

DIN EN ISO 22313



ICS 03.100.01; 03.100.70

EntwurfEinsprüche bis 2019-06-19
Vorgesehen als Ersatz für
DIN EN ISO 22313:2016-05**Sicherheit und Resilienz –
Business Continuity Management Systems –
Leitlinie (ISO/DIS 22313:2019);
Deutsche und Englische Fassung prEN ISO 22313:2019**Security and resilience –
Business continuity management systems –
Guidance (ISO/DIS 22313:2019);
German and English version prEN ISO 22313:2019Sécurité et résilience –
Systèmes de management de la continuité d'activité –
Lignes directrices (ISO/DIS 22313:2019);
Version allemande et anglaise prEN ISO 22313:2019**Anwendungswarnvermerk**

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-04-19 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe 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 info@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Organisationsprozesse (NAOrg), 10772 Berlin, Saatwinkler Damm 42/43, 13627 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 153 Seiten

DIN-Normenausschuss Organisationsprozesse (NAOrg)

Nationales Vorwort

Dieses Dokument (prEN ISO 22313:2019) 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 NEN (Niederlande) gehalten wird.

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

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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

ISO 19011:2018	siehe	DIN EN ISO 19011:2018-10
ISO 22300	siehe	DIN EN ISO 22300
ISO 22301	siehe	DIN EN ISO 22301
ISO 31000:2018	siehe	DIN ISO 31000:2018-10

Änderungen

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

- a) Anpassung des Dokuments an die aktuellen Vorgaben für Managementsystemnormen nach DIN SPEC 36601;
- b) Einleitung, Abschnitt 0.2 und 0.5 wurden hinzugefügt;
- c) Abschnitt 3.1 wurde hinzugefügt;
- d) Abschnitt 4.4 wurde technisch überarbeitet;
- e) Abschnitt 5.2 wurde technisch überarbeitet;
- f) Abschnitt 5.2.1 und 5.2.2 wurden hinzugefügt;
- g) Tabelle 4, Tabelle 5 und Tabelle 6 wurden hinzugefügt;
- h) Abschnitt 6.3 wurde hinzugefügt;
- i) Abschnitt 8.1.1, 8.3.2.4, 8.3.3.3 und 8.4.1 wurden hinzugefügt;
- j) Abschnitt 8.2.2 wurde technisch überarbeitet;
- k) Abschnitt 9.1 wurde technisch überarbeitet;
- l) Abschnitt 9.3.1 und 9.3.2 wurden hinzugefügt.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 19011:2018-10, *Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2018); Deutsche und Englische Fassung EN ISO 19011:2018*

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

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

DIN ISO 31000:2018-10, *Risikomanagement — Leitlinien (ISO 31000:2018)*

— Leerseite —

Sicherheit und Resilienz — Business Continuity Management Systems — Leitlinie (ISO/DIS 22313:2019)

*Sécurité et résilience — Systèmes de management de la continuité d'activité — Lignes directrices
(ISO/DIS 22313:2019)*

Security and resilience — Business continuity management systems — Guidance (ISO/DIS 22313:2019)

ICS:

Deskriptoren:

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokumentstufe: parallele Umfrage
Dokumentsprache: D

STD Version 2.9p

Inhalt

	Seite
Europäisches Vorwort.....	4
Vorwort.....	5
Einleitung.....	6
1 Anwendungsbereich.....	15
2 Normative Verweisungen	15
3 Begriffe.....	15
3.1 Auswertung und Bedeutung.....	16
4 Kontext der Organisation	16
4.1 Verstehen der Organisation und ihres Kontextes.....	16
4.2 Verstehen der Bedürfnisse und Erwartungen der interessierten Parteien.....	17
4.2.1 Allgemeines.....	17
4.2.2 Rechtliche und behördliche Anforderungen.....	18
4.3 Festlegung des Anwendungsbereichs des Business Continuity Managements.....	19
4.3.1 Allgemeines.....	19
4.3.2 Anwendungsbereich des BCMS	19
4.4 Business Continuity Management System	20
5 Führung.....	20
5.1 Führung und Selbstverpflichtung.....	20
5.2 Politik	21
5.2.1 Verantwortlichkeiten der obersten Leitung.....	21
5.2.2 Bestimmungen zur Aufrechterhaltung der Betriebsfähigkeit.....	22
5.3 Funktionen, Verantwortlichkeiten und Befugnisse innerhalb der Organisation	23
6 Planung.....	25
6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten.....	25
6.2 Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit und Planung zur Zielerreichung.....	26
6.3 Planung von Änderungen am BCMS.....	26
7 Unterstützung.....	27
7.1 Ressourcen.....	27
7.1.1 Allgemeines.....	27
7.1.2 BCMS-Ressourcen.....	27
7.2 Kompetenz	27
7.3 Bewusstseinsbildung	29
7.4 Kommunikation.....	31
7.5 Dokumentierte Information	31
7.5.1 Allgemeines.....	31
7.5.2 Erstellen und Aktualisieren.....	33
7.5.3 Lenkung dokumentierter Information	33
8 Betrieb.....	34
8.1 Ablaufplanung und Steuerung.....	34
8.1.1 Business Continuity Management (BCM).....	35
8.1.2 Aufrechterhaltung der Betriebsfähigkeit.....	37
8.2 Business Impact Analyse und Risikobewertung.....	37

8.2.1	Allgemeines	37
8.2.2	Business Impact Analyse	38
8.2.3	Risikobewertung.....	42
8.3	Strategien und Lösungen zur Aufrechterhaltung der Betriebsfähigkeit.....	43
8.3.1	Allgemeines	43
8.3.2	Identifikation und Auswahl der Strategien und Lösungen.....	43
8.3.3	Festlegen des Ressourcenbedarfs.....	46
8.3.4	Umsetzung von Lösungen.....	54
8.4	Pläne und Verfahren zur Aufrechterhaltung der Betriebsfähigkeit.....	55
8.4.1	Allgemeines	55
8.4.2	Reaktionsstruktur	55
8.4.3	Warnung und Kommunikation.....	57
8.4.4	Pläne zur Aufrechterhaltung der Betriebsfähigkeit.....	59
8.4.5	Wiederherstellung	69
8.5	Übungsprogramm.....	70
8.5.1	Allgemeines	70
8.5.2	Gestaltung des Übungsprogramms	70
8.5.3	Übungen zu Plänen für die Aufrechterhaltung der Betriebsfähigkeit.....	71
8.5.4	Instandhaltung.....	75
9	Leistungsüberprüfung.....	76
9.1	Überwachung, Messung, Analyse und Bewertung	76
9.1.1	Allgemeines	76
9.1.2	Bewertung der Pläne zur Aufrechterhaltung der Betriebsfähigkeit, Verfahren und Leistungsfähigkeiten	77
9.1.3	Messen der Effektivität.....	78
9.1.4	Ergebnisse.....	78
9.2	Internes Audit.....	79
9.3	Managementüberprüfung.....	80
9.3.1	Allgemeines	80
9.3.2	Eingaben für die Managementüberprüfung	80
9.3.3	Ergebnisse der Managementüberprüfung	81
10	Verbesserung.....	81
10.1	Nichtkonformität und Korrekturmaßnahmen	81
10.2	Ständige Verbesserung	82
	Literaturhinweise.....	83

Europäisches Vorwort

Dieses Dokument (prEN ISO 22313:2019) 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 NEN gehalten wird.

Dieses Dokument ist derzeit zur parallelen Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/DIS 22313:2019 wurde von CEN als prEN ISO 22313:2019 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.

ISO 22313 wurde vom Technischen Komitee ISO/TC 292 *Sicherheit und Schutz des Gemeinwesens* erarbeitet.

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 22301:201x Security and resilience — Business continuity management systems — Requirements festgelegten Anforderungen und bietet Empfehlungen („sollte“) und Zulässigkeiten („darf“) im Hinblick auf diese 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. Es bestehen weitere ISO-Publikationen, die zusätzliche Leitlinien enthalten können. Tabelle 1 gibt weitere Normen und technische Spezifikationen an, auf die in diesem Dokument verwiesen wird. Technische Spezifikationen unterliegen nicht dem gleichen Maß an Überprüfung wie Anforderungen oder Leitlinien-Normen und unterliegen nicht denselben Abstimmungsanforderungen. Darüber hinaus kann sich ihr Anwendungsbereich über die Anforderungen von ISO 22301 hinaus erstrecken. Organisationen sollten daher zur Verifizierung der zu erfüllenden Anforderungen immer Bezug auf ISO 22301 und dieses Dokument nehmen.

Tabelle 1 — Unterstützende Dokumente

Nummer	Titel
ISO/TS 22317	Societal security – Business continuity management systems – Guidelines for business impact analysis (BIA)
ISO/TS 22318	Societal security – Business continuity management systems – Guidelines for supply chain continuity
ISO 22322	Societal security - Emergency management – Guidelines for public warning
ISO/TS 22330	Security and resilience – Business continuity management systems – Guidelines for people aspects of business continuity
ISO/TS 22331	Security and resilience – Business continuity management systems – Guidelines for business continuity strategy
ISO 22398	Societal security – Guidelines for exercising

Zur weiteren Klärung und Erläuterung von Kernaussagen enthält dieses Dokument verschiedene Bilder. Diese 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:

- des Verstehens der Bedürfnisse und geschäftlichen Zielsetzungen einer Organisation;
- der Einbindung von Personen mit geeigneten Kenntnissen, Fertigkeiten und Erfahrung;
- der Einführung einer Politik und von Leitlinien zur Aufrechterhaltung der Betriebsfähigkeit;
- der Verbesserung der Fähigkeit der Organisation, mit Betriebsunterbrechungen umzugehen;
- der Übernahme einer Führungsrolle durch die oberste Leitung;
- der Leistung und Wirksamkeit von Plänen und Verfahren;
- einer ständigen Verbesserung auf Grundlage objektiver Messungen.

Wie jedes Managementsystem verfügt ein BCMS über:

- a) eine Politik;
- b) kompetente Personen mit festgelegten Verantwortlichkeiten;
- c) Managementprozesse in Bezug auf:
 - Leitlinien;
 - Planung;
 - Umsetzung und Betrieb;
 - Leistungsbewertung;
 - Managementüberprüfung;
 - ständige 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 widerstandsfähigeren Gesellschaft bei.

0.2 Vorteile eines BCMS

Die Vorteile eines BCMS beinhalten ein höheres Maß an Bereitschaft zum Umgang mit Unterbrechungen, ein verbessertes Verstehen der internen und externen Beziehungen einer Organisation, eine bessere Kommunikation mit interessierten Parteien und die Entwicklung einer ständigen Verbesserungsumgebung. Potenziell bestehen zahlreiche weitere Vorteile der Implementierung eines BCMS in Übereinstimmung mit den in diesem Dokument enthaltenen Empfehlungen.

- a) Die Implementierung der Empfehlungen in Abschnitt 4 (Kontext der Organisation) erfordert, dass die Organisation:
- ihre strategischen Zielsetzungen überprüft, um sicherzustellen, dass das BCMS diese Zielsetzungen unterstützt;
 - die Bedürfnisse, Erwartungen und Anforderungen interessierter Parteien überdenkt;
 - die anzuwendenden gesetzlichen, regulatorischen und sonstigen Verpflichtungen kennt;
- b) Abschnitt 5 (Führung) erfordert, dass die Organisation:
- Managementzuständigkeiten und Verantwortlichkeiten überdenkt;
 - eine Kultur der ständigen Verbesserung fördert;
 - eine Leistungsüberwachung und -berichterstattung einführt;
- c) Abschnitt 6 (Führung) erfordert, dass die Organisation:
- Risiken und Chancen erneut prüft und Maßnahmen identifiziert, um diese zu behandeln und davon zu profitieren;
 - ein effektives Änderungsmanagement einführt;
- d) Abschnitt 7 (Unterstützung) erfordert, dass die Organisation:
- ein effektives Management ihrer BCMS-Ressourcen einschließlich des Kompetenzmanagements einführt;
 - die Kenntnis der Beschäftigten über für das Management wichtige Themen verbessert;
 - über wirksame Mechanismen für die interne und externe Kommunikation verfügt;
 - ihre Dokumentation wirksam verwaltet;
- e) Abschnitt 8 (Betrieb) erfordert, dass die Organisation:
- sich der unbeabsichtigten Auswirkungen von Änderungen bewusst ist;
 - ihre Abhängigkeit von externen Lieferanten und ihrer Lieferkette überdenkt;
 - Schwachstellen aus Sicht der Auswirkung überdenkt;
 - die Risiken von Betriebsunterbrechungen bewertet und die Umgangsweise mit solchen Risiken identifiziert;
 - erfinderische Lösungen für den Betrieb des Geschäfts mit begrenzten Ressourcen entwickelt;
 - wirksame Strukturen und Verfahren für den Umgang mit Betriebsunterbrechungen implementiert;
 - ihre Verantwortungen gegenüber der Gemeinschaft und anderen interessierten Parteien kennt;

- f) Abschnitt 9 (Leistungsüberprüfung) erfordert, dass die Organisation:
 - über wirksame Mechanismen für die Überwachung, Messung und Bewertung der Leistung verfügt;
 - das Leitungsgremium an der Überwachung der Leistung und Unterstützung der Wirksamkeit des BCMS beteiligt;
- g) Abschnitt 10 (Verbesserung) erfordert, dass die Organisation:
 - über Verfahren zur Überwachung der Leistung und Verbesserung der Wirksamkeit verfügt;
 - von der ständigen Verbesserung ihrer Managementsysteme profitiert.

Demzufolge kann die Umsetzung des BCMS:

- a) das Leben, Eigentum und die 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 Betriebsunterbrechungen fortzuführen;
- d) die aus Betriebsunterbrechungen und der Verbesserung der Fähigkeit der Organisation, auch während Betriebsunterbrechungen wirksam zu bleiben, resultierenden Kosten reduzieren;
- e) zur allgemeinen Resilienz 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, demonstrieren.

0.3 Das Planen-Durchführen-Prüfen-Handeln-Modell (PDCA-Modell)

Dieses Dokument 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.

0.4 Bestandteile des PDCA in diesem Dokument

Es besteht ein direkter Zusammenhang zwischen dem Inhalt von Bild 1 und den Abschnitten dieses Dokuments:

Tabelle 3 — 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: <ul style="list-style-type: none">— der Erfordernisse und Erwartungen interessierter Parteien;— ihrer rechtlichen und behördlichen Verpflichtungen;— des geforderten Anwendungsbereichs des BCMS.
	Abschnitt 5 (Führung) legt die 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 die Umsetzung des BCMS einzuführen.
	Abschnitt 7 (Unterstützung) identifiziert die Elemente, die vorhanden sein müssen, d. h. Ressourcen, Kompetenzen, Bewusstseinsbildung, Kommunikation und dokumentierte Information.
Durchführen (Umsetzen und Betreiben)	Abschnitt 8 (Betrieb) identifiziert die notwendigen Prozesse, 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 seiner Leistung.
Handeln (Aufrechterhalten und Verbessern)	Abschnitt 10 (Verbesserung) behandelt erforderliche Korrekturmaßnahmen für Abweichungen, die anhand einer Leistungsbewertung festgestellt wurde.

0.5 Inhalt dieses Dokuments

Die Abschnitte 1 bis 3 in diesem Dokument legen den Anwendungsbereich, die normativen Verweisungen und Begriffe fest, die für die Verwendung dieses Dokuments gelten, während die Abschnitte 4 bis 10 Leitlinien zu den Anforderungen beschreiben, die zur Beurteilung der Konformität mit ISO 22301 zu verwenden sind.

In diesem Dokument werden die folgenden Verbformen verwendet:

- a) „sollte“ bezeichnet eine Empfehlung;
- i) „darf“ bezeichnet eine Erlaubnis;
- j) „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 Betriebsunterbrechung mit akzeptabler, zuvor festgelegter Kapazität fortzusetzen. Das Business Continuity Management (BCM) ist der Prozess der Umsetzung und Aufrechterhaltung der Betriebsfähigkeit, um sich auf Betriebsunterbrechungen 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 Aufträge ausgeführt werden. Daher gilt sie gleichermaßen für große, mittlere und kleine Unternehmen, die im industriellen, kommerziellen, öffentlichen und gemeinnützigen Bereich tätig sind.

Betriebsunterbrechungen 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 Vorfall in ungeplanter Weise zu reagieren, ermöglicht der Organisation die Wiederaufnahme von Betriebsabläufen, bevor ein inakzeptables Ausmaß an Auswirkungen entsteht.

Das BCM umfasst Folgendes:

- a) die Identifizierung der Produkte und Dienstleistungen einer Organisation sowie der Tätigkeiten zu deren Bereitstellung;
- b) die Analyse der Nichtwiederaufnahme der Tätigkeiten und der Ressourcen, die diese erfordern;
- c) das Verständnis der Bedrohungen für diese Tätigkeiten und ihrer Abhängigkeiten;
- d) die Festlegung von Prioritäten, Strategien und Zeitrahmen für die Wiederaufnahme der Lieferung von Produkten und Dienstleistungen, Tätigkeiten und ihrer Abhängigkeiten;
- e) die Verfügbarkeit von Lösungen und Plänen zur Wiederaufnahme der Tätigkeiten innerhalb der geforderten Zeitrahmen nach einer Betriebsunterbrechung;
- f) das Sicherstellen, dass diese Vorkehrungen regelmäßig überprüft und aktualisiert werden, damit sie unter allen Umständen wirksam sind.

Der BCM-Ansatz und das Dokumentationssystem der Organisation sollten für ihren Kontext geeignet sein (z. B. Betriebsumgebung, Komplexität, Bedürfnisse und Ressourcen).

Die Aufrechterhaltung der Betriebsfähigkeit kann sowohl bei plötzlichen Betriebsunterbrechungen (z. B. Explosionen) als auch bei allmählich eintretenden Betriebsunterbrechungen (z. B. Pandemien) 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 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 und Informationen), ihrer Lieferkette, ihrer Interessengruppen und ihres Rufs unternommen werden muss, bevor eine Betriebsunterbrechung eintritt. Durch dieses Kenntnis ist die Organisation in der Lage, eine Reaktionsstruktur zu entwickeln, um die Konsequenzen einer Unterbrechung selbstsicher zu managen.

Die folgenden Diagramme (Bild 2 und Bild 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.

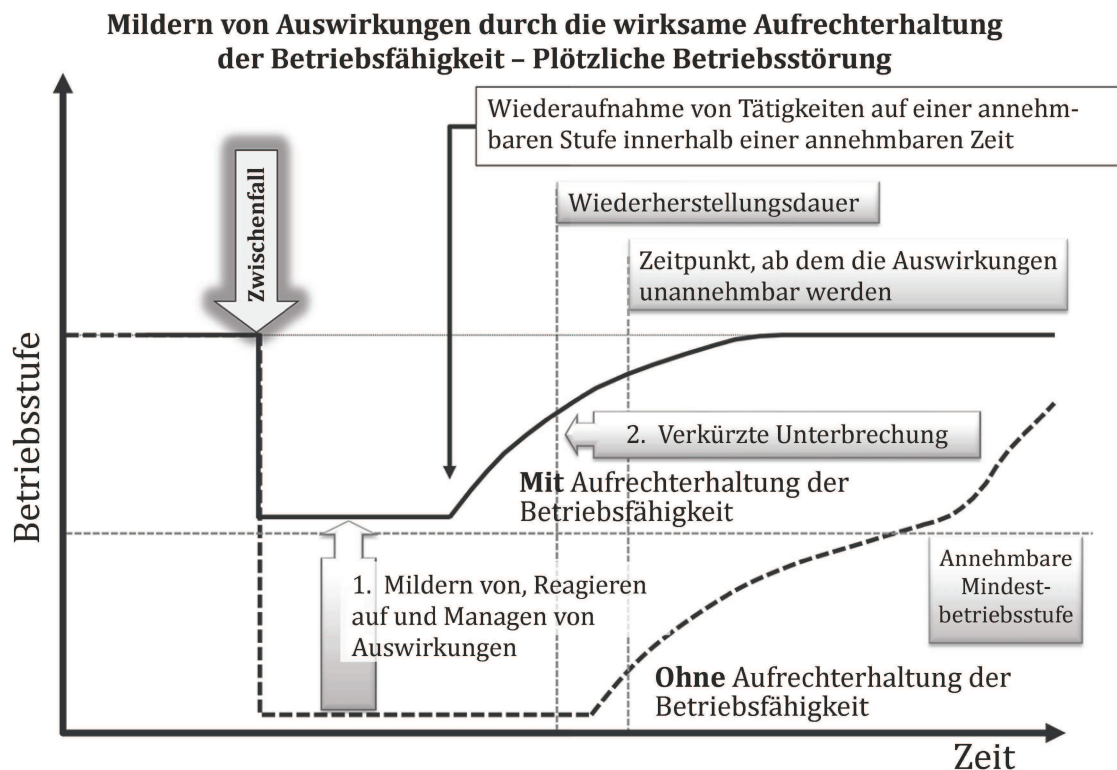


Bild 2 — Darstellung einer wirksamen Aufrechterhaltung der Betriebsfähigkeit bei plötzlicher Betriebsunterbrechung

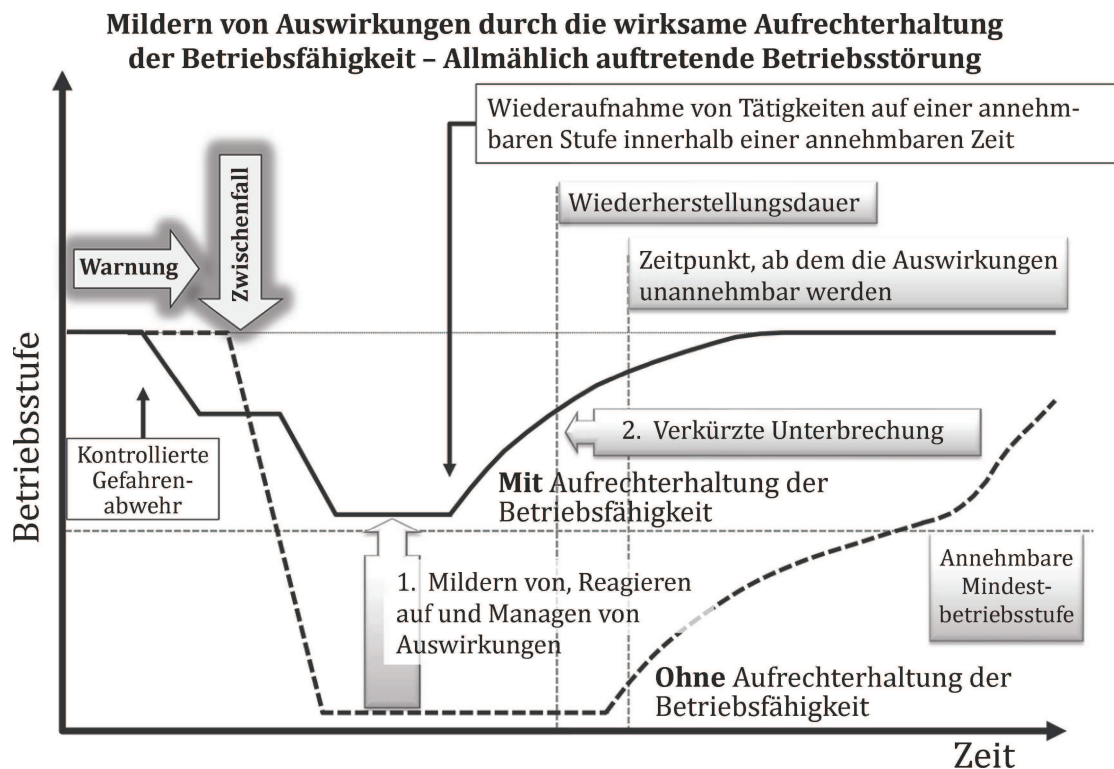


Bild 3 — Darstellung einer wirksamen Aufrechterhaltung der Betriebsfähigkeit bei allmählich eintretender Betriebsunterbrechung (z. B. herannahende Pandemie)

1 Anwendungsbereich

Dieses Dokument enthält Leitlinien auf der Grundlage anerkannter internationaler Praktiken.

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 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 umsetzen und aufrechterhalten wollen;
- b) die Übereinstimmung mit der Politik einer Organisation im Hinblick auf die Aufrechterhaltung der Betriebsfähigkeit sicherstellen möchten;
- c) die Belieferung mit Produkten und Dienstleistungen mit einer akzeptablen, zuvor festgelegten Kapazität während einer Betriebsunterbrechung fortsetzen möchten;
- d) ihre Resilienz verbessern möchten;
- e) eine Eigenfeststellung oder eine Selbsterklärung der Übereinstimmung mit diesem Dokument erstellen möchten.

Dieses Dokument sollte 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, *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 und ISO 22301.

3.1 Auswertung und Bedeutung

Aus Gründen der Klarheit und um die Lesbarkeit zu verbessern und unnötige Wiederholungen zu vermeiden, gelten für ISO 22301 und ISO 22313 die folgenden Konventionen:

- a) Anstatt den Ausdruck „Planen, Erstellen, Umsetzen, Betreiben, Überwachen, Überprüfen, Aufrechterhalten und ständig Verbessern“ vollständig zu wiederholen oder mit ein oder zwei gelöschten Begriffen zu verwenden:
 - wird für BCMS „Umsetzen und Aufrechterhalten“;
 - für dokumentierte Informationen „Dokumentieren und Pflegen“;
 - für Prozesse „Umsetzen und Aufrechterhalten“;
 - für Fähigkeiten „Erstellen und Aufrechterhalten“ verwendet.
- b) Der Begriff „während einer Betriebsunterbrechung“ umfasst den Zeitraum vom Einsetzen einer Betriebsunterbrechung bis zur Rückkehr zum normalen Betrieb oder einer neuen stabilen Situation.

4 Kontext der Organisation

4.1 Verstehen der Organisation und ihres Kontextes

Dieser Abschnitt behandelt die Anforderungen an das Verstehen des Kontextes der Organisation in Verbindung dem BCMS. Die Erstellung und die Verwaltung des BCMS werden in Abschnitt 8.1 behandelt.

Die Organisation sollte die internen und externen Faktoren, die für ihren Zweck und den Betrieb relevant sind (diese können positive und negative Faktoren oder Bedingungen zur Betrachtung enthalten), bewerten und verstehen. Diese Information sollte bei der Umsetzung und Aufrechterhaltung des BCMS der Organisation und bei der Zuordnung von Prioritäten berücksichtigt werden.

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

- 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 (siehe auch ISO/TS 22318);
- Faktoren (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 und Technologien);
- bestehende Managementsysteme;
- Informationssysteme, Informationsflüsse und Entscheidungsprozesse (formal und andere);
- interessierte Parteien innerhalb der Organisation einschließlich interner Lieferanten (Berücksichtigung der Leistungsvereinbarungen (SLA), der beurteilten Resilienz und der Wiederherstellungsvereinbarungen) (siehe ISO/TS 22318);
- Leitlinien und Zielsetzungen 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. Führung, Funktionen und Verantwortlichkeiten);
- interne Kommunikationskanäle, die für den Austausch von Informationen mit den Mitarbeitern genutzt werden (z. B. soziale Netzwerke).

4.2 Verstehen der Bedürfnisse und Erwartungen der interessierten Parteien

4.2.1 Allgemeines

Die Organisation hat eine Fürsorgeverantwortung 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 (Bild 4), und auf Grundlage von deren Bedürfnissen und Erwartungen ihre 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 Betriebsunterbrechung mit allen interessierten Parteien zu kommunizieren, kann es unangemessen sein, bei der Umsetzung und Aufrechterhaltung eines BCM mit allen Interessengruppen zu kommunizieren (8.1.1).

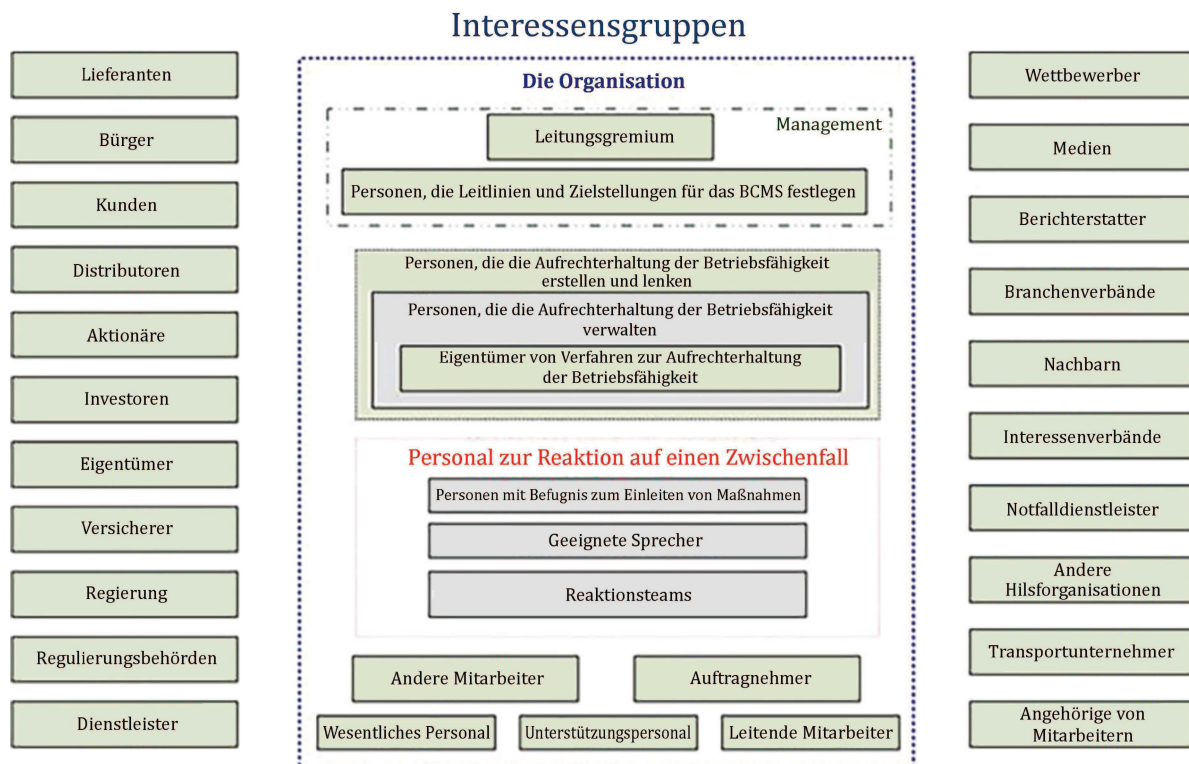


Bild 4 — Beispiele für zu berücksichtigende interessierte Parteien im öffentlichen und privaten Bereich

4.2.2 Rechtliche und behördliche Anforderungen

Die Anwendung dieses Dokuments setzt die Kenntnis der anzuwendenden gesetzlichen und regulatorischen 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 zu aktuellen und ausstehenden gesetzlichen und regulatorischen Anforderungen mit Relevanz für die Standorte ihres Betriebs hat, und wie diese Anforderungen erfüllt werden. Diese Anforderungen können Folgendes umfassen:

- Reaktion auf einen Zwischenfall: einschließlich Gefahrenabwehr und anderer relevanter Rechtsvorschriften;
- Aufrechterhaltung der Betriebsfähigkeit: kann den Anwendungsbereich des Programms oder den Umfang oder die Geschwindigkeit der Reaktion festlegen;
- Risiko: Anforderungen, die den Anwendungsbereich oder Risikomanagementverfahren festlegen;
- Gefährdungen: beispielsweise 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 Managements

4.3.1 Allgemeines

Die Organisation sollte den Anwendungsbereich des BCMS festlegen und sicherstellen, dass dieser allen interessierten Parteien in geeigneter Weise zur Verfügung steht. Es ist wichtig, dass die Grenzen und die Anwendbarkeit des BCMS deutlich zu erkennen sind und dass der Anwendungsbereich die in Abschnitt 4.1 (externe und interne Faktoren) und Abschnitt 4.2 (Bedürfnisse und Erwartungen der interessierten Parteien) festgelegten Punkte berücksichtigt.

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 ICT, Beschaffung, Personalwesen) an jedem Standort, die direkt oder indirekt an der Lieferung des Produkts an den Kunden beteiligt sind, eingebunden werden.

4.3.2 Anwendungsbereich des BCMS

Der Zweck der Festlegung des Anwendungsbereichs ist es, die Berücksichtigung aller relevanten Tätigkeiten, Standorte und Lieferanten sicherzustellen.

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 Anforderungen der Organisation an das BCMS unter Berücksichtigung ihres Auftrags, ihrer Ziele, der gesetzlichen Verantwortlichkeiten und externen sowie internen Verpflichtungen festlegen;
- b) durch Verweis auf den geografischen Standort oder die Produkte und Dienstleistungen die Teile der Organisation identifizieren, die im Anwendungsbereich des BCMS enthalten sind. Der Anwendungsbereich könnte beispielsweise:
 - nur die Lieferung eines bestimmten Produkts an ein Land oder eine Region beinhalten;
 - ein Produkt ausschließen, das nicht mehr brauchbar oder von geringem Wert für die Organisation ist;
 - eine Dienstleistung ausschließen, zu deren Lieferung die Organisation nicht mehr verpflichtet ist;
 - nur einen Teil der Produkte und Dienstleistungen einbinden;
- c) die Produkte und Dienstleistungen der Organisation so bezeichnen, dass alle damit verbundenen Tätigkeiten, Ressourcen und Lieferketten ermittelt werden können;
- d) die Bedürfnisse und Interessen interessierter Parteien berücksichtigen.

Der Anwendungsbereich darf:

- a) eine Angabe über das Ausmaß oder die Größe eines Vorfalls, der durch das BCMS abgedeckt ist, enthalten;
- b) festlegen, wie das BCMS in die Geschäftsstrategie und das allgemeine Risikomanagement (sofern vorhanden) der Organisation einzuordnen ist.

Ausschlüsse aus dem Anwendungsbereich des BCMS sollten dokumentiert und begründet 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 dieser Klausel ist es, das Erfordernis für die Organisation, Prozesse zu implementieren und aufrechtzuerhalten, die es dem BCMS ermöglichen werden, die Anforderungen nach ISO 22301:20XX einschließlich im Hinblick auf die Wechselwirkungen zwischen den Prozessen zu erfüllen, zu betonen.

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

- a) die erforderlichen erwarteten Eingaben und Ausgaben 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 Überwachungsmessungen 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 implementieren, um sicherzustellen, dass diese Prozesse die beabsichtigten Ergebnisse erreichen;
- h) die Prozesse und das BCMS verbessern.

Soweit erforderlich, sollte die Organisation:

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

5 Führung

5.1 Führung und Selbstverpflichtung

Die oberste Leitung ist dafür verantwortlich, Führung und Selbstverpflichtung zu demonstrieren, indem sie sicherstellt, dass die Anforderungen erfüllt werden, die Bedeutung des BCMS kommunizieren, die ständige Verbesserung fördern und andere relevante Managementfunktionen unterstützen. Alle Ebenen des Leitungsgremiums der gesamten Organisation sollten Führung und Selbstverpflichtung in ihren Verantwortungsbereichen demonstrieren.

Die spezifischen Verantwortlichkeiten der obersten Leitung umfassen Folgendes:

- Bestimmen des Anwendungsbereichs des BCMS (4.3);
- Einführen von Leitlinien und Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit im Einklang mit den Zielsetzungen, Verpflichtungen und der strategischen Ausrichtung der Organisation (5.2);
- Ernennen einer oder mehrerer Personen mit den entsprechenden Befugnissen und Kompetenzen, die für das BCMS und dessen wirksame Anwendung verantwortlich sind (5.3);
- Sicherstellen der Verfügbarkeit notwendiger Ressourcen, einschließlich eines angemessenen Umfangs finanzieller Mittel (7.1).

Die Verantwortlichkeiten aller Managementebenen umfassen:

- die Integration aller BCMS-Anforderungen in die Geschäftsprozesse der Organisation;
- die Kenntnis anzuwendender gesetzlicher Anforderungen (z.B. regulatorisch) und anderer Anforderungen, denen die Organisation unterliegt (4.2.2);
- Sicherstellen, dass die Funktionen, Verantwortlichkeiten und Kompetenzen innerhalb des BCMS festgelegt werden (5.3 und 7.2);
- Vermitteln der Wichtigkeit der Einhaltung von Leitlinien und Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit innerhalb der Organisation (7.4);
- aktive Teilnahme an Übungen und Überprüfungen (8.5);
- Sicherstellung, dass interne Audits des BCMS durchgeführt werden (9.2);
- Durchführen von Überprüfungen der wirksamen Lenkung des BCMS (9.3);
- Anleiten und Unterstützen der Verbesserung des BCMS (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.

5.2 Politik

Die Politik zur Aufrechterhaltung der Betriebsfähigkeit ist eine präzise allgemeine Beschreibung der Absicht und Ausrichtung der obersten Leitung für das BCMS.

5.2.1 Verantwortlichkeiten der obersten Leitung

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

- a) dem Zweck der Organisation entsprechen (d. h. ihrer Größe, Art und Komplexität und unter Beachtung ihrer Kultur, Abhängigkeiten und Betriebsumgebung);
- b) ein Rahmenwerk für die Erstellung von Zielsetzungen bereitstellen;

- c) eine klare Verpflichtung zur Erfüllung der anzuwendenden Anforderungen einschließlich gesetzlicher und regulatorischer Verpflichtungen enthalten;
- d) eine Verpflichtung zu einer ständigen Verbesserung des BCMS enthalten.

5.2.2 Bestimmungen zur Aufrechterhaltung der Betriebsfähigkeit

Die Politik zur Aufrechterhaltung der Betriebsfähigkeit sollte:

- a) als dokumentierte Informationen verfügbar sein und aufrechterhalten werden;
- b) vermittelt, verstanden und in der gesamten Organisation angewendet werden;
- c) nach Genehmigung durch die Leitung interessierten Parteien 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 Politik sollte:

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

Die Politik darf Folgendes enthalten:

- 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 in Verbindung mit anderen Managementsystemen zu integrieren.

5.3 Funktionen, Verantwortlichkeiten und Befugnisse innerhalb der Organisation

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

Ein Mitglied der obersten Leitung sollte die Verantwortung für das BCMS tragen. Vertreter sollten ungeachtet ihrer sonstigen Verantwortlichkeiten für festgelegte Rollen, Verantwortlichkeiten und Befugnisse ernannt werden, um:

- sicherzustellen, dass das BCMS die Anforderungen der Politik zur Aufrechterhaltung der Betriebsfähigkeit erfüllt;
- der obersten Leitung zu Überprüfungszwecken und als Grundlage für Verbesserungen über die Leistung des BCM Bericht zu erstatten (Abschnitt 9 und 10);
- die Bewusstseinsbildung hinsichtlich der Aufrechterhaltung der Betriebsfähigkeit innerhalb der Organisation zu fördern;
- 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:

- einen spezifischen Titel wie etwa „Business Continuity Manager“, „Business Continuity Officer“ oder „Resilience Manager“ tragen;
- weitere Verantwortungsbereiche innerhalb der Organisation haben;
- aus jedem Bereich der Organisation stammen.

Vertreter von Funktionen oder Standorten der Organisation dürfen dazu ernannt werden, an der Umsetzung des BCMS mitzuarbeiten (z. B. für Risikoangelegenheiten zuständige Vertreter). 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. Tabelle 4 enthält Beispiele für möglicherweise geeignete Rollen und Verantwortlichkeiten.

Die oberste Leitung darf weitere Gremien benennen, wie z. B. einen Lenkungsausschuss, um die Umsetzung und die laufende Überwachung des BCMS zu beaufsichtigen.

Je nach Größe der Organisation könnten die in Tabelle 4 beschriebenen Rollen und Verantwortlichkeiten anders eingerichtet werden. Es ist wichtig, sicherzustellen, dass alle Verantwortlichkeiten Teil einer Rolle sind und einem Verantwortlichen zugewiesen sind.

Tabelle 4 —Beispiele für BCM-Rollen und -Verantwortlichkeiten

Rolle	Verantwortlichkeiten
BCM-Vertreter	<ul style="list-style-type: none"> — Ist für das BCMS verantwortlich — Vertritt das BCM bei Managementprüfungen
BCM-Manager	<ul style="list-style-type: none"> — Ist für das BCMS verantwortlich — Erstellt und demonstriert die Selbstverpflichtung zur Politik für die Aufrechterhaltung der Betriebsfähigkeit — Leitet alle Programmaktivitäten und stimmt sich mit anderen Funktionen ab — Ernennet Teammitglieder mit geeigneter Führungsposition und Befugnis — Unterstützt die Genehmigung von Lösungen, Verfahren und Übungsprogrammen — Legt Teamempfehlungen bei Managementprüfungsbesprechungen vor
Vorfallmanager	<ul style="list-style-type: none"> — Beteiligt sich an der Entwicklung des Vorfallmanagementplans — Stellt sicher, dass der Vorfallmanagementplan regelmäßig aktualisiert wird — Stellt sicher, dass Sicherheitsverfahren während eines Vorfalls korrekt eingehalten werden — Fördert das Bewusstsein für das Vorfallmanagement in der gesamten Organisation — Ist der Hauptansprechpartner für die Vorfallmanagementteams — Legt Fortschrittsberichte während der Beurteilung von Vorfällen vor — Steuert den Vorfallmanagementprozess
BCM-Team	<ul style="list-style-type: none"> — Setzt das BCM in der gesamten Organisation um — Pflegt die Dokumentation — Stellt sicher, dass Programme zeitgerecht überprüft werden — Beurteilt die Eignung der Aufrechterhaltung der Betriebsfähigkeit der Abteilungen — Organisiert und koordiniert Programme zur Aufklärung über die Aufrechterhaltung der Betriebsfähigkeit — Erstellt Übungsprogramme und holt die Genehmigung der entsprechenden befugten Stelle ein — Führt Übungseinweisungen und Nachbesprechungen durch — Informiert interessierte Parteien laufend über das Programm — Stellt sicher, dass die Übungen in Übereinstimmung mit dem Übungsprogramm durchgeführt werden — Stellt sicher, dass interne Audits und Managementprüfungen rechtzeitig durchgeführt werden — Pflegt Beziehungen zu Abteilungen und kontaktiert diese im Rahmen von Betriebsunterbrechungen — Informiert die oberste Leitung laufend über den Status der Wiederaufnahme und Wiederherstellung — Koordiniert die Beurteilung von Vorfällen zwischen den Teams — Stellt sicher, dass Korrekturmaßnahmenpläne zeitgerecht umgesetzt werden — Unterstützt die Bemühungen der Abteilungsvertreter/-verantwortlichen

Rolle	Verantwortlichkeiten
Abteilungsvertreter/ -verantwortliche	<ul style="list-style-type: none">— Pflegen die Abteilungsverfahren zur Aufrechterhaltung der Betriebsfähigkeit— Informieren den Business Continuity Manager über den Bereitschaftsstatus der Abteilungen— Führen Programmtätigkeiten nach Anweisungen durch und berichten hierüber— Bestätigen, dass die Pläne der Lieferanten zur Aufrechterhaltung der Betriebsfähigkeit geprüft und aufrechterhalten werden— Koordinieren die Beteiligung der Abteilungsmitarbeiter an Übungen— Pflegen die Aufzeichnungen der Abteilungs-BCM-Übungen— Informieren das Team laufend über Änderungen, die sich auf die Aufrechterhaltung der Betriebsfähigkeit auswirken können— Verfolgen die der Abteilung zugewiesenen Korrekturmaßnahmen zeitnah— Informieren den Business Continuity Manager laufend über den Fortschritt der Korrekturmaßnahmen

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

6 Planung

Die Leitlinien in diesem Abschnitt beziehen sich hauptsächlich auf das Managementsystem und nicht auf den in Abschnitt 8 behandelten Betrieb der Organisation.

6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten

Die Organisation sollte Maßnahmen zur Behandlung der Aspekte in 4.1, der in 4.2 beschriebenen Bedürfnisse und Erwartungen der interessierten Parteien und der in 4.2.2 angegebenen gesetzlichen und regulatorischen Anforderungen bestimmen.

Diese Bestimmung sollte die Betrachtung der Risiken und Chancen und ihrer potenziellen Auswirkung auf die Wirksamkeit des BCMS beinhalten. Risiken und Chancen dürfen Folgendes enthalten:

- unzureichende Finanzierung des BCMS und die daraus resultierende unwirksame Reaktion;
- eine Fähigkeit, in neue Märkte vorzudringen, in denen die Aufrechterhaltung der Betriebsfähigkeit eine Anforderung ist;
- schlecht dokumentierte Informationen;
- fehlende Mitarbeiter mit nachgewiesener Kompetenz;
- unzureichender Managementprüfungsprozess;
- fehlende Führung und Selbstverpflichtung der obersten Leitung;
- erweiterte Schulungen für an der Planung der Aufrechterhaltung der Betriebsfähigkeit beteiligte Mitarbeiter.

Die Bestimmung sollte darüber hinaus die Beurteilung des Planungsbedarfs beinhalten, um:

- unerwünschte Ergebnisse zu vermeiden;
- jegliche Gelegenheit zur Verbesserung des BCMS zu ergreifen.

Sofern notwendig, sollte außerdem Folgendes berücksichtigt werden:

- das Sicherstellen der Konsistenz mit bestehenden Risikomanagementprogrammen, sofern vorhanden;
- die Einbindung und die Umsetzung dieser Maßnahmen im BCMS-Prozess (8.1);
- die Sicherstellung, dass dokumentierte Informationen verfügbar sind, mit denen bewertet werden kann, ob die Maßnahmen effektiv umgesetzt wurden (9.1).

6.2 Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit und Planung zur Zielerreichung

Die Organisation sollte die Implementierung und Aufrechterhaltung des BMC planen (wie in Abschnitt 8 beschrieben). Dies sollte auf den Kontinuitätszielen der Organisation basieren, mit den allgemeinen Zielsetzungen der Organisation übereinstimmen und die Identifizierung der Verantwortlichkeiten und die Festlegung geeigneter und realistischer Ziele für die Erfüllung der Aufgaben beinhalten. Die Planung sollte in der gesamten Organisation kommuniziert und der Fortschritt ihrer Umsetzung sollte überwacht und dokumentiert werden.

Wenn sich das BCMS weiterentwickelt, sollte dieser Plan regelmäßig geprüft und gegebenenfalls aktualisiert werden.

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:yyyy bis *Datum*“;
- „Erlangen einer Zertifizierung nach ISO 22301:yyyy bis *Datum*“;
- „bis *Datum*“ verfügen wir über eine Aufrechterhaltung der Betriebsfähigkeit, die unseren Verpflichtungen gegenüber *benannten* Hauptkunden entspricht“;
- „Umsetzung eines BCM zum Schutz von *benannten* Produkten und Dienstleistungen bis *Datum*“.

6.3 Planung von Änderungen am BCMS

Das Änderungsmanagement ist ein wichtiger Aspekt für alle Managementprozesse einschließlich des BCMS.

Bei der Änderung des BCMS sollte die Organisation sicherstellen, dass der beabsichtigte Zweck vollständig untersucht und verstanden wird. Dies sollte eine Betrachtung der Auswirkungen der geplanten Änderungen und die Sicherstellung, dass erwartete und unbeabsichtigte Auswirkungen berücksichtigt werden, beinhalten.

Die Organisation sollte darüber hinaus sicherstellen, dass geeignete und ausreichende Ressourcen zur Verfügung stehen und eine geeignete Zuweisung oder Neuzuweisung von Verantwortlichkeiten und Befugnissen stattfindet.

7 Unterstützung

7.1 Ressourcen

7.1.1 Allgemeines

Die Organisation sollte die Ressourcen festlegen, ihre Verfügbarkeit sicherstellen und Ressourcen 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 BCMS, intern und extern, ermöglicht wird;
- d) die laufende Anwendung und die ständige Verbesserung des BCMS sichergestellt werden.

Die Ressourcen sollten zeitnah und wirksam zur Verfügung stehen.

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:
 - die Zeit, die benötigt wird, um die Funktionen und Verantwortlichkeiten in Verbindung mit dem BCMS wahrzunehmen;
 - Schulung, Weiterbildung, Bewusstseinsbildung und Übungen;
 - 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 interessierten Parteien (siehe Bild 4);
- 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.

7.2 Kompetenz

Die Organisation sollte ein geeignetes und wirksames System zur Lenkung der Kompetenz von Personen festlegen, die BCMS-Arbeiten unter der Leitung der Organisation durchführen.

Das Management sollte die Kompetenzen bestimmen, die für sämtliche Funktionen und Verantwortlichkeiten innerhalb des BCMS erforderlich sind, sowie das Bewusstsein, das Wissen, das Verständnis, die Fertigkeiten und Erfahrungen, um diese Funktionen und Verantwortlichkeiten erfüllen zu können. Alle Personen, denen innerhalb der Organisation Funktionen zugeteilt wurden, sollten die

erforderlichen Kompetenzen darlegen und sollten Schulungen, Ausbildungen, Weiterbildungen und andere Unterstützung erhalten, um ihre Aufgabe zu erfüllen. Dies darf als Kompetenzentwicklungsprogramm bezeichnet werden und kann Folgendes umfassen:

- Beurteilung von Kompetenzen für die zu übernehmende(n) Funktion(en);
- Erstellen eines persönlichen Entwicklungsprogramms, in dem Schulungen, Ausbildungen, Weiterbildungen und andere Unterstützung zum Erlangen der Kompetenzen festgelegt sind;
- Bereitstellen von Schulung und Betreuung einschließlich der Auswahl von geeigneten Verfahren und Unterlagen;
- der Bewertung der Leistung;
- Wissensaustausch;
- Arbeitsplatzteilung;
- Einstellen oder vertragliche Verpflichtung von kompetenten Personen;
- Schulung von Zielgruppen;
- Dokumentation und Überwachung von durchgeführten Schulungen;
- Bewertung von durchgeführten Schulungen im Hinblick auf den festgelegten Schulungsbedarf und die Schulungsanforderungen, um die Übereinstimmung mit den BCMS-Schulungsanforderungen zu bestätigen;
- gegebenenfalls Verbesserung des Entwicklungsprogramms.

Die Organisation sollte über einen Prozess verfügen, mit dem die nötigen Schulungen über die Aufrechterhaltung der Betriebsfähigkeit für alle Teilnehmer ermittelt und vermittelt werden und die Effektivität ihrer Vermittlung bewertet wird.

Die Schulungsarten, die für die Erstellung, Steuerung und Aufrechterhaltung des BCMS geeignet sein können, umfassen Folgendes:

- Erstellen und Lenken eines BCM;
- Durchführen einer Business Impact Analyse;
- Durchführung einer Risikobeurteilung;
- Kommunikationsfähigkeiten;
- Projektmanagement;
- Entwickeln und Umsetzen einer Dokumentation über die Aufrechterhaltung der Betriebsfähigkeit;
- Betreiben eines Übungsprogramms.

Änderungen der Betriebsumgebung und der Betriebsabläufe beeinflussen den Ansatz und die Art und Weise wie Tätigkeiten zur Aufrechterhaltung der Betriebsfähigkeit geplant, gestaltet und umgesetzt werden. Die Organisation darf darlegen, dass sie sich über die Entwicklungen im BCM bewusst ist, indem sie beispielsweise aktiv an BCM-Aktivitäten der Branche teilnimmt, zu denen Folgende zählen können:

- Mitgliedschaft in einem Branchenverband;
- Mitgliedschaft in einem Konferenzorganisationsausschuss;
- Halten von Präsentationen auf Konferenzen und Seminaren;
- Teilnahme an lokalen oder internationalen BCM-Konferenzen.

Aktive Teilnahme darf mithilfe einer oder mehrerer der folgenden Möglichkeiten demonstriert werden:

- Mitgliedschaft in einem Organisationsausschuss für Konferenzen und Seminare;
- Fachvorträge auf Konferenzen und Seminaren.

Kompetenzen dürfen durch Folgendes bekräftigt werden:

- Einbindung von BCMS-Erfolgen in den Belohnungs- und Anerkennungsprozess der Organisation;
- Einbindung von BCMS-Erfolgen in den Leistungs- und Beurteilungsprozess der Organisation;
- Einbindung von BCMS-Funktionen, -Zuständigkeiten, -Verantwortungen und -Befugnissen in die Tätigkeits- und Fertigkeitsbeschreibungen der Organisation;
- aktive Teilnahme der Geschäftskunden und des Leitungsgremiums an Proben, Übungen und Überprüfungen.

Die Organisation sollte Auftragnehmer, die in ihrem Auftrag arbeiten, dazu verpflichten, nachzuweisen, dass die unter ihrer Leitung arbeitenden Personen über die notwendigen Kompetenzen für das BCMS und für ihre Reaktionsfunktion, die sie ausüben werden, verfügen.

7.3 Bewusstseinsbildung

Die Organisation sollte sicherstellen, dass alle Personen, die unter dem Namen der Organisation tätig sind (z. B. Auftragnehmer, Lieferanten), sich der Aufrechterhaltung der Betriebsfähigkeit und der Zielsetzungen der Organisation für die Aufrechterhaltung der Betriebsfähigkeit bewusst sind und:

- die Reduzierung der Wahrscheinlichkeit von Betriebsunterbrechungen und ihrer Funktion im Hinblick auf die Vermeidung, Erkennung, die Minderung, den Selbstschutz, die Evakuierung, die Reaktion, die Aufrechterhaltung der Betriebsfähigkeit und die Wiederherstellung;
- die Wichtigkeit der Übereinstimmung mit Leitlinien und Verfahren zur Aufrechterhaltung der Betriebsfähigkeit;
- Abhängigkeiten von Lieferanten und Beschaffungspartnern und alle damit verbundenen Risiken für die geschäftlichen Zielsetzungen;
- die Auswirkungen von Änderungen im Betriebsablauf der Organisation;
- ihr Beitrag zur Wirksamkeit des BCMS einschließlich dessen Vorteile hinsichtlich einer besseren Aufrechterhaltung der Betriebsfähigkeit;
- ihre Funktion und Verantwortung für die erfolgreiche Übereinstimmung mit den Anforderungen.

Die Organisation sollte BCM aufbauen, fördern und innerhalb der Organisationskultur einbetten, sodass:

- es Teil der Grundwerte und des Managements der Organisation wird;
- interessierte Parteien sich der Politik zur Aufrechterhaltung der Betriebsfähigkeit und ihrer Funktion in den damit verbundenen Verfahren bewusst sind.

Eine Organisation mit einem in ihre Kultur eingebetteten BCM wird:

- eine Aufrechterhaltung der Betriebsfähigkeit wirksamer entwickeln;
- Vertrauen bei ihren interessierten Parteien (besonders bei Mitarbeitern und Kunden) im Hinblick auf ihre Fähigkeit zum Umgang mit Betriebsunterbrechungen wecken;
- im Laufe der Zeit ihre Belastbarkeit erhöhen, indem sie sicherstellt, dass Auswirkungen auf die Aufrechterhaltung der Betriebsfähigkeit bei Entscheidungen auf allen Ebenen berücksichtigt werden;
- die Wahrscheinlichkeit und die Auswirkung von Betriebsstörungen minimieren.

Die Einbettung des BCM in die Organisationskultur wird unterstützt durch:

- Einbeziehung des gesamten Personals der Organisation;
- Führungsteilung innerhalb der Organisation;
- Zuweisen von Verantwortlichkeiten;
- Messungen auf Grundlage von Leistungsindikatoren;
- Einbinden der Aufrechterhaltung der Betriebsfähigkeit in die gewöhnlichen Managementpraktiken;
- Bewusstseinsbildung;
- Schulung von Fertigkeiten;
- Übungen zum Ausführen von Plänen zur Aufrechterhaltung der Betriebsfähigkeit.

Ein Programm zur Bewusstseinsbildung darf umfassen:

- ein Beratungsprozess mit den Mitarbeitern innerhalb der gesamten Organisation im Hinblick auf die Erstellung und das Lenken des BCM;
- Auseinandersetzungen mit der Aufrechterhaltung der Betriebsfähigkeit in Newslettern, Besprechungen, Einführungsveranstaltungen oder Magazinen der Organisation (einschließlich der Einführungsprogramme für neue Mitarbeiter);
- Einbinden der Aufrechterhaltung der Betriebsfähigkeit in die eigenen Internetseiten;
- Einbinden des BCM als Thema auf Mitarbeiterversammlungen und Führungsgruppensitzungen;
- gezielte Veröffentlichung von Berichten über Zwischenfälle nach einem Zwischenfall;
- Unterweisung der obersten Leitung;
- Besichtigungen alternativer Standorte (z. B. Wiederherstellungsort);

- regelmäßige Kommunikation mit Lieferanten, um sicherzustellen, dass sie die Anforderungen an die Aufrechterhaltung der Betriebsfähigkeit der Organisation verstehen und um ihre Fähigkeit zur Erfüllung der vereinbarten Anforderungen an die Aufrechterhaltung der Betriebsfähigkeit zu demonstrieren.

7.4 Kommunikation

Die Organisation sollte die für das BCMS relevante Kommunikation bestimmen.

Die für das BCMS relevante Kommunikation ermöglicht es der Organisation, auf die Bedürfnisse und Erwartungen interessierter Parteien zu reagieren (4.2). Für eine wirksame Kommunikation sollte die Organisation Folgendes bestimmen und gegebenenfalls die Kriterien für dessen Bestimmung festlegen:

- Worüber sie kommuniziert:** Kommunikation hinsichtlich des BCMS kann je nach Art der Organisation und Situation erforderlich sein; einige Organisationen unterliegen beispielsweise einer gesetzlichen oder regulatorischen Kommunikationsverpflichtung;
- Wann Kommunikation stattfinden sollte:** Es können Schwellenwerte bestehen, bei deren Überschreitung die Organisation zur Kommunikation verpflichtet ist, und der Kontext der Organisation kann vorschreiben, wie häufig Kommunikation stattfinden sollte;
- Mit wem sie kommuniziert:** Alle interessierten Parteien werden von Zeit zu Zeit Kommunikation benötigen; es ist daher wichtig, für jede interessierte Partei zu bestimmen, unter welchen Umständen und mit welchen Prioritäten Kommunikation erforderlich sein wird;
- Die Kommunikationsmittel:** Die Bestimmung der Verfahren, Instrumente und Kanäle der Kommunikation im Vorfeld, einschließlich Alternativen, wird es der Organisation ermöglichen, wirksam zu kommunizieren;
- Die Personen, die die Kommunikation ausführen:** Die Organisation sollte Sprecher zur Vertretung der Organisation identifizieren und bestimmte Personen zu Ansprechpartnern für die Kommunikation ernennen.

Die Organisation darf auf ihr BCMS und auf Vorkehrungen zur Aufrechterhaltung der Betriebsfähigkeit in Newslettern für und Unterweisungen von Lieferanten und Kunden verweisen.

Die Organisation sollte eine effektive externe Kommunikation als Teil ihres Programms zur Bewusstseinsbildung (7.3) und als Reaktion auf einen Zwischenfall (8.4.4) vorweisen.

7.5 Dokumentierte Information

7.5.1 Allgemeines

Dokumentierte Informationen liefern Nachweise für die Erfüllung der Anforderungen und die effektive Anwendung des Managementsystems.

Der Begriff „Verfahren“ bedeutet eine festgelegte Weise zur Durchführung einer Tätigkeit oder eines Prozesses. Ein „dokumentiertes Verfahren“ bedeutet, dass das Verfahren auf einem geeigneten Medium eingerichtet und aufrechterhalten werden sollte.

Ein einzelnes Dokument darf die Anforderungen an ein oder mehrere dokumentierte Verfahren beinhalten und eine Anforderung an ein dokumentiertes Verfahren darf in einem Dokument oder in mehreren Dokumenten enthalten sein.

Die durch dieses Dokument geforderten dokumentierten Informationen umfassen:

- Verstehen der Organisation und ihres Kontextes (4.1);
- rechtliche und behördliche Anforderungen (4.2.2);
- Anwendungsbereich des BCMS und sämtliche Ausnahmen (4.3.2);
- Leitlinien (5.2);
- Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit und Planung zur Zielerreichung (6.2);
- Kompetenzen (7.2);
- Business Impact Analyse und Risikobewertung (8.2);
- Strategien und Lösungen zur Aufrechterhaltung der Betriebsfähigkeit (8.3), einschließlich der betrachteten Lösungsoptionen;
- Pläne und Verfahren zur Aufrechterhaltung der Betriebsfähigkeit (8.4);
- Übungsberichte zu Übungsprogrammen (8.5);
- Überwachung, Messung, Analyse und Bewertung (9.1);
- internes Audit (9.2);
- Managementbewertung (9.3);
- Abweichungen und Korrekturmaßnahmen (10.1).

Zusätzlich darf die Dokumentation folgender Informationen gefordert werden, um die Effektivität des BCMS sicherzustellen:

- Kundenverträge und Dienstleistungsgrad;
- Ergebnisse der Business Impact Analysen;
- Ergebnisse der Risikobewertungen;
- Bestimmung und Auswahl der Lösungen zur Aufrechterhaltung der Betriebsfähigkeit;
- Überblick über die Einsätze zur Gefahrenabwehr;
- Programm zur Bewusstseinsbildung;
- Kommunikation zum BCMS und zu Zwischenfällen mit Mitarbeitern und mit Interessengruppen — wie z. B. Newsletter, Sitzungsprotokolle und Warnungen;
- Schulungsprogramme für die Organisation und für Einzelpersonen;
- Übungsplan;
- Verträge und Leistungsvereinbarungen mit Lieferanten;

- Politik und Pläne zur Aufrechterhaltung der Betriebsfähigkeit von Auftragnehmern und Lieferanten einschließlich des Nachweises der Risikoüberwachung ihrer Lieferanten und Nachweis, dass die Pläne zur Aufrechterhaltung ihrer Lieferanten aufrechterhalten und geübt werden;
- Verfahren zur Benachrichtigung von und zur Gefahrenabwehr bei Vertragsnehmern und Lieferanten;
- Nachweis von Inspektionen, Wartungen und Kalibrierungen;
- Berichte über Vorfälle und Beinahe-Unfälle;
- Protokolle von Sitzungen zur Überprüfung des BCMS.

7.5.2 Erstellen und Aktualisieren

Um die Anforderungen an die Erstellung und Aktualisierung dokumentierter Informationen zu erfüllen:

- sollten alle dokumentierten Informationen eindeutig identifizierbar sein (z. B. Name, Referenznummer, Beschreibung, Datum, Autor, Version);
- sollte die Organisation zulässige Formate (z. B. Sprache, Softwareversion, Bilder) und Medien (z. B. auf Papier, elektronisch) zur Speicherung dokumentierter Informationen eindeutig festlegen;
- sollte die Eignung und Angemessenheit des verwendeten Formats und Mediums überprüft und genehmigt werden.

Der Umfang der dokumentierten Informationen für das BCMS darf zwischen Organisationen aufgrund folgender Faktoren voneinander abweichen:

- die Größe der Organisation, deren Produkte und Dienstleistungen und die Art der Tätigkeiten, die sie durchführt;
- die Komplexität der Tätigkeiten und deren Wechselbeziehungen;
- die Kompetenzen der Personen.

7.5.3 Lenkung dokumentierter Information

Alle erforderlichen dokumentierten Informationen sollten kontrolliert werden.

Der Zweck der Kontrolle von Dokumentationen ist es, sicherzustellen, dass Organisationen Dokumente auf geeignete und ausreichende Art und Weise erstellen, pflegen und schützen, um das BCMS umzusetzen und anzuwenden. Das Hauptaugenmerk sollte eher auf diesem Zweck liegen, als auf der Einführung eines komplexen Dokumentenkontrollsystems.

Beispiele für den Schutz umfassen, Dokumente davor zu bewahren, beschädigt, ohne Befugnis geändert und versehentlich gelöscht zu werden.

Es gibt verschiedene Stufen von Zugangsberechtigungen und Kombinationen davon, die erteilt werden dürfen, wie beispielsweise nur Sichtrechte, Sicht- und Änderungsrechte und eingeschränkte Sichtrechte.

Ein dokumentiertes Verfahren sollte eingeführt werden, um die Kontrollen festzulegen, die für Folgendes benötigt werden:

- Verteilung der dokumentierten Information;
- Einrichten des Zugriffs auf diese (der Zugriff umfasst beispielsweise die Erlaubnis und Befugnis zur Ansicht oder Änderung der dokumentierten Information);
- Genehmigung der Eignung von Dokumenten vor der Ausgabe;
- Überprüfung und gegebenenfalls Aktualisierung und erneute Bestätigung von Dokumenten;
- Sicherstellen, dass Änderungen und der aktuelle Revisionsstatus von Dokumenten identifiziert werden;
- Sicherstellen, dass die relevanten Versionen aller anzuwendenden Dokumente am Nutzungsort verfügbar sind;
- Sicherstellen, dass Dokumente dauerhaft lesbar und direkt identifizierbar sind;
- Sicherstellen, dass Dokumente externen Ursprungs, die von der Organisation als notwendig für die Planung und Durchführung des BCMS bestimmt wurden, gekennzeichnet werden und deren Verteilung kontrolliert wird;
- Verhindern der versehentlichen Anwendung von nicht mehr gültigen Dokumenten und Anbringen einer geeigneten Kennzeichnung, falls diese für irgendeinen Zweck aufbewahrt werden;
- Festlegen von Vorgaben zum Aufbewahren und Archivieren von Dokumenten;
- Sicherstellen des Schutzes und der Geheimhaltung von vertraulichen Informationen.

Organisationen sollten die Integrität der dokumentierten Information sicherstellen, indem sie diese manipulationssicher machen, Sicherungskopien erstellen, den Zugriff nur autorisiertem Personal ermöglichen und sie vor Beschädigung, Zerstörung oder Verlust schützen.

Die Organisation sollte die Kenntnis aller relevanten Rechtsvorschriften und Verordnungen, die die Aufbewahrung von dokumentierter Information betreffen, nachweisen und die Nachweise der Einhaltung aufbewahren.

8 Betrieb

8.1 Ablaufplanung und Steuerung

Die Organisation sollte diejenigen Tätigkeiten festlegen, planen, umsetzen und steuern, die erforderlich sind, um ihre Leitlinien und Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit zu erfüllen und den geltenden Bedürfnissen und Anforderungen zu entsprechen.

Diese Tätigkeiten erstellen ein Programm, mit dem sichergestellt wird, dass die Aufrechterhaltung der Betriebsfähigkeit der Organisation auf angemessene Weise gelenkt wird und ihre Effektivität erhalten bleibt.

Die Organisation sollte Steuerungsmechanismen innerhalb des Programms einführen, die Folgendes umfassen:

- a) Entscheidungen darüber, wie diese Tätigkeiten festgelegt, geplant, umgesetzt und gesteuert werden sollten, z. B. indem ein Umsetzungsplan erstellt und eine geeignete Methodik für die Umsetzung und Aufrechterhaltung des BCMS vereinbart wird;

- b) Sicherstellen, dass die Steuerung dieser Tätigkeiten in Übereinstimmung mit den getroffenen Entscheidungen umgesetzt wird, z.B. indem Meilensteine für das Projekt und die geforderten Ergebnisse genau benannt werden;
- c) Aufbewahren von dokumentierter Information zur Darlegung, dass die Prozesse planmäßig durchgeführt wurden.

Die Organisation sollte sicherstellen, dass die geplanten Änderungen gesteuert werden, unbeabsichtigte Änderungen überprüft werden und geeignete Maßnahmen ergriffen werden.

8.1.1 Business Continuity Management (BCM)

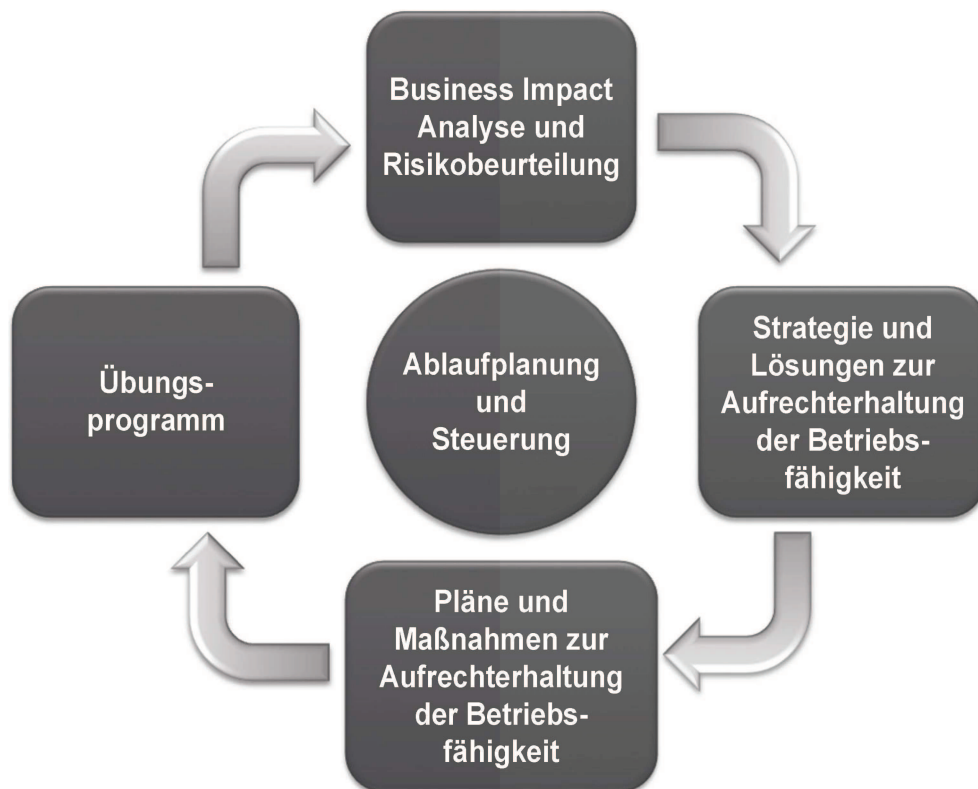


Bild 5 — Elemente des BCM

Das BCM umfasst die folgenden fünf Elemente:

1) Ablaufplanung und Steuerung (8.1)

Eine wirksame Ablaufplanung und Steuerung sind die Grundlage für das Business Continuity Management. Sie sollte von einer verantwortlichen Person geleitet werden, die vom Leitungsgremium ernannt wurde.

2) Business Impact Analyse und Risikobewertung (8.2)

Die Zustimmung und das Verständnis für die Prioritäten und Voraussetzungen für die Aufrechterhaltung der Betriebsfähigkeit werden durch die Analyse der geschäftlichen Auswirkungen und die Risikobewertung (RA, en: risk assessment) erreicht. Das Verständnis der im Fall einer Unterbrechung der Tätigkeiten auftretenden geschäftlichen Auswirkungen ermöglicht der Organisation, der Wiederaufnahme derjenigen Tätigkeiten Priorität einzuräumen, die ihre Produkte und Dienstleistungen unterstützen. Das Verständnis der Risiken für Schwerpunkttätigkeiten und ihre Abhängigkeiten ermöglicht es der Organisation, diese Risiken zu handhaben, potenzielle Strategien zur Aufrechterhaltung der Betriebsfähigkeit zu identifizieren und geeignete Lösungen zur Aufrechterhaltung der Betriebsfähigkeit auszuwählen.

3) Strategien und Lösungen zur Aufrechterhaltung der Betriebsfähigkeit (8.3)

Die Identifizierung und Bewertung zahlreicher Strategien zur Aufrechterhaltung der Betriebsfähigkeit ermöglicht der Organisation, geeignete Lösungen zur Reduzierung des Risikos und zur Minderung der Auswirkung der Unterbrechung ihrer Schwerpunkttätigkeiten zu identifizieren sowie mit allen auftretenden Betriebsunterbrechungen umzugehen. Die ausgewählten Lösungen zur Aufrechterhaltung der Betriebsfähigkeit ermöglichen die Wiederaufnahme der Lieferung von Produkten und Dienstleistungen (Produktions- oder Dienstleistungsniveau) innerhalb der vereinbarten Zeiträume.

4) Pläne und Verfahren zur Aufrechterhaltung der Betriebsfähigkeit (8.4)

Pläne und Verfahren zur Aufrechterhaltung der Betriebsfähigkeit ermöglichen es der Organisation eine Betriebsunterbrechung zu handhaben und Tätigkeiten auf der Grundlage ihrer Anforderungen an die Aufrechterhaltung der Betriebsfähigkeit fortzusetzen. Eine festgelegte Reaktionsstruktur, die das für die Reaktion auf Betriebsunterbrechungen verantwortliche Team identifiziert, muss verfügbar sein (8.4.2). Die Organisation muss Pläne und Verfahren für die Warnung und Kommunikation (8.4.3), die Reaktion auf Vorfälle (8.4.4.1 a)) und die Wiederherstellung (Rückkehr zum normalen Betrieb) (8.4.5) erstellen und umsetzen.

5) Übungsprogramm (8.5)

Das Übungsprogramm der Organisation sollte sicherstellen, dass ihre Aufrechterhaltung der Betriebsfähigkeit wirksam und mit den Zielen der Aufrechterhaltung der Betriebsfähigkeit abgestimmt bleibt und der Organisation die Möglichkeit bietet:

- die Bewusstseinsbildung und die Kompetenzentwicklung des Personals zu fördern;
- sicherzustellen, dass die Pläne und die Verfahren zur Aufrechterhaltung der Betriebsfähigkeit vollständig, aktuell und angemessen sind;
- ihre Betriebsfähigkeit aufrechtzuerhalten.

Die oberste Leitung sollte ihre Anforderungen an die formale Abzeichnung jedes Elements identifizieren.

8.1.2 Aufrechterhaltung der Betriebsfähigkeit

Die wirksame Aufrechterhaltung der Betriebsfähigkeit umfasst:

- Sicherstellen der fortlaufenden Zweckdienlichkeit des Anwendungsbereichs und der Funktionen und Verantwortlichkeiten für die Aufrechterhaltung der Betriebsfähigkeit;
- Fördern und Einbinden des BCM innerhalb der gesamten Organisation und anderer interessierter Parteien, sofern zutreffend;
- Lenken der Kosten in Verbindung mit der Aufrechterhaltung der Betriebsfähigkeit;
- Einführen und Überwachen von Systemen des Änderungs- und Nachfolgemanagements innerhalb des BCMS;
- Einrichten oder Anbieten von Mitarbeiterschulungen und von Schulungen zur Bewusstseinsbildung;
- Aufrechterhalten einer Dokumentation des Programms, die für die Größe und Komplexität der Organisation angemessen ist.

Jede Komponente der Vorkehrungen einer Organisation zur Aufrechterhaltung der Betriebsfähigkeit, einschließlich der Dokumentation, sollte regelmäßig überprüft, geübt und aktualisiert werden. Diese Arrangements sollten außerdem immer dann überprüft und aktualisiert werden, wenn eine bedeutende Änderung der Betriebsumgebung, der Struktur, des Standorts, des Personals, der Prozesse oder der Technologien der Organisation erfolgt, oder wenn durch eine Übung oder einen Zwischenfall Mängel aufgezeigt worden sind.

Die Organisation darf eine anerkannte Projektmanagementmethode anwenden, um sicherzustellen, dass das BCM wirksam gelenkt wird.

Verfahren zur Sicherstellung der dauerhaften Wirksamkeit der Aufrechterhaltung der Betriebsfähigkeit umfassen:

- die Implementierung anerkannter Praktiken;
- das Verwalten des Übungsprogramms;
- das Koordinieren regelmäßiger Überprüfungen und Aktualisierungen der Aufrechterhaltung der Betriebsfähigkeit, einschließlich Überprüfungen oder Überarbeitungen der geschäftlichen Auswirkungen und des Risikomanagements;
- das Sicherstellen, dass Verfahren zur Aufrechterhaltung der Betriebsfähigkeit für die Bedürfnisse der Reaktionsteams angemessen bleiben.

8.2 Business Impact Analyse und Risikobewertung

8.2.1 Allgemeines

Eine Organisation erreicht ihre Ziele, indem sie ihre Produkte und Dienstleistungen an Kunden ausliefert. Aus diesem Grund ist es wichtig, ein Verständnis zu erzeugen, welche nachteilige Auswirkung über einen zeitlichen Verlauf eine Unterbrechung dieser Produktlieferungen und Dienstleistungen (und Tätigkeiten, die diese unterstützen) auf die Organisation und interessierte Parteien haben würde. Es ist außerdem von Bedeutung, die Beziehungen und den Ressourcenbedarf der Tätigkeiten zur Unterstützung der Produkte und Dienstleistungen sowie die Bedrohungen für diese zu verstehen.

Die Organisation sollte einen Prozess zur Analyse der geschäftlichen Auswirkungen (8.2.2) und Risikobewertung (8.2.3) von Betriebsunterbrechungen umsetzen und aufrechterhalten. Die effektive Analyse von geschäftlichen Auswirkungen und die Risikobewertung werden es der Organisation ermöglichen, Strategien und Lösungen zur Aufrechterhaltung der Betriebsfähigkeit (8.3) zu identifizieren.

Die Organisation kann die Reihenfolge bestimmen, in der die Analyse der geschäftlichen Auswirkung und die Risikobewertung durchgeführt werden, solange die Risiken für ihre Schwerpunkttätigkeiten (8.2.3) bewertet werden.

8.2.2 Business Impact Analyse

Der Hauptzweck der Business Impact Analyse besteht darin, der Organisation zu ermöglichen, Tätigkeiten zu identifizieren, die als dringlich eingestuft werden, um inakzeptable Auswirkungen auf das Geschäft während einer Betriebsunterbrechung zu vermeiden (Schwerpunkttätigkeiten), und Prioritäten für die Wiederaufnahme aller Tätigkeiten festzulegen.

Jede Organisation beschreibt ihren Betrieb auf ihre eigene Weise. Eine Organisation darf beispielsweise Produkte und Dienstleistungen als durch aus Tätigkeiten bestehenden Prozessen geschaffen beschreiben. Tätigkeiten dürfen außerdem als Aufgaben oder Reihen von Aufgaben beschrieben werden, die die Organisation ausführt, um Produkte und Dienstleistungen herzustellen und zu liefern.

Bei der Durchführung der Business Impact Analyse sollten die verwendeten Begriffe die Art und Weise wiedergeben, in der die Organisation ihre eigene Tätigkeit beschreibt.

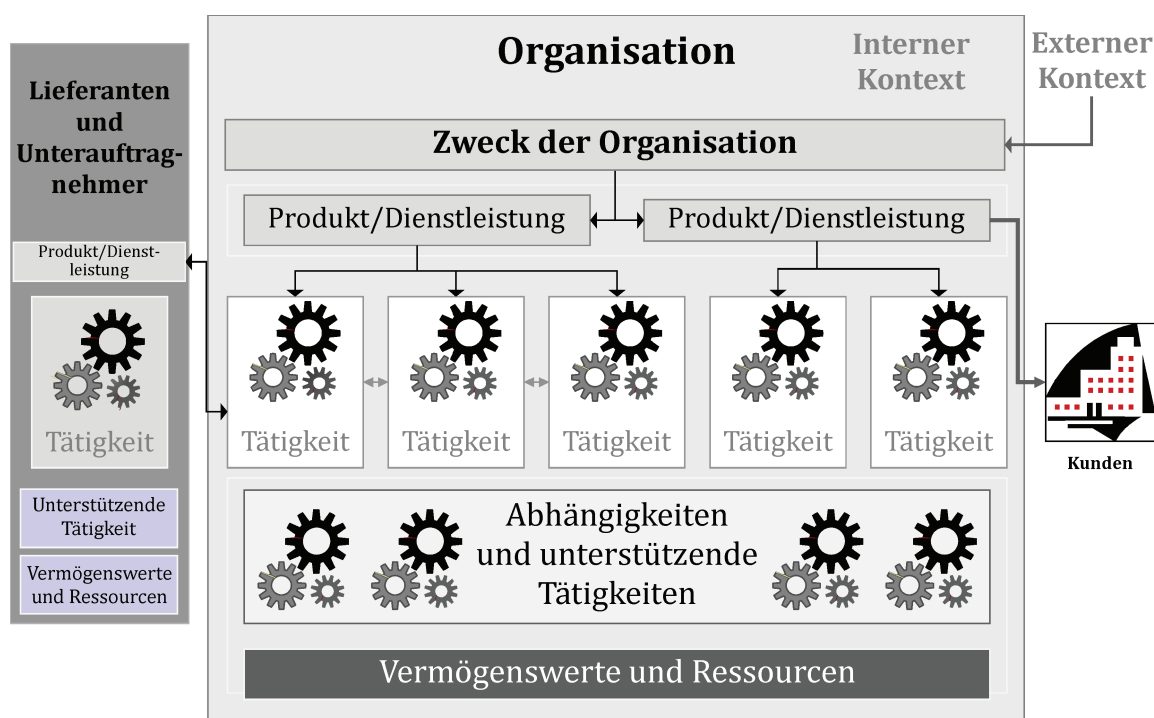


Bild 6 — Organisationsverständnis

ISO/TS 22317 enthält weitere Leitlinien für die Durchführung einer Business Impact Analyse. Hierbei handelt es sich um eine technische Spezifikation, die einen gestuften Ansatz als Verfahren zur Erfüllung der Anforderungen nach ISO 22301 präsentiert.

Die Business Impact Analyse ermöglicht es der Organisation, die negativen Auswirkungen von Betriebsunterbrechungen auf ihre Tätigkeit zu bestimmen und als Ergebnis eine Erklärung und Begründung der Anforderungen an die Aufrechterhaltung der Betriebsfähigkeit zu erstellen.

Die Analyse ermöglicht es einer Organisation darüber hinaus:

- ein Verständnis über die Produkte und Dienstleistungen sowie über die Tätigkeiten für deren Erstellung zu erlangen;
- Prioritäten, Strategien und Zeitrahmen für die Wiederaufnahme der Lieferung von Produkten und Dienstleistungen zu bestimmen;
- die Ressourcen zu ermitteln, die voraussichtlich für die Aufrechterhaltung der Betriebsfähigkeit und die Wiederherstellung erforderlich sind;
- Abhängigkeiten (interne und externe) zu ermitteln.

Die Organisation sollte einen formalen Bewertungsprozess einführen, um die geschäftlichen Auswirkungen zu analysieren und die Prioritäten und Ziele für die Aufrechterhaltung der Betriebsfähigkeit zu bestimmen.

Der Prozess sollte die Festlegung von Bewertungskriterien für die Business Impact Analyse einschließlich der Arten der Auswirkungen und der zu berücksichtigenden Zeitrahmen beinhalten. Beides sollte auf dem Kontext, den Geschäftszielen und den Zielen der Organisation basieren und die Bedürfnisse interessierter Parteien berücksichtigen. Die Bewertungskriterien sollten regelmäßig und häufiger in Zeiten von Veränderungen geprüft werden.

Arten von Auswirkungen sind beispielsweise:

Finanziell: Verluste durch Geldbußen, Geldstrafen, entgangene Gewinne oder verringerte Marktanteile

Rufschädigung: Negative Meinung oder Schädigung der Marke

Betrieblich: Umfang und Dauer der Unterbrechung der betrieblichen Abläufe

Gesetzlich und regulatorisch: Haftung im Rahmen von Rechtsstreitigkeiten und Entzug der Handelszulassung

Vertraglich: Verstoß gegen Verträge oder Verpflichtungen zwischen Organisationen

Geschäftsziele: Nichterreichen von Zielen oder Nichtnutzung von Chancen

Die Dauer, nach der Auswirkungen inakzeptabel werden, kann Sekunden oder auch mehrere Monate betragen. Die Zeitrahmen werden von der Zeitempfindlichkeit der Produkte und Dienstleistungen der Organisation abhängen. Um beispielsweise Produkte zu handhaben, die sehr zeitempfindlich sind, können Zeitrahmen von Minuten oder Stunden erforderlich sein. Längere Zeitrahmen wären für Organisationen mit weniger zeitempfindlichen Produkten und Dienstleistungen geeignet.

Die Organisation muss während der Analyse erkennen, dass eine Unterbrechung der Tätigkeit indirekt zu einer Unterbrechung der Lieferung von Produkten und Dienstleistungen führen kann. Beispielsweise kann der Verlust der Zahlungsfähigkeit gegenüber Lieferanten für die Organisation rufschädigend sein und dazu führen, dass Lieferanten die Lieferung von Waren verweigern, was dazu führt, dass weder Produkte hergestellt noch Dienstleistungen erbracht werden.

Produkte und Dienstleistungen unterliegen darüber hinaus täglichen Schwankungen und können konjunkturabhängig sein. Häufig gibt es jahreszeitlich bedingte Schwankungen und ein höheres Tätigkeitsaufkommen in Verbindung mit wöchentlichen, monatlichen oder jährlichen Fristen oder Projektfertigstellungsterminen. Die Annahme, dass eine Betriebsunterbrechung zum ungünstigsten Zeitpunkt während dieser Perioden eintreten könnte, stellt sicher, dass die größtmögliche Auswirkung beurteilt wird.

Die oberste Leitung der Organisation bestimmt, welches Maß an Auswirkung für die Organisation inakzeptabel ist. Die Zeit, nach der eine Auswirkung inakzeptabel werden würde, kann als „maximal zulässige Störungsdauer“ (MTPD), „maximal zulässige Dauer“ oder „maximal zulässige Unterbrechung“ bezeichnet werden. Die Mindestniveaustufe für Dienstleistungen und/oder Produkte, die für die Organisation akzeptabel ist, kann als „Mindestzielsetzung für die Aufrechterhaltung der Betriebsfähigkeit“ (MBCO, en: minimum business continuity objective) bezeichnet werden.

Die Business Impact Analyse sollte darüber hinaus die Identifizierung der Abhängigkeiten von Schwerpunkttätigkeiten beinhalten. Dies wird es der Organisation ermöglichen, sicherzustellen, dass diese in die Risikobewertung (8.2.3) aufgenommen werden und zur Bestimmung der Strategie und Lösungen zur Aufrechterhaltung der Betriebsfähigkeit (8.3) zur Verfügung stehen.

Die Organisation sollte bei der Erstellung der Ressourcenanforderungen (8.3.3) vor der Auswahl der Lösungen zur Aufrechterhaltung der Betriebsfähigkeit (8.3.2) vorsichtig sein, da die Abhängigkeiten der Schwerpunkttätigkeiten möglicherweise nicht für die ausgewählten Lösungen zur Aufrechterhaltung der Betriebsfähigkeit relevant sind.

Die Business Impact Analyse sollte Folgendes beinhalten:

- a) die Festlegung der Bewertungskriterien einschließlich:
 - i) Arten von Auswirkungen;
 - ii) Zeitrahmen;
- b) die Anwendung der Bewertungskriterien zur Messung der Auswirkungen;
- c) das Identifizieren von Tätigkeiten, die die Lieferung der Produkte und Dienstleistungen der Organisation unterstützen;
- d) die Analyse der potenziellen Auswirkung der Unterbrechung dieser Tätigkeiten im Verlauf der Zeit;
- e) die Schätzung der Zeit, innerhalb der die Auswirkungen der Nichtwiederaufnahme von Tätigkeiten inakzeptabel werden würden;
- f) die Festlegung von Zeitrahmen für die priorisierte Wiederaufnahme von Tätigkeiten innerhalb der in e) oben identifizierten Zeit und Angabe der akzeptablen Mindestkapazitäten, bei denen Tätigkeiten wiederaufgenommen werden sollten (Bild 2 und Bild 3);
- g) die Identifizierung von Schwerpunkttätigkeiten auf der Grundlage der zeitbasierten Business Impact Analyse;
- h) die Identifizierung der Abhängigkeiten der Schwerpunkttätigkeiten von unterstützenden Ressourcen einschließlich der in 8.3.3 identifizierten Arten von Ressourcen;
- i) die Identifizierung der Abhängigkeiten der Schwerpunkttätigkeiten von anderen Tätigkeiten, von denen einige gegebenenfalls nicht als Schwerpunkttätigkeiten identifiziert wurden.

In diesem Dokument wird der geplante zeitliche Rahmen zur Wiederaufnahme einer Tätigkeit oder Abhängigkeit als Wiederherstellungsdauer (RTO, en: Recovery Time Objective) bezeichnet. Organisationen sollten darüber hinaus die Kapazität bestimmen, bei der Tätigkeiten und ihre Abhängigkeiten wiederaufzunehmen sind.

Die RTO einer Tätigkeit sollte auf eine Zeit, bevor Auswirkungen inakzeptabel werden (siehe e) oben), festgelegt werden. Diese Zeit muss darüber hinaus gegebenenfalls Folgendes berücksichtigen:

- Abhängigkeiten von verwandten Tätigkeiten;
- die Komplexität des Wiederherstellungsprozesses.

Es darf für Organisationen mit komplexen Wiederherstellungsprozessen angemessen sein, mehrere RTO für eine Reihe akzeptabler Kapazitäten festzulegen.

Die Organisation sollte bei der Betrachtung der Abhängigkeit der Tätigkeiten von Informationen und Daten (8.3.3.4) sicherstellen, dass die für die Wiederaufnahme einer Tätigkeit erforderlichen Informationen und Daten entsprechend aktuell sind. Die Organisation darf den Begriff „Wiederherstellungszeitpunkt“ (RPO, en: Recovery Point Objective) verwenden, um dies zu erreichen. Der RPO ist der Zeitpunkt, zu dem die von einer Tätigkeit verwendeten Informationen und Daten wiederhergestellt werden, um die Ausführung der Tätigkeit bei Wiederherstellung zu ermöglichen. Der RPO darf darüber hinaus verwendet werden, um die erforderliche Häufigkeit der Datensicherung zu bestimmen, um einen inakzeptablen Verlust von Daten und Informationen zu vermeiden, der oftmals als „maximaler Datenverlust“ bezeichnet wird. Da der Verlust von Informationen und Daten die Wiederaufnahme von Tätigkeiten verhindern könnte, kann es angemessen sein, Datensicherungen und die Bestimmung des RPO für alle von Tätigkeiten benötigten Daten zu berücksichtigen.

ISO/IEC 27031 enthält weitere Leitlinien zur Sicherstellung der Aktualität elektronisch gespeicherter Daten. ISO/IEC 27002 enthält Leitlinien zur fortlaufenden Sicherung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten.

Die Business Impact Analyse sollte dokumentiert werden, einschließlich:

- der Identifizierung rechtlicher, regulatorischer und vertraglicher Anforderungen (Verpflichtungen) und ihrer Auswirkung auf die Anforderungen an die Aufrechterhaltung der Betriebsfähigkeit (4.2.2);
- der Bestätigung oder Änderung des Anwendungsbereichs des BCMS der Organisation (4.3.2);
- der Bewertung der Auswirkungen auf die Organisation im Verlauf der Zeit als Begründung der Anforderungen an die Aufrechterhaltung der Betriebsfähigkeit (Zeit und Fähigkeit);
- der Identifizierung der Beziehungen zwischen Produkten und Dienstleistungen, Tätigkeiten und Ressourcen;
- der Identifizierung der unterstützenden Ressourcen, von denen Schwerpunkttätigkeiten abhängen;
- der Identifizierung von Abhängigkeiten von anderen Tätigkeiten, Lieferketten, Partnern und anderen interessierten Parteien.

Informationen dürfen aus folgenden Quellen stammen:

- Befragungen;
- Fragebögen;
- Workshops;
- anderen internen und externen Quellen.

8.2.3 Risikobewertung

Zweck der Risikobewertung ist es, der Organisation die Möglichkeit zu geben, die Risiken der unterbrochenen Schwerpunkttätigkeiten zu bewerten, um geeignete Maßnahmen zur Behandlung dieser Risiken treffen zu können.

Die Organisation sollte einen formalen Prozess für die Risikobewertung umsetzen und aufrechterhalten, der systematisch die Risiken einer Unterbrechung von Schwerpunkttätigkeiten sowie von Prozessen, Systemen, Informationen, Personen, Vermögenswerten, Lieferanten und anderen Ressourcen, die sie unterstützen, ermittelt, analysiert und bewertet.

Die Risikobewertung bietet einen strukturierten Prozess, mit dem ein Risiko im Hinblick auf dessen Wahrscheinlichkeit und Auswirkungen analysiert wird, bevor eine Entscheidung über weitere gegebenenfalls erforderliche Maßnahmen getroffen wird. Durch diesen strukturierten Prozess sollen einige grundlegende Fragen beantwortet werden:

- a) Was kann passieren?
- b) Wie hoch ist die Wahrscheinlichkeit ihres Eintretens?
- c) Was können die Konsequenzen sein?
- d) Gibt es etwas, das die Konsequenzen mildern oder die Wahrscheinlichkeit verringern kann?

Der Prozess muss den Kontext der Organisation und die Bedürfnisse und Erwartungen interessierter Parteien (4.1 und 4.2) berücksichtigen.

Die Organisation sollte die Bedrohungen für die und Schwachstellen der Ressourcen verstehen, die für die Tätigkeiten der Organisation erforderlich sind, und insbesondere:

- Tätigkeiten mit höherer Priorität oder
- Tätigkeiten mit einer langen Vorbereitungszeit für deren Austausch.

Die Organisation sollte eine geeignete Methode zur Identifizierung, Analyse und Bewertung von Risiken auswählen, die zu Betriebsunterbrechungen führen könnten. ISO 31000 legt Grundsätze für das Risikomanagement und die dazugehörigen Richtlinien fest. Typische Elemente, die im Kontext dieses Dokuments eingebunden werden sollten, sind folgende:

- **Identifikation von Risiken:** Die Identifizierung der potenziellen Risikoquellen für die Schwerpunkttätigkeiten einer Organisation und für die Prozesse, Systeme, Daten, Personen, Vermögenswerte, Lieferanten und anderen Ressourcen, die diese unterstützen. Diese können zurückzuführen sein auf:
 - spezifische Bedrohungen, die irgendwann Tätigkeiten und Ressourcen unterbrechen könnten (z. B. Bedrohungen wie Feuer, Überschwemmungen, Stromausfall, Verlust von Mitarbeitern, Abwesenheit von Mitarbeitern, Computerviren und Geräteausfall);
 - Betriebsunterbrechungen, die aus den Schwachstellen der Ressourcen hervorgehen können (z. B. Einzelausfälle, unangemessener Brandschutz, Mangel an elektrischer Belastbarkeit, unangemessene Personaldecke und mangelhafte IT-Sicherheit und -Belastbarkeit);