

DIN EN ISO 22313

ICS 03.100.01

**Sicherheit und Schutz des Gemeinwesens –
Business Continuity Management Systems –
Leitlinie (ISO 22313:2012);
Deutsche Fassung EN ISO 22313:2014**

Societal security –
Business continuity management systems –
Guidance (ISO 22313:2012);
German version EN ISO 22313:2014

Sécurité sociétale –
Systèmes de management de la continuité d'activité –
Lignes directrices (ISO 22313:2012);
Version allemande EN ISO 22313:2014

Gesamtumfang 67 Seiten

DIN-Normenausschuss Feuerwehrwesen (FNFW)

Nationales Vorwort

Der Text von ISO 22313:2012 wurde vom Technischen Komitee ISO/TC 223 „Societal Security“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO 22313:2012 durch das Technische Komitee CEN/TC 391 „Schutz und Sicherheit der Bürger“, dessen Sekretariat vom NEN (Niederlande) gehalten wird, ohne Änderungen übernommen.

Für die deutsche Mitarbeit ist das Gremium NA 031-05 FBR „Fachbereichsausschuss Sicherheit und Schutz des Gemeinwesens — SpA zu ISO/TC 223 Societal security“ im Normenausschuss Feuerwehrwesen (FNFW) im DIN verantwortlich.

Die Begriffsübersetzungen wurden einheitlich mit denen in der Terminologienorm DIN EN ISO 22300, mit denen in DIN EN ISO 22301 und in Anpassung an die verwendeten Fachtermini abweichend von Vorzugsübersetzungen erstellt. Ergänzend wurden folgende Fachtermini abweichend von Vorzugsübersetzungen übersetzt:

- Die englischen Fachbezeichnungen für Business Impact Analyse (BIA) und Business Continuity Management (BCM) wurden in den deutschen Text ohne Übersetzung übernommen, da es sich um etablierte Begrifflichkeiten auch im deutschen Sprachgebrauch handelt.
- Der englische Begriff „incident response“ wurde mit „Reaktion auf einen Zwischenfall“ übersetzt. Als Fachterminus wird im Deutschen hierfür auch die Bezeichnung „Einsatz zur Gefahrenabwehr“ verwendet. Damit einhergehend wurde für den englischen Begriff „response“ je nach passendem Kontext synonym im Deutschen „Reaktion“ oder „Gefahrenabwehr“ verwendet.

Für die in diesem Dokument zitierten Internationalen Normen wird im Folgenden auf die entsprechenden Deutschen Normen hingewiesen:

ISO 19011	siehe DIN EN ISO 19011
ISO 22300	siehe DIN EN ISO 22300
ISO 22301	siehe DIN EN ISO 22301
ISO 27002	siehe DIN EN ISO 27002

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 19011, *Leitfaden zur Auditierung von Managementsystemen*

DIN EN ISO 22300, *Sicherheit und Schutz des Gemeinwesens — Terminologie*

DIN EN ISO 22301, *Sicherheit und Schutz des Gemeinwesens — Business Continuity Management System — Anforderungen*

DIN ISO/IEC 27002, *Informationstechnik — IT-Sicherheitsverfahren — Leitfaden für das Informationssicherheits-Management*

Deutsche Fassung

Sicherheit und Schutz des Gemeinwesens —
Business Continuity Management Systems —
Leitlinie (ISO 22313:2012)

Societal security —
Business continuity management systems —
Guidance (ISO 22313:2012)

Sécurité sociétale —
Systèmes de management de la continuité d'activité —
Lignes directrices (ISO 22313:2012)

Diese Europäische Norm wurde vom CEN am 18. Oktober 2014 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Management-Zentrum des CEN-CENELEC oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

CEN-CENELEC Management-Zentrum: Avenue Marnix 17, B-1000 Brüssel

Inhalt

Seite

Europäisches Vorwort	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich	11
2 Normative Verweisungen	11
3 Begriffe	11
4 Kontext der Organisation	12
4.1 Verstehen der Organisation und ihres Kontextes	12
4.2 Verstehen der Bedürfnisse und Erwartungen der Interessengruppen	13
4.2.1 Allgemeines	13
4.2.2 Rechtliche und behördliche Anforderungen	14
4.3 Festlegung des Anwendungsbereichs des Managementsystems	14
4.3.1 Allgemeines	14
4.3.2 Anwendungsbereich des BCMS	15
4.4 Business Continuity Management System	15
5 Führung	15
5.1 Führung und Selbstverpflichtung	15
5.2 Selbstverpflichtung der Leitung	15
5.3 Leitlinien	16
5.4 Funktionen, Verantwortlichkeiten und Befugnisse innerhalb der Organisation	17
6 Planung	18
6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten	18
6.2 Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit und Pläne zur Zielerreichung	18
7 Unterstützung	18
7.1 Ressourcen	18
7.1.1 Allgemeines	18
7.1.2 BCMS-Ressourcen	19
7.1.3 Personal zur Reaktion auf einen Zwischenfall	19
7.2 Kompetenz	20
7.3 Bewusstseinsbildung	22
7.4 Kommunikation	23
7.5 Dokumentierte Information	24
7.5.1 Allgemeines	24
7.5.2 Erstellung und Aktualisierung	25
7.5.3 Steuerung dokumentierter Information	25
8 Betrieb	26
8.1 Ablaufplanung und Steuerung	26
8.1.1 Elemente des BCM	27
8.1.2 Lenken der BCM-Umgebung	28
8.1.3 Instandhaltung des Systems zur der Aufrechterhaltung der Betriebsfähigkeit	29
8.1.4 Messen der Effektivität	29
8.1.5 Ergebnisse	29

8.2	Business Impact Analyse und Risikobewertung.....	30
8.2.1	Allgemeines	30
8.2.2	Business Impact Analyse	31
8.2.3	Risikobewertung	33
8.3	Strategie zur Aufrechterhaltung der Betriebsfähigkeit.....	34
8.3.1	Festlegung und Auswahl	34
8.3.2	Festlegen des Ressourcenbedarfs	36
8.3.3	Schutz und Schadensminderung.....	42
8.4	Einführung und Umsetzung von Maßnahmen zur Aufrechterhaltung der Betriebsfähigkeit.....	43
8.4.1	Allgemeines	43
8.4.2	Struktur zur Reaktion auf einen Zwischenfall.....	43
8.4.3	Warnung und Kommunikation.....	44
8.4.4	Pläne zur Aufrechterhaltung der Betriebsfähigkeit.....	46
8.4.5	Wiederherstellung.....	54
8.5	Übungen und Überprüfungen	55
8.5.1	Allgemeines	55
8.5.2	Übungsprogramm	55
8.5.3	Übungen zu Plänen für die Aufrechterhaltung der Betriebsfähigkeit.....	56
9	Leistungsüberprüfung.....	58
9.1	Überwachung, Messung, Analyse und Bewertung.....	58
9.1.1	Allgemeines	58
9.1.2	Bewertung der Verfahren zur Aufrechterhaltung der Betriebsfähigkeit.....	59
9.2	Internes Audit.....	61
9.3	Managementüberprüfung	62
10	Verbesserung	63
10.1	Abweichung und Korrekturmaßnahmen.....	63
10.2	Ständige Verbesserung.....	64
	Literaturhinweise.....	65

Europäisches Vorwort

Der Text von ISO 22313:2012 wurde vom Technischen Komitee ISO/TC 223 „Societal security“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO 22313:2016 durch das Technische Komitee CEN/TC 391 „Schutz und Sicherheit der Bürger“ übernommen, dessen Sekretariat vom NEN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Mai 2015, und etwaige entgegenstehende nationale Normen müssen bis Mai 2015 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN und/oder CENELEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die ehemalige jugoslawische Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO 22313:2012 wurde vom CEN als EN ISO 22313:2014 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Föderation von Nationalen Normungsorganisationen (ISO Mitglieder). Die Erstellung von Internationalen Normen wird normalerweise von ISO Technischen Komitees durchgeführt. Jede Mitgliedsorganisation, das Interesse an einem Thema hat, für welches ein Technisches Komitee gegründet wurde, hat das Recht in diesem Komitee vertreten zu sein. Internationale Organisationen, staatlich und nicht-staatlich, in Liaison, nehmen ebenfalls an der Erarbeitung teil. ISO arbeitet eng mit der Internationalen Elektrotechnischen Kommission (IEC) bei allen elektrotechnischen Themen zusammen.

Internationale Normen werden in Übereinstimmung mit den Regeln nach ISO/IEC Direktive, Teil 2 erarbeitet.

Die Hauptaufgabe von Technischen Komitees ist es Internationale Normen zu erarbeiten. Internationale Norm-Entwürfe, die von Technischen Komitees verabschiedet wurden, werden den Mitgliedsorganisationen zur Abstimmung zur Verfügung gestellt. Für die Veröffentlichung als Internationale Norm werden mindestens 75 % Zustimmung der Mitgliedsorganisationen benötigt.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

ISO 22313:2012 wurde vom Technischen Komitee ISO/TC 233 „*Societal security*“, erarbeitet.

Einleitung

Allgemeines

Diese Internationale Norm enthält Leitlinien, sofern angemessen, zu den in ISO 22301:2012 festgelegten Anforderungen und bietet Empfehlungen („sollte“) und Zulässigkeiten („darf“) im Hinblick auf diese Anforderungen. Diese Internationale Norm beabsichtigt nicht, zu allen Aspekten der Aufrechterhaltung der Betriebsfähigkeit allgemeine Leitlinien zu liefern.

Diese Internationale Norm enthält die gleichen Überschriften wie die ISO 22301, aber sie wiederholt nicht die Anforderungen Business Continuity Management Systeme und damit verbundene Begriffe. Organisationen, die sich darüber informieren möchten, müssen dafür ISO 22301 und ISO 22300 heranziehen.

Zur weiteren Klärung und Erläuterung von Kernaussagen enthält diese Internationale Norm eine Anzahl von Bildern. Diese Bilder dienen ausschließlich der Veranschaulichung, und der damit zusammenhängende Text im Hauptteil dieser Internationalen Norm hat Vorrang vor den Bildern.

Ein Business Continuity Management System (BCMS) betont die Bedeutung:

- des Verstehens der Bedürfnisse einer Organisation sowie der Notwendigkeit der Einführung von Leitlinien und Zielsetzungen für die Aufrechterhaltung der Betriebsfähigkeit;
- des Einführens und Betreibens von Kontrollen und Maßnahmen zum Managen der Gesamtfähigkeit einer Organisation, mit Zwischenfällen mit Betriebsunterbrechung umzugehen;
- des Überwachens und Überprüfens der Leistung und der Effektivität des BCMS; und
- einer ständigen Verbesserung auf Grundlage objektiver Messungen.

Ein BCMS hat, wie jedes andere Managementsystem, folgende zentrale Bestandteile:

- a) eine Leitlinie;
- b) Personen mit festgelegten Verantwortlichkeiten;
- c) Managementprozess in Bezug auf:
 - 1) Leitlinien,
 - 2) Planung,
 - 3) Umsetzung und Betrieb,
 - 4) Leistungsbewertung,
 - 5) Bewertung des Managements, und
 - 6) Verbesserung;
- d) Dokumentationsunterlagen zur Bereitstellung auditierbarer Nachweise; und
- e) jeden Prozess des BCMS, der für die Organisation relevant ist.

Die Aufrechterhaltung der Betriebsfähigkeit erfolgt in der Regel organisationsspezifisch, deren Umsetzung kann allerdings von großer Tragweite für die Allgemeinheit und andere Drittparteien sein. Eine Organisation ist mit großer Wahrscheinlichkeit abhängig von externen Organisationen, und es wird andere Organisationen geben, die von ihr abhängig sind. Eine wirksame Aufrechterhaltung der Betriebsfähigkeit trägt daher zu einer widerstandsfähigeren Gesellschaft bei.

Das Planen-Durchführen-Prüfen-Handeln-Modell

Diese Internationale Norm wendet das „Planen-Durchführen-Prüfen-Handeln“-Modell (PDCA, en: Plan-Do-Check-Act) an, um das BCMS einer Organisation zu planen, einzuführen, umzusetzen, zu betreiben, zu überwachen, zu überprüfen, aufrechtzuerhalten und dessen Effektivität ständig zu verbessern.

Bild 1 stellt dar, wie das BCMS die Anforderungen der Interessengruppen als Eingaben für das Business Continuity Management (BCM) verwendet und mittels der geforderten Maßnahmen und Prozesse Kontinuitätsergebnisse (d.h. eine gelenkte Aufrechterhaltung der Betriebsfähigkeit) erzeugt, die diese Anforderungen erfüllen.

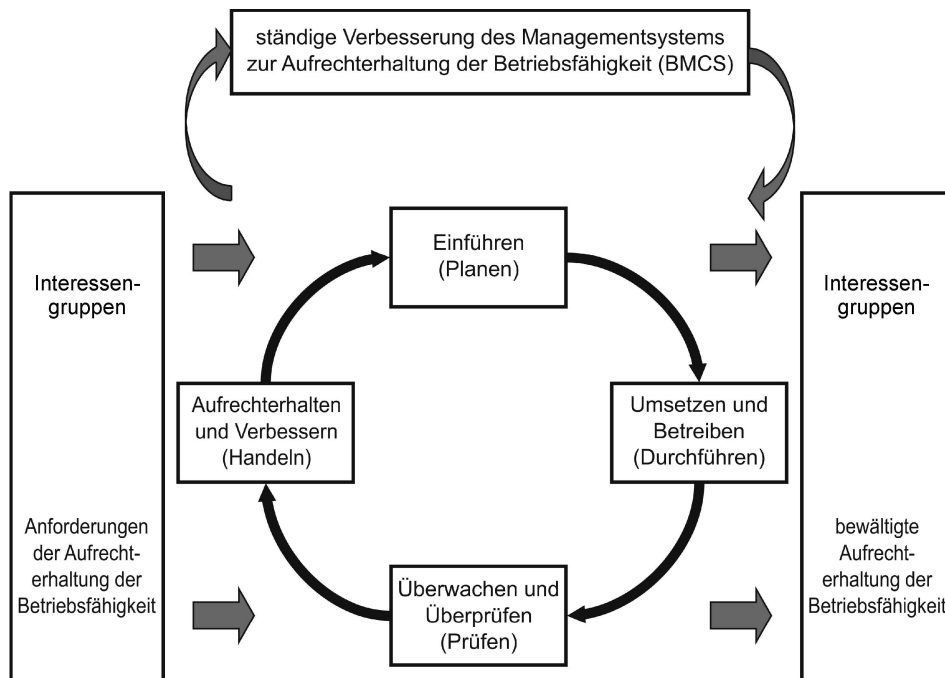


Bild 1 — Auf die BCMS-Prozesse angewandetes PDCA-Modell

Tabelle 1 — Erläuterungen zum PDCA-Modell

Planen (Einführen)	Einführen von Leitlinien, Zielsetzungen, Kontrollen, Prozessen und Verfahren zur Aufrechterhaltung der Betriebsfähigkeit, die für die Verbesserung der Aufrechterhaltung der Betriebsfähigkeit relevant sind, um Ergebnisse zu erzielen, die sich mit den übergeordneten Leitlinien und Zielsetzungen der Organisation in Übereinstimmung befinden.
Durchführen (Umsetzen und Betreiben)	Umsetzen und Anwenden der Leitlinien, Kontrollen, Prozesse und Verfahren zur Aufrechterhaltung der Betriebsfähigkeit.
Prüfen (Überwachen und Überprüfen)	Überwachen und Überprüfen der Leistung vor dem Hintergrund der Leitlinien und Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit, Berichten der Ergebnisse an das Management zum Zwecke der Überprüfung, Festlegung und Autorisierung von Maßnahmen zur Korrektur und Verbesserung.
Handeln (Aufrechterhalten und Verbessern)	Aufrechterhalten und Verbessern des BCMS durch die Ausführung von Korrekturmaßnahmen auf Grundlage der Ergebnisse der Managementüberprüfung sowie Neubeurteilung des Anwendungsbereichs des BCMS sowie der Leitlinien und Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit.

Bestandteile des PDCA-Modells in dieser Internationalen Norm

Es besteht ein direkter Zusammenhang zwischen dem Inhalt von Bild 1 und den Abschnitten dieser Internationalen Norm.

Tabelle 2 — Zusammenhang zwischen dem PDCA-Modell und den Abschnitten 4 bis 10

Bestandteil des PDCA-Modells	Abschnitt, in dem der Bestandteil des PDCA-Modells behandelt wird
Planen (Einführen)	Abschnitt 4 (Kontext der Organisation) legt fest, was die Organisation zu unternehmen hat, damit sichergestellt ist, dass das BCMS ihre Anforderungen erfüllt, unter Berücksichtigung aller relevanten internen und externen Faktoren, einschließlich: — der Bedürfnisse und Erwartungen der Interessengruppen; — ihrer rechtlichen und behördlichen Verpflichtungen; — des geforderten Anwendungsbereichs des BCMS.
	Abschnitt 5 (Führung) legt die zentrale Funktion des Managements im Hinblick darauf fest, dass die Selbstverpflichtung nachgewiesen wird und Leitlinien, Funktionen, Verantwortlichkeiten und Befugnisse festgelegt werden.
	Abschnitt 6 (Planung) beschreibt die Maßnahmen, die erforderlich sind, um strategische Zielsetzungen und Leitsätze für das BCMS als Ganzes einzuführen. Diese Maßnahmen legen den Kontext für die Business Impact Analyse und für die Risikobewertung (8.2) sowie die Strategie zur Aufrechterhaltung der Betriebsfähigkeit (8.3) fest.
	Abschnitt 7 (Unterstützung) identifiziert die zentralen Elemente, die vorhanden sein müssen, um das BCMS zu unterstützen, d. h. Ressourcen, Kompetenzen, Bewusstseinsbildung, Kommunikation und dokumentierte Information.
Durchführen (Umsetzen und Betreiben)	Abschnitt 8 (Betrieb) legt die Elemente des Business Continuity Managements (BCM) fest, die erforderlich sind, um die Aufrechterhaltung der Betriebsfähigkeit zu erreichen.
Prüfen (Überwachen und Überprüfen)	Abschnitt 9 (Leistungsüberprüfung) enthält die Grundlage zur Verbesserung des BCMS durch Messen und Bewerten von dessen Leistung.
Handeln (Aufrechterhalten und Verbessern)	Abschnitt 10 (Verbesserung) behandelt erforderliche Korrekturmaßnahmen für Abweichungen, die anhand einer Leistungsbewertung festgestellt wurde.

Aufrechterhaltung der Betriebsfähigkeit

Die Aufrechterhaltung der Betriebsfähigkeit ist die Fähigkeit der Organisation, die Belieferung mit Produkten oder Dienstleistungen nach einem Zwischenfall mit Betriebsunterbrechung auf akzeptablen, zuvor festgelegten Niveaus fortzusetzen. Das Business Continuity Management (BCM) ist der Prozess zum Erreichen der Aufrechterhaltung der Betriebsfähigkeit und bereitet eine Organisation darauf vor, mit Zwischenfällen mit Betriebsunterbrechung umzugehen, die die Organisation andernfalls davon abhalten könnten, ihre Ziele zu erreichen.

Durch die Einordnung des BCM in den Rahmen und die Bereiche eines Managementsystems ergibt sich ein Business Continuity Management System (BCMS), das dem BCM ermöglicht, kontrolliert, bewertet und ständig verbessert zu werden.

In dieser Internationalen Norm wird das Wort „Betrieb“ als ein allumfassender Begriff für die Abläufe und Dienste verwendet, die von einer Organisation beim Verfolgen ihrer Ziele, ihres Zwecks oder Aufträge ausgeführt werden. Daher gilt sie gleichermaßen für große, mittlere und kleine Unternehmen, die im industriellen, kommerziellen, öffentlichen und gemeinnützigen Bereich tätig sind.

Jeder Zwischenfall, egal ob klein oder groß, ob natürlicher Art, durch einen Unfall oder vorsätzlich herbeigeführt, besitzt das Potential, eine größere Störung der Betriebsabläufe der Organisation und deren Fähigkeit, Produkte und Dienstleistungen zu liefern, hervorzurufen. Die Umsetzung der Maßnahmen zur Aufrechterhaltung der Betriebsfähigkeit bevor eine Störung eintritt, anstelle darauf zu warten, dass eine Störung eintritt, ermöglicht der Organisation die Wiederaufnahme von Betriebsabläufen, bevor ein inakzeptables Ausmaß an Auswirkungen entsteht.

Das BCM umfasst Folgendes:

- a) ein klares Verständnis der zentralen Produkte und Dienstleistungen einer Organisation sowie über die Tätigkeiten zu deren Bereitstellung;
- b) die Kenntnis über die Prioritäten bei der Wiederaufnahme von Tätigkeiten und über die Ressourcen, die diese erfordern;
- c) ein klares Verständnis der Bedrohungen für diese Tätigkeiten, inklusive der Abhängigkeiten zwischen ihnen und der Kenntnis der Auswirkungen, falls diese Tätigkeiten nicht wieder aufgenommen werden;
- d) die Verfügbarkeit bewährter und zuverlässiger Vorkehrungen zur Wiederaufnahme dieser Tätigkeiten nach einem Zwischenfall mit Betriebsunterbrechung; und
- e) das Sicherstellen, dass diese Vorkehrungen regelmäßig überprüft und aktualisiert werden, damit sie unter allen Umständen wirksam sind.

Die Aufrechterhaltung der Betriebsfähigkeit kann sowohl bei plötzlichen Zwischenfällen mit Betriebsunterbrechung (z. B. Explosionen) als auch bei allmählich eintretenden Zwischenfällen mit Betriebsunterbrechung (z. B. Grippepandemien) wirksam sein.

Tätigkeiten können durch die verschiedensten Vorfälle unterbrochen werden, von denen die meisten schwer vorherzusagen oder zu analysieren sind. Durch Konzentration auf die Auswirkungen einer Betriebsstörung und nicht auf die Ursache werden bei der Aufrechterhaltung der Betriebsfähigkeit diejenigen Tätigkeiten identifiziert, die für die Organisation überlebenswichtig sind, und ermöglicht der Organisation zu bestimmen, was zur weiteren Erfüllung ihrer Verpflichtungen erforderlich ist. Durch die Aufrechterhaltung der Betriebsfähigkeit kann eine Organisation erkennen, was zum Schutz ihrer Ressourcen (z. B. Personen, Betriebsgelände, Technologien und Informationen), ihrer Lieferkette, ihrer Interessengruppen und ihres Rufes unternommen werden muss, bevor ein Zwischenfall mit Betriebsunterbrechung eintritt. Durch diese Erkenntnis ist die Organisation in der Lage, ihre Reaktionen realistisch zu betrachten, die voraussichtlich benötigt werden, falls eine Betriebsstörung eintritt, sodass sie selbstsicher Konsequenzen managen und inakzeptable Auswirkungen vermeiden kann.

Eine Organisation mit einer angemessenen Aufrechterhaltung der Betriebsfähigkeit kann außerdem Gelegenheiten wahrnehmen, die andernfalls als zu risikoreich bewertet werden würden.

Die folgenden Diagramme (Bilder 2 und 3) verdeutlichen konzeptionell, wie die Aufrechterhaltung der Betriebsfähigkeit durch Abschwächen von Auswirkungen in bestimmten Situationen wirksam werden kann. Die relativen Abstände zwischen den in den Diagrammen dargestellten Stufen dienen nicht der Darstellung bestimmter zeitlicher Abstände.

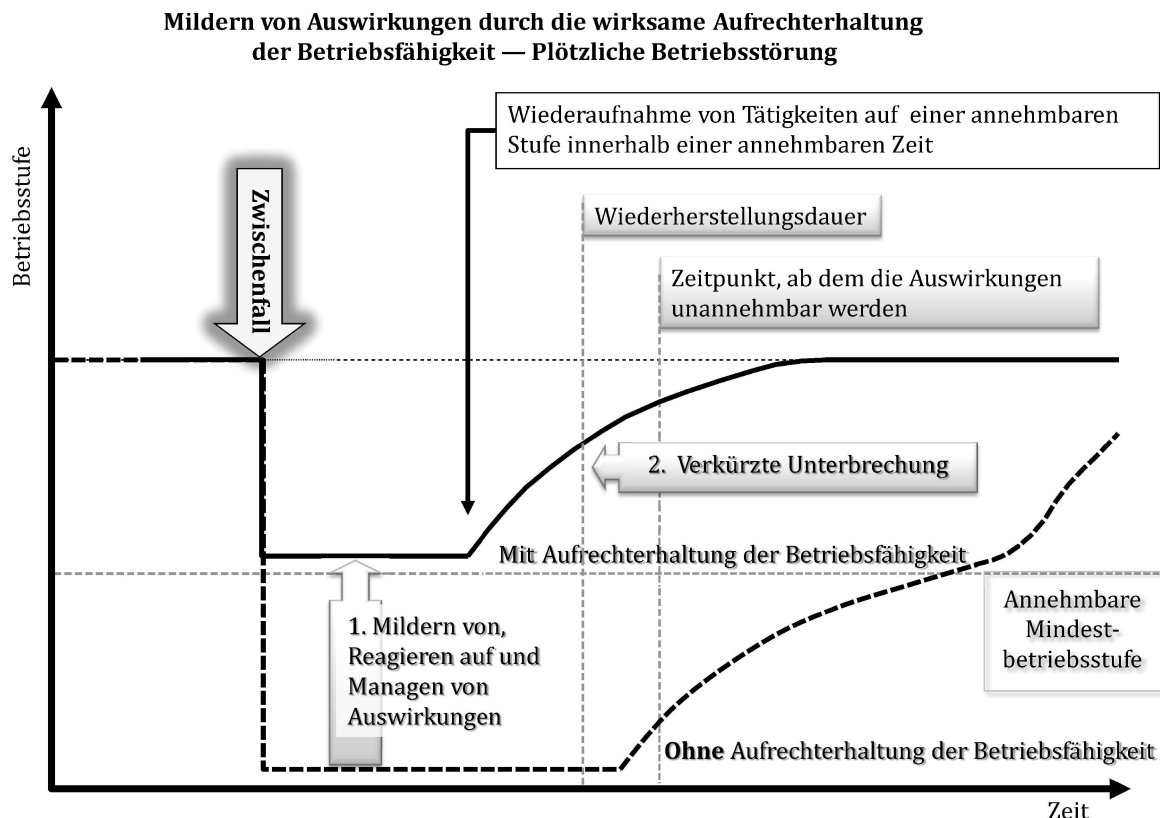


Bild 2 — Darstellung einer wirksamen Aufrechterhaltung der Betriebsfähigkeit bei plötzlicher Betriebsstörung

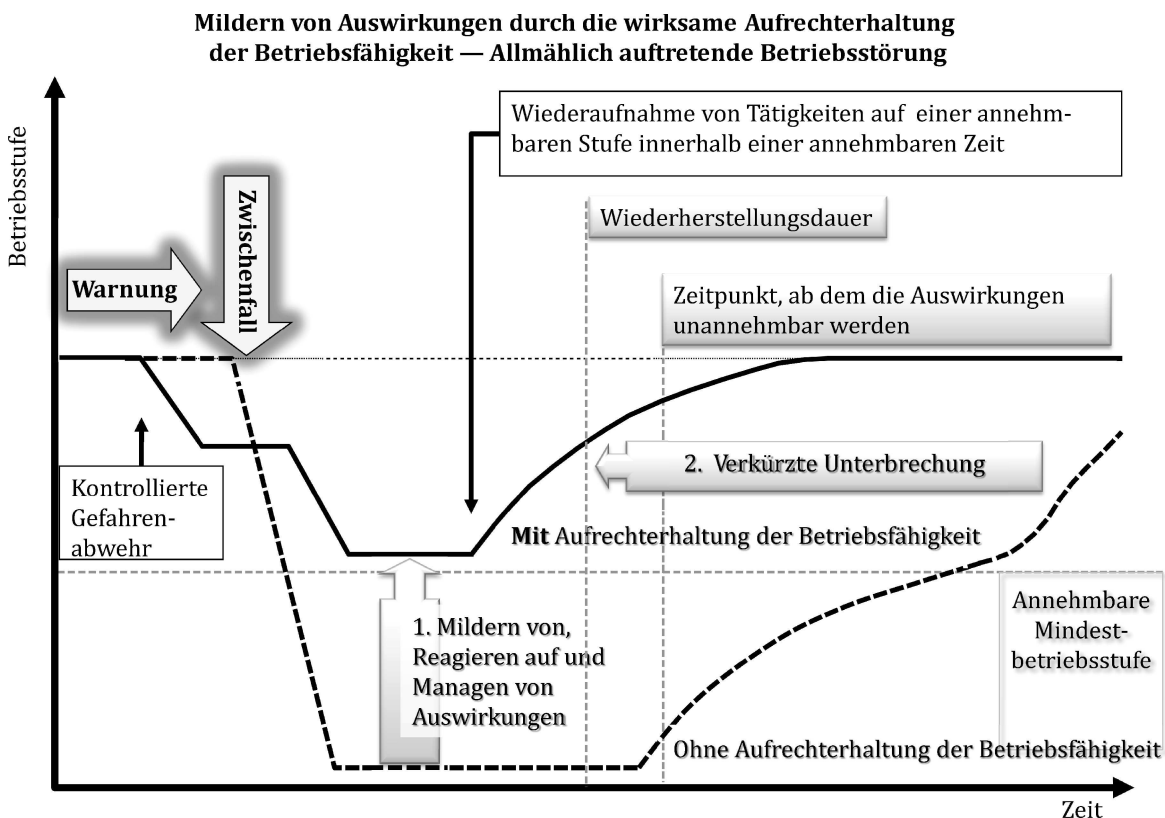


Bild 3 — Darstellung einer wirksamen Aufrechterhaltung der Betriebsfähigkeit bei allmählich eintretender Betriebsstörung (z. B. herannahende Pandemie)

1 Anwendungsbereich

Diese Internationale Norm für Business Continuity Management Systeme enthält Leitlinien, die auf international anerkannten Praktiken zur Planung, Einführung, Umsetzung, Betrieb, Überwachung, Überprüfung, Aufrechterhaltung und ständigen Verbesserung eines dokumentierten Managementsystems beruhen, die Organisationen ermöglichen, sich auf Zwischenfälle mit Betriebsunterbrechung vorzubereiten, auf sie zu reagieren und sich nach ihrem Eintreten von ihnen zu erholen.

Diese Internationale Norm beabsichtigt keine Einheitlichkeit im Aufbau eines BCMS, setzt jedoch bei einer Organisation voraus, dass diese ein BCMS gestaltet, das, ihren Bedürfnissen entspricht und die Anforderungen ihrer Interessengruppen erfüllt. Diese Bedürfnisse werden durch rechtliche, behördliche, organisatorische und branchenspezifische Anforderungen, durch die Produkte und Dienstleistungen, die eingesetzten Prozesse, die Betriebsumgebung, die Größe und Struktur der Organisation und die Anforderungen der Interessengruppen geprägt.

Diese Internationale Norm ist generisch und gilt für alle Organisationsgrößen und -typen, einschließlich großer, mittlerer und kleiner Unternehmen, die im industriellen, kommerziellen, öffentlichen und gemeinnützigen Bereich tätig sind und

- a) ein BCMS einführen, umsetzen, aufrechterhalten und verbessern möchten,
- b) die Übereinstimmung mit den Leitlinien einer Organisation im Hinblick auf die Aufrechterhaltung der Betriebsfähigkeit sicherstellen möchten oder
- c) eine Eigenfeststellung oder eine Selbsterklärung der Übereinstimmung mit dieser Internationalen Norm erstellen möchten.

Diese Internationale Norm kann nicht dazu angewendet werden, die Befähigung einer Organisation zur Erfüllung der eigenen Kontinuitätsbedürfnisse oder der Erfüllung von Kunden-, gesetzlichen oder behördlichen Bedürfnissen zu bewerten. Organisationen, die dies wünschen, können die Anforderungen von ISO 22301 anwenden, um anderen die Übereinstimmung nachzuweisen oder um die Zertifizierung ihres BCMS durch eine akkreditierte dritte Stelle Zertifizierungsstelle zu ersuchen.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO 22300, *Societal security — Terminology*

ISO 22301, *Societal security — Business continuity management systems — Requirements*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO 22300 und ISO 22301.

4 Kontext der Organisation

4.1 Verstehen der Organisation und ihres Kontextes

Dieser Abschnitt handelt vom Verstehen des Kontextes der Organisation in Verbindung mit der Erstellung und Lenkung des BCMS. Die Erstellung und die Verwaltung des BCMS werden in 8.1 behandelt.

Die Organisation sollte die internen und externen Faktoren, die für ihren Zweck und ihre Tätigkeiten relevant sind, bewerten und verstehen. Diese Information sollte bei der Einführung, Umsetzung, Aufrechterhaltung und Verbesserung des BCMS der Organisation und bei der Zuordnung von Prioritäten berücksichtigt werden.

Die Bewertung des externen Kontextes einer Organisation sollte, sofern relevant, folgende Faktoren beinhalten:

- das politische, gesetzliche und behördliche Umfeld, ob international, national, regional oder lokal;
- das soziale und kulturelle, finanzielle, technologische, wirtschaftliche, natürliche und wettbewerbliche Umfeld, ob international, national, regional oder lokal;
- die Verpflichtungen und Beziehungen hinsichtlich der Lieferkette;
- die Betrachtung interner Risikostudien, unter Berücksichtigung anderer relevanter Informationsmanagementsysteme sowie generell aller Informationen aus dem Wissensmanagement;
- die entscheidenden Faktoren und Trends, die eine Auswirkung auf die Ziele und den Betrieb der Organisation haben; und
- die Beziehungen zu Interessengruppen außerhalb der Organisation und deren Ansichten und Werte.

Die Bewertung des internen Kontextes einer Organisation sollte, sofern relevant, folgende Faktoren beinhalten:

- Produkte und Dienstleistungen, Tätigkeiten, Ressourcen, Lieferketten und Beziehungen zu Interessengruppen;
- die Fähigkeiten im Sinne von Ressourcen und Wissen (z. B. Kapital, Zeit, Personen, Prozesse, Systeme und Technologien);
- Informationssysteme, Informationsflüsse und Entscheidungsfindungsprozesse (beide, formal und formlos);
- Interessengruppen innerhalb der Organisation;
- Leitlinien und Zielsetzungen sowie die Strategien, mit denen diese umgesetzt werden;
- Zukunftschancen und Unternehmensprioritäten;
- Ansichten, Werte und Kultur;
- Normen und Referenzmodelle, die von der Organisation angewendet werden; und
- Strukturen (z. B. Führung, Funktionen und Verantwortlichkeiten).

4.2 Verstehen der Bedürfnisse und Erwartungen der Interessengruppen

4.2.1 Allgemeines

Bei der Einführung ihres BCMS sollte die Organisation sicherstellen, dass die Bedürfnisse und Anforderungen der Interessengruppen berücksichtigt werden.

Die Organisation sollte alle Interessengruppen ermitteln, die für das BCMS von Bedeutung sind und auf Grundlage deren Bedürfnisse und Erwartungen ihre Anforderungen bestimmen. Es ist wichtig, nicht nur verbindliche und angegebene Anforderungen zu erkennen, sondern auch alle Anforderungen, die sich implizit ergeben.

ANMERKUNG Die Organisation muss sich über alle Gruppen bewusst sein, die ein Interesse an der Organisation besitzen, wie z. B. Medien, die Öffentlichkeit vor Ort, Wettbewerber usw.

Bei der Planung und Umsetzung des BCMS ist es wichtig, Tätigkeiten zu ermitteln, die gegenüber den Interessengruppen angemessen sind, aber zwischen verschiedenen Fällen unterscheiden. Während es beispielsweise angemessen sein kann, nach einem Zwischenfall mit Betriebsunterbrechung mit allen Interessengruppen zu kommunizieren, kann es unangemessen sein, bei der Erstellung und Verwaltung eines BCM mit allen Interessengruppen zu kommunizieren (8.1.1).

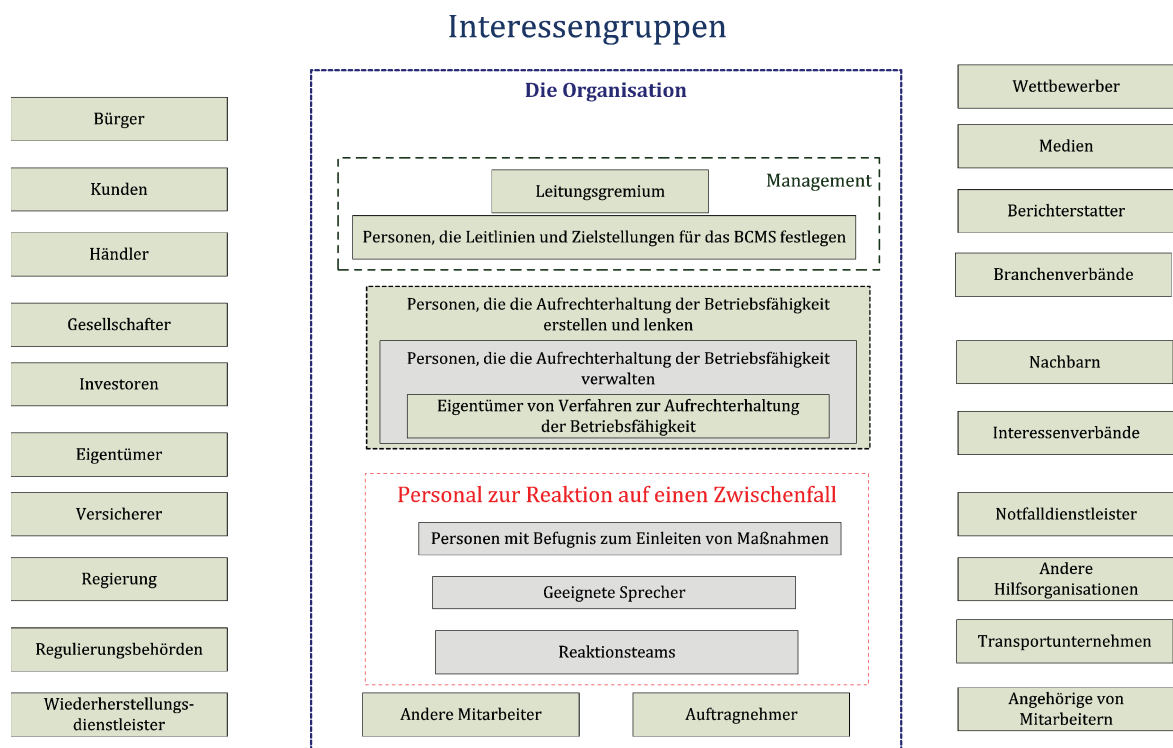


Bild 4 — Beispiele für zu berücksichtigende Interessengruppen im öffentlichen und privaten Bereich

4.2.2 Rechtliche und behördliche Anforderungen

Alle Managementsysteme sollten innerhalb des gesetzlichen und behördlichen Rahmens agieren, in dem die Organisation tätig ist. Die Organisation sollte deshalb alle relevanten und maßgeblichen gesetzlichen und behördlichen Anforderungen, denen sie unterliegt, sowie die Bedürfnisse der Interessengruppen ermitteln und in das BCMS aufnehmen.

Die Informationen über diese Anforderungen sollten dokumentiert und stets aktuell gehalten werden. Neue oder geänderte rechtliche, behördliche und andere Anforderungen sollten allen betroffenen Mitarbeitern und anderen Interessengruppen mitgeteilt werden.

Bei der Einführung, Umsetzung und Aufrechterhaltung des BCMS sollte die Organisation die maßgeblichen gesetzlichen Anforderungen und sonstigen Anforderungen, denen sie unterliegt, sowie die Bedürfnisse der Interessengruppen berücksichtigen und dokumentieren.

Die Organisation sollte sicherstellen, dass ihr BCMS im Rahmen und zugunsten ihrer gesetzlichen Verpflichtungen und maßgeblichen Anforderungen der Interessengruppen funktioniert.

Die Organisation sollte die jeweils aktuellen und anstehenden gesetzlichen und behördlichen Anforderungen vor Ort überprüfen, zu denen folgende zählen können:

- a) Reaktion auf einen Zwischenfall: einschließlich Gefahrenabwehr und Rechtsvorschriften zu Gesundheit, Sicherheit und Wohlergehen;
- b) Aufrechterhaltung: darf den Geltungsbereich des Programms oder den Umfang oder die Geschwindigkeit der Reaktion festlegen;
- c) Risiko: Anforderungen, die den Geltungsbereich oder die Verfahren eines Risikomanagementprogramms festlegen; und
- d) Gefährdungen: betriebliche Anforderungen in Bezug auf gefährliche Materialien, die vor Ort gelagert werden.

ANMERKUNG Organisationen, die an mehreren Standorten tätig sind, müssen oftmals die Anforderungen verschiedener Rechtssysteme erfüllen.

4.3 Festlegung des Anwendungsbereichs des Managementsystems

4.3.1 Allgemeines

Die Organisation sollte den Anwendungsbereich des BCMS festlegen und sicherstellen, dass dieser den Interessengruppen in geeigneter Weise mitgeteilt werden kann. Es ist wichtig, dass die Grenzen und die Anwendbarkeit des BCMS deutlich zu erkennen sind und dass der Anwendungsbereich die in 4.1 und 4.2 festgelegten Punkte berücksichtigt.

Im Anwendungsbereich sind die Produkte und Dienstleistungen, Standorte, Funktionen, Prozesse und Tätigkeiten festgelegt, für die das BCMS gilt. Daraus ergibt sich, dass sämtliche Abhängigkeiten im Anwendungsbereich enthalten sind, auch wenn sie nicht ausdrücklich in den Angaben zum Anwendungsbereich genannt werden. Wenn beispielsweise die „Arbeitnehmervergütung“ im Anwendungsbereich festgelegt ist, dann sind standardmäßig die Verfügbarkeit der finanziellen Mittel, die Zustimmung des Managements und die Anweisungen an die Finanzabteilung zur Zahlungsleistung ebenfalls im Anwendungsbereich enthalten.

Die Organisation sollte den Anwendungsbereich und den Kontext des BCMS eindeutig dokumentieren.

4.3.2 Anwendungsbereich des BCMS

Die Organisation sollte den Anwendungsbereich des BCMS so festlegen und dokumentieren, wie es im Hinblick auf Größe, Art und Komplexität der Organisation angemessen ist.

Der Anwendungsbereich sollte:

- a) die Bereiche der Organisation festlegen, die im BCMS enthalten sind;
- b) die Anforderungen der Organisation an das BCMS unter Berücksichtigung ihres Auftrags, ihrer Ziele, der gesetzlichen Verantwortlichkeiten und internen sowie externen Verpflichtungen festlegen;
- c) die Produkte und Dienstleistungen der Organisation so bezeichnen, dass alle damit verbundenen Tätigkeiten, Ressourcen und Lieferketten ermittelt werden können; und
- d) die Bedürfnisse und Interessen der Interessengruppen berücksichtigen.

Der Anwendungsbereich darf außerdem

- eine Angabe über das Ausmaß der Vorfälle, die durch das BCMS abgedeckt werden, sowie über die Risikobereitschaft der Organisation enthalten,
- festlegen, wie das BCMS in die allgemeine Risikomanagementstrategie (sofern vorhanden) der Organisation einzuordnen ist.

Wenn ein Bereich der Organisation vom Anwendungsbereich des BCMS ausgenommen ist, sollte die Organisation diese Ausnahme dokumentieren und begründen.

Der Zweck der Festlegung des Anwendungsbereichs ist es, die Berücksichtigung aller relevanten Tätigkeiten, Standorte und Lieferanten sicherzustellen (8.2.1, Bild 6).

4.4 Business Continuity Management System

Es wird normativ auf ISO 22301:2012 verwiesen, in der die Anforderungen an ein BCMS festgelegt sind. Eine Anleitung wird an dieser Stelle nicht zur Verfügung gestellt.

5 Führung

5.1 Führung und Selbstverpflichtung

Alle relevanten Managementebenen innerhalb der Organisation sollten die Umsetzung von Leitlinien und Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit führen und Selbstverpflichtung demonstrieren. Diese Demonstration kann durch Motivation, Engagement und die Übertragung von Verantwortung verwirklicht werden.

5.2 Selbstverpflichtung der Leitung

Das Leitungsgremium sollte seine Selbstverpflichtung hinsichtlich des BCMS demonstrieren.

Das Leitungsgremium sollte einen Nachweis über seine Selbstverpflichtung zur Entwicklung und Umsetzung des BCMS und zur ständigen Verbesserung seiner Effektivität durch Folgendes liefern:

- a) Einhaltung maßgeblicher gesetzlicher Anforderungen und anderer Anforderungen, denen die Organisation unterliegt (4.2.2);
- b) Eingliederung von BCMS-Prozessen in die vorhandenen Verfahren zur Aufrechterhaltung und Überprüfung;
- c) Einführen von Leitlinien und Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit im Einklang mit den Zielsetzungen, Verpflichtungen und der strategischen Ausrichtung der Organisation (5.3);

- d) Ernennen einer oder mehrerer Personen mit den entsprechenden Befugnissen und Kompetenzen, die für das BCMS und dessen wirksame Anwendung verantwortlich sind (5.4);
- e) Sicherstellen, dass die Funktionen, Verantwortlichkeiten und Kompetenzen innerhalb des BCMS festgelegt werden (5.4);
- f) Sicherstellen der Verfügbarkeit ausreichender Ressourcen, einschließlich eines angemessenen Umfangs finanzieller Mittel (7.1);
- g) Vermitteln der Wichtigkeit der Einhaltung von Leitlinien und Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit innerhalb der Organisation (7.4);
- h) aktive Teilnahme an Übungen und Überprüfungen (8.5);
- i) Sicherstellung, dass interne Audits des BCMS durchgeführt werden (9.2);
- j) Durchführen von Überprüfungen der wirksamen Lenkung des BCMS (9.3); und
- k) Anleiten und Unterstützen der Verbesserung des BCMS (Abschnitt 10).

Die Selbstverpflichtung der Leitung darf außerdem durch Folgendes dargelegt werden:

- Beteiligung an Betriebsabläufen durch Lenkungsausschüsse;
- Aufnahme der Aufrechterhaltung der Betriebsfähigkeit als festen Tagesordnungspunkt auf Leitungssitzungen.

5.3 Leitlinien

Das Leitungsgremium sollte die Leitlinien zur Aufrechterhaltung der Betriebsfähigkeit unter dem Aspekt der Zielsetzung und Verpflichtung der Organisation festlegen und sicherstellen, dass diese

- dem Zweck der Organisation entsprechen (d. h. ihrer Größe, Art und Komplexität und unter Beachtung ihrer Kultur, Abhängigkeiten und Betriebsumgebung),
- ein Rahmenwerk für die Erstellung von Zielsetzungen bereitstellen,
- eindeutige Verpflichtungen bezüglich maßgeblichen Anforderungen, einschließlich gesetzlicher und behördlicher Verpflichtungen und die Verpflichtung zur ständigen Verbesserung des BCMS enthalten,
- innerhalb der Organisation kommuniziert und verstanden werden,
- anderen relevanten Leitlinien ergänzen, und
- nach Genehmigung durch die Leitung, Interessengruppen zur Verfügung gestellt werden.

Geeignete Vorkehrungen sollten für die Genehmigung der Leitlinien, zum Aufbewahren dokumentierter Informationen darüber und zu regelmäßigen Überprüfungen der Leitlinien (z. B. jährlich) und immer dann, wenn bedeutende Änderungen der internen oder externen Faktoren auftreten (z. B. Änderungen im Leitungsgremium oder Einführung neuer Rechtsvorschriften), getroffen werden. Die Eignung solcher Vorkehrungen ist abhängig von der Größe, Komplexität, Art und Ausmaß der Organisation.

Die Leitlinie sollte außerdem

- die Reichweite des Anwendungsbereichs und die Grenzen der Aufrechterhaltung der Betriebsfähigkeit der Organisation enthalten, einschließlich Einschränkungen und Ausnahmen,
- jegliche erforderlichen Befugnisse und Bevollmächtigungen festlegen, einschließlich der Person oder Personen, die für das BCMS der Organisation verantwortlich ist/sind,
- die Kriterien für die Art und das Ausmaß der zu behandelnden Zwischenfälle festlegen, und
- Verweisungen auf Normen, Richtlinien, Vorschriften oder Leitlinien enthalten, die das BCMS berücksichtigen oder erfüllen sollte.

Die Leitlinien zur Aufrechterhaltung der Betriebsfähigkeit dürfen Folgendes enthalten:

- wesentliche Begriffe;
- Verpflichtung zur Finanzierung;
- Verweisungen auf andere relevante Leitlinien;
- eine Forderung zur Umsetzung der Aufrechterhaltung der Betriebsfähigkeit;
- eine Verpflichtung zur Ausführung und Beibehaltung der Aufrechterhaltung der Betriebsfähigkeit.

5.4 Funktionen, Verantwortlichkeiten und Befugnisse innerhalb der Organisation

Das Leitungsgremium sollte die Vergabe und Bekanntgabe der Verantwortlichkeiten und Befugnisse innerhalb des BCMS sicherstellen.

Ein Mitglied des Leitungsgremiums sollte die Gesamtverantwortung für das BCMS tragen und rechenschaftspflichtig sein.

Das Leitungsgremium der Organisation sollte einen oder mehrere spezifische(n) Managementbeauftragte(n) benennen, der/die unabhängig von seinen/ihren anderen Verantwortungen festgelegte Funktionen, Verantwortlichkeiten und Befugnisse haben sollte(n), um

- sicherzustellen, dass das BCM in Übereinstimmung mit den Leitlinien zur Aufrechterhaltung der Betriebsfähigkeit eingeführt, umgesetzt und aufrechterhalten wird,
- dem Leitungsgremium zu Überprüfungszwecken und als Grundlage für Verbesserungen über die Leistung des BCM Bericht zu erstatten;
- die Bewusstseinsbildung hinsichtlich der Aufrechterhaltung der Betriebsfähigkeit innerhalb der Organisation zu fördern, und
- die Effektivität von Verfahren sicherzustellen, die für die Reaktion auf einen Zwischenfall entwickelt worden sind, aber nicht unbedingt bei deren Umsetzung während eines Zwischenfalls.

Der Managementbeauftragte darf

- als „Business Continuity Manager“ bezeichnet werden,
- weitere Verantwortungsbereiche innerhalb der Organisation haben, und
- je nach Größe, Umfang und Komplexität der Organisation in mehreren Bereichen einer Organisation ansässig sein.

Vertreter jedes Funktionsbereichs oder jedes Standorts der Organisation dürfen dazu ernannt werden, an der Umsetzung des BCMS mitzuarbeiten. Ihre Funktionen, Rechenschaftspflichten, Verantwortungen und Befugnisse sollten in die Tätigkeitsbeschreibungen aufgenommen werden, die dadurch gefestigt werden können, dass sie in die Leitlinien der Organisation zur Beurteilung, Vergütung und Anerkennung aufgenommen werden.

Das Leitungsgremium darf weitere Gremien benennen, wie z. B. einen Lenkungsausschuss, um die Umsetzung und die laufende Überwachung des BCM zu beaufsichtigen.

Alle Funktionen, Verantwortlichkeiten und Befugnisse für das BCM sollten definiert und dokumentiert und Audits unterzogen werden.

6 Planung

6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten

Die Organisation sollte festlegen, wie die Sachverhalte aus 4.1 und die Anforderungen aus 4.2 behandelt werden sollen.

Dabei sollte die Notwendigkeit eines Maßnahmenplans bewertet werden, um

- unerwünschte Ergebnisse zu vermeiden,
- jegliche Gelegenheiten zur Verbesserung des BCMS zu ergreifen.

Sofern notwendig, sollte außerdem Folgendes berücksichtigt werden:

- die Einbindung und die Umsetzung dieser Maßnahmen im BCMS-Prozess (8.1); und
- die Sicherstellung, dass dokumentierte Informationen verfügbar sind, mit denen bewertet werden kann, ob die Maßnahmen effektiv umgesetzt wurden (7.5).

6.2 Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit und Pläne zur Zielerreichung

Ein Plan zur Erstellung und Lenkung des BCM (wie in Abschnitt 8 festgelegt) sollte erarbeitet werden und sollte die Festlegung von Verantwortlichkeiten sowie die Festlegung von angemessenen und realistischen Einzelzielen bei der Erledigung von Aufgaben enthalten. Der Plan sollte auf den Kontinuitätszielen basieren, die festgelegt und den entsprechenden Funktionen und Ebenen innerhalb der Organisation mitgeteilt wurden. Eine Weiterentwicklung des Plans sollte überwacht und dokumentiert werden.

Dieser Plan sollte überprüft werden und es kann erforderlich sein, diesen regelmäßig bei Weiterentwicklung des BCMS zu aktualisieren.

Im Folgenden sind Beispiele für Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit angegeben, die unter gewissen Umständen die in ISO 22301 festgelegten Anforderungen erfüllen können:

- „Erstellen eines BCMS in Übereinstimmung mit ISO 22313 bis zum *Datum*“;
- „Erlangen einer Zertifizierung nach ISO 22301:2012 bis zum *Datum*“;
- „Ab dem *Datum* verfügen wir über eine funktionierende Aufrechterhaltung der Betriebsfähigkeit, die unseren Verpflichtungen gegenüber Hauptkunden entspricht“;
- „Umsetzung eines BCM zum Schutz von zentralen Produkten und Dienstleistungen bis zum *Datum*“.

7 Unterstützung

7.1 Ressourcen

7.1.1 Allgemeines

Die Organisation sollte die Ressourcen festlegen und bereitstellen, die für das BCMS notwendig sind und mit denen

- a) ihre Leitlinien und Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit erreicht werden,
- b) die sich ändernden Anforderungen der Organisation erfüllt werden,
- c) die effektive Kommunikation über Belange des Business Continuity Management Systems, intern und extern, ermöglicht wird, und
- d) die für die laufende Anwendung und die ständige Verbesserung des Business Continuity Management Systems zur Verfügung stehen.

Diese Ressourcen sollten zeitnah und wirksam zur Verfügung gestellt werden.

7.1.2 BCMS-Ressourcen

Bei der Festlegung der für das BCMS erforderlichen Ressourcen sollte die Organisation Folgendes in angemessenem Umfang vorsehen:

- a) Personen und personenbezogene Ressourcen, einschließlich:
 - 1) die Zeit, die benötigt wird, um die Funktionen und Verantwortlichkeiten in Verbindung mit dem BCMS wahrzunehmen;
 - 2) Schulung, Weiterbildung, Bewusstseinsbildung und Übungen;
 - 3) Lenkung des BCMS-Personals;
- b) Einrichtungen, einschließlich geeigneter Arbeitsplätze und Infrastruktur;
- c) Informations- und Kommunikationstechnologie (IKT), einschließlich Anwendungen zur Unterstützung eines wirksamen und effizienten Programmmanagements;
- d) Verwaltung und Kontrolle aller Formen von dokumentierter Information;
- e) Kommunikation mit den Interessengruppen (siehe Bild 4); und
- f) Finanzen und Mittelbeschaffung.

Ressourcen und deren Verteilung sollten regelmäßig überprüft werden, um deren Angemessenheit sicherzustellen. Es kann angebracht sein, das Leitungsgremium in diese Überprüfung einzubeziehen.

7.1.3 Personal zur Reaktion auf einen Zwischenfall

Die Organisation sollte Personal zur Reaktion auf einen Zwischenfall benennen, das über die notwendigen Verantwortlichkeiten, Befugnisse und Kompetenzen zur Behandlung eines Zwischenfalls besitzt.

Das Personal zur Reaktion auf einen Zwischenfall sollte eine Gruppe bilden, die für die Behandlung sämtlicher Zwischenfälle mit Betriebsunterbrechung, die erhebliche Auswirkungen auf die Organisation haben oder die über das Potential verfügen, erhebliche Auswirkungen auf die Organisation haben zu können, zuständig ist.

Mitarbeiter dürfen entsprechend ihrer dargelegten Kompetenzen zum Umgang mit verschiedenen Aspekten der Reaktion auf einen Zwischenfall in Teams eingeteilt werden, wie z. B.:

- Zwischenfallmanagement/strategisches Management (8.4.4.3.1);
- Kommunikation (8.4.4.3.2);
- Schutz und Wohlergehen (8.4.4.3.3);
- Bergung und Sicherung (8.4.4.3.4);
- Wiederaufnahme von Tätigkeiten (8.4.4.3.5);
- Wiederherstellung der IKT (8.4.4.3.6).

Alle Mitarbeiter dieser Gruppen sollten über eindeutig festgelegte Verantwortlichkeiten und Befugnisse verfügen, die vor, während und nach einem Zwischenfall gelten.