu üben. Anhand von Alarmierungsübungen sollte getestet werden, ob die organisatorischen und technischen Maßnahmen eine Alarmierung im erforderlichen Zeitraum (auch außerhalb der üblichen Geschäftszeiten) sicherstellen. Ausgehend von einer Information einer Meldestelle wird über die zentrale Entscheidungsinstanz eine Alarmierungsmeldung und infolgedessen die Alarmierungskette ausgelöst und nachverfolgt. Innerhalb der Alarmierungsübung sollten die Reaktionszeiten ermittelt und dokumentiert werden. Alarmierungsübungen können in technikorientierte Tests und anwendungsorientierte Übungen unterschieden werden.

In technikorientierten Tests wird überprüft, ob die Kommunikationsmittel und -verfahren, die im Notfall eingesetzt werden, funktionsfähig sind. In anwendungsorientierten Übungen werden die vorhandene Alarmierungsdokumentation sowie organisatorischen

Regelungen, z. B. die Erreichbarkeit und Verfügbarkeit der relevanten Rolleninhabenden und der Stellvertretungen, überprüft. Darüber hinaus kann die Geschwindigkeit der Reaktion getestet und eingeübt werden.

Anwendungsorientierte Alarmierungsübungen setzen voraus, dass ein abgestimmter Alarmierungspfad mit aktuellen Kontaktdaten vorliegt und die zu nutzenden Kommunikationswege und -mittel zwischen den Teilnehmenden organisatorisch und technisch festgelegt, dokumentiert, umgesetzt und funktionstüchtig sind.

13.8.1 Vorbereitung einer Alarmierungsübung

Der Aufwand einer Alarmierungsübung ist aufgrund der geringen Komplexität deutlich kleiner als der einer Stabsübung. Typischerweise übernimmt der oder die BCB selbst diese Aufgabe.

Neben den üblichen Einträgen im Übungskonzept sollte abhängig vom definierten Alarmierungsprozess bei anwendungsorientierten Übungen entschieden werden, ob die Erreichbarkeit nur innerhalb oder auch außerhalb der üblichen Dienstzeit getestet werden soll (siehe 5.2.3 *Alarmierung der BAO (R+AS)*). 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, dann ist es wichtig, die erforderlichen Stellen vorab zu informieren, z. B. den Personal- oder Betriebsrat oder die IT-Abteilung.

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 Rolleninhabenden der BAO den Alarm positiv quittiert haben.

Falls die Institution eine Erreichbarkeit der entsprechenden Stellen im Alarmierungspfad außerhalb der üblichen Dienstzeit festgelegt hat, sollten Alarmierungsübungen über einen festgelegten Zeitraum auch die Alarmierung außerhalb der üblichen Dienstzeit testen.

Notfallszenario

Ein ausführliches 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 oder die BCB sollte in seiner Jahresplanung darauf achten, dass über einen festgelegten Zeitraum alle definierten Alarmierungswege getestet werden.

13.8.2 Durchführung einer Alarmierungsübung

In der Praxis hat es sich bewährt, die Alarmierungsübung unangekündigt durchzuführen, um möglichst reale Voraussetzungen zu schaffen. Gegebenenfalls können die Teilnehmenden aber zuvor von der oder dem BCB informiert werden, dass eine Alarmierungsübung innerhalb eines vorgegebenen Zeitraums stattfinden wird, um deren Kooperationsbereitschaft weiterhin zu erhalten.

13.9 Funktionstest (R optional +AS)

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, Notfallpläne und damit verbundenen Notfallmaßnahmen dahingehend überprüft, ob diese wie vorgesehen funktionieren. Anhand von Funktionstests sollte systematisch und, wenn vertretbar, realitätsnah überprüft werden, ob die Inhalte in der Betriebsdokumentation und den Notfallplänen 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 Mitarbeitenden einer Fachabteilung an einen Auswahlort verlagern und dort arbeiten lassen. (Szenario Standortausfall)*
- *Geschäftsvorgänge anhand der Schritte, die im Geschäftsfortführungsplan beschrieben sind, durch eine Person einer anderen Abteilung erledigen lassen. (Szenario Personalausfall)*
- *Temporär ein vorhandenes alternatives Dienstleistungsunternehmen nutzen. (Szenario Ausfall eines Dienstleistungsunternehmens)*
- *Mehrere untereinander abhängige Ausweichserver und alternative Netzverbindungen in Betrieb nehmen. (Szenario IT-Ausfall)*
- *Vorhandene IT-Wiederanlaufpläne und -Maßnahmen 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 Risikos 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.*

13.9.1 Vorbereitung eines Funktionstests

Eine Voraussetzung für die Funktionstests ist, dass die ressourcenzuständigen Organisationseinheiten anhand von Komponententests überprüft haben, ob die einzelnen Ressourcen, die für die Notfallvorsorge oder den Wiederanlauf im Notfall erforderlich sind, verfügbar sind und in Betrieb genommen werden können. In Komponententests wird geprüft, ob die Notfallmaßnahmen für einzelne Hardwarekomponenten, wie z. B. Server, Router etc., oder Softwarekomponenten, wie z. B. Applikationen, Services etc., wirksam und angemessen sind. Dies erfolgt typischerweise anhand von Tests, die nicht primär im BCM liegen, jedoch damit korrespondieren. Es ist daher empfehlenswert, die Planung der Komponententest und die des BCM aufeinander abzustimmen. Darunter fallen z. B.:

- 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 Aspekte 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 oder die -autorin 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 mögli-

chen Auswirkungen auf den Geschäftsbetrieb eine Freigabe von der Institutionsleitung einzuholen. Zudem sollten anhand der Risikoeinschätzung 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, vor allem im Reaktiv-BCMS. 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. Falls vor dem Test eine Testumgebung vorbereitet werden muss, ist es empfehlenswert, den Funktionstest in der Institution anzukündigen.

Hinweis

Die Herstellung und der Rückbau der Testumgebung müssen geplant werden. Die Planung wird am besten von ausgewählten Spezialisten aus Bewältigungsteams 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 Mitarbeitenden im Umgang mit dem Notfallplan*
- *die Überprüfung, ob die Zielvorgaben aus dem Notfallplan eingehalten werden können*

13.9.2 Durchführung eines Funktionstests

Funktionstests finden auf Basis der Ressourcenkategorien statt, die dem Notfallplan zugrunde liegen. Damit die Notfallpläne möglichst realistisch getestet werden, ist es empfehlenswert, den Ablauf des Funktionstests möglichst nah an der BC-Planung auszurichten. Die Übungsleitung hat die Aufgabe, den Ablauf des Funktionstests unter Beachtung der Ziele und der Zeitplanung zu steuern. Bei sehr einfachen Funktionstests, z. B. dem Testen eines Notfall-Laptops, kann die Übungsleitung durch die testende Person selbst wahrgenommen werden. Bei komplexen Funktionstests sollte hingegen die Übungslei-

tung durch eine separate Person besetzt sein, welche die Vorgänge koordiniert. Eine protokollierende Person oder weitere Unterstützungsrollen können den Ablauf sowie die Auswertung unterstützen und die anderen Beteiligten damit entlasten.

Es ist empfehlenswert, anhand einer einheitlichen Protokollvorlage pro getesteter Maßnahme oder Ressource zu dokumentieren, ob diese „ohne Befund" funktioniert hat oder ob es Auffälligkeiten gab oder Anmerkungen gegeben wurden.

Die Tabelle 40 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.*	*Aktualisierungsprozess prüfen*
Notfallarbeitsplatz	*Notfallrelevante Software prüfen*	***Teilweise erfolgreich***	*E-Mail und Warenwirtschaftssystem verfügbar. Kundschaftskartei nicht erreichbar.*	*Kundschaftskartei für standortübergreifende Zugriffe freischalten*

Tabelle 40: Beispiel für den Aufbau eines Testprotokolls

Eine protokollierende Person oder weitere Unterstützungsrollen können den Ablauf sowie die Auswertung unterstützen und die anderen Beteiligten damit entlasten. Zwingend notwendig ist dies jedoch nicht.

13.10 Auswertung und Nachbereitung von Übungen (R+AS)

Alle durchgeführten Übungen müssen ausgewertet und nachbereitet werden. Dies ist Voraussetzung, um das BCM weiterentwickeln und Korrekturbedarfe und Verbesserungsmöglichkeiten identifizieren zu können. 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 BC-Aufbauorganisation oder dem BCM-Prozess oder dem 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 Rolleninhabenden des Stabes zählen dazu.

Es sollten sowohl die für die Übung herangezogenen Dokumente, wie die Notfallpläne, als auch in der Übung erstellte Dokumente ausgewertet werden. Erstellte Dokumente sind zum einen Übungsprotokolle und Feedbackbögen der Übungsteilnehmenden. Zum anderen geben auch Ergebnisobjekte der Stabsübung, wie Visualisierungen, Protokolle oder fiktive Pressemitteilungen, Auskunft über die Reife des BCM. Alle Übungsergebnisse und identifizierte Korrekturbedarfe und Verbesserungsmöglichkeiten sollten in einem Übungsbericht dokumentiert werden. Der oder die BCB sollte anhand der Ergebnisse bewerten, wie ausgereift das BCM der Institution bereits ist.

Hinweis

*Mit der **Darstellung des Übungserfolges** ist hier nicht gemeint, dass beurteilt wird, ob die Teilnehmenden immer „richtig", d. h. wie geplant und 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. Darüber hinaus kann aber auch dann von einer erfolgreichen Übung gesprochen werden, wenn Korrekturbedarfe und Verbesserungsmöglichkeiten identifiziert wurden und diese Erkenntnisse genutzt werden, um das BCMS weiter zu verbessern.*

13.10.1 Zusätzliche Aspekte zur Auswertung und Nachbereitung einer Stabs(rahmen)übung

Im Anschluss an Stabs(rahmen)übungen sollte eine Auswertungsrunde mit allen Übungsteilnehmenden durchgeführt werden. Es ist empfehlenswert, dass diese zum vorgesehenen Zeitpunkt durch die Übungsleitung oder einen im Vorfeld festgelegten, geeigneten Moderator gestartet wird. Die Teilnehmenden 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 Teilnehmenden 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.

13.10.2 Zusätzliche Aspekte zur Auswertung einer Alarmierungsübung

Wird eine Alarmierungssoftware eingesetzt, ist es empfehlenswert, die von dieser Alarmierungssoftware erzeugten Protokolle auszuwerten. Diese können zusammen mit manuell im Übungsverlauf erzeugten Protokollen im Anschluss der Übung ausgewertet werden.

Ferner ist es in der Auswertung empfehlenswert, die BAO-Reaktionszeit anhand der tatsächlich benötigten Zeit für die Alarmierung zu überprüfen. Hierbei gilt es jedoch zu berücksichtigen, dass die BAO-Reaktionszeit neben der Alarmierungszeit und Zeit bis zum Ausruf eines Notfalls auch die Detektionszeit umfasst (siehe 7 *Business-Impact-Analyse (R+AS)*). Alarmierungsübungen und Kombinationen aus Alarmierungsübung und Stabs (-rahmen-)übungen können somit immer nur einen Teil dieser BAO-Reaktionszeit überprüfen. Die tatsächliche Detektionszeit kann letztendlich nur geschätzt oder aus realen Ereignissen abgeleitet werden.

13.10.3 Ergebnisvorstellung und Festlegung der Folgeschritte

Der Übungsbericht muss an den oder die BCB kommuniziert werden. Der oder die BCB sollte diese im Maßnahmenplan aufgreifen und in der Korrektur und Verbesserung des BCMS weiterbehandeln (siehe Kapitel 15 *Aufrechterhaltung und Verbesserung (R+AS)*).

14 Leistungsüberprüfung und Berichterstattung (AS)

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 Korrektur und Verbesserung des BCMS behandelt werden (siehe Kapitel 15 *Aufrechterhaltung und Verbesserung (R+AS)*). Die Institutionsleitung erhält durch die Berichte aus der Leistungsüberprüfung die Möglichkeit, potenzielle Fehlentwicklungen zu identifizieren und proaktiv darauf reagieren zu können. Je nach gewählter BC-Strategie kann es zudem erforderlich sein, neben dem eigenen BCMS, die BC-Fähigkeiten von zeitkritischen Dienstleistungsunternehmen zu überwachen und zu bewerten, insbesondere, wenn zeitkritische Lieferketten abzusichern sind. Abbildung 55 gibt einen Überblick über die notwendigen Schritte zur Leistungsüberprüfung und Berichterstattung.

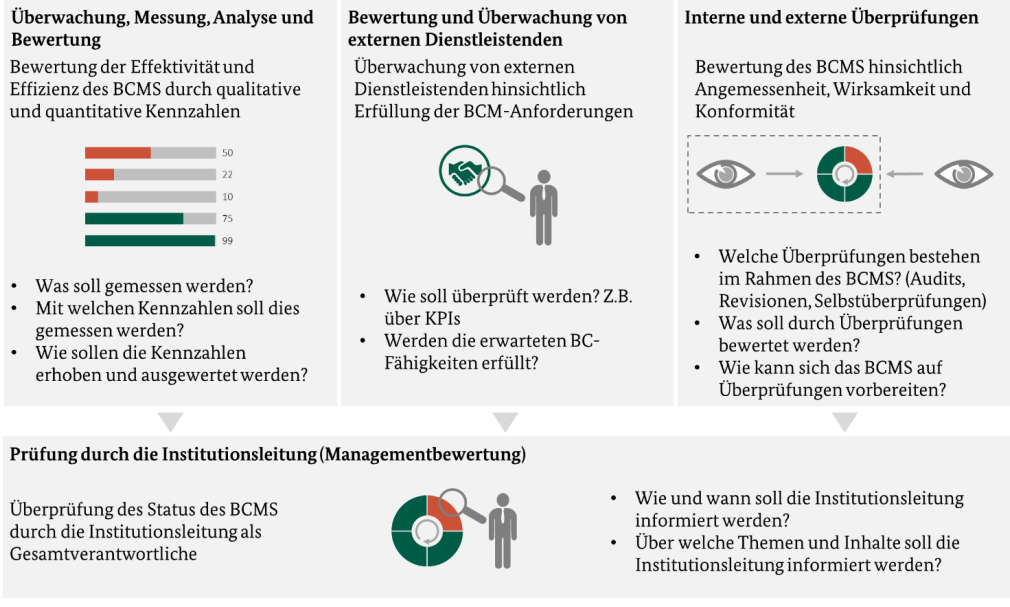

Abbildung 55: BCM-Prozessschritte zur Leistungsüberprüfung

14.1 Überwachung, Messung, Analyse und Bewertung (AS)

Um die Effektivität und Effizienz des BCMS sicherzustellen, bedarf es einer regelmäßigen Überwachung, Messung, Analyse und Bewertung aller BCM-Prozessschritte. Hierzu soll-

ten Kennzahlen definiert und erhoben werden, die dann mit definierten Zielwerten abgeglichen werden.

Auswahl von Messzielen, Kennzahlen und Zielwerten

Im ersten Schritt muss die Institution festlegen, was mittels Kennzahlen gemessen werden soll, d. h. **Messziele** festlegen. In der Praxis werden 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. Die Messziele müssen in der Gesamtheit einen jeweils aktuellen Überblick über den Status des BCMS und die einzelnen BCM-Prozessschritte ermöglichen. Übergreifend muss die Effektivität und Effizienz des BCMS eingeschätzt werden.

Hinweis

*Anstelle von (Leistungs-)Kennzahlen wird in einigen Institutionen die englische Bezeichnung **Key Performance Indicator (KPI)** genutzt. In diesem Standard wird einheitlich aus Gründen der einfacheren Lesbarkeit der Begriff Kennzahlen benutzt, obwohl im näheren Sinn damit Leistungskennzahlen gemeint sind.*

Es müssen messbare Kennzahlen identifiziert und definiert werden, die es ermöglichen, die mit den festgelegten Messzielen erwünschten Aspekte zu messen. Die Kennzahlen müssen auf einer sinnvollen Datengrundlage beruhen bzw. es muss für die Kennzahlen eine angemessene Datengrundlage geschaffen werden. Die BCM-Prozessschritte müssen regelmäßig auf Vollständigkeit, Aktualität, Angemessenheit, Wirksamkeit, Plausibilität und Effizienz überprüft werden. Dabei kann zwischen quantitativen und qualitativen Aspekten unterschieden werden:

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 werden. Beispielsweise können hierzu Kennzahlen zur Aktualität oder Konsistenz der Daten sowie zu Fehlern festgelegt werden.

In Tabelle 41 sind beispielhafte 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

Geschäfts-prozess	***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 41: Beispiele für Kennzahlen ohne Zielwerte

Darüber hinaus können Kennzahlen auch einen eher informativen Charakter besitzen, der nicht primär dazu dient, die Qualität des BCMS zu bewerten. Sie können dazu dienen, wesentliche Ergebnisse des BCMS zu zählen und zusammenzufassen. Ein typisches Beispiel hierfür wäre die Anzahl der Geschäftsprozesse je MTPD-Stufe.

Kennzahlen lassen sich immer im Kontext der Institution unterschiedlich interpretieren. So könnte eine insgesamt hohe Prozentzahl zeitkritischer Geschäftsprozesse entweder bedeuten, dass es sinnvoll ist, die BIA-Methodik daraufhin zu überprüfen, ob die Parameter angemessen sind oder ob die Schadensanalyse durch die Prozessfachleute 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 aufzuzeigen, sollten, wo möglich, Zielwerte für diese festgelegt werden. Insbesondere die grundlegenden Zielsetzungen des BCMS, die allgemeinen Anforderungen sowie die aktuelle und gewünschte Reife sollten dabei beachtet werden (siehe *3.1 Übernahme der Verantwortung durch die Leitungsebene (R+AS)*, 4.2.1 *Identifizierung von Anforderungen und Einflussfaktoren an das BCMS (AS)*).

Tabelle 42 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 42: Beispiele für Kennzahlen mit definierten Zielwerten

Erhebung der Kennzahlen

Mittels der Kennzahlen muss regelmäßig ein aktueller Überblick über den Status des BCMS und die einzelnen BCM-Prozessschritte erfasst werden. Hierbei ist es wichtig, insbesondere die Abarbeitung der Korrekturbedarfe und Aufgaben im Maßnahmenplan mit einzubeziehen (siehe Kapitel 15.3 *Umsetzung und Überwachung von Korrektur- und Verbesserungsmaßnahmen (AS)*). Die Institution muss festlegen, durch wen und in welchen Abständen die Kennzahlen erhoben und ausgewertet werden. Die definierten Kennzahlen können zentral durch den oder die BCB oder dezentral durch die BC-Koordinierenden oder andere zuständige BCM-Rolleninhabende erhoben werden.

Der oder die BCB kann für die dezentrale Erhebung der 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 überprüft werden.

Analyse und Bewertung der Kennzahlen

Die erhobenen Kennzahlen müssen dokumentiert werden. Dabei ist es empfehlenswert, die Dokumentation der Kennzahlen zentral zusammenzuführen, um einen ganzheitlichen Überblick über alle Kennzahlen zu erhalten. Indem die Kennzahlen ausgewertet

werden, muss regelmäßig ein aktueller Überblick über den Status des BCMS und die einzelnen BCM-Prozessschritte erstellt werden.

Die erhobenen Kennzahlen sollten ausgewertet werden, z. B. indem sie mit den Zielwerten, sofern vorhanden, verglichen und Abweichungen bewertet werden. Hierzu sollte zum einen die Ursache identifiziert und zum anderen die Schwere der Abweichung bewertet werden. Grobe Abweichungen vom Zielwert können im anschließenden kontinuierlichen Verbesserungsprozess priorisiert behandelt werden. Identifizierte Ursachen helfen dabei, konkrete Korrektur- und Verbesserungsmaßnahmen abzuleiten.

Beispiel

Kennzahl	*Teilschritt des BCMS-Prozesses*	*Zielwert*	*Ist-Wert*	*Abweichung*	*Ursache*	*Schweregrad*
Abdeckungsgrad der Geschäftsprozesse 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 BC-Koordinierenden benannt.*	*hoch*
Abdeckungsgrad zeitkritischer Geschäftsprozesse in der Übungsplanung	*Notfallkonzept*	*N = 100 %*	*50 %*	*Ja*	*In mehreren OE sind keine BC-Koordinierenden benannt.*	*hoch*

Tabelle 43: Beispiel zur Priorisierung von Abweichungen

Darüber hinaus sollten Trends ermittelt werden, z. B. anhand von Vergleichswerten aus den Vorjahren. Zusätzlich ist es empfehlenswert, auch eindeutig negative Trends näher zu untersuchen.

Hinweis

Da anhand von Kennzahlen der Fortschritt oder der Erfüllungsgrad einer Anforderung oder eines gewünschten Zielzustands gemessen werden kann, sind Kennzahlen auch ein geeignetes Mittel für Selbstüberprüfungen im BCMS. Insbesondere aus qualitativen Kennzahlen können Verbesserungspotenziale oder die Reife des BCMS abgeleitet werden.

14.2 Bewertung und Überwachung von externen Dienstleistungsunternehmen (AS)

Falls aufgrund der gewählten BC-Strategie „Ausreichende BC-Fähigkeit von Dienstleistungsunternehmen" der Wiederanlauf zeitkritischer Geschäftsprozesse von externen Dienstleistungsunternehmen abhängig ist, dann ist es für die Institution entscheidend, dass das Dienstleistungsunternehmen auch tatsächlich über die notwendigen BC-Fähigkeiten verfügt. Entsprechend müssen durch die Institution bei dieser BC-Strategie die erwarteten BC-Fähigkeiten der relevanten, zeitkritischen Dienstleistungsunternehmen anhand von BC-Anforderungen bewertet werden. Da die Bewertung der BC-Fähigkeiten der relevanten Dienstleistungsunternehmen nur eine Momentaufnahme darstellt, sollte die Institution durch geeignete Überwachungsverfahren, z. B. Dokumentenprüfungen, Vor-Ort-Audits und Revisionen, fortlaufend sicherstellen, dass die idealerweise vertraglich festgelegten BC-Anforderungen über den gesamten Zeitraum der Leistungserbringung durch das Dienstleistungsunternehmen erfüllt werden.

Zusätzlich kann es sinnvoll sein, die BC-Fähigkeit der relevanten Dienstleistungsunternehmen anhand definierter Leistungskennzahlen zu überwachen oder sich diese anhand von Berichten regelmäßig mitteilen zu lassen. Die Leistungskennzahlen der Dienstleistenden können, neben den Kennzahlen zum Zustand des eigenen BCMS, im Bericht zum Gesamtstatus des BCMS berücksichtigt werden. Dies bietet sich insbesondere im Fall von zeitkritischen Lieferketten an, da deren Resilienz wesentlich von der BC-Fähigkeit der verschiedenen Dienstleistungsunternehmen abhängig ist und daher im Sinne einer Gesamteinschätzung zur BC-Fähigkeit von großer Bedeutung sind.

Ferner ist es empfehlenswert, zu überlegen, wie eine Wiederherstellung des Geschäftsbetriebs ermöglicht wird, ohne dass der oder die ursprüngliche Dienstleistende wieder die Arbeit aufnimmt (Exit-Strategie).

Hinweis

Das Hilfsmittel Vorschläge zu BC-Strategien beinhaltet eine detaillierte Vorgehensweise, wie die notwendige BC-Fähigkeit der Dienstleistungsunternehmen aus Sicht der Institution definiert, bewertet und überwacht werden kann.

14.3 Interne und externe Überprüfungen (AS)

Das BCMS muss in regelmäßigen Abständen daraufhin überprüft werden, ob es angemessen, wirksam und anforderungsgerecht ist. Für alle Überprüfungen müssen die Ziele und der Geltungsbereich festgelegt sein. Das BCMS sollte jährlich und anlassbezogen durch interne Revisionen, externe Revisionen oder Audits überprüft werden. Die Häufigkeit, Detailtiefe und der Untersuchungsbereich der Überprüfungen sollte sich an der Risikosituation der Institution und der Bedeutung der BCM-Prozessschritte ausrichten. Die Überprüfungen sollten von unabhängigen Personen durchgeführt werden, die weder an der Planung noch am Aufbau des BCMS beteiligt waren.

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 Mitarbeitende der Institution durchgeführt.*

*Ferner kann eine **Selbsteinschätzung** zum BCMS z. B. durch den oder die BCB selbst erfolgen.*

Audits

Audits des BCMS werden entweder freiwillig oder aufgrund der Anforderungen externer Interessensgruppen durch die Institution angefordert. In regulierten Branchen, beispielsweise im Banken- und Versicherungssektor, können Audits auch von Aufsichtsorganen initiiert werden. Mit der Durchführung von Audits werden in der Regel qualifizierte unabhängige Dritte beauftragt, z. B. zugelassene Auditoren. 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.

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. Die interne Revision muss überprüfen, ob das BCMS die bestehenden Anforderungen erfüllt, d.h. die Ziele aus der Leitlinie, Anforderungen der Interessengruppen, die Anforderungen aus diesem Standard sowie die Anforderungen aus den einzelnen BCMS-Prozessschritten. Korrektur- und Verbesserungsmaßnahmen als Ergebnis vorangegangener Überprüfungen müssen als Grundlage einer aktuellen Überprüfung herangezogen werden.

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 oder die BCB 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 Dokumentvorlagen 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 Überprüfungen vorzubereiten. Bei einer Selbsteinschätzung obliegt es dem Untersuchenden selbst, zu entscheiden wann und wie die aufgedeckten Mängel und damit verbundenen Korrekturbedarfe und Verbesserungsmöglichkeiten behandelt werden.

Vorbereitung von Revisionen und Audits

Da alle Überprüfungen mit entsprechendem zeitlichem und personellem Aufwand verbunden sind, sollte der oder die BCB eine zeitliche Übersicht der verschiedenen, geplanten Überprüfungen erstellen. Diese zeitliche Übersicht dient dazu, mögliche Engpässe der Mitarbeitenden 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 müssen als Grundlage einer aktuellen Überprüfung dienen)
- Ressourcenbedarf zur Unterstützung
- benötigte Dokumente und Informationen

Der oder die BCB muss festlegen, wie auf Revisions- und Audit-Ankündigungen angemessen und zielgerichtet reagiert werden kann und welche Dokumente und Informationen innerhalb einer Überprüfung bereitgestellt werden sollen. Dazu ist es hilfreich, die eigenen Aktivitäten im BCM auf die Revisions- und Audit-Termine abzustimmen.

Zudem sollte der oder die BCB bei einer Revision oder einem Audit die Revisoren oder Auditoren aktiv bei der Auswahl der Dokumente und Kontaktpersonen unterstützen. Zu-

sätzlich ist es empfehlenswert, die BCM-Rolleninhabenden über die bevorstehende Überprüfung zu informieren. Für eine externe Revision oder für ein Audit sind in der Regel folgende Aspekte relevant:

- aktuell gültige Dokumente des BCM
- Nachweise der Umsetzung und Ergebnisobjekte aller BCM-Prozessschritte
- aktueller Maßnahmenkatalog
- aktuell erhobene Kennzahlen
- frühere Ergebnisse von Überprüfungen
- Nachweise geschlossener Abweichungen vorangegangener Überprüfungen

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. Darin festgestellte Abweichungen müssen innerhalb der Aufrechterhaltung und Verbesserung zeitnah bewertet und für das BCMS angemessene Korrektur- und Verbesserungsmaßnahmen aus der Bewertung abgeleitet und umgesetzt werden. Analog zu den Vorgaben des Kapitels 14.1 *Überwachung, Messung, Analyse und Bewertung (AS)* 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, dokumentiert und durch Korrekturmaßnahmen behandelt werden (siehe Kapitel 15 *Aufrechterhaltung und Verbesserung (R+AS)*). 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.

14.4 Managementbewertung (AS)

Der oder die BCB muss die Institutionsleitung regelmäßig über den Status des BCMS informieren. Der oder die BCB sollte dafür die Ergebnisse der Leistungsüberprüfung ziel-

gruppengerecht 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 muss die Institutionsleitung strategische oder taktische Entscheidungen treffen, um eine Neuausrichtung des BCMS zu erreichen und Fehlentwicklungen entgegenzuwirken. Die Institutionsleitung muss folgende Punkte berücksichtigen. Diese sollten im Bericht des oder der BCB aufgeführt werden:

- Status von Maßnahmen aus dem vorangegangenen BCMS-Zyklus oder aus den Entscheidungen der Institutionsleitung
- interne und externe Veränderungen des Umfeldes des BCMS
- identifizierte Abweichungen, Trends und weitere Erkenntnisse aus Leistungsüberprüfungen (siehe Kapitel:14.1 *Überwachung, Messung, Analyse und Bewertung (AS)* und hier insbesondere Audit und Revisionsergebnisse sowie erhobene Kennzahlen)
- Rückmeldungen von Interessengruppen zum BCMS
- Bewertung der Angemessenheit der Leitlinie BCMS 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 4.4 *Dokumentation (R+AS)*)
- Unzureichend abgesicherte Risiken vorangegangener BCM-Risikoanalysen
- Erkenntnisse aus Störungen mit Notfallpotenzial und eingetretenen Notfällen sowie
- Chancen zur Verbesserung

Der oder die BCB sollte mit der Institutionsleitung vereinbaren, wie häufig der Status zum BCMS berichtet werden soll. Die Institutionsleitung kann entscheiden, ob der oder die BCB 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 Überprüfungen aufgrund interner oder externer Anforderungen
- Korrekturbedarfe und Verbesserungsmöglichkeiten an der Leistungsüberprüfung, um deren Effizienz und Effektivität zu steigern
- Konsequenzen der geplanten Änderungen

Die Ergebnisse der Bewertung durch die Institutionsleitung müssen dokumentiert und an die relevanten internen und externen Interessengruppen kommuniziert werden. Grundlage bilden die in der Planung und Konzeption identifizierten Interessengruppen (siehe Kapitel 4.2.1 *Identifizierung von Anforderungen und Einflussfaktoren an das BCMS (AS)*) sowie die festgelegten Informationsansprüche (siehe Kapitel 4.4.2 *Festlegung von Dokumentinformationen (AS)*).

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, können die Reife des BCMS konkreter eingeschätzt und Verbesserungen kenntlich gemacht werden.

Als Grundlage des Berichts zum Gesamtstatus des BCMS kann auf die Übersicht möglicher Kriterien zur Einschätzung der Reife des BCMS zurückgegriffen werden, wie im folgenden Beispiel dargestellt (siehe Tabelle 44: Übersicht möglicher Kriterien zur Einschätzung der Reife des BCMS (Beispiele)).

Beispiel

Kriterien	***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 dem BIA-Vorfilter 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.*

Kriterien	*Quelle*
Fähigkeiten und Kenntnisse der BCM-Rolleninhabenden und Grad der BCM-Kultur in der Institution	*identifizierte Korrekturbedarfe und Verbesserungsmöglichkeiten aus durchgeführten Schulungen, Sensibilisierungsmaßnahmen sowie Rückmeldungen der Rolleninhabenden in Stabsübungen*
Im Rahmen des Reaktiv-BCMS identifizierte Korrekturbedarfe und Verbesserungsmöglichkeiten	*Maßnahmenliste*

Tabelle 44: Übersicht möglicher Kriterien zur Einschätzung der Reife des BCMS (Beispiele)

15 Aufrechterhaltung und Verbesserung (R+AS)

Anhand der identifizierten Korrekturbedarfe und Verbesserungsmöglichkeiten müssen im Rahmen der **Aufrechterhaltung und Verbesserung** konkrete Maßnahmen entwickelt und umgesetzt werden. Diese sollten in einem Maßnahmenplan festgehalten werden:

- **Korrekturmaßnahmen und Maßnahmen zur Aufrechterhaltung** dienen dazu, Abweichungen des Managementsystems und der BC-Planung zu den Anforderungen an das BCMS zu identifizieren und 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 der Rolle BCB, 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. Die Eignung, Angemessenheit und Wirksamkeit des BCMS muss durch geeignete Maßnahmen fortlaufend verbessert werden. 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 BC-Planung stets den geltenden Anforderungen entsprechen.

Das Reaktiv-BCMS befähigt die Institution nur zu einer rudimentären Notfall- und Krisenbewältigung und bedarf daher einer nahtlos anschließenden Weiterentwicklung zum Aufbau- oder Standard-BCMS, sobald der erste PDCA-Zyklus beendet ist (siehe Kapitel 15.4 *Weiterentwicklung des Reaktiv-BCMS (R)*). Typisch für ein Reaktiv-BCMS sind auch eine erhebliche Anzahl an „Lücken in der Absicherung", die in dem Maßnahmenplan dokumentiert sind und aufgrund ihrer teilweise weitreichenden Bedeutung erst im Aufbau- oder Standard-BCMS systematisch behoben werden können.

R

Sofern über einen längeren Zeitraum oder aus einzelnen BCM-Prozessschritten im Rahmen **des Aufbau- oder Standard-BCMS** 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 oder die BCB muss daher stetig prüfen, ob erkannte Abweichungen dokumentiert, angemessen korrigiert und Verbesserungsmöglichkeiten in das BCMS überführt werden.	**AS**

Die folgende Abbildung gibt einen Überblick über das Vorgehen zur Korrektur und Verbesserung des BCMS.

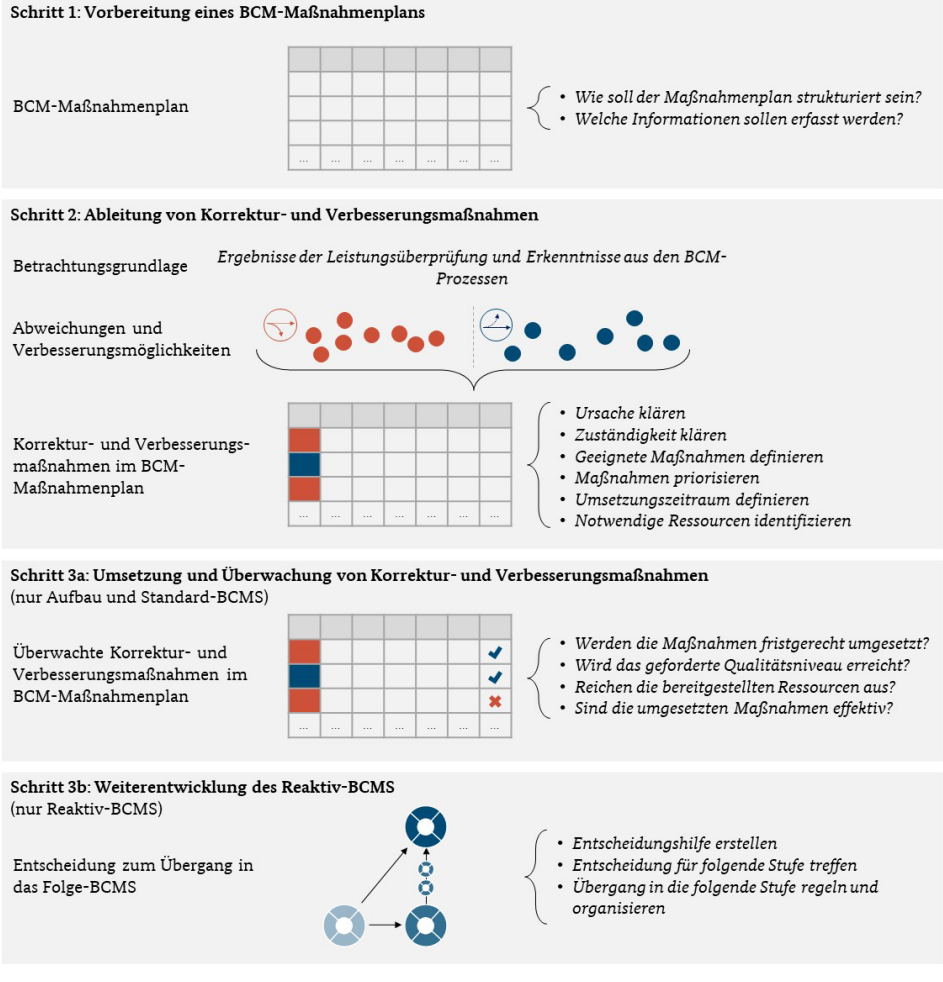

Abbildung 56: BCM-Prozessschritte zur Aufrechterhaltung und Verbesserung des BCMS

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.

15.1 Vorbereitung eines BCM-Maßnahmenplans (R+AS)

Um den Gesamtüberblick über alle Korrektur- und Verbesserungsmaßnahmen zu behalten und diese leichter steuern zu können, sollte der oder die BCB eine Dokumentvorlage für einen BCM-Maßnahmenplan vorbereiten. Die wesentlichen Inhalte eines BCM-Maßnahmenplans werden im folgenden Beispiel veranschaulicht und im Kapitel 15.2 *Ableitung von Korrektur- und Verbesserungsmaßnahmen (R+AS)* näher beschrieben. Falls nicht das Hilfsmittel Dokumentvorlage *BCM-Maßnahmenplan* benutzt wird, sollten die aufgeführten Punkte in der Dokumentvorlage 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* *Mitarbeitende 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 Mitarbeitenden nicht in die Bearbeitung von Geschäftsfortführungsplänen eingewiesen worden sind.*	*Ursache hierfür ist, dass diese Mitarbeitenden sich nicht im Schulungs- und Sensibilisierungsplan befanden. Grund hierfür ist, dass diese dem oder der BCB nicht als neue Mitarbeitende gemeldet wurden. Mit der Organisationseinheit Personal wurde bislang kein Meldeprozess definiert für den Fall, dass Mitarbeitende die Organisationseinheit wechseln oder die Institution verlassen.*
Vorgesehene Korrektur- oder Verbesserungsmaßnahme	*Zur kurzfristigen Behandlung der Abweichung werden die Geschäftsfortführungspläne gemeinsam mit den BCKs 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 Wechsel von Mitarbeitenden und Benennung von BCM-Rolleninhabenden gemeinsam mit der Organisationseinheit Personal überarbeitet und entsprechende Kontrollmechanismen entwickelt werden.*
Zuständige Stelle(n)	*BCB, BCKs*	*Organisationseinheit Personal*
Festgelegte Priorität	***Hoch*** – ~~*Mittel*~~ – ~~*Gering*~~	~~*Hoch*~~ – ***Mittel*** – ~~*Gering*~~
Geplanter Fertigstellungstermin	*16.08.2022 (Heute + 2 Wochen)*	*31.12.2023*
Notwendige Ressourcen	*Verfügbarkeit der zuständigen BCKs und der zuständigen Mitarbeitenden*	*Verfügbarkeit der Mitarbeitenden 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 BCB* *14.08.: GFP wurden aktualisiert.*	*01.08.: Maßnahme freigegeben durch BCB*

Tabelle 45: Struktur des BCM-Maßnahmenplans am Beispiel einer fiktiven Abweichung

15.2 Ableitung von Korrektur- und Verbesserungsmaßnahmen (R+AS)

Anhand des BCM-Maßnahmenplans sollte der oder die BCB alle Korrektur- und Verbesserungsmaßnahmen dokumentieren. 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. Verbesserungsmöglichkeiten umzusetzen
- Umsetzungsstatus der Korrektur- oder Verbesserungsmaßnahme(n)
- Für die Umsetzung zuständige Stellen
- benötigten Ressourcen (finanziell, personell und zeitlich)

Für jede Korrektur- und Verbesserungsmaßnahme sollte zudem der Fertigstellungstermin dokumentiert werden. Ferner ist es empfehlenswert, die folgenden Inhalte im Maßnahmenplan zusätzlich zu dokumentieren.

- Eindeutige Kennung der Korrektur- oder Verbesserungsmaßnahmen
- Priorisierung der Maßnahme
- Dokumentation relevanter Umsetzungsdetails

Hinweis

Üblicherweise behandeln Korrektur- und Verbesserungsmaßnahmen einzelne Teilprozesse des BCMS sowie der BC-Planung. 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.

15.3 Umsetzung und Überwachung von Korrektur- und Verbesserungsmaßnahmen (AS)

Nachdem die Korrektur- oder Verbesserungsmaßnahmen geplant und dokumentiert wurden, müssen diese durch die jeweils zuständigen Stellen bestätigt und umgesetzt werden. Der oder die BCB muss den Umsetzungsstatus regelmäßig anhand des Maßnahmenplans 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 oder die BCB diese mithilfe der Mittel zur Überprüfung des BCMS (siehe Kapitel 13 und 14) dahingehend untersuchen, ob sie angemessen und wirksam sind. Das Ergebnis der Untersuchung sollte der oder die BCB 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.

15.4 Weiterentwicklung des Reaktiv-BCMS (R)

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 BC-Planung bestehen.

In dem BIA-Vorfilter 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 BC-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.
- 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 57 sind die hierfür erforderlichen Schritte in einer Übersicht dargestellt:

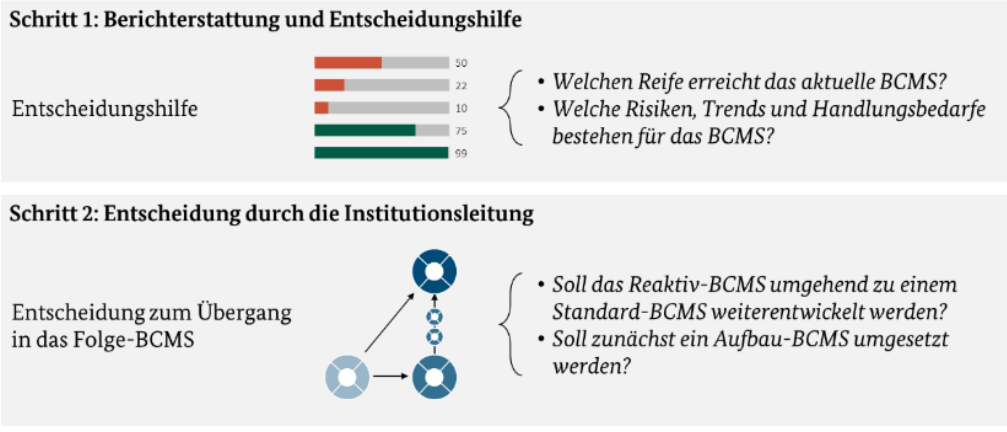

Abbildung 57: BCM-Prozessschritte zur Weiterentwicklung des Reaktiv-BCMS

15.4.1 Berichterstattung und Entscheidungshilfe (R)

Es ist empfehlenswert, dass der oder die BCB die gewonnenen Erkenntnisse zum BCMS zusammenfasst und der Institutionsleitung als Entscheidungshilfe zur Verfügung stellt. Ziel der Entscheidungshilfe ist es, die wesentlichen Erkenntnisse vorzustellen und die erforderlichen Schritte und Maßnahmen zur Weiterentwicklung des BCMS abzustimmen. Hierbei ist es sinnvoll, insbesondere zu analysieren, 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, ist es empfehlenswert, die vorliegenden Erkenntnisse zu verdichten, die Risiken, Trends und Handlungsbedarfe im BCM abzuleiten und Lösungsoption vorzuschlagen. Je geringer die Zielerreichung durch den oder die BCB eingeschätzt wird, desto eher ist eine Weiterentwicklung anhand eines Aufbau-BCMS empfehlenswert. Tabelle 46 listet mögliche Erkenntnisse auf.

Beispiel

Kriterien	***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 dem BIA-Vorfilter und der BIA*
Abdeckungsgrad ausreichend abgesicherter Ressourcen gemäß RTA vs. RTO	*Soll-Ist-Vergleich*

Kriterien	*Quelle*
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-Rolleninhabenden und Grad der BCM-Kultur in der Institution	*identifizierte Korrekturbedarfe und Verbesserungsmöglichkeiten aus durchgeführten Schulungen, Sensibilisierungsmaßnahmen sowie Rückmeldungen der Rolleninhabenden in Stabsübungen*
Im Rahmen des Reaktiv-BCMS identifizierte Korrekturbedarfe und Verbesserungsmöglichkeiten	*Maßnahmenliste*

Tabelle 46: Übersicht möglicher Kriterien zur Einschätzung der Reife des BCMS (Beispiele)

15.4.2 Entscheidung durch die Institutionsleitung (R)

Anhand der Entscheidungshilfe muss 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 Aufbau-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.

Option 2: Direkter Übergang in ein Standard-BCMS sieht vor, dass alle Teilschritte eines Standard-BCMS durchlaufen werden und der gesamte BCMS-Geltungsbereich untersucht und bedarfsgerecht abgesichert wird. Mit dem direkten 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 diese Expertise zum Aufbau eines Standard-BCMS extern zu beschaffen, z. B. durch einen Erfahrungsaustausch in Arbeitsgremien.

Hinweis

Im Aufbau- und Standard-BCMS werden die Rahmenbedingungen sehr viel detaillierter in einer erneuten Planungsphase betrachtet als bisher. Daher ist zu erwarten, dass die Ziele nicht nur in Bezug auf die ausgewählte Stufe hin geändert werden müssen. Dies kann auch grundlegende Auswirkungen auf die Leitlinie BCMS haben.

Anhang A: Anforderungskatalog

Der Anforderungskatalog zu diesem Standard wird auf der BSI-Webseite als separate Excel-Datei zur Verfügung gestellt.

Anhang B: Hinweise zu den Hilfsmitteln

Auf den BSI-Webseiten bietet das BSI ergänzend zum BSI-Standard 200-4 verschiedene Hilfsmittel und Dokumentvorlagen an, die die Anwendenden darin unterstützen sollen, die beschriebenen Prozesse und Methoden im BCM effektiv umzusetzen. Diese Hilfsmittel werden kontinuierlich weiterentwickelt und ausgebaut. Daher ist eine aktuelle Übersicht der Hilfsmittel immer auf den Webseiten des BSI zu finden.

Anhang C: Glossar

Das Glossar zu diesem Standard mit integriertem Abkürzungsverzeichnis wird auf der BSI-Webseite als separates Dokument zur Verfügung gestellt.

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 and resilience – Business continuity management systems – Guidance on the use of ISO 22301, ISO/TC 292, 2020

[22316] ISO 22316:2017, International Organization for Standardization (Hrsg.), Security and resilience – Organizational resilience – Guidance on the use of ISO 22301, ISO/TC 292, 2020

[22317] ISO/TS 22317:2021, 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/DE/Infothek/Glossar/glossar_node.html

[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/DE/Mediathek/Publikationen/LUEKEX/glossar-luekex18.pdf

[BCMN] BCM-Info Newsletter des BSI, Bundesamt für Sicherheit in der Informationstechnik, 2020, https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Newsletter/newsletter.html

[BRLN] Katastrophenschutzgesetz des Landes Berlin, https://gesetze.berlin.de/bsbe/?docId=jlr-KatSchGBE2021rahmen&query=JURISLINK%3A%22KatSchG+BE%22

[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/Oeffentliche-Verwaltung/Sicherheitspruefungen/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, https://im.baden-wuerttemberg.de/fileadmin/redaktion/m-im/intern/dateien/pdf/20170213_VwV-Stabsarbeit.pdf

[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 BCMS 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

[BMI2] Konzeption Zivile Verteidigung, Bundesministerium des Innern (Hrsg.), 2016, https://www.bmi.bund.de/DE/themen/bevoelkerungsschutz/zivil-und-katastrophenschutz/konzeption-zivile-verteidigung/konzeption-zivile-verteidigung-node.html

[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