

DIN EN ISO 22301



ICS 03.100.01; 03.100.70

Einsprüche bis 2019-03-25
Vorgesehen als Ersatz für
DIN EN ISO 22301:2014-12

Entwurf

**Sicherheit und Schutz des Gemeinwesens –
Business Continuity Management System –
Anforderungen (ISO/DIS 22301:2019);
Deutsche und Englische Fassung prEN ISO 22301:2019**

Security and resilience –
Business continuity management systems –
Requirements (ISO/DIS 22301:2019);
German and English version prEN ISO 22301:2019

Sécurité et résilience –
Systèmes de management de la continuité d'activité –
Exigences (ISO/DIS 22301:2019);
Version allemande et anglaise prEN ISO 22301:2019

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-01-25 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 70 Seiten

DIN-Normenausschuss Organisationsprozesse (NAOrg)

Nationales Vorwort

Der Text von ISO/DIS 22301:2019 wurde vom Technischen Komitee ISO/TC 292 „Security and resilience“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO 22301:2019 durch das Technische Komitee CEN/TC 391 „Schutz und Sicherheit der Bürger“ ohne Änderungen übernommen, dessen Sekretariat von NEN (Niederlande) gehalten wird.

Für die deutsche Mitarbeit ist das Gremium NA 175-00-05 GA „Gemeinschaftsausschuss Sicherheit und Business Continuity“ im DIN-Normenausschuss Organisationsprozesse (NAOrg) verantwortlich.

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.

ISO 9001	siehe DIN EN ISO 9001
ISO 14001	siehe DIN EN ISO 14001
ISO 19011	siehe DIN EN ISO 19011
ISO 22300	siehe DIN EN ISO 22300
ISO/IEC 27001	siehe DIN EN ISO/IEC 27001
ISO 28000	siehe DIN ISO 28000
ISO 31000	siehe DIN ISO 31000

Änderungen

Gegenüber DIN EN ISO 22301:2014-12 wurden folgende Änderungen vorgenommen:

- a) Anpassung an die ISO-Grundstruktur für Managementsystemnormen;
- b) Einleitung angepasst;
- c) einige Begriffe hinzugefügt;
- d) die Unterabschnitte 4.1, 4.2, 4.3, 4.4, 6.1, 6.2, 8.1, 9.1, 9.1.1 und 9.3 geändert;
- e) die Abschnitte 5, 7 und 10 neu aufgenommen.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 9001, *Qualitätsmanagementsysteme — Anforderungen*

DIN EN ISO 14001, *Umweltmanagementsysteme — Anforderungen mit Anleitung zur Anwendung*

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

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

DIN EN ISO/IEC 27001, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen*

DIN ISO 28000, *Spezifikation für Sicherheitsmanagementsysteme für die Lieferkette*

DIN ISO 31000, *Risikomanagement — Leitlinien*

— Leerseite —

Sicherheit und Schutz des Gemeinwesens — Business Continuity Management System — Anforderungen (ISO/DIS 22301:2019)

Sécurité et résilience — Systèmes de management de la continuité d'activité — Exigences (ISO/DIS 22301:2019)

Security and resilience — Business continuity management systems — Requirements (ISO/DIS 22301:2019)

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	10
2 Normative Verweisungen	10
3 Begriffe	10
4 Kontext der Organisation	21
4.1 Verstehen der Organisation und ihres Kontextes	21
4.2 Verstehen der Bedürfnisse und Erwartungen der interessierten Parteien	21
4.2.1 Allgemeines	21
4.2.2 Rechtliche und behördliche Anforderungen	21
4.3 Festlegung des Anwendungsbereichs des Business Continuity Managements	21
4.3.1 Allgemeines	21
4.3.2 Anwendungsbereich des BCMS	22
4.4 Business Continuity Management System	22
5 Führung	22
5.1 Führung und Verpflichtung	22
5.2 Leitlinien	23
5.2.1 Die oberste Leitung muss Leitlinien zur Aufrechterhaltung der Betriebsfähigkeit einführen, die:	23
5.2.2 Leitlinien zur Aufrechterhaltung der Betriebsfähigkeit müssen:	23
5.3 Funktionen, Verantwortlichkeiten und Befugnisse innerhalb der Organisation	23
6 Planung	23
6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten	23
6.2 Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit und Planung zur Zielerreichung	24
6.3 Planung von Änderungen am BCMS	24
7 Unterstützung	25
7.1 Ressourcen	25
7.2 Kompetenz	25
7.3 Bewusstseinsbildung	25
7.4 Kommunikation	25
7.5 Dokumentierte Information	26
7.5.1 Allgemeines	26
7.5.2 Erstellung und Aktualisierung	26
7.5.3 Steuerung dokumentierter Information	26
8 Betrieb	27
8.1 Ablaufplanung und Kontrolle	27
8.2 Business Impact Analyse und Risikobewertung	27
8.2.1 Allgemeines	27
8.2.2 Business Impact Analyse	27
8.2.3 Risikobewertung	28
8.3 Strategien und Lösungen zur Aufrechterhaltung der Betriebsfähigkeit	28

8.3.1	Allgemeines	28
8.3.2	Festlegung und Auswahl der Strategien und Lösungen	28
8.3.3	Ressourcenbedarf	29
8.3.4	Umsetzung von Lösungen.....	29
8.4	Pläne und Verfahren zur Aufrechterhaltung der Betriebsfähigkeit.....	29
8.4.1	Allgemeines	29
8.4.2	Reaktionsstruktur.....	30
8.4.3	Warnung und Kommunikation.....	30
8.4.4	Pläne zur Aufrechterhaltung der Betriebsfähigkeit.....	31
8.4.5	Wiederherstellung.....	32
8.5	Übungsprogramm	32
9	Leistungsüberprüfung.....	32
9.1	Überwachung, Messung, Analyse und Bewertung.....	32
9.1.1	Allgemeines	32
9.1.2	Bewertung der Pläne zur Aufrechterhaltung der Betriebsfähigkeit, Verfahren und Leistungsfähigkeiten.....	33
9.2	Internes Audit.....	33
9.2.1	Die Organisation muss:	33
9.3	Managementüberprüfung	33
9.3.1	Allgemeines	33
9.3.2	Eingaben für die Managementüberprüfung	34
9.3.3	Ergebnisse der Managementüberprüfung	34
10	Verbesserung.....	35
10.1	Nichtkonformität und Korrekturmaßnahmen.....	35
10.2	Ständige Verbesserung.....	35
	Literaturhinweise.....	36

Europäisches Vorwort

Dieses Dokument (prEN ISO 22301:2019) 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.

Dieses Dokument wird EN ISO 22301:2014 ersetzen.

Anerkennungsnotiz

Der Text von ISO/DIS 22301:2019 wurde von CEN als prEN ISO 22301:2019 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 22301 wurde vom Technischen Komitee ISO/TC 292, *Security and resilience*, erarbeitet.

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

Einleitung

0.1 Allgemeines

Dieses Dokument legt die Struktur und Anforderungen für die Implementierung und Verwaltung eines effektiven Systems zur Aufrechterhaltung der Betriebsfähigkeit (Business Continuity Management System, BCMS) fest.

Eine Organisation sollte ein Maß an Betriebsfähigkeit entwickeln, das der Größe und Art der Auswirkungen angemessen ist, die nach einer Störung akzeptiert werden dürfen oder nicht. Die Ergebnisse der Aufrechterhaltung eines BCMS werden durch rechtliche, behördliche, organisationstechnische und industrielle Anforderungen geprägt sowie durch Produkte und gebotene Dienstleistungen, eingesetzte Prozesse, Größe und Aufbau der Organisation und die Anforderungen ihrer interessierten Parteien.

Ein BCMS betont die Bedeutung:

des Verstehens der Bedürfnisse der Organisation sowie der Notwendigkeit der Einführung von Leitlinien und Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit;

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 ständigen Verbesserung auf Grundlage qualitativer und quantitativer Messungen.

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

- a) Leitlinien;
- b) kompetente Personen mit festgelegten Verantwortlichkeiten;
- c) Managementprozess in Bezug auf:

Leitlinien;

Planung;

Umsetzung und Betrieb;

Leistungsbewertung;

Managementüberprüfung;

ständige Verbesserung;

- d) dokumentierte Informationen, die die betriebliche Kontrolle unterstützen und eine Leistungsbewertung ermöglichen.

0.2 Vorteile eines BCMS

Das BCMS dient der Vorbereitung, Bereitstellung und Aufrechterhaltung von Kontrollen und Funktionen für die Verwaltung der allgemeinen Fähigkeit eines Unternehmens, den Betrieb während einer Störung fortzusetzen. Um dies zu erreichen, muss die Organisation:

- a) aus geschäftlicher Sicht:
 - seine strategischen Zielsetzungen unterstützen;
 - einen Wettbewerbsvorteil bereitstellen;
 - seinen Ruf und seine Glaubwürdigkeit schützen und verbessern;
 - zur Belastbarkeit der Organisation beitragen;
- b) aus finanzieller Sicht:
 - auf Geschäftspartner und deren Erfolg vertrauen;
 - rechtliche und finanzielle Risiken verringern;
 - direkte und indirekte Kosten von Störungen reduzieren;
- c) aus der Sicht der interessierten Parteien:
 - das Leben, Eigentum und die Umwelt schützen;
 - Erwartungen der interessierten Parteien berücksichtigen;
- d) aus Sicht der internen Prozesse:
 - die Fähigkeit verbessern, auch während einer Störung betriebsfähig zu bleiben;
 - proaktive Kontrolle der Risiken effektiv und effizient demonstrieren;
 - betriebliche Schwachstellen erkennen.

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

Dieses Dokument wendet das PDCA-Modell an (PDCA, en: Plan-Do-Check-Act), um das BCMS einer Organisation zu planen, einzuführen, umzusetzen, zu betreiben, zu überwachen, zu überprüfen, aufrechtzuerhalten und dessen Effektivität ständig zu verbessern.

Dies stellt ein bestimmtes Ausmaß an Übereinstimmung mit anderen Normen zu Managementsystemen, wie z. B. ISO 9001, *Quality management systems*, ISO 14001, *Environmental management systems*, ISO/IEC 27001, *Information security management systems*, ISO/IEC 20000-1, *Information technology – Service management* und ISO 28000, *Specification for security management systems for the supply chain*, sicher und unterstützt dadurch die einheitliche und integrierte Umsetzung und den Betrieb mit ähnlichen Managementsystemen.

0.4 Bestandteile des PDCA-Modells in diesem Dokument

Innerhalb des PDCA-Modells behandeln die Abschnitte 4 bis 10 dieses Dokuments die folgenden Bestandteile:

Abschnitt 4 ist Bestandteil des Elements „Planen“. Er führt Anforderungen ein, die notwendig sind, um den Kontext des BCMS, der für die Organisation gilt, sowie Bedürfnisse, Anforderungen und den Anwendungsbereich festzulegen.

Abschnitt 5 ist Bestandteil des Elements „Planen“. Er fasst die Anforderungen zusammen, die für die Funktion der obersten Leitung innerhalb des BCMS gelten, und wie die Führung ihre Erwartungen gegenüber der Organisation durch eine Grundsaterklärung ausdrückt.

Abschnitt 6 ist Bestandteil des Elements „Planen“. Er beschreibt Anforderungen, da er sich auf die Einführung strategischer Zielsetzungen und Leitsätze für das BCMS als Ganzes bezieht.

Abschnitt 7 ist Bestandteil des Elements „Planen“. Er unterstützt BCMS-Abläufe, die sich auf die Festlegung von Kompetenz und die Kommunikation mit interessierten Parteien auf einer periodisch wiederkehrenden oder bedarfsorientierten Grundlage beziehen, während sie die geforderte dokumentierte Information erfassen, lenken, erhalten und aufbewahren.

Abschnitt 8 ist Bestandteil des Elements „Durchführen“. Er legt die Anforderungen an die Aufrechterhaltung der Betriebsfähigkeit fest, bestimmt den Umgang mit diesen und entwickelt die Verfahren für das Management einer Organisation während einer Störung.

Abschnitt 9 ist Bestandteil des Elements „Prüfen“. Er fasst die Anforderungen zusammen, die zum Messen der Leistung der Betriebsfähigkeit sowie der Übereinstimmung des BCMS mit diesem Dokument und der Managementüberprüfung erforderlich sind.

Abschnitt 10 ist Bestandteil des Elements „Handeln“. Er identifiziert die Abweichung vom BCMS und ständige Verbesserungen und reagiert auf diese durch Korrekturmaßnahmen.

0.5 Inhalte dieses Dokuments

Dieses Dokument entspricht den Anforderungen von ISO an Managementsystemnormen. Diese Anforderungen schließen eine „ISO-Grundstruktur für Managementsystemnormen“ ein. Dazu gehören ein identischer Haupttext und gemeinsame Begriffe mit Kerndefinitionen, die entworfen wurden, um die Umsetzung für diejenigen Anwender zu erleichtern, die mehrere ISO-Managementsystemnormen verwirklichen.

Dieses Dokument enthält keine Anforderungen, die für andere Managementsysteme spezifisch sind, obwohl seine Elemente mit Anforderungen anderer Managementsysteme in Einklang stehen können oder in diese integriert werden können.

Dieses Dokument enthält Anforderungen, die von einer Organisation zur Implementierung eines BCMS und zur Bewertung der Konformität verwendet werden können. Eine Organisation, welche Konformität mit diesem Dokument nachweisen möchte, hat hierzu folgende Möglichkeiten:

Durchführung einer Selbstbewertung und Selbsterklärung; oder

Erlangen einer Bestätigung ihrer Konformität durch Parteien, die ein Interesse an der Organisation haben, wie z. B. Kunden; oder

Erlangen einer Bestätigung ihrer Selbsterklärung durch einen Externen; oder

Erlangen einer Zertifizierung/Registrierung ihres BCMS durch eine externe Organisation.

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 die Anforderungen beschreiben, die zur Beurteilung der Konformität mit diesem Dokument verwendet werden.

In diesem Dokument werden die folgenden Verbformen verwendet:

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

Als „ANMERKUNG“ gekennzeichnete Informationen dienen als Anleitung zum Verständnis oder zur Erläuterung der zugehörigen Anforderung. Als „Anmerkung zum Begriff“ gekennzeichnete Informationen im Abschnitt 3 dienen der zusätzlichen Erläuterung und können Anforderungen im Zusammenhang mit dem Begriff enthalten.

1 Anwendungsbereich

Dieses Dokument legt Anforderungen fest, um ein Managementsystem zu planen, einzuführen, umzusetzen, zu betreiben, zu überwachen, zu überprüfen, aufrechtzuerhalten und ständig zu verbessern, um sich gegen Störungen zu schützen, die Wahrscheinlichkeit ihres Auftretens zu vermindern, sich auf diese vorzubereiten, auf diese zu reagieren und sich von diesen zu erholen, wann immer sie auftreten.

Die Anforderungen dieses Dokuments sind allgemeiner Art und dafür vorgesehen, für sämtliche Organisationen oder Teile dieser, unabhängig von ihrer Art, Größe oder Beschaffenheit zu gelten. Der Umfang der Anwendung dieser Anforderungen ist von der betrieblichen Umgebung und der Komplexität der jeweiligen Organisation abhängig.

Dieses Dokument gilt für sämtliche Arten und Größen von Organisationen, die:

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

Dieses Dokument kann dazu genutzt werden, die Befähigung einer Organisation zur Erfüllung ihrer eigenen Bedürfnisse und Verpflichtungen in Bezug auf die Aufrechterhaltung der Betriebsfähigkeit zu bewerten.

2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

3 Begriffe

Für die Anwendung dieses Dokuments gelten 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 <http://www.iso.org/obp>
- IEC Electropedia: verfügbar unter <http://www.electropedia.org>

3.1

Tätigkeit

eine oder mehrere Aufgaben mit einem definierten Ergebnis

[QUELLE: ISO 22300:2018, 3.1, geändert. Anmerkung zum Begriff gelöscht.]

3.2

Audit

systematischer, unabhängiger und dokumentierter *Prozess* (3.40) zur Erlangung von Auditnachweisen und zu deren objektiver Auswertung, um zu ermitteln, inwieweit die Auditkriterien erfüllt sind

Anmerkung 1 zum Begriff: Zu den grundlegenden Elementen eines Audits zählt die Ermittlung der *Übereinstimmung* (3.8) eines *Objekts* (3.29) nach einem *Verfahren* (3.39), das von *Personal* (3.35) durchgeführt wird, das für das auditierte Objekt nicht verantwortlich ist.

Anmerkung 2 zum Begriff: Ein Audit kann ein internes Audit (Erstparteien-Audit) oder externes Audit (Zweit- oder Drittparteien-Audit) Audit sein und es kann ein kombiniertes Audit (Kombination zweier oder mehrerer Wissensgebiete) sein.

Anmerkung 3 zum Begriff: Ein internes Audit wird von der Organisation durchgeführt, oder von einer externen Stelle in ihrem Auftrag. Das interne Audit kann zum Zwecke der Managementüberprüfung (Management (3.24), Überprüfung (3.47)) und für andere interne Zwecke durchgeführt werden und die Grundlage für eine durch die Organisation verfasste Konformitätserklärung bilden. Unabhängigkeit kann durch die Freiheit von der Verantwortung für die zu auditierende Tätigkeit (3.1) demonstriert werden.

Anmerkung 4 zum Begriff: Zu externen Audits gehören im Allgemeinen solche, die als Zweit- oder Drittparteien-Audit bezeichnet werden. Zweitparteien-Audits werden von Parteien durchgeführt, die ein Interesse an der Organisation haben, wie Kunden, oder von anderen in deren Auftrag. Drittparteien-Audits werden von externen unabhängigen Auditierungsorganisationen durchgeführt, zu denen zum Beispiel solche gehören, die die Zertifizierung/Registrierung von Konformitätserklärungen anbieten, oder von Regierungsbehörden.

Anmerkung 5 zum Begriff: „Auditnachweis“ und „Auditkriterium“ sind in ISO 19011 definiert.

[QUELLE: ISO 22300:2018, 3.13, geändert. Anmerkung 5, 6 und 8 zum Begriff gelöscht.]

3.3

Aufrechterhaltung der Betriebsfähigkeit

Fähigkeit einer *Organisation* (3.31), die Belieferung mit *Produkten und Dienstleistungen* (3.41) innerhalb akzeptabler Zeiträume mit zuvor festgelegter Kapazität im Zusammenhang mit einer *Störung* (3.12) fortzusetzen

[QUELLE: ISO 22300:2018, 3.24, geändert]

3.4

Business Continuity Management System BCMS

Managementsystem (3.25) zur *Aufrechterhaltung der Betriebsfähigkeit* (3.3)

Anmerkung 1 zum Begriff: Das Managementsystem umfasst den organisatorischen Aufbau, Leitlinien, Planungstätigkeiten (*Planung* (3.36), *Tätigkeit* (3.1)), Verantwortlichkeiten, *Verfahren* (3.39), *Prozesse* (3.40) und Ressourcen

[QUELLE: ISO 22300:2018, 3.26, geändert]

3.5

Plan zur Aufrechterhaltung der Betriebsfähigkeit

dokumentierte Informationen (3.13), die eine *Organisation* (3.31) dabei leiten, auf eine *Störung* (3.12) zu reagieren und die Belieferung mit Produkten und Dienstleistungen, die den Zielen der Aufrechterhaltung der Betriebsfähigkeit entsprechen, fortzusetzen, wieder aufzunehmen und wiederherzustellen

[QUELLE: ISO 22300:2018, 3.27, geändert. Anmerkung 1 zum Begriff gelöscht.]

3.6

Business Impact Analyse

Prozess (3.40) der Analyse des *Einflusses* (3.18) einer *Störung* (3.12) auf die *Organisation* (3.31)

Anmerkung 1 zum Begriff: Das Ergebnis ist eine Feststellung und Begründung der *Anforderungen* (3.45) an die *Aufrechterhaltung der Betriebsfähigkeit* (3.3).

[QUELLE: ISO 22300:2018, 3.29, geändert. Anmerkung 1 zum Begriff hinzugefügt.]

3.7

Kompetenz

Fähigkeit, Wissen und Fertigkeiten anzuwenden, um beabsichtigte Ergebnisse zu erzielen

[QUELLE: ISO 22300:2018, 3.44]

3.8

Übereinstimmung

Erfüllen einer *Anforderung* (3.45)

[QUELLE: ISO 22300:2018, 3.45]

3.9

Auswirkung

Ergebnis eines *Ereignisses* (3.16), welches die *Ziele* (3.30) betrifft

Anmerkung 1 zum Begriff: Eine Auswirkung kann gewiss oder ungewiss sein und sich direkt oder indirekt bzw. positiv oder negativ auf Ziele auswirken.

Anmerkung 2 zum Begriff: Auswirkungen können qualitativ oder quantitativ beschrieben werden.

Anmerkung 3 zum Begriff: Jede Auswirkung kann durch kumulative Effekte eskalieren.

[QUELLE: ISO 31000:2018, 3.6]

3.10

ständige Verbesserung

wiederkehrende *Tätigkeit* (3.1) zur *Leistungssteigerung* (3.33)

[QUELLE: ISO 22300:2018, 3.48]

3.11

Korrekturmaßnahme

Maßnahme zum Beseitigen der Ursache einer *Nichtkonformität* (3.28) und zum Verhindern des erneuten Auftretens

Anmerkung 1 zum Begriff: Im Fall anderer unerwünschter Ergebnisse sind Maßnahmen notwendig, um die Ursachen zu verringern oder zu beseitigen und um den *Einfluss* (3.18) gering zu halten oder wiederholtes Auftreten zu verhindern. Solche Maßnahmen befinden sich außerhalb des Konzeptes der „Korrekturmaßnahme“ im Sinne dieser Definition.

[QUELLE: ISO 22300:2018, 3.54]

3.12

Störung

Zwischenfall (3.19), ob vorhergesehen oder unvorhergesehen, der entsprechend den *Zielsetzungen* (3.30) einer *Organisation* (3.31) eine ungeplante, negative Abweichung von der erwarteten Lieferung von Produkten und Dienstleistungen (3.41) verursacht

[QUELLE: ISO 22300:2018, 3.70, geändert.]

3.13

dokumentierte Information

Information (3.20), die von einer *Organisation* (3.31) gelenkt und aufrechterhalten werden muss, und das Medium, auf dem sie enthalten ist

Anmerkung 1 zum Begriff: Eine dokumentierte Information kann jegliches Format haben, auf einem beliebigen Medium vorliegen und aus jeder erdenklichen Quelle stammen.

Anmerkung 2 zum Begriff: Eine dokumentierte Information kann Bezug nehmen auf:

das *Managementsystem* (3.25), einschließlich damit verbundener *Prozesse* (3.40);

zusammengestellte Informationen, die die Organisation in die Lage versetzen, arbeiten zu können (Dokumentation);

den Nachweis erzielter Ergebnisse (*Aufzeichnungen* (3.43)).

[QUELLE: ISO 22300:2018, 3.72]

3.14

Effektivität

Ausmaß, in dem geplante *Tätigkeiten* (3.1) umgesetzt und geplante Ergebnisse erreicht werden

[QUELLE: ISO 22300:2018, 3.76]

3.15

Notfall

plötzliches, dringendes, normalerweise unvorhergesehenes Vorkommnis oder *Ereignis* (3.16), das unverzügliche Maßnahmen erfordert

Anmerkung 1 zum Begriff: Ein Notfall ist üblicherweise eine *Störung* (3.12) oder ein Zustand, die/der zwar oftmals vorhergesehen oder vorbereitet werden kann, sich aber selten genau voraussagen lässt.

[QUELLE: ISO 22300:2018, 3.77]

3.16

Ereignis

Eintritt oder Veränderung einer bestimmten Kombination von Umständen

Anmerkung 1 zum Begriff: Ein Ereignis kann einmal oder mehrmals eintreten und mehrere Ursachen und mehrere *Auswirkungen* (3.9) haben.

Anmerkung 2 zum Begriff: Ein Ereignis kann auch etwas sein, das erwartet wird und nicht eintritt oder etwas, das unerwartet eintritt.

Anmerkung 3 zum Begriff: Ein Ereignis kann eine Risikoquelle sein.

[QUELLE: ISO 31000:2018, 3.5]

3.17

Übung

Prozess (3.40) des Trainierens, Bewertens, Übens und Verbesserns der *Leistung* (3.33) innerhalb einer *Organisation* (3.31)

Anmerkung 1 zum Begriff: Übungen können für die Überprüfung von Leitlinien, Plänen, *Verfahren* (3.39), *Schulungen* (3.54), Ausrüstung und organisationsübergreifenden Vereinbarungen genutzt werden, für die Aufklärung und Schulung des *Personals* (3.35) für Rollen und Verantwortlichkeiten, zur Verbesserung der organisationsübergreifenden Koordination und Kommunikation, zur Ermittlung von Fehlbeständen in den Ressourcen, zur Verbesserung der Einzelleistung und zur Bestimmung von Verbesserungsmöglichkeiten, und sie können eine geregelte Möglichkeit darstellen, das Improvisationsvermögen zu schulen. Eine Übung setzt keine Erwartung von Bestehen oder Nichtbestehen voraus.

Anmerkung 2 zum Begriff: Siehe auch *Überprüfung* (3.52).

[QUELLE: ISO 22300:2018, 3.83, geändert, „Eine Übung setzt keine Erwartung von Bestehen oder Nichtbestehen voraus.“ wurde hinzugefügt.]

3.18

Einfluss

Ergebnis einer Störung (3.12), welche die Zielsetzungen (3.30) betrifft

[QUELLE: ISO 22300:2018, 3.107, geändert.]

3.19

Zwischenfall

Ereignis (3.16), das eine *Störung* (3.12), ein Verlust, ein *Notfall* (3.15) oder eine Krise sein kann oder dazu führen könnte

[QUELLE: ISO 22300:2018, 3.111, geändert.]

3.20

Informationen

Daten, die verarbeitet, organisiert und korreliert werden, um Sinn herzustellen

[QUELLE: ISO 22300:2018, 3.116]

3.21

interessierte Partei

Anspruchsgruppe

Person oder *Organisation* (3.31), die eine Entscheidung oder *Tätigkeit* (3.1) beeinflussen kann, die davon beeinflusst sein kann, oder die sich davon beeinflusst fühlen kann

BEISPIEL Kunden, Eigentümer, *Personal* (3.35), Anbieter, Bankiers, Regulierungsbehörden, Gewerkschaften, Partner oder die Gesellschaft, die Wettbewerber oder opponierende Interessengruppen einschließen kann.

Anmerkung 1 zum Begriff: Ein Entscheidungsträger kann eine interessierte Partei sein.

Anmerkung 2 zum Begriff: Betroffene Gemeinschaften und die lokale Bevölkerung werden als externe interessierter Parteien angesehen.

[QUELLE: ISO 22300:2018, 3.124, geändert. Das Beispiel wurde geändert. Anmerkung 3 zum Begriff wurde gelöscht.]

3.22

internes Audit

Audit (3.2), das durch eine *Organisation* (3.31) selbst oder im Auftrag dieser zum Zwecke der Managementüberprüfung (*Management* (3.24), *Überprüfung* (3.47)) und für andere interne Zwecke durchgeführt wird und das die Grundlage für eine durch die Organisation verfasste *Konformitätserklärung* (3.8) bilden kann

Anmerkung 1 zum Begriff: In vielen Fällen, und insbesondere bei kleineren Organisationen, kann Unabhängigkeit durch die Freiheit von der Verantwortung für die auditierte *Tätigkeit* (3.1) demonstriert werden.

[QUELLE: ISO 22300:2018, 3.126]

3.23

Wahrscheinlichkeit

Möglichkeit, dass etwas geschieht

Anmerkung 1 zum Begriff: In der Terminologie des *Risikomanagements* (3.50) bezeichnet der Begriff „Wahrscheinlichkeit“ die Möglichkeit, dass etwas geschieht, gleichgültig ob diese Möglichkeit objektiv oder subjektiv, qualitativ oder quantitativ definiert, gemessen oder bestimmt und mit allgemeinen Begriffen oder mathematisch (z. B. durch die statistische Wahrscheinlichkeit oder die Häufigkeit in einem bestimmten Zeitraum) beschrieben wird.

Anmerkung 2 zum Begriff: Der englische Begriff „likelihood“ hat in einigen Sprachen keine direkte Entsprechung, wo für „likelihood“ (subjektive Wahrscheinlichkeit) und „probability“ (objektive, mathematische Wahrscheinlichkeit) oft ein und dasselbe Wort verwendet wird. In der englischen Sprache ist der Begriff „probability“ jedoch oftmals sehr eng als mathematischer Begriff definiert. Deshalb wird in der englischen Terminologie des Risikomanagements der Begriff „likelihood“ mit der Absicht verwendet, dass er dieselbe weit gefasste Bedeutung haben sollte wie der Begriff „Wahrscheinlichkeit“ in vielen anderen Sprachen.

[QUELLE: ISO 31000:2018, 3.7]

3.24

Management

koordinierte *Tätigkeiten* (3.1) zur Steuerung und Lenkung einer *Organisation* (3.31)

[QUELLE: ISO 22300:2018, 3.135]

3.25

Managementsystem

Satz zusammenhängender oder sich gegenseitig beeinflussender Elemente einer *Organisation* (3.31), zur Festlegung von *Leitlinien* (3.37) und *Zielsetzungen* (3.30) sowie *Prozessen* (3.40) zum Erreichen dieser Zielsetzungen

Anmerkung 1 zum Begriff: Ein Managementsystem kann auf einen einzelnen Bereich oder auf verschiedene Bereiche ausgerichtet sein.

Anmerkung 2 zum Begriff: Zu den Elementen des Systems gehören Struktur, Rollen und Verantwortlichkeiten, *Planung* (3.36) und Betrieb der Organisation.

Anmerkung 3 zum Begriff: Der Anwendungsbereich eines Managementsystems darf die Gesamtheit der Organisation, bestimmte und identifizierte Funktionen der Organisation, bestimmte und festgelegte Abteilungen der Organisation oder eine oder mehrere Funktionen innerhalb einer Gruppe von Organisationen umfassen.

[QUELLE: ISO 22300:2018, 3.137. Anmerkung 3 wurde geändert, „darf“ wurde anstelle von „kann“ benutzt.]

3.26

Messung

Prozess (3.40) zum Bestimmen eines Werts

[QUELLE: ISO 22300:2018, 3.143]

3.27

Überwachung

Überprüfung des Zustands eines Systems, eines *Prozesses* (3.40) oder einer *Tätigkeit* (3.1)

[QUELLE: ISO 22300:2018, 3.147, geändert.]

3.28

Nichtkonformität

Nichterfüllung einer *Anforderung* (3.45)

[QUELLE: ISO 22300:2018, 3.149]

3.29

Objekt

einzelne und eindeutige Einheit, die sich identifizieren lässt

[QUELLE: ISO 22300:2018, 3.151]

3.30

Zielsetzung

zu erreichendes Ergebnis

Anmerkung 1 zum Begriff: Eine Zielsetzung kann strategisch, taktisch oder betrieblich sein.

Anmerkung 2 zum Begriff: Zielsetzungen können sich auf verschiedene Bereiche beziehen (z. B. finanzielle, gesundheits-, sicherheits- und umweltbezogene Zielsetzungen) und können auf verschiedenen Ebenen auftreten (z. B. strategisch, organisationsweit, Projekt, Produkt und *Prozess* (3.40)).

Anmerkung 3 zum Begriff: Eine Zielsetzung kann anderweitig ausgedrückt werden, z. B. als beabsichtigtes Ergebnis, Zweck, betriebstechnisches Kriterium, oder durch Verwendung anderer Worte mit ähnlicher Bedeutung (z. B. Zielvorgabe, Zielstellung oder Einzelziel).

Anmerkung 4 zum Begriff: Im Zusammenhang mit *Business Continuity Management Systemen* (3.4) werden zum Erreichen bestimmter Ergebnisse Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit durch die Organisation in Übereinstimmung mit deren *Leitlinien* (3.37) festgelegt.

[QUELLE: ISO 22300:2018, 3.30. Anmerkung 4 zum Begriff wurde geändert, um BCMS wiederzugeben.]

3.31

Organisation

Einzelperson oder Gruppe von Menschen mit eigenen Aufgabenbereichen verbunden mit Verantwortlichkeiten, Befugnissen und Beziehungen, um eigene *Zielsetzungen* (3.30) zu erreichen

Anmerkung 1 zum Begriff: Das Konzept einer Organisation umfasst, ist jedoch nicht begrenzt auf Ein-Mann-Unternehmen, Unternehmen, Kapitalgesellschaften, Firmen, Wirtschaftsunternehmen, Behörden, Partnerschaften, Wohlfahrtseinrichtungen oder Anstalten oder Teile bzw. Kombinationen davon, eingetragen oder nicht, öffentlich oder privat.

Anmerkung 2 zum Begriff: Bei Organisationen mit mehr als einer Betriebseinheit kann eine einzelne Einheit als Organisation bezeichnet werden.

[QUELLE: ISO 22300:2018, 3.31]

3.32

ausgliedern

Treffen einer Übereinkunft, der zufolge eine Organisation einen Teil der Funktionen oder *Prozesse* (3.40) einer externen *Organisation* (3.31) überträgt

Anmerkung 1 zum Begriff: Eine externe Organisation ist außerhalb des Anwendungsbereichs des *Managementsystems* (3.25), obwohl sich die ausgegliederte Funktion oder der ausgegliederte Prozess innerhalb des Anwendungsbereichs dieses Managementsystems befindet.

[QUELLE: ISO 22300:2018, 3.160]

3.33

Leistung

messbares Ergebnis

Anmerkung 1 zum Begriff: Leistung kann sich auf quantitative oder qualitative Ergebnisse beziehen.

Anmerkung 2 zum Begriff: Leistung kann sich auf das *Management* (3.24) von *Tätigkeiten* (3.1), *Prozessen* (3.40), *Produkten und Dienstleistungen* (3.41), Systemen oder *Organisationen* (3.31) beziehen.

[QUELLE: ISO 22300:2018, 3.157, geändert – Verweisung auf „Produkte und Dienstleistungen“.]

3.34

Leistungsbewertung

Prozess (3.40) zur Ermittlung messbarer Ergebnisse anhand der festgelegten Kriterien

[QUELLE: ISO 22300:2018, 3.168, geändert, „anhand der festgelegten Kriterien“ wurde hinzugefügt und „zur Ermittlung“ wurde anstatt „der Ermittlung“ benutzt.]

3.35

Personal

Personen, die unter Beaufsichtigung durch oder für eine *Organisation* (3.31) arbeiten

Anmerkung 1 zum Begriff: Der Begriff umfasst Angestellte, Teilzeitbeschäftigte und Leiharbeitskräfte, ist jedoch nicht auf diese beschränkt.

[QUELLE: ISO 22300:2018, 3.169]

3.36

Planung

Teil des *Managements* (3.24), der sich darauf konzentriert, *Zielsetzungen* (3.30) für die *Aufrechterhaltung der Betriebsfähigkeit* (3.3) festzulegen und erforderliche betriebliche *Prozesse* (3.30) und damit verbundene Ressourcen zu bestimmen, die erforderlich sind, um die Zielsetzungen für die Aufrechterhaltung der Betriebsfähigkeit zu erfüllen

[QUELLE: ISO 22300:2018, 3.170, geändert, um die „Aufrechterhaltung der Betriebsfähigkeit“ wiederzugeben.]

3.37

Politik

Absichten und Ausrichtung einer *Organisation* (3.31), wie von der *obersten Leitung* (3.53) formell ausgedrückt

[QUELLE: ISO 22300:2018, 3.171]