

DIN EN ISO 22313

ICS 03.100.01

Einsprüche bis 2014-08-06

Entwurf**Sicherheit und Schutz des Gemeinwesens –
Aufrechterhaltung der Betriebsfähigkeit –
Leitlinie (ISO 22313:2012);
Deutsche Fassung FprEN ISO 22313:2014**

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

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

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2014-06-06 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an fnfw@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den Normenausschuss Feuerwehrwesen (FNFW) im DIN, 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 63 Seiten

Normenausschuss Feuerwehrwesen (FNFW) im DIN

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 FprEN ISO 22313:2014 durch das Technische

Komitee CEN/TC 391 „Schutz und Sicherheit der Bürger“ ohne Änderungen übernommen, dessen Sekretariat vom NEN (Niederlande) gehalten wird.

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 DIN verantwortlich.

Sicherheit und Schutz des Gemeinwesens — Aufrechterhaltung der Betriebsfähigkeit — Leitlinie (ISO 22313:2012)

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

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

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: einstufiges Annahmeverfahren
Dokument-Sprache: D
STD Version 2.5a

Inhalt

Seite

Vorwort	4
Einleitung.....	5
1 Anwendungsbereich	10
2 Normative Verweisungen	10
3 Begriffe	10
4 Kontext der Organisation.....	11
4.1 Verstehen der Organisation und ihres Kontextes.....	11
4.2 Verstehen der Bedürfnisse und Erwartungen der Interessensgruppen.....	12
4.2.1 Allgemeines.....	12
4.2.2 Gesetzliche und behördliche Anforderungen.....	12
4.3 Festlegung des Anwendungsbereichs des Managementsystems	13
4.3.1 Allgemeines.....	13
4.3.2 Anwendungsbereich des BCMS.....	13
4.4 Managementsystem zur Aufrechterhaltung der Betriebsfähigkeit.....	14
5 Führung	14
5.1 Führung und Selbstverpflichtung	14
5.2 Selbstverpflichtung der Leitung.....	14
5.3 Leitlinien	15
5.4 Funktionen, Verantwortlichkeiten und Befugnisse innerhalb der Organisation	16
6 Planung.....	16
6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten	16
6.2 Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit und Pläne zur Zielerreichung	17
7 Unterstützung.....	17
7.1 Ressourcen	17
7.1.1 Allgemeines.....	17
7.1.2 BCMS-Ressourcen.....	17
7.1.3 Personal zur Gefahrenabwehr.....	18
7.2 Kompetenz.....	18
7.3 Bewusstseinsbildung.....	20
7.4 Kommunikation.....	21
7.5 Dokumentation.....	22
7.5.1 Allgemeines.....	22
7.5.2 Erstellung und Aktualisierung.....	23
7.5.3 Dokumentationskontrolle	24
8 Betrieb.....	25
8.1 Ablaufplanung und Kontrolle	25
8.1.1 Elemente des BCM.....	25
8.1.2 Lenken der BCM-Umgebung	26
8.1.3 Warten der Aufrechterhaltung der Betriebsfähigkeit.....	27
8.1.4 Messen der Wirksamkeit.....	27
8.1.5 Ergebnisse.....	27
8.2 Business Impact Analyse und Risikobeurteilung	28
8.2.1 Allgemeines.....	28
8.2.2 Business Impact Analyse	29
8.2.3 Risikobeurteilung.....	31

8.3	Strategie zur Aufrechterhaltung der Betriebsfähigkeit	32
8.3.1	Festlegung und Auswahl	32
8.3.2	Festlegen des Ressourcenbedarfs	34
8.3.3	Schutz und Schadensminderung	40
8.4	Einführung und Umsetzung von Maßnahmen zur Aufrechterhaltung der Betriebsfähigkeit	40
8.4.1	Allgemeines	40
8.4.2	Struktur zur Gefahrenabwehr	40
8.4.3	Warnung und Kommunikation	41
8.4.4	Pläne zur Aufrechterhaltung der Betriebsfähigkeit	43
8.4.5	Wiederherstellung	50
8.5	Übungen und Erprobungen	51
8.5.1	Allgemeines	51
8.5.2	Übungsprogramm	52
8.5.3	Übungen zu Plänen für die Aufrechterhaltung der Betriebsfähigkeit	52
9	Leistungsüberprüfung	54
9.1	Überwachung, Messung, Analyse und Bewertung	54
9.1.1	Allgemeines	54
9.1.2	Bewertung der Verfahren zur Aufrechterhaltung der Betriebsfähigkeit	55
9.2	Interne Audits	57
9.3	Managementbewertung	58
10	Verbesserung	59
10.1	Nichtkonformität und Korrekturmaßnahmen	59
10.2	Ständige Verbesserung	59
	Literaturhinweise	61

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 FprEN ISO 22313:2014 durch das Technische Komitee CEN/TC 391 „Schutz und Sicherheit der Bürger“ übernommen, dessen Sekretariat vom NEN gehalten wird.

Dieses Dokument ist derzeit zum einstufigen Annahmeverfahren vorgelegt.

Anerkennungsnotiz

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

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 zwar die gleichen Überschriften wie die ISO 22301, aber sie wiederholt nicht die Anforderungen an Managementsysteme zur Aufrechterhaltung der Betriebsfähigkeit und damit verbundene Begriffe. Organisationen, die sich darüber informieren möchten, müssen dafür ISO 22301 und ISO 22300 heranziehen.

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

Ein Managementsystem zur Aufrechterhaltung der Betriebsfähigkeit (BCMS, en: Business Continuity Management System) betont Folgendes:

- das Verstehen der Bedürfnisse einer Organisation sowie der Notwendigkeit der Einführung von Leitlinien und Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit;
- das Einführen und Umsetzen von Kontrollen und Maßnahmen zum Managen der Gesamtfähigkeit einer Organisation, mit Betriebsunterbrechung umzugehen;
- das Überwachen und Überprüfen der Leistung und der Wirksamkeit des BCMS; und
- ständige Verbesserungen 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) Implementierung und Betrieb,
 - 4) Leistungsbewertung,
 - 5) Bewertung des Managements, und
 - 6) Verbesserung;
- d) Dokumentationsunterlagen zur Bereitstellung auditierbarer Nachweise; und
- e) jeden Managementprozess zur Aufrechterhaltung der Betriebsfähigkeit, 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, Plan-Do-Check-Act) an, um das BCMS einer Organisation zu planen, einzuführen, umzusetzen, zu betreiben, zu überwachen, zu überprüfen, aufrechtzuerhalten und dessen Wirksamkeit ständig zu verbessern.

Bild 1 stellt dar, wie das BCMS die Anforderungen der Interessensgruppen als Input für das Management zur Aufrechterhaltung der Betriebsfähigkeit (BCM) verwendet und mittels der notwendigen Maßnahmen und Prozesse Kontinuitätsergebnisse (d. h. eine gelenkte Aufrechterhaltung der Betriebsfähigkeit) erzeugt, die diese Anforderungen erfüllen.

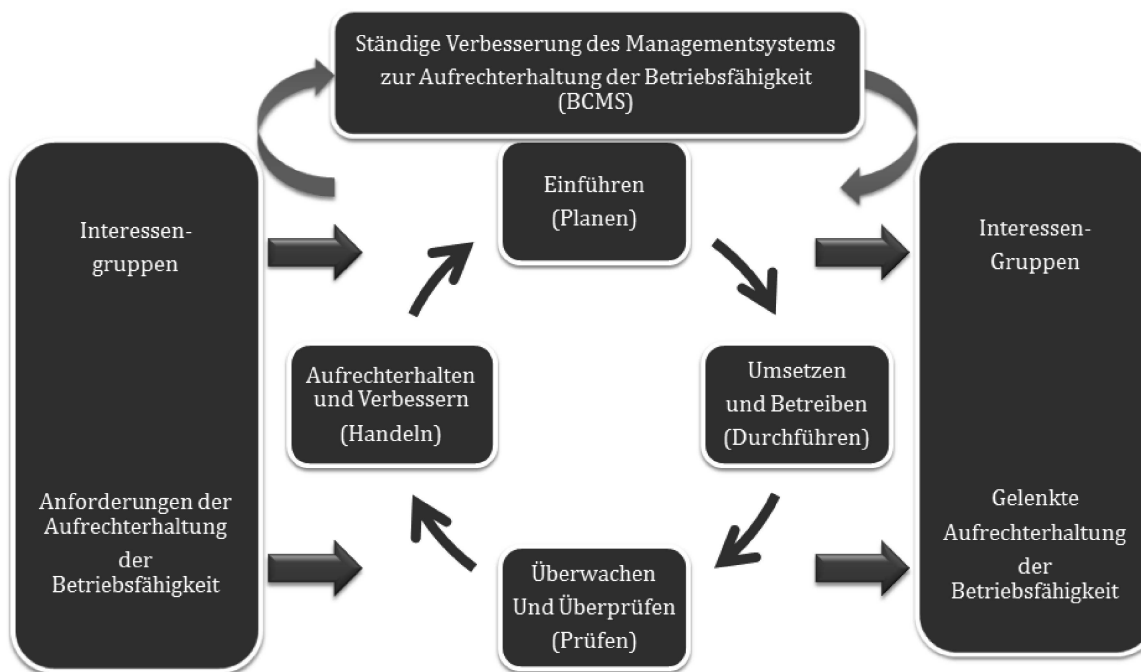


Bild 1 — An die BCMS-Prozesse angepasstes PDCA-Modell

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 Ausführen)	Umsetzen und Ausführen 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 Überprüfung durch das Management sowie Neufassung 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 deren Anforderungen erfüllt, unter Berücksichtigung aller relevanten internen und externen Faktoren, einschließlich: — der Bedürfnisse und Erwartungen der Interessensgruppen; — deren 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, Leitlinien festgelegt werden und Funktionen, Verantwortlichkeiten und Befugnisse verteilt 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 Risiko-beurteilung (8.2) sowie die Strategie zur Aufrechterhaltung der Betriebsfähigkeit (8.3) fest.
	Abschnitt 7 (Unterstützung) legt die zentralen Elemente fest, die vorhanden sein müssen, um das BCMS zu unterstützen, d. h. Ressourcen, Kompetenzen, Bewusstseinsbildung, Kommunikation und Dokumentation.
Durchführen (Umsetzen und Ausführen)	Abschnitt 8 (Betrieb) legt die Elemente des Managements zur Aufrechterhaltung der Betriebsfähigkeit (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 die Korrekturmaßnahmen, die im Hinblick auf Nichtkonformität, die anhand einer Leistungsbewertung festgestellt wurde, erforderlich sind.

Aufrechterhaltung der Betriebsfähigkeit

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

Durch die Einordnung des BCM in den Rahmen und den Bereich eines Managementsystems ergibt sich ein Managementsystem zur Aufrechterhaltung der Betriebsfähigkeit (BCMS), das dem BCM ermöglicht, kontrolliert, bewertet und ständig verbessert zu werden.

In dieser Internationalen Norm wird das Wort „Betriebsfähigkeit“ als ein allumfassender Begriff für die Betriebsabläufe und Dienste verwendet, die von einer Organisation beim Streben nach ihren Zielsetzungen, Einzelzielen oder Aufträgen ausgeführt werden. Daher gilt sie gleichermaßen für große, mittlere und kleine Unternehmen, die im industriellen, kommerziellen, öffentlichen und gemeinnützigen Bereich tätig sind.

Jeder Vorfall, egal ob klein oder groß, ob natürlicher Art, durch einen Unfall oder bewusst 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 in Bezug auf die zentralen Produkte und Dienstleistungen einer Organisation sowie über die Tätigkeiten, zur Herstellung;
- b) die Kenntnis über die Prioritäten bei der Wiederaufnahme von Tätigkeiten und über die Ressourcen, die diese Tätigkeiten erfordern;
- c) ein klares Verständnis über die Bedrohungen, die für diese Tätigkeiten gelten sowie deren Abhängigkeiten und die Kenntnis über die Auswirkungen, falls diese Tätigkeiten nicht wieder aufgenommen werden;
- d) die Verfügbarkeit über bewährte und vertraute Vorkehrungen zur Wiederaufnahme dieser Tätigkeiten nach einem Vorfall mit Betriebsunterbrechung; und
- e) Sicherstellen, dass diese Vorkehrungen regelmäßig überprüft und aktualisiert werden, damit sie unter allen Umständen wirksam sind.

Die Aufrechterhaltung der Betriebsfähigkeit betrifft sowohl plötzliche Vorfälle mit Betriebsunterbrechung (z. B. Explosionen) als auch schleichend eintretende auftretende Vorfälle mit Betriebsunterbrechung (z. B. Grippepandemien).

Tätigkeiten können durch die verschiedensten Vorfälle unterbrochen werden, von denen die meisten schwer vorherzusagen oder zu analysieren sind. Durch Fokussieren auf die Auswirkung einer Unterbrechung und nicht auf die Ursache, werden bei der Aufrechterhaltung der Betriebsfähigkeit diejenigen Tätigkeiten erkannt, die für die Organisation überlebenswichtig sind. Dies ermöglicht der Organisation zu bestimmen, was zur weiteren Einhaltung 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 Vorfall mit Betriebsunterbrechung eintritt. Durch diese Erkenntnis ist die Organisation in der Lage, einen realistischen Blick auf die Maßnahmen zur Gefahrenabwehr zu werfen, die voraussichtlich benötigt wird, falls eine Unterbrechung eintritt, damit sie beim Lenken von Konsequenzen selbstsicher handelt und dadurch inakzeptable Auswirkungen vermieden werden.

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

Die folgenden Diagramme (Bilder 2 und 3) sollen zeigen, wie die Aufrechterhaltung der Betriebsfähigkeit durch Abschwächen von Auswirkungen in bestimmten Situationen umgesetzt werden kann. Die relativen Abstände zwischen den in den Diagrammen dargestellten Stufen basieren nicht auf einem bestimmten zeitlichen Rahmen.

Mildern von Auswirkungen durch die wirksame Aufrechterhaltung der Betriebsfähigkeit — Plötzliche Betriebsunterbrechung

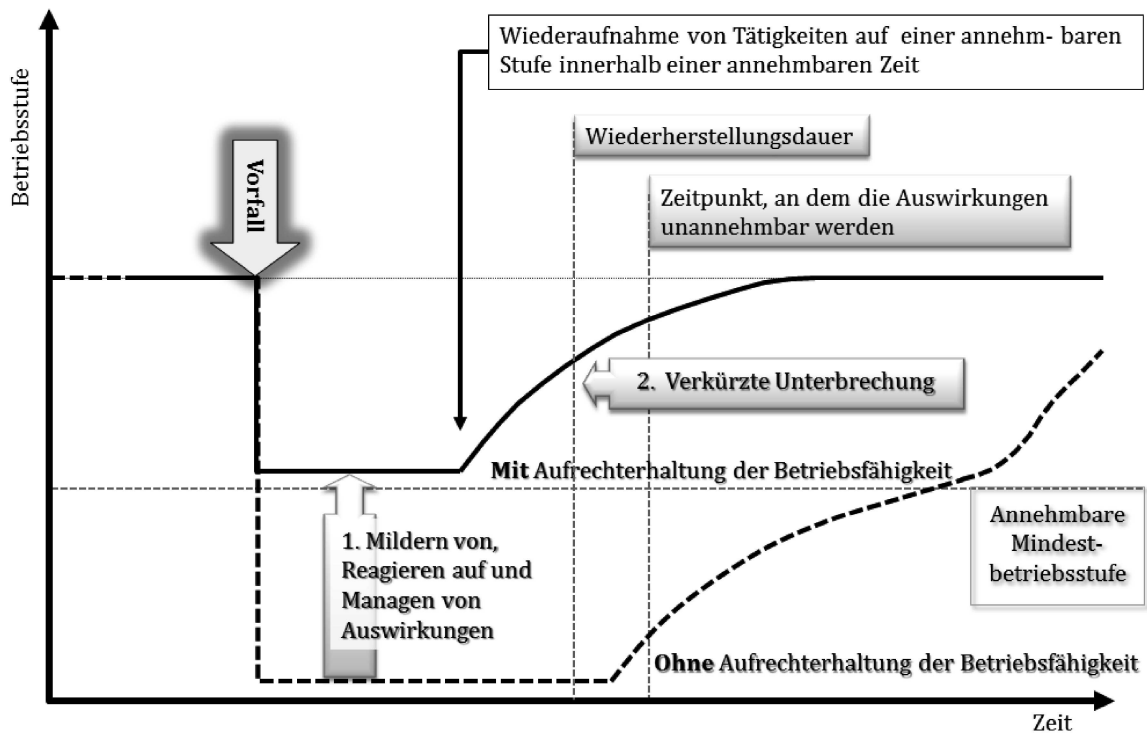


Bild 2 — Darstellung einer wirksamen Aufrechterhaltung der Betriebsfähigkeit bei plötzlicher Betriebsunterbrechung

Mildern von Auswirkungen durch die wirksame Aufrechterhaltung der Betriebsfähigkeit — Schrittweise auftretende Betriebsunterbrechung

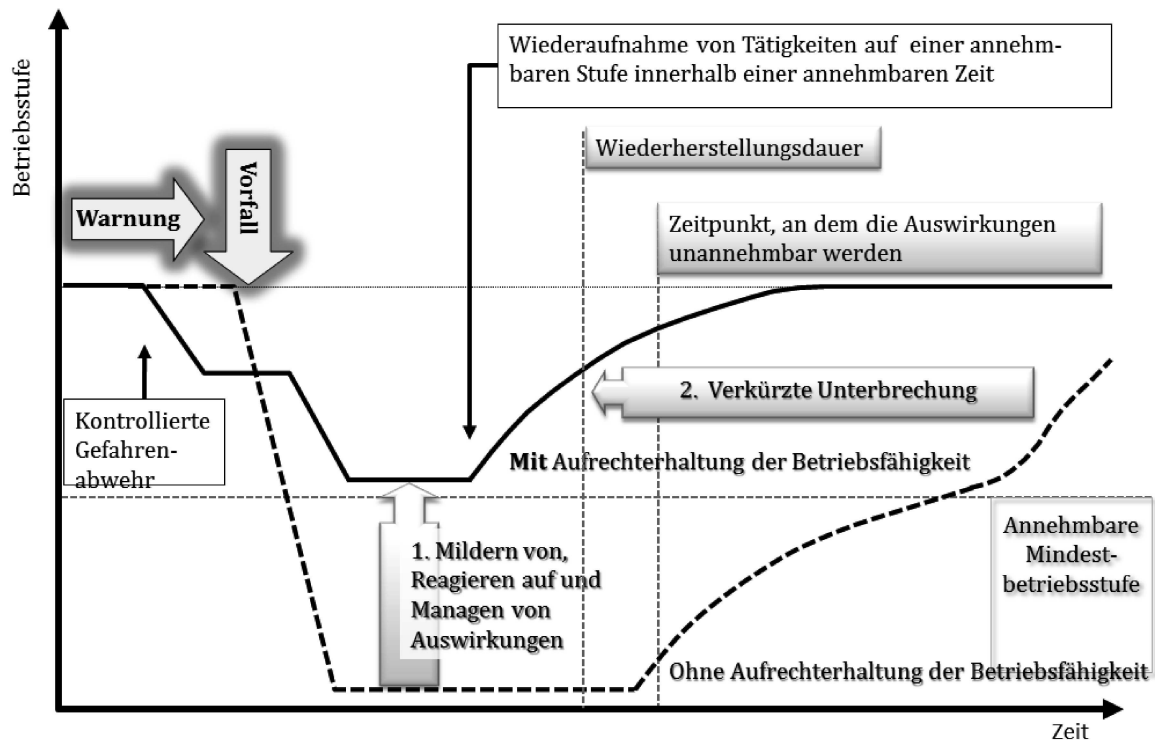


Bild 3 — Darstellung einer wirksamen Aufrechterhaltung der Betriebsfähigkeit bei schrittweise auftretender Betriebsunterbrechung (z. B. herannahende Pandemie)

1 Anwendungsbereich

Diese Internationale Norm für Managementsysteme zur Aufrechterhaltung der Betriebsfähigkeit enthält Leitlinien, die auf international anerkannten Praktiken zur Planung, Einführung, Umsetzung, Durchführung, Überwachung, Überprüfung, Aufrechterhaltung und ständigen Verbesserung eines dokumentierten Managementsystem beruhen, die den Organisationen ermöglichen, sich auf Vorfälle vorzubereiten, auf sie zu reagieren und sich nach ihrem Eintreten von ihnen zu erholen.

Es ist nicht die Absicht dieser Internationalen Norm, Einheitlichkeit in die Struktur eines BCMS zu bringen, sondern ein BCMS für eine Organisation zu gestalten, das deren Bedürfnissen entspricht und die Anforderungen der Interessengruppen erfüllt. Diese Bedürfnisse sind durch gesetzliche, behördliche, organisatorische und industrielle 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 eine Fachgrundnorm und gilt für alle Organisationsgrößen und -typen, einschließlich großer, mittlerer und kleiner Organisationen, 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 eigene Konformitätsfeststellung oder eine eigene Konformitätserklärung mithilfe dieser Internationalen Norm erstellen möchten.

Diese Internationale Norm kann nicht dazu angewendet werden, die Befähigung einer Organisation zur Erfüllung von weder den eigenen Kontinuitätsbedürfnissen noch den Bedürfnissen der Kunden, der gesetzlichen oder der behördlichen Bedürfnisse zu bewerten. Organisationen, die dies vorhaben, können die Anforderungen von ISO 22301 anwenden, um anderen die Übereinstimmung nachzuweisen oder um die Zertifizierung ihres BCMS durch eine amtlich zugelassene Zertifizierungsstelle einer Drittpartei 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 Lenkung des BCMS werden in 8.1 behandelt.

Die Organisation sollte die internen und externen Faktoren, die für ihre Zwecke und Betriebsabläufe 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 betreffen:

- das politische, gesetzliche und behördliche Umfeld, ob international, national, regional oder lokal;
- das soziale und kulturelle, finanzielle, technologische, wirtschaftliche, natürliche und wettbewerbsfähige Umfeld, ob international, national, regional oder lokal;
- Selbstverpflichtungen und Beziehungen hinsichtlich der Versorgungskette;
- Betrachtung interner Risikostudien, unter Berücksichtigung anderer relevanter Informationsmanagementsysteme sowie generell aller Informationen aus dem Wissensmanagement;
- entscheidende Faktoren und Trends, die eine Auswirkung auf die Zielsetzung und die Betriebsabläufe der Organisation haben; und
- Beziehungen zu Interessengruppen außerhalb der Organisation und deren Wahrnehmung und Nutzen.

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

- 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 (formal und formlos);
- Interessengruppen innerhalb der Organisation;
- Leitlinien und Zielsetzungen sowie die Strategien, mit denen sie umgesetzt werden;
- Zukunftschancen und Unternehmensprioritäten;
- Wahrnehmungen, Werte und Kultur;
- Normen und Referenzmodelle, die von der Organisation eingebunden werden; und
- Strukturen (z. B. Führung, Funktionen und Verantwortlichkeiten).

4.2 Verstehen der Bedürfnisse und Erwartungen der Interessensgruppen

4.2.1 Allgemeines

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

Die Organisation sollte alle Interessensgruppen ermitteln, die für das BCMS von Bedeutung sind und auf Grundlage ihrer Bedürfnisse und Erwartungen deren Anforderungen bestimmen. Es ist wichtig nicht nur verbindliche und angegebene Anforderungen zu erkennen, sondern auch alle Anforderungen, die indirekt damit einhergehen.

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

Bei der Planung und Umsetzung des BCMS ist es wichtig, Tätigkeiten zu ermitteln, die zwar in Bezug auf die Interessensgruppe relevant sind, die aber zwischen den verschiedenen Gruppen unterschieden werden. Während es beispielsweise angemessen sein kann, nach einer Betriebsunterbrechung mit allen Interessensgruppen zu kommunizieren, kann es unangemessen sein, bei der Erstellung und Lenkung des BCM mit allen Interessensgruppen zu kommunizieren (8.1.1).

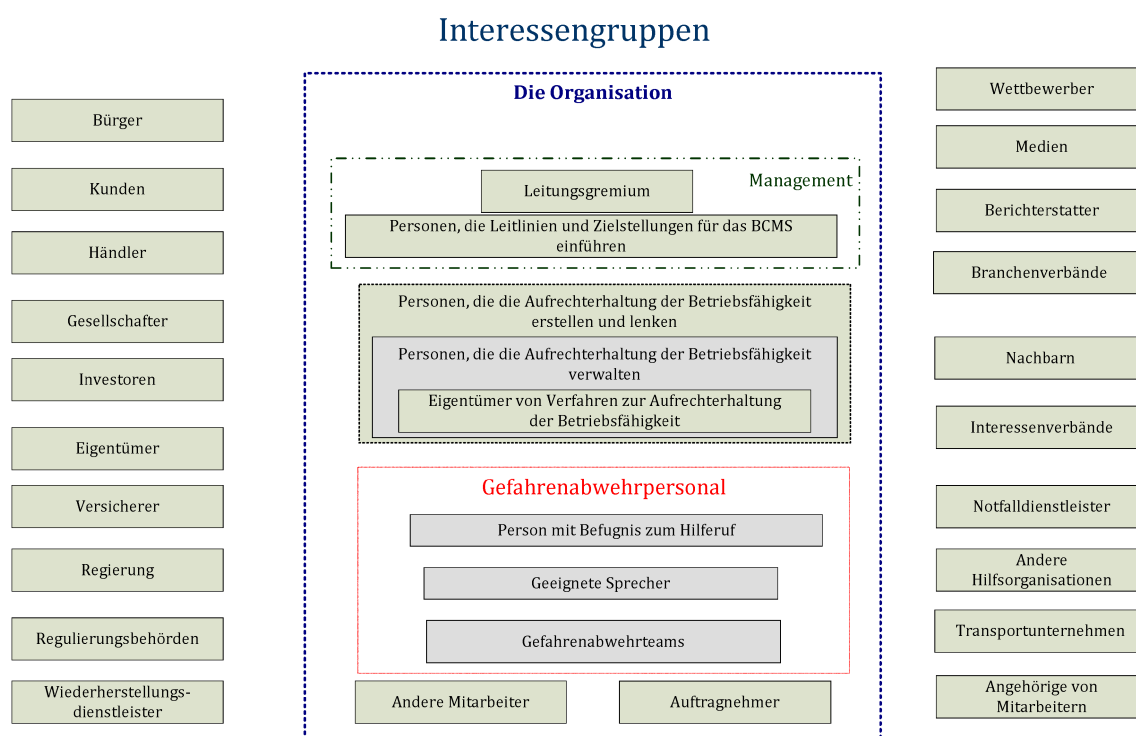


Bild 4 — Beispiele für zu berücksichtigende Interessensgruppen in öffentlichen und privaten Bereichen

4.2.2 Gesetzliche und behördliche Anforderungen

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

Die Informationen über diese Anforderungen sollten dokumentiert und stets aktualisiert werden. Neue oder geänderte gesetzliche, behördliche und andere Anforderungen sollten allen betroffenen Mitarbeitern und anderen Interessensgruppen mitgeteilt werden.

Bei der Einführung, Umsetzung und Aufrechterhaltung des BCMS sollte die Organisation die geltenden gesetzlichen Anforderungen und sonstige Anforderungen, denen sie unterliegt, und 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 zurzeit gültige und anstehende gesetzliche und behördliche Anforderungen vor Ort überprüfen, zu denen folgende zählen können:

- a) Gefahrenabwehr: einschließlich Notfallmanagement und Rechtsvorschriften zu Gesundheit, Sicherheit und Wohlergehen;
- b) Aufrechterhaltung: kann den Geltungsbereich des Programms oder den Umfang oder die Geschwindigkeit der Gefahrenabwehr 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 Zuständigkeitsbereiche 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 wird. 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, die für das BCMS gelten. Daraus ergibt sich, dass sämtliche Abhängigkeiten im Anwendungsbereich enthalten sind, auch wenn sie nicht ausdrücklich in den Angaben zum Anwendungsbereich genannt werden. Wenn die „Arbeitnehmervergütung“ im Anwendungsbereich festgelegt ist, dann würden standardmäßig die Verfügbarkeit der finanziellen Mittel, die Zustimmung des Managements und die Anweisungen an das Finanzinstitut zur Zahlungsleistung ebenfalls im Anwendungsbereich enthalten sein.

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 an das BCMS der Organisation unter Berücksichtigung ihrer Aufträge, ihrer Einzelziele, der juristischen Zuständigkeiten und internen sowie externen Verpflichtungen festlegen;
- c) die Produkte und Dienstleistungen der Organisation so bezeichnen, dass alle damit verbundenen Tätigkeiten, Ressourcen und Lieferketten bezeichnet werden; 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 gesamte Risikomanagementstrategie (sofern vorhanden) der Organisation einzuordnen ist.

Wenn ein Bereich der Organisation vom Anwendungsbereich des BCMS ausgeschlossen ist, sollte die Organisation diesen Ausschluss dokumentieren und begründen.

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

4.4 Managementsystem zur Aufrechterhaltung der Betriebsfähigkeit

Es wird auf ISO 22301:2012 verwiesen, in der die Anforderungen an ein BCMS festgelegt sind. Es liegen keine Leitlinien hierzu vor.

5 Führung

5.1 Führung und Selbstverpflichtung

Alle Ebenen des relevanten Managements innerhalb der Organisation sollten ihre Selbstverpflichtung und die Führung bei der Umsetzung von Leitlinien und Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit darlegen. Die Darlegung kann durch Motivation, Engagement und Bevollmächtigungen erfolgen.

5.2 Selbstverpflichtung der Leitung

Das Leitungsgremium sollte seine Selbstverpflichtung hinsichtlich des BCMS verdeutlichen.

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

- a) Übereinstimmung mit geltenden gesetzlichen Anforderungen und mit anderen 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, die für das BCMS verantwortlich sind und über die entsprechenden Befugnisse und Kompetenzen verfügen, um für dessen wirksame Ausführung verantwortlich zu sein (5.4);
- e) Sicherstellen, dass die Funktionsverteilung, Verantwortlichkeiten und Kompetenzen innerhalb des BCMS eingeführt werden (5.4);
- f) Sicherstellen der Verfügbarkeit ausreichender Ressourcen, einschließlich eines angemessenen Umfangs der finanziellen Mittel (7.1);
- g) Mitteilung über die Bedeutung der Einhaltung von Leitlinien und Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit an die Organisation (7.4);
- h) aktive Teilnahme an Übungen und Erprobungen (8.5);
- i) Sicherstellung, dass interne Audits zum BCMS durchgeführt werden (9.2);

- j) Durchführen von Überprüfungen der wirksamen Lenkung des BCMS (9.3); und
- k) Anleiten und Unterstützen von Verbesserungen 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 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 sollte sicherstellen, dass sie

- 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 in Verbindung mit geltenden Anforderungen enthalten, einschließlich gesetzlicher und behördlicher Verpflichtungen und Verpflichtungen zur ständigen Verbesserung des BCMS,
- innerhalb der Organisation kommuniziert und verstanden werden,
- ergänzend zu anderen relevanten Leitlinien gelten, und
- den Interessengruppen, denen von der Leitung zugestimmt wurde, zur Verfügung gestellt werden.

Geeignete Vorkehrungen sollten für die Genehmigung der Leitlinien, zum Zurückhalten von Informationen darüber und zu regelmäßigen Überprüfungen der Leitlinien (beispielsweise jährlich) und immer dann, wenn bedeutende Änderungen der internen oder externen Faktoren auftreten (z. B. Änderungen im Leitungsgremium oder Einführung einer neuen Rechtsvorschrift), getroffen werden.

Die Leitlinie sollte außerdem

- die Reichweite des Anwendungsbereichs und die Grenzen der Aufrechterhaltung der Betriebsfähigkeit der Organisation enthalten, einschließlich Einschränkungen und Ausschlüsse,
- jegliche erforderlichen Befugnisse und Vertretungen festlegen, einschließlich der Person oder Personen, die für das BCMS der Organisation verantwortlich ist/sind,
- die Kriterien für die zu behandelnde Art und das zu behandelnde Ausmaß von Vorfällen einführen, und
- Verweisungen auf Normen, Leitsätze und Richtlinien oder Leitlinien enthalten, die das BCMS berücksichtigen oder erfüllen sollte.

Die Leitlinien zur Aufrechterhaltung der Betriebsfähigkeit dürfen Folgendes enthalten:

- wesentliche Begriffe;
- Verpflichtung zur Finanzausstattung;
- Verweisung auf andere relevante Leitlinien;
- eine Anforderung 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 Mitteilung 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, Verantwortungen und Befugnisse haben sollte(n), um

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

Der Managementbeauftragte darf

- als „Business Continuity Manager“ bezeichnet werden,
- weitere Verantwortungen innerhalb der Organisation tragen, 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 Funktionsbeschreibungen aufgenommen werden, die dadurch untermauert werden, dass sie in die Leitlinien der Organisation zur Beurteilung, Vergütung und Anerkennung aufgenommen werden.

Das Leitungsgremium darf weitere Stellen 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 sowie einem Audit unterzogen werden.

6 Planung

6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten

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

Dabei sollte die Notwendigkeit eines Maßnahmenplans bewertet werden, um

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

Sofern notwendig, sollte außerdem Folgendes berücksichtigt werden:

- die Einbindung und die Umsetzung dieser Maßnahmen in den BCMS-Prozess (8.1); und
- die Sicherstellung, dass Dokumentationen 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 Kontinuitätszielsetzungen 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 bei Weiterentwicklung des BCMS regelmäßig überprüft und gegebenenfalls aktualisiert werden.

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

- ‚Erstellen eines BCMS in Übereinstimmung mit ISO 22313 bis zum *Datum*‘;
- ‚Erhalt der 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 des 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 bestimmen 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 in Bezug auf Belange des BCMS, intern und extern, ermöglicht werden, und
- d) die für den Betriebsablauf und die ständige Verbesserung des Managementsystems zur Aufrechterhaltung der Betriebsfähigkeit 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 auszuführen;
 - 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;