

DIN EN ISO 22313

ICS 03.100.01; 03.100.70

Ersatz für
DIN EN ISO 22313:2016-05

**Sicherheit und Resilienz –
Business Continuity Management System –
Anleitung zur Verwendung von ISO 22301 (ISO 22313:2020);
Deutsche Fassung EN ISO 22313:2020**

Security and resilience –
Business continuity management systems –
Guidance on the use of ISO 22301 (ISO 22313:2020);
German version EN ISO 22313:2020

Sécurité et résilience –
Systèmes de management de la continuité d'activité –
Lignes directrices sur l'utilisation de l'ISO 22301 (ISO 22313:2020);
Version allemande EN ISO 22313:2020

Gesamtumfang 82 Seiten

DIN-Normenausschuss Organisationsprozesse (NAOrg)

Nationales Vorwort

Dieses Dokument (EN ISO 22313:2020) wurde vom Technischen Komitee ISO/TC 292 „Security and resilience“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 391 „Schutz und Sicherheit der Bürger“ erarbeitet, dessen Sekretariat von AFNOR (Frankreich) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 175-00-05 GA „Sicherheit und Business Continuity“ im DIN-Normenausschuss Organisationsprozesse (NAOrg).

Für die in diesem Dokument zitierten internationalen Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 19011	siehe	DIN EN ISO 19011
ISO 22300	siehe	DIN EN ISO 22300
ISO 22301	siehe	DIN EN ISO 22301
ISO 31000	siehe	DIN ISO 31000
ISO/IEC 27002	siehe	DIN EN ISO/IEC 27002

Änderungen

Gegenüber DIN EN ISO 22313:2016-05 wurden folgende Änderungen vorgenommen:

- a) Inhalt und Struktur des Dokuments wurden an die aktuelle Ausgabe von ISO 22301 angepasst;
- b) zusätzliche Erläuterungen zu einzelnen Begriffen hinzugefügt;
- c) Inhalte von 8.4 wurden entfernt, um diese zukünftig in ISO/TS 22332 aufzunehmen;
- d) redaktionelle Überarbeitung der Norm.

Frühere Ausgaben

DIN EN ISO 22313: 2016-05

Nationaler Anhang NA (informativ)

Literaturhinweise

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

DIN EN ISO 22300, *Sicherheit und Resilienz — Vokabular*

DIN EN ISO 22301, *Sicherheit und Resilienz — Business Continuity Management System — Anforderungen*

DIN EN ISO/IEC 27002, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen*

DIN ISO 31000, *Risikomanagement — Leitlinien*

— Leerseite —

Deutsche Fassung

Sicherheit und Resilienz —
Business Continuity Management Systems —
Anleitung zur Verwendung von ISO 22301
(ISO 22313:2020)

Security and resilience —
Business continuity management systems —
Guidance on the use of ISO 22301
(ISO 22313:2020)

Sécurité et résilience —
Systèmes de management de la continuité d'activité —
Lignes directrices sur l'utilisation de l'ISO 22301
(ISO 22313:2020)

Diese Europäische Norm wurde vom CEN am 18. Februar 2020 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 CEN-CENELEC-Management-Zentrum 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, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, 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: Rue de la Science 23, B-1040 Brüssel

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich	15
2 Normative Verweisungen	15
3 Begriffe	15
4 Kontext der Organisation	16
4.1 Verstehen der Organisation und ihres Kontextes	16
4.2 Verstehen der Erfordernisse und Erwartungen der interessierten Parteien	17
4.2.1 Allgemeines	17
4.2.2 Rechtliche und behördliche Anforderungen	17
4.3 Festlegung des Anwendungsbereichs des Business Continuity Management Systems	18
4.3.1 Allgemeines	18
4.3.2 Anwendungsbereichs des Business Continuity Management Systems	18
4.3.3 Ausschlüsse aus dem Anwendungsbereich	19
4.4 Business Continuity Management System	19
5 Führung	20
5.1 Führung und Verpflichtung	20
5.1.1 Allgemeines	20
5.1.2 Oberste Leitung	20
5.1.3 Andere Managementfunktionen	20
5.2 Politik	21
5.2.1 Erstellen der Politik zur Aufrechterhaltung der Betriebsfähigkeit	21
5.2.2 Kommunikation der Politik zur Aufrechterhaltung der Betriebsfähigkeit	22
5.3 Rollen, Verantwortlichkeiten und Befugnisse	22
6 Planung	24
6.1 Maßnahmen zum Umgang mit Risiken und Chancen	24
6.1.1 Bestimmung von Risiken und Chancen	24
6.1.2 Umgang mit Risiken und Chancen	24
6.2 Ziele zur Aufrechterhaltung der Betriebsfähigkeit und Planung, um diese zu erreichen	25
6.2.1 Festlegung von Zielen zur Aufrechterhaltung der Betriebsfähigkeit	25
6.2.2 Bestimmung der Ziele für die Aufrechterhaltung der Betriebsfähigkeit	25
6.3 Planung von Änderungen am BCMS	26
7 Unterstützung	26
7.1 Ressourcen	26
7.1.1 Allgemeines	26
7.1.2 BCMS-Ressourcen	26
7.2 Kompetenz	27
7.3 Bewusstsein	28
7.4 Kommunikation	30
7.5 Dokumentierte Information	30
7.5.1 Allgemeines	30
7.5.2 Erstellen und Aktualisieren	32
7.5.3 Lenkung dokumentierter Information	32

8	Betrieb	33
8.1	Betriebliche Planung und Steuerung	33
8.1.1	Allgemeines	33
8.1.2	Business Continuity Management	34
8.1.3	Aufrechterhaltung der Betriebsfähigkeit	35
8.2	Business-Impact-Analyse und Risikobeurteilung	36
8.2.1	Allgemeines	36
8.2.2	Business-Impact-Analyse	36
8.2.3	Risikobeurteilung	40
8.3	Strategien und Lösungen zur Aufrechterhaltung der Betriebsfähigkeit	42
8.3.1	Allgemeines	42
8.3.2	Festlegung der Strategien und Lösungen	42
8.3.3	Auswahl der Strategien und Lösungen	45
8.3.4	Ressourcenbedarf	46
8.3.5	Umsetzung von Lösungen	53
8.4	Pläne und Verfahren zur Aufrechterhaltung der Betriebsfähigkeit	54
8.4.1	Allgemeines	54
8.4.2	Reaktionsstruktur	54
8.4.3	Warnung und Kommunikation	56
8.4.4	Pläne zur Aufrechterhaltung der Betriebsfähigkeit	57
8.4.5	Wiederherstellung	64
8.5	Übungsprogramm	65
8.5.1	Allgemeines	65
8.5.2	Gestaltung des Übungsprogramms	65
8.5.3	Übungen zu Plänen für die Aufrechterhaltung der Betriebsfähigkeit	66
8.6	Bewertung der Dokumentation und Fähigkeiten zur Aufrechterhaltung der Betriebsfähigkeit	70
8.6.1	Allgemeines	70
8.6.2	Messen der Wirksamkeit	71
8.6.3	Ergebnisse	72
9	Bewertung der Leistung	73
9.1	Überwachung, Messung, Analyse und Bewertung	73
9.1.1	Allgemeines	73
9.1.2	Aufbewahrung von Nachweisen	73
9.1.3	Bewertung der Leistung	73
9.2	Internes Audit	73
9.2.1	Allgemeines	73
9.2.2	Auditprogramm(e)	74
9.3	Managementbewertung	74
9.3.1	Allgemeines	74
9.3.2	Eingaben für die Managementbewertung	74
9.3.3	Ergebnisse der Managementbewertung	75
10	Verbesserung	75
10.1	Nichtkonformität und Korrekturmaßnahmen	75
10.1.1	Allgemeines	75
10.1.2	Auftreten von Nichtkonformitäten	76
10.1.3	Aufbewahrung dokumentierter Informationen	76
10.2	Fortlaufende Verbesserung	77
	Literaturhinweise	78

Europäisches Vorwort

Dieses Dokument (EN ISO 22313:2020) wurde vom Technischen Komitee ISO/TC 292 „Security and resilience“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 391 „Schutz und Sicherheit der Bürger“ erarbeitet, dessen Sekretariat von AFNOR gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis August 2020, und etwaige entgegenstehende nationale Normen müssen bis August 2020 zurückgezogen werden.

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

Dieses Dokument ersetzt EN ISO 22313:2014.

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

Anerkennungsnotiz

Der Text von ISO 22313:2020 wurde von CEN als EN ISO 22313:2020 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsorganisationen (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird üblicherweise von Technischen Komitees von ISO durchgeführt. Jede Mitgliedsorganisation, die Interesse an einem Thema hat, für welches ein Technisches Komitee gegründet wurde, hat das Recht, in diesem Komitee vertreten zu sein. Internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO stehen, nehmen ebenfalls an der Arbeit teil. ISO arbeitet bei allen elektrotechnischen Themen eng mit der Internationalen Elektrotechnischen Kommission (IEC) zusammen.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Es sollten insbesondere die unterschiedlichen Annahmekriterien für die verschiedenen ISO-Dokumentenarten beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

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. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/TC 292, *Security and resilience* erarbeitet.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO 22313:2012), die technisch überarbeitet wurde. Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

- es wurden strukturelle und inhaltliche Änderungen vorgenommen, um dieses Dokument an die neueste Ausgabe von ISO 22301 anzugleichen;
- es wurden zusätzliche Leitlinien hinzugefügt, um wichtige Konzepte und Begriffe zu erläutern;
- aus 8.4 wurde Inhalt entfernt, der in die ISO/TS 22332 (in Erarbeitung) übernommen wird.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

Einleitung

0.1 Allgemeines

Dieses Dokument enthält Leitlinien, sofern angemessen, zu den in ISO 22301 festgelegten Anforderungen. Dieses Dokument beabsichtigt nicht, zu allen Aspekten der Aufrechterhaltung der Betriebsfähigkeit allgemeine Leitlinien zu liefern.

Dieses Dokument enthält die gleichen Überschriften wie ISO 22301, aber wiederholt nicht die Anforderungen und damit verbundene Begriffe und Definitionen.

Absicht dieser Leitlinien ist es, die Bedeutung und den Zweck der Anforderungen in ISO 22301 zu erläutern und zu klären sowie die Lösung von Interpretationsproblemen zu unterstützen. Weitere Internationale Normen und Technische Spezifikationen, die zusätzliche Leitlinien enthalten und die in diesem Dokument in Bezug genommen werden, sind ISO/TS 22317, ISO/TS 22318, ISO 22322, ISO/TS 22330, ISO/TS 22331 und ISO 22398. Der Anwendungsbereich dieser Dokumente kann sich über die Anforderungen von ISO 22301 hinaus erstrecken. Organisationen sollten daher zur Verifizierung der zu erfüllenden Anforderungen immer Bezug auf ISO 22301 nehmen.

Zur weiteren Klärung und Erläuterung von Kernaussagen enthält dieses Dokument verschiedene Bilder. Die Bilder dienen ausschließlich der Veranschaulichung und der damit zusammenhängende Text im Hauptteil dieses Dokuments hat Vorrang vor den Bildern.

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

- der Einführung von Leitlinien und Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit, die mit den Zielen der Organisation übereinstimmen;
- des Betreibens und Pflegens von Prozessen, Fähigkeiten und Reaktionsstrukturen, um sicherzustellen, dass die Organisation Störungen übersteht;
- des Überwachens und Überprüfens der Leistung und der Effektivität des BCMS;
- einer fortlaufenden Verbesserung auf Grundlage qualitativer und quantitativer Messungen.

Ein BCMS enthält, wie jedes andere Managementsystem, die folgenden Bestandteile:

- a) eine Politik;
- b) kompetente Personen mit festgelegten Verantwortlichkeiten;
- c) Managementprozesse in Bezug auf:
 - 1) Politik;
 - 2) Planung;
 - 3) Umsetzung und Betrieb;
 - 4) Leistungsbewertung;
 - 5) Managementbewertung;
 - 6) fortlaufende Verbesserung;
- d) dokumentierte Informationen, die die betriebliche Kontrolle unterstützen und eine Leistungsbewertung ermöglichen.

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 belastbaren Gesellschaft bei.

0.2 Vorteile eines Business Continuity Management Systems

Ein BCMS erhöht die Bereitschaft des Unternehmens zur Aufrechterhaltung des Betriebs bei Unterbrechungen. Außerdem führt es zu einem verbesserten Verstehen der internen und externen Beziehungen einer Organisation, einer besseren Kommunikation mit interessierten Parteien und zur Entwicklung eines Umfelds für fortlaufende Verbesserungen. Potenziell bestehen zahlreiche weitere Vorteile der Implementierung eines BCMS in Übereinstimmung mit den in diesem Dokument enthaltenen Empfehlungen und in Übereinstimmung mit den Anforderungen von ISO 22301.

- Die Umsetzung der Empfehlungen in Abschnitt 4 („Kontext der Organisation“) beinhaltet, dass die Organisation:
 - ihre strategischen Ziele überprüft, um sicherzustellen, dass das BCMS diese Zielsetzungen unterstützt;
 - die Bedürfnisse, Erwartungen und Anforderungen interessierter Parteien überdenkt;
 - die anzuwendenden rechtlichen, behördlichen und sonstigen Verpflichtungen kennt.
- Abschnitt 5 („Führung“) beinhaltet, dass die Organisation:
 - Managementzuständigkeiten und Verantwortlichkeiten überdenkt;
 - eine Kultur der fortlaufenden Verbesserung fördert;
 - Verantwortlichkeiten für die Leistungsüberwachung und -berichterstattung zuweist.

- Abschnitt 6 („Planung“) beinhaltet, dass die Organisation:
 - Risiken und Chancen erneut prüft und Maßnahmen identifiziert, um diese zu behandeln und davon zu profitieren;
 - ein effektives Änderungsmanagement einführt.
- Abschnitt 7 („Unterstützung“) beinhaltet, dass die Organisation:
 - ein effektives Management ihrer BCMS-Ressourcen einschließlich des Kompetenzmanagements einführt;
 - das Bewusstsein der Beschäftigten über Themen, die für das Management wichtig sind, verbessert;
 - über wirksame Mechanismen für die interne und externe Kommunikation verfügt;
 - ihre Dokumentation wirksam verwaltet.
- Abschnitt 8 („Betrieb“) führt dazu, dass die Organisation Folgendes berücksichtigt:
 - die unbeabsichtigten Auswirkungen von Veränderungen;
 - die Prioritäten und Anforderungen für die Aufrechterhaltung der Betriebsfähigkeit;
 - Abhängigkeiten;
 - Schwachstellen aus Sicht der Auswirkung;
 - Risiken von Betriebsstörungen und die Identifizierung der bestmöglichen Umgangsweise mit solchen Risiken;
 - alternative Lösungen für den Betrieb des Geschäfts mit begrenzten Ressourcen;
 - wirksame Strukturen und Verfahren für den Umgang mit Betriebsstörungen;
 - Verantwortlichkeiten gegenüber der Gemeinschaft und anderen interessierten Parteien.
- Abschnitt 9 („Bewertung der Leistung“) beinhaltet, dass die Organisation:
 - über wirksame Mechanismen für die Überwachung, Messung und Bewertung der Leistung verfügt;
 - das Leitungsgremium in die Überwachung der Leistung und die Mitwirkung an der Wirksamkeit des BCMS eingebunden wird.
- Abschnitt 10 („Verbesserung“) beinhaltet, dass die Organisation:
 - über Verfahren zur Überwachung der Leistung und Verbesserung der Wirksamkeit verfügt;
 - von der fortlaufenden Verbesserung ihrer Managementsysteme profitiert.

Demzufolge kann die Umsetzung des BCMS:

- a) Leben, Vermögenswerte und Umwelt schützen;
- b) den Ruf und die Glaubwürdigkeit der Organisation schützen und verbessern;
- c) zum Wettbewerbsvorteil einer Organisation beitragen, indem es ihr ermöglicht, den Betrieb auch während Betriebsstörungen fortzuführen;
- d) die aus Betriebsstörungen und der Verbesserung der Fähigkeit der Organisation, auch währenddessen handlungsfähig zu bleiben, resultierenden Kosten reduzieren;
- e) zur organisatorischen Belastbarkeit der Organisation beitragen;
- f) dabei helfen, das Vertrauen interessierter Parteien in den Erfolg der Organisation zu stärken;
- g) die rechtlichen und finanziellen Risiken der Organisation verringern;
- h) die Fähigkeit der Organisation, mit Risiken umzugehen und betriebliche Schwachstellen zu behandeln, aufzeigen.

0.3 Planen-Durchführen-Prüfen-Handeln-Zyklus (PDCA-Zyklus)

Dieses Dokument wendet den Planen-Durchführen-Prüfen-Handeln-Zyklus (en: Plan-Do-Check-Act, PDCA) an, um das BCMS einer Organisation zu planen, einzuführen, umzusetzen, zu betreiben, zu überwachen, zu überprüfen, aufrechtzuerhalten und dessen Effektivität ständig zu verbessern. Eine Erläuterung des PDCA-Zyklus ist in Tabelle 1 wiedergegeben.

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

Tabelle 1 — Erläuterungen zum PDCA-Zyklus

Planen (Einführen)	Einführen von Politik, Zielen, Kontrollen, Prozessen und Verfahren, die für die Verbesserung der Aufrechterhaltung der Betriebsfähigkeit relevant sind, um Ergebnisse zu erzielen, die sich mit der übergeordneten Politik und den übergeordneten Zielen der Organisation in Übereinstimmung befinden.
Durchführen (Umsetzen und Betreiben)	Umsetzen und Anwenden der Politik, Kontrollen, Prozesse und Verfahren zur Aufrechterhaltung der Betriebsfähigkeit.
Prüfen (Überwachen und Überprüfen)	Überwachen und Überprüfen der Leistung vor dem Hintergrund der Politik und Zielen zur Aufrechterhaltung der Betriebsfähigkeit, Berichten der Ergebnisse an das Management zum Zweck der Überprüfung, und 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 Managementbewertung sowie Neubeurteilung des Anwendungsbereichs des BCMS sowie der Leitlinien und Ziele zur Aufrechterhaltung der Betriebsfähigkeit.

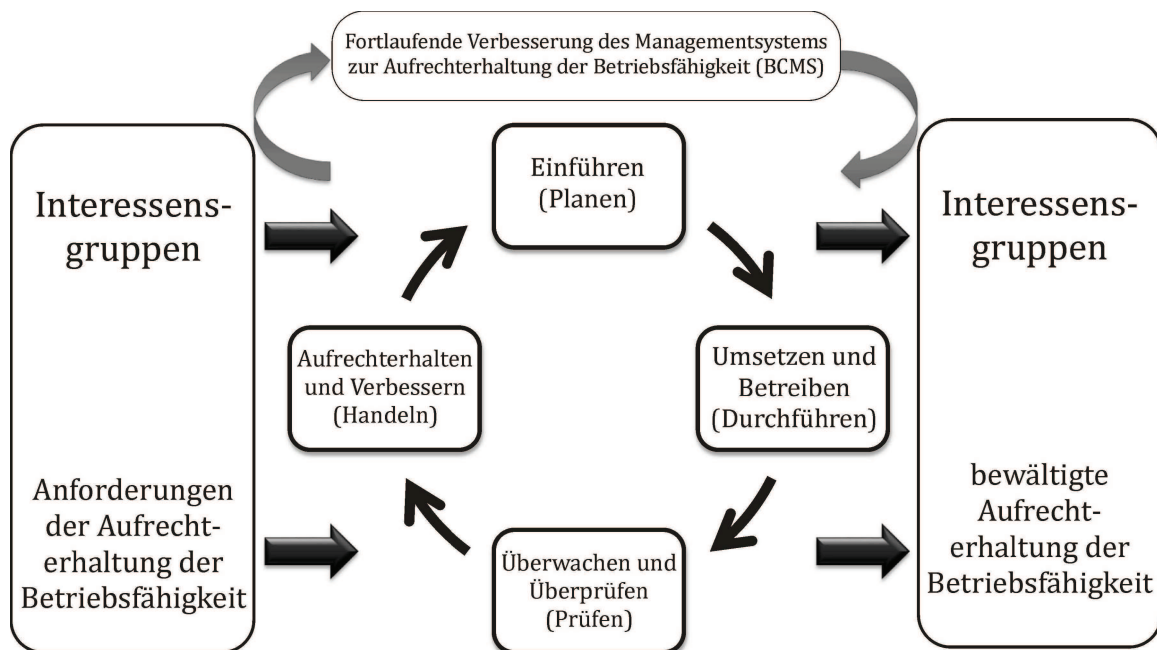


Bild 1 — Auf die BCMS-Prozesse angewendeter PDCA-Zyklus

0.4 Bestandteile des PDCA-Modells in diesem Dokument

Tabelle 2 zeigt den direkten Zusammenhang zwischen dem Inhalt von Bild 1 und den Abschnitten dieses Dokuments:

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

Bestandteil des PDCA-Modells	Abschnitt, in dem der Bestandteil des PDCA-Zyklus behandelt wird
Planen (Einführen)	Abschnitt 4 („Kontext der Organisation“) legt fest, was die Organisation unternehmen sollte, damit sichergestellt ist, dass das BCMS ihre Anforderungen erfüllt, unter Berücksichtigung aller relevanten internen und externen Faktoren, einschließlich: <ul style="list-style-type: none"> — der Erfordernisse und Erwartungen interessierter Parteien; — seiner rechtlichen und behördlichen Verpflichtungen; — des geforderten Anwendungsbereichs des BCMS.
	Abschnitt 5 („Führung“) legt die Rolle des Managements im Hinblick darauf fest, dass die Selbstverpflichtung nachgewiesen wird und Politik, Funktionen, Verantwortlichkeiten und Befugnisse festgelegt werden.
	Abschnitt 6 („Planung“) beschreibt die Maßnahmen zur Einführung von strategischen Zielen und Leitsätzen für die Umsetzung des BCMS.
	Abschnitt 7 („Unterstützung“) identifiziert die Elemente des BCMS, die vorhanden sein sollten, insbesondere Ressourcen, Kompetenzen, Bewusstsein, Kommunikation und dokumentierte Information.
Durchführen (Umsetzen und Betreiben)	Abschnitt 8 („Betrieb“) identifiziert die Prozesse zur Schaffung und Aufrechterhaltung der Betriebsfähigkeit.
Prüfen (Überwachen und Überprüfen)	Abschnitt 9 („Bewertung der Leistung“) enthält die Grundlage zur Verbesserung des BCMS durch Messen und Bewerten seiner Leistung.
Handeln (Aufrechterhalten und Verbessern)	Abschnitt 10 („Verbesserung“) behandelt Korrekturmaßnahmen für Abweichungen, die anhand einer Leistungsbewertung festgestellt wurden.

0.5 Inhalt dieses Dokuments

Dieses Dokument 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 und insbesondere Kunden und Beschäftigten 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.

Dieses Dokument ist nicht dazu bestimmt, zur Bewertung der Befähigung einer Organisation zur Erfüllung der eigenen Kontinuitätsbedürfnisse oder der Erfüllung von Kunden-, gesetzlichen oder behördlichen Bedürfnissen angewendet zu werden. Organisationen, die dies wünschen, können die Anforderungen in ISO 22301 anwenden.

Die Abschnitte 1 bis 3 in diesem Dokument legen den Anwendungsbereich, die normativen Verweisungen und Begriffe fest, die für die Verwendung dieses Dokuments gelten. Die Abschnitte 4 bis 10 enthalten Leitlinien bezüglich der Anforderungen, die in ISO 22301 angegeben sind.

In diesem Dokument werden die folgenden Verbformen verwendet:

- a) „sollte“ bezeichnet eine Empfehlung;
- b) „darf“ bezeichnet eine Erlaubnis;
- c) „kann“ bezeichnet eine Möglichkeit oder Fähigkeit.

0.6 Aufrechterhaltung der Betriebsfähigkeit

Die Aufrechterhaltung der Betriebsfähigkeit ist die Fähigkeit der Organisation, die Belieferung mit Produkten oder Dienstleistungen nach einer Betriebsstörung mit akzeptabler, zuvor festgelegter Kapazität fortzusetzen. Das Business Continuity Management ist der Prozess der Umsetzung und Aufrechterhaltung der Betriebsfähigkeit (siehe 8.1.2 und Bild 5), um Verluste zu vermeiden und sich auf Betriebsstörungen vorzubereiten, diese zu mindern und mit ihnen umzugehen.

Die Einführung eines BCMS ermöglicht der Organisation, ihre Aufrechterhaltung der Betriebsfähigkeit zu steuern, zu bewerten und ständig zu verbessern.

In diesem Dokument wird das Wort „Betrieb“ als ein allumfassender Begriff für die Abläufe und Dienste verwendet, die von einer Organisation beim Verfolgen ihrer Ziele, Zwecke oder Mission ausgeführt werden. Daher gilt es gleichermaßen für große, mittlere und kleine Unternehmen, die im industriellen, kommerziellen, öffentlichen und gemeinnützigen Bereich tätig sind.

Betriebsstörungen besitzen das Potenzial, die gesamten Betriebsabläufe der Organisation und deren Fähigkeit, Produkte und Dienstleistungen zu liefern, zu unterbrechen. Die Umsetzung eines BCMS, bevor eine Unterbrechung eintritt, anstelle nach einem Zwischenfall in ungeplanter Weise zu reagieren, ermöglicht der Organisation die Wiederaufnahme von Betriebsabläufen, bevor ein inakzeptables Ausmaß an Auswirkungen entsteht.

Das Business Continuity Management umfasst Folgendes:

- a) die Identifizierung der Produkte und Dienstleistungen einer Organisation sowie der Tätigkeiten zu deren Bereitstellung;
- b) die Analyse der Auswirkungen einer Nichtwiederaufnahme der Tätigkeiten sowie der Ressourcen, die diese erfordern;
- c) das Verständnis des Risikos der Betriebsstörung;
- d) die Bestimmung von Prioritäten, Zeitrahmen, Kapazitäten und Strategien zur Wiederaufnahme der Lieferung von Produkten und Dienstleistungen;
- e) die Verfügbarkeit von Lösungen und Plänen zur Wiederaufnahme der Tätigkeiten innerhalb der geforderten Zeitrahmen nach einer Betriebsunterbrechung;
- f) das Sicherstellen, der regelmäßigen Überprüfung und Aktualisierung diese Vorkehrungen, damit sie unter allen Umständen wirksam sind.

Der Ansatz des Unternehmens für das Business Continuity Management und seine dokumentierten Informationen sollte für seinen Kontext geeignet sein (z. B. Betriebsumgebung, Komplexität, Bedürfnisse und Ressourcen).

Die Aufrechterhaltung der Betriebsfähigkeit kann sowohl bei plötzlichen Betriebsstörungen (z. B. Explosionen) als auch bei allmählich eintretenden Betriebsstörungen (z. B. Pandemien) wirksam sein.

Tätigkeiten können durch die verschiedensten Zwischenfälle 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 wesentlich sind, um ihre Verpflichtungen zu erfüllen. Durch die Aufrechterhaltung der Betriebsfähigkeit kann eine Organisation erkennen, was zum Schutz ihrer Ressourcen (z. B. Personen, Betriebsgelände, Technologien, Informationen), ihrer Lieferkette, ihrer Interessengruppen und ihres Rufs unternommen werden muss, bevor eine Betriebsstörung eintritt. Durch diese Kenntnis ist die Organisation in der Lage, eine Reaktionsstruktur zu entwickeln, um sicher zu gehen, die Konsequenzen einer Störung zu managen.

Bild 2 und Bild 3 verdeutlichen konzeptionell, wie die Aufrechterhaltung der Betriebsfähigkeit wirksam die Auswirkungen in bestimmten Situationen mildern kann. Die relativen Abstände zwischen den in den Diagrammen dargestellten Stufen dienen nicht der Darstellung bestimmter zeitlicher Abstände.

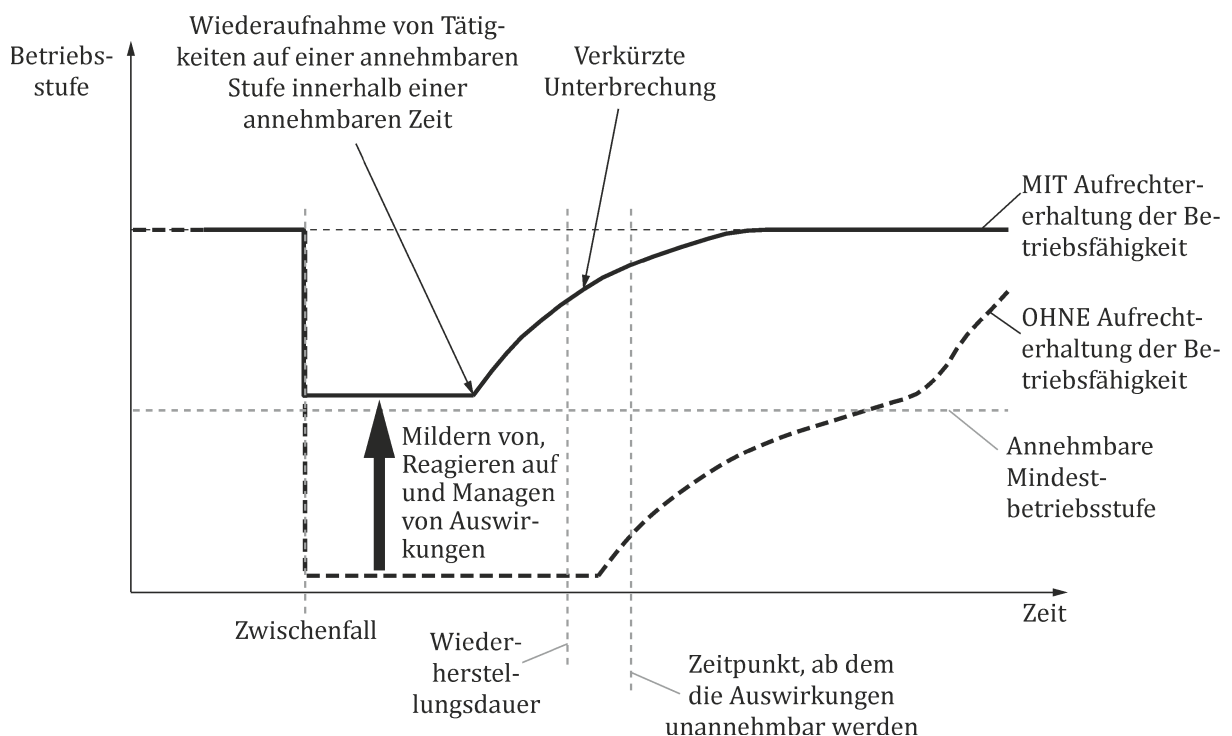


Bild 2 — Darstellung einer wirksamen Aufrechterhaltung der Betriebsfähigkeit bei plötzlicher Betriebsstörung

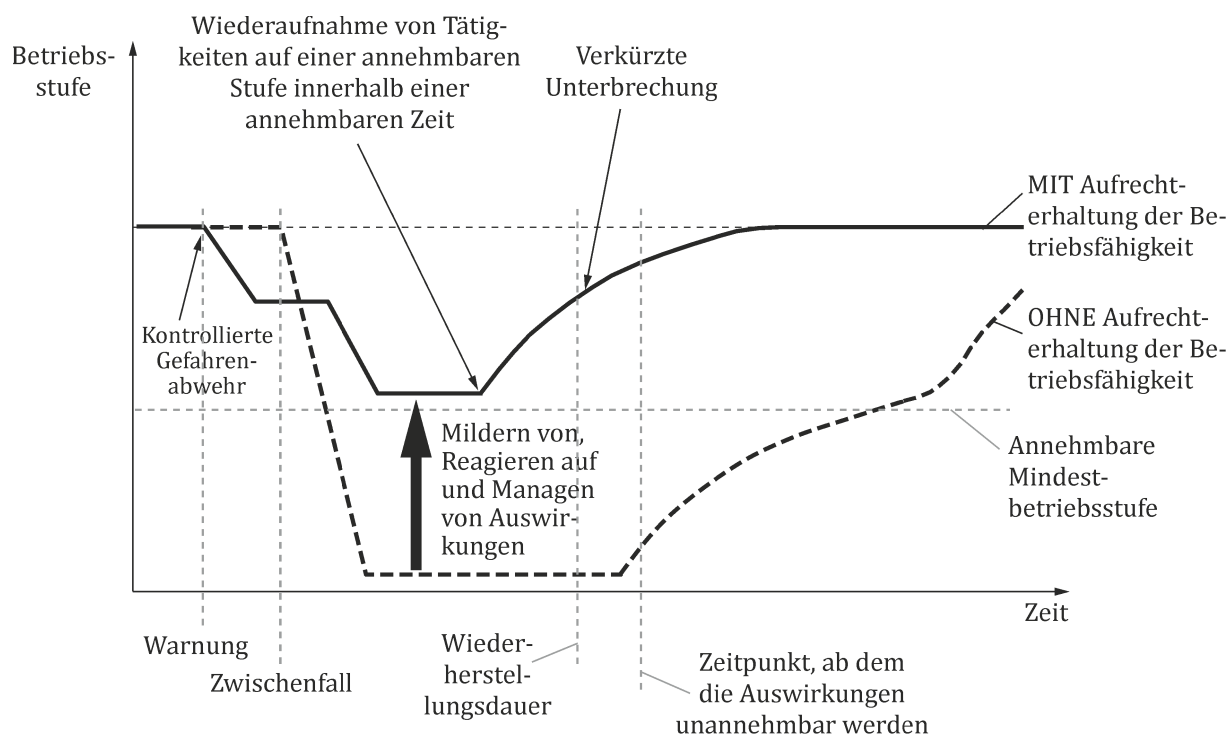


Bild 3 — Darstellung einer wirksamen Aufrechterhaltung der Betriebsfähigkeit bei allmählich eintretender Betriebsstörung (z. B. herannahende Pandemie)

1 Anwendungsbereich

Dieses Dokument gibt Leitlinien und Empfehlungen zur Anwendung der Anforderungen des Business Continuity Management Systems (BCMS), die in ISO 22301 vorgegeben sind. Die Leitlinien und Empfehlungen beruhen auf anerkannter internationaler Praxis.

Dieses Dokument ist auf Organisationen anwendbar, die:

- a) ein BCMS umsetzen, aufrechterhalten und verbessern;
- b) eine Übereinstimmung mit der erklärten Politik zur Aufrechterhaltung der Betriebsfähigkeit sicherstellen wollen;
- c) die Fähigkeit benötigen, die Belieferung mit Produkten und Dienstleistungen mit einer akzeptablen, zuvor festgelegten Kapazität während einer Betriebsstörung fortzusetzen;
- d) versuchen, ihre Resilienz durch die effektive Anwendung des BCMS zu verbessern.

Die Leitlinien und Empfehlungen sind anwendbar für alle Organisationsgrößen und -typen, einschließlich großer, mittlerer und kleiner Unternehmen, die im industriellen, kommerziellen, öffentlichen und gemeinnützigen Bereich tätig sind. Die angewendete Vorgehensweise ist von der betrieblichen Umgebung und der Komplexität der jeweiligen Organisation abhängig.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. 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, *Security and resilience — Vocabulary*

ISO 22301, *Security and resilience — Business continuity management systems — Requirements*

3 Begriffe

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

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>
- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>

3.1

Business Continuity Management

Prozess der Umsetzung und Aufrechterhaltung der Betriebsfähigkeit

4 Kontext der Organisation

4.1 Verstehen der Organisation und ihres Kontextes

Dieser Abschnitt enthält Empfehlungen zum Verständnis des Kontextes der Organisation in Bezug auf das BCMS. Empfehlungen für die Schaffung und Aufrechterhaltung der Betriebsfähigkeit werden in 8.1 behandelt.

Die Organisation sollte die internen und externen Themen, die für die allgemeinen Zielsetzungen der Organisation, ihre Produkte und Dienstleistungen sowie die Höhe und Art des Risikos, das sie eingehen darf oder nicht, relevant sind (darunter positive und negative Faktoren oder Bedingungen zur Abwägung), bewerten und verstehen. Diese Information sollte bei der Schaffung und Aufrechterhaltung des BCMS der Organisation und bei der Zuordnung von Prioritäten berücksichtigt werden.

Der externe Kontext einer Organisation beinhaltet, sofern relevant, folgende Faktoren:

- das politische, rechtliche und behördliche Umfeld, ob international, national, regional oder lokal;
- soziale und kulturelle Aspekte;
- das finanzielle, technologische, wirtschaftliche, natürliche und wettbewerbliche Umfeld, ob international, national, regional oder lokal;
- die Verpflichtungen und Beziehungen hinsichtlich der Lieferkette (siehe auch ISO/TS 22318);
- Einflussfaktoren (z. B. Risiko, Technologie) und Trends, die eine Auswirkung auf die Ziele und den Betrieb der Organisation haben;
- die Beziehungen zu Interessengruppen außerhalb der Organisation und deren Ansichten und Werte;
- Kommunikationskanäle einschließlich sozialer Netzwerke, die für die Sicherstellung und Bildung solcher Beziehungen genutzt werden.

Der interne Kontext der Organisation beinhaltet, sofern relevant, folgende Faktoren:

- 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, Technologien);
- bestehende Managementsysteme;
- Informationen und Daten (aufbewahrt in physischer oder elektronischer Form) und Entscheidungsprozesse (formal und andere);
- interessierte Parteien innerhalb der Organisation einschließlich interner Lieferanten [Berücksichtigung der Leistungsvereinbarungen (SLA, en: service level agreements), der beurteilten Resilienz und der Wiederherstellungsvereinbarungen], siehe ISO/TS 22318;
- Politik und Ziele sowie die Geschäftsstrategien, mit denen diese umgesetzt werden;
- Zukunftschancen und Unternehmensprioritäten;
- Ansichten, Werte und Kultur;
- Normen und Referenzmodelle, die von der Organisation angewendet werden;
- Strukturen (z. B. Unternehmensführung, Rollen, Zuständigkeiten);
- interne Kommunikationskanäle, die für den Austausch von Informationen mit den Mitarbeitern genutzt werden (z. B. soziale Netzwerke).

4.2 Verstehen der Erfordernisse und Erwartungen der interessierten Parteien

4.2.1 Allgemeines

Die Organisation hat eine Sorgfaltspflicht für eine Vielzahl von Personen innerhalb und außerhalb der Organisation (siehe auch ISO/TS 22330). Bei der Einführung ihres BCMS sollte die Organisation sicherstellen, dass die Bedürfnisse und Anforderungen aller interessierten Parteien berücksichtigt werden.

Die Organisation sollte alle Interessengruppen ermitteln, die für das BCMS von Bedeutung sind (siehe Bild 4), und auf Grundlage von deren Bedürfnissen und Erwartungen deren Anforderungen bestimmen. Es ist wichtig, nicht nur verbindliche und angegebene Anforderungen zu erkennen, sondern auch alle Anforderungen, die sich implizit ergeben.

Bei der Planung und Umsetzung des BCMS ist es wichtig, Tätigkeiten zu ermitteln, die gegenüber den Interessengruppen angemessen sind, aber zwischen diesen unterscheiden. Während es beispielsweise angemessen sein kann, nach einer Betriebsstörung mit allen interessierten Parteien zu kommunizieren, kann es unangemessen sein, bei der Umsetzung und Aufrechterhaltung eines Business Continuity Managements mit allen Interessengruppen zu kommunizieren (siehe 8.1.2).

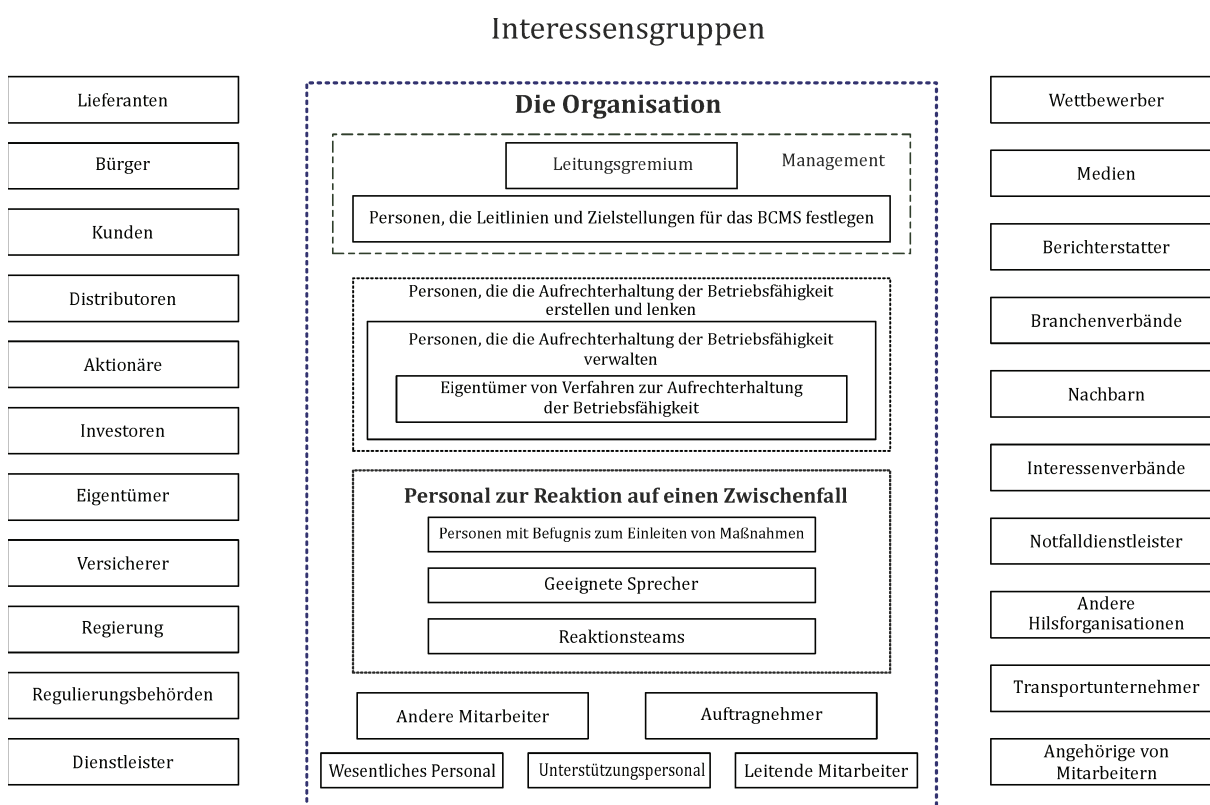


Bild 4 — Beispiele für zu berücksichtigende interessierte Parteien im öffentlichen und privaten Bereich

4.2.2 Rechtliche und behördliche Anforderungen

Die Anwendung dieses Dokuments setzt die Kenntnis der anzuwendenden rechtlichen und behördlichen Anforderungen voraus.

Anforderungen können impliziert, angegeben oder verbindlich sein. Die Informationen über diese Anforderungen sollten dokumentiert und stets aktuell gehalten werden. Neue Anforderungen oder Änderungen bestehender Anforderungen sollten den betroffenen Mitarbeitern und anderen interessierten Parteien mitgeteilt werden.

Die Organisation sollte zeigen, dass sie Zugang hat zu aktuellen rechtlichen und behördlichen Anforderungen mit Relevanz für ihren Betrieb und denen, die sich in Vorbereitung befinden, und die Art und Weise, wie diese Anforderungen erfüllt werden. Diese Anforderungen können Folgendes umfassen:

- a) Reaktion auf einen Zwischenfall, einschließlich Gefahrenabwehr und anderer relevanter Rechtsvorschriften;
- b) Aufrechterhaltung der Betriebsfähigkeit, die den Anwendungsbereich des Programms oder den Umfang oder die Geschwindigkeit ihrer Wiederherstellung festlegen kann;
- c) Risiko, Anforderungen, die den Anwendungsbereich oder das Verfahren des Risikomanagements festlegen;
- d) Gefährdungen (z. B. betriebliche Anforderungen in Bezug auf gefährliche Materialien, die vor Ort gelagert werden).

Organisationen mit Betrieben an mehreren Standorten müssen gegebenenfalls die Anforderungen verschiedener Länder erfüllen.

4.3 Festlegung des Anwendungsbereichs des Business Continuity Management Systems

4.3.1 Allgemeines

Der Zweck der Bestimmung des Anwendungsbereichs des BCMS ist es, dessen Grenzen und die Anwendbarkeit zu identifizieren, um die Berücksichtigung aller relevanten Produkte und Dienstleistungen, Aktivitäten, Standorte, Ressourcen, Lieferanten und anderer Abhängigkeiten sicherzustellen.

Der Anwendungsbereich sollte auf die in 4.1 behandelten Themen, auf die in 4.2 bestimmten Anforderungen der interessierten Parteien sowie auf den Auftrag, die Ziele und die Verpflichtungen der Organisation eingehen.

Die Organisation sollte eine Erklärung erstellen, in der der Anwendungsbereich des BCMS in einer Art und Weise und mit einer Terminologie dargestellt wird, wie es im Hinblick auf Größe, Art und Komplexität der Organisation angemessen ist. Die Erklärung sollte den interessierten Parteien zur Verfügung stehen.

4.3.2 Anwendungsbereichs des Business Continuity Management Systems

Die Organisation sollte:

- a) durch Verweis auf die Produkte und Dienstleistungen die Teile der Organisation festlegen, die im Anwendungsbereich des BCMS enthalten bzw. von diesem ausgeschlossen sind, z. B. jene, welche:
 - 1) nur die Lieferung eines bestimmten Produkts an ein Land oder eine Region beinhalten;
 - 2) ein Produkt ausschließen, das nicht mehr brauchbar oder von geringem Wert für die Organisation ist;
 - 3) nur einen Teil der Produkte und Dienstleistungen einbinden;
- b) die Produkte und Dienstleistungen der Organisation so bezeichnen, dass alle damit verbundenen Tätigkeiten, Ressourcen und Lieferketten ermittelt werden können.

Der Anwendungsbereich darf:

- eine Angabe über das Ausmaß oder die Größe eines Zwischenfalls, der durch das BCMS abgedeckt ist, enthalten;
- festlegen, wie das BCMS in die Geschäftsstrategie und den Ansatz für das Risikomanagement der Organisation einzuordnen ist.

4.3.3 Ausschlüsse aus dem Anwendungsbereich

Im Anwendungsbereich sind die Standorte, Produkte und Dienstleistungen, Tätigkeiten und Ressourcen 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 ein Produktionsunternehmen ein Produkt in den Anwendungsbereich seines BCMS aufnimmt, müssen auch die Lieferung der Rohmaterialien, die Verarbeitung, die Lieferung und alle unterstützenden Funktionen (wie etwa Datenverarbeitung, Beschaffung und Personalwesen) an jedem Standort, die direkt oder indirekt an der Lieferung des Produkts an den Kunden beteiligt sind, eingebunden werden.

Ausschlüsse sollten nicht die Fähigkeit der Organisation gefährden, die in der Business-Impact-Analyse (siehe 8.2.2) festgelegten Anforderungen an die Aufrechterhaltung der Betriebsfähigkeit zu erfüllen. Tätigkeiten, Ressourcen und Lieferketten, die erforderlich sind, um im Anwendungsbereich enthaltene Produkte und Dienstleistungen zu liefern, können nicht ausgeschlossen werden.

Ausschlüsse aus dem Anwendungsbereich des BCMS sollten dokumentiert und ihre Begründung sollte erläutert werden.

Wenn das BCMS in ein bestehendes Managementsystem integriert wird, sollte die Organisation sicherstellen, dass alle Elemente des BCMS eingebunden werden.

4.4 Business Continuity Management System

Zweck dieses Unterabschnitts ist es, das Erfordernis für die Organisation zu betonen, Prozesse umzusetzen und aufrechtzuerhalten, die es dem BCMS ermöglichen, die Anforderungen nach ISO 22301 einschließlich der Wechselwirkungen zwischen den Prozessen zu erfüllen.

Bei der Bestimmung der Prozesse und ihrer Anwendung in der gesamten Organisation sollte diese:

- a) die erforderlichen Eingaben und die erwarteten Ergebnisse dieser Prozesse bestimmen;
- b) die Abfolge und Wechselwirkung dieser Prozesse bestimmen;
- c) die für den effektiven Betrieb und die Steuerung dieser Prozesse erforderlichen Kriterien und Verfahren (einschließlich Überwachung, Messungen und die damit verbundenen Leistungsindikatoren) bestimmen;
- d) die erforderlichen Ressourcen für diese Prozesse bestimmen und ihre Verfügbarkeit sicherstellen;
- e) die Verantwortlichkeiten und Befugnisse für diese Prozesse zuweisen;
- f) die in 6.1 bestimmten Risiken und Chancen behandeln;
- g) diese Prozesse bewerten und alle notwendigen Änderungen umzusetzen, um sicherzustellen, dass diese Prozesse die beabsichtigten Ergebnisse erreichen;
- h) die Prozesse und das BCMS verbessern.

Soweit erforderlich, sollte die Organisation:

- dokumentierte Informationen zur Unterstützung des Betriebs ihrer Prozesse aufrechterhalten;
- dokumentierte Informationen bewahren, sodass darauf vertraut werden kann, dass die Prozesse wie geplant durchgeführt werden.

5 Führung

5.1 Führung und Verpflichtung

5.1.1 Allgemeines

Alle Ebenen der Leitung der gesamten Organisation sollten Führung und Verpflichtung in ihren Verantwortungsbereichen demonstrieren.

5.1.2 Oberste Leitung

Die oberste Leitung sollte Führung und Verpflichtung demonstrieren durch:

- a) Zuweisung von Managementfunktionen und Sicherstellung, dass diese ausgefüllt werden (siehe 5.1.3);
- b) Einführung einer Politik zur Aufrechterhaltung der Betriebsfähigkeit (siehe 5.2);
- c) Ernennung einer oder mehrerer Personen mit angemessenen Befugnissen und Kompetenzen, die für das BCMS verantwortlich und für dessen wirksame Anwendung zuständig sind (siehe 5.3);
- d) Kommunikation der Bedeutung der Aufrechterhaltung der Betriebsfähigkeit und der Erfüllung der BCMS-Anforderungen;
- e) Verfügbarmachung der notwendigen Ressourcen, einschließlich eines angemessenen Umfangs finanzieller Mittel (siehe 7.1);
- f) Förderung der fortlaufenden Verbesserung (siehe 10.2);
- g) Sicherstellung, dass die beabsichtigten Ergebnisse des BCMS erreicht werden;
- h) Unterstützung anderer Ebenen der Leitung, damit diese Führung und Verpflichtung in ihren Verantwortungsbereichen demonstrieren können.

5.1.3 Andere Managementfunktionen

Andere Managementebenen sollten ihre Führung und Verpflichtung demonstrieren durch:

- a) Zielsetzungen für die Aufrechterhaltung der Betriebsfähigkeit, die mit den strategischen Zielen der Organisation vereinbar sind (siehe 6.2), festlegen;
- b) die Integration von BCMS-Anforderungen in die Geschäftsprozesse der Organisation (siehe 8.1);
- c) das Bewusstsein über die anzuwendenden rechtlichen, behördlichen und sonstigen Anforderungen (siehe 4.2.2) zeigen;
- d) Festlegung der Rollen, Verantwortlichkeiten und Kompetenzen innerhalb des BCMS (siehe 5.3 und 7.2);
- e) Erreichung der beabsichtigten Ergebnisse des BCMS;
- f) aktive Teilnahme am Übungsprogramm (siehe 8.5);
- g) Durchführung interner BCMS-Audits (siehe 9.2);
- h) Durchführung von wirksamen Qualitätsmanagementbewertungen des BCMS (siehe 9.3);
- i) Anleitung und Unterstützung der Verbesserung des BCMS (siehe Abschnitt 10).

Die Verpflichtung der Leitung darf außerdem durch Folgendes dargelegt werden:

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

5.2 Politik

5.2.1 Erstellen der Politik zur Aufrechterhaltung der Betriebsfähigkeit

Das Leitungsgremium sollte die Politik zur Aufrechterhaltung der Betriebsfähigkeit unter dem Aspekt der Ziele und Verpflichtung der Organisation festlegen und sicherstellen, dass diese:

- a) eine präzise allgemeine Beschreibung der Absicht und Ausrichtung der obersten Leitung für das BCMS ist;
- b) dem Zweck der Organisation entspricht (d. h. ihrer Größe, Art und Komplexität und unter Beachtung ihrer Kultur, Abhängigkeiten und Betriebsumgebung);
- c) ein Rahmenwerk für die Erstellung von Zielen bereitstellt;
- d) eine klare Verpflichtung zur Erfüllung der anzuwendenden Anforderungen einschließlich rechtlicher und behördlicher Verpflichtungen enthält;
- e) eine Verpflichtung zu einer fortlaufenden Verbesserung des BCMS enthält.

Die Politik sollte:

- die Reichweite des Anwendungsbereichs und die Grenzen der Aufrechterhaltung der Betriebsfähigkeit der Organisation, einschließlich Einschränkungen und Ausnahmen, angeben (siehe 4.3);
- jegliche erforderlichen Befugnisse und Bevollmächtigungen festlegen, einschließlich der Person oder Personen, die für das BCMS der Organisation verantwortlich ist/sind (siehe 5.3);
- Verweisungen auf Normen, Richtlinien, Vorschriften oder Leitlinien enthalten, die das BCMS berücksichtigen oder erfüllen sollte.

Die Politik darf Folgendes enthalten:

- eine 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.

Für Organisationen mit bestehenden Managementsystemen kann es angemessen sein, die BCMS-Politik in Politiken von anderen Managementsystemen zu integrieren.

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