

ISO 22301:2019



EN ISO 22301:2019

NBN EN ISO 22301:2019



**Sicherheit und Resilienz - Business Continuity Management
System - Anforderungen (ISO 22301:2019)**

Gültig ab 28-11-2019

Ersetzt NBN EN ISO 22301:2014

ICS: 03.100.01, 03.100.70

EUROPÄISCHE NORM
 EUROPEAN STANDARD
 NORME EUROPÉENNE

EN ISO 22301

November 2019

ICS 03.100.01; 03.100.70

Ersetzt EN ISO 22301:2014

Deutsche Fassung

**Sicherheit und Resilienz - Business Continuity Management
 System - Anforderungen (ISO 22301:2019)**

Security and resilience - Business continuity
 management systems - Requirements (ISO
 22301:2019)

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

Diese Europäische Norm wurde vom CEN am 14. Oktober 2019 angenommen.

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

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

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



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

CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich.....	10
2 Normative Verweisungen	10
3 Begriffe	10
4 Kontext der Organisation	17
4.1 Verstehen der Organisation und ihres Kontextes	17
4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien	17
4.2.1 Allgemeines	17
4.2.2 Rechtliche und behördliche Anforderungen	17
4.3 Festlegung des Anwendungsbereichs des Business Continuity Management Systems.....	17
4.3.1 Allgemeines	17
4.3.2 Anwendungsbereich des Business Continuity Management Systems.....	18
4.4 Business Continuity Management System.....	18
5 Führung.....	18
5.1 Führung und Verpflichtung.....	18
5.2 Politik.....	19
5.2.1 Festlegung der Politik zur Aufrechterhaltung der Betriebsfähigkeit	19
5.2.2 Bekanntmachung der Politik zur Aufrechterhaltung der Betriebsfähigkeit.....	19
5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation.....	19
6 Planung.....	19
6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten	19
6.1.1 Bestimmung von Auditrisiken und -möglichkeiten.....	19
6.1.2 Umgang mit Risiken und Chancen.....	20
6.2 Ziele zur Aufrechterhaltung der Betriebsfähigkeit und Planung zu deren Erreichung	20
6.2.1 Festlegung von Zielen zur Aufrechterhaltung der Betriebsfähigkeit.....	20
6.2.2 Bestimmung der Ziele zur Aufrechterhaltung der Betriebsfähigkeit	20
6.3 Planung von Änderungen am BCMS.....	21
7 Unterstützung	21
7.1 Ressourcen.....	21
7.2 Kompetenz	21
7.3 Bewusstsein.....	21
7.4 Kommunikation	22
7.5 Dokumentierte Information.....	22
7.5.1 Allgemeines	22
7.5.2 Erstellen und Aktualisieren.....	22
7.5.3 Lenkung dokumentierter Information.....	22
8 Betrieb	23
8.1 Betriebliche Planung und Steuerung	23
8.2 Business-Impact-Analyse und Risikobeurteilung	23
8.2.1 Allgemeines	23
8.2.2 Business-Impact-Analyse.....	24

8.2.3	Risikobeurteilung.....	24
8.3	Strategien und Lösungen zur Aufrechterhaltung der Betriebsfähigkeit	25
8.3.1	Allgemeines	25
8.3.2	Identifizierung der Strategien und Lösungen.....	25
8.3.3	Auswahl der Strategien und Lösungen.....	25
8.3.4	Ressourcenbedarf	25
8.3.5	Umsetzung von Lösungen.....	26
8.4	Pläne und Verfahren zur Aufrechterhaltung der Betriebsfähigkeit.....	26
8.4.1	Allgemeines	26
8.4.2	Reaktionsstruktur.....	26
8.4.3	Warnung und Kommunikation.....	27
8.4.4	Pläne zur Aufrechterhaltung der Betriebsfähigkeit.....	28
8.4.5	Wiederherstellung	29
8.5	Übungsprogramm	29
8.6	Bewertung der Dokumentation und Fähigkeiten zur Aufrechterhaltung der Betriebsfähigkeit.....	29
9	Bewertung der Leistung.....	30
9.1	Überwachung, Messung, Analyse und Bewertung.....	30
9.2	Internes Audit.....	30
9.2.1	Allgemeines	30
9.2.2	Auditprogramm(e).....	30
9.3	Managementbewertung.....	31
9.3.1	Allgemeines	31
9.3.2	Eingaben für die Managementbewertung.....	31
9.3.3	Ergebnisse der Managementbewertung.....	31
10	Verbesserung.....	32
10.1	Nichtkonformität und Korrekturmaßnahmen.....	32
10.2	Fortlaufende Verbesserung.....	33
	Literaturhinweise.....	34

EN ISO 22301:2019 (D)**Europäisches Vorwort**

Dieses Dokument (EN 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 AFNOR gehalten wird.

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

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

Dieses Dokument ersetzt EN ISO 22301:2014.

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

Anerkennungsnotiz

Der Text von ISO 22301:2019 wurde von CEN als EN 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.

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

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO 22301:2012), die technisch überarbeitet wurde. Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

- es wurden die ISO-Anforderungen für Managementsystemnormen, die sich seit 2012 weiterentwickelt haben, angewendet;
- die Anforderungen wurden präzisiert, ohne neue Anforderungen hinzuzufügen;
- bereichsspezifische Anforderungen an die Aufrechterhaltung der Betriebsfähigkeit befinden sich nun fast vollständig in Abschnitt 8;
- Abschnitt 8 wurde neu strukturiert, um ein besseres Verständnis der Schlüsselanforderungen zu ermöglichen;
- eine Reihe an bereichsspezifischen Begriffen in Zusammenhang mit der Aufrechterhaltung der Betriebsfähigkeit wurde abgeändert, um die Übersichtlichkeit zu verbessern und den aktuellen Erkenntnissen Rechnung zu tragen.

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 legt die Struktur und Anforderungen für die Implementierung und Aufrechterhaltung eines Business Continuity Management Systems (BCMS) fest, das der Größe und Art der Auswirkungen angemessen ist, die eine Organisation nach einer Störung akzeptieren darf oder nicht.

Die Ergebnisse der Aufrechterhaltung eines BCMS werden durch rechtliche, behördliche, organisationstechnische und industrielle Anforderungen geprägt sowie durch bereitgestellte Produkte und 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 Betriebens 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) eine Politik;
- b) kompetente Personen mit festgelegten Verantwortlichkeiten;
- c) Managementprozesse in Bezug auf:
 - 1) Politik;
 - 2) Planung;
 - 3) Umsetzung und Betrieb;
 - 4) Leistungsbewertung;
 - 5) Managementbewertung;
 - 6) fortlaufende Verbesserung;
- d) dokumentierte Informationen, die die betriebliche Kontrolle unterstützen und eine Bewertung der Leitung ermöglichen.

0.2 Vorteile eines Business Continuity Management Systems

Der Zweck eines BCMS ist das Vorbereiten, Bereitstellen und Aufrechterhalten von Kontrollen und des Vermögens, die allgemeine Fähigkeit eines Unternehmens zu steuern, den Betrieb während einer Störung aufrechtzuerhalten. Ist dies erreicht, wird die Organisation:

- a) aus geschäftlicher Sicht:
 - 1) seine strategischen Zielsetzungen unterstützen;
 - 2) einen Wettbewerbsvorteil kreieren;
 - 3) seinen Ruf und seine Glaubwürdigkeit schützen und verbessern;
 - 4) zur Belastbarkeit der Organisation beitragen;
- b) aus finanzieller Sicht:
 - 1) rechtliche und finanzielle Gefahren verringern;
 - 2) direkte und indirekte Kosten von Störungen reduzieren;
- c) aus der Sicht der interessierten Parteien:
 - 1) Leben, Eigentum und die Umwelt schützen;
 - 2) Erwartungen der interessierten Parteien berücksichtigen;
 - 3) Vertrauen in die Erfolgsfähigkeit des Unternehmens schaffen;
- d) aus Sicht der internen Prozesse:
 - 1) die Fähigkeit verbessern, auch während einer Störung betriebsfähig zu bleiben;
 - 2) proaktive Kontrolle der Risiken effektiv und effizient demonstrieren;
 - 3) sich mit betrieblichen Anfälligkeiten befassen.

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

Dieses Dokument wendet den Planen- (einführen), Umsetzen- (implementieren und durchführen), Überprüfen- (überwachen und überprüfen) und Handeln- (aufrechterhalten und verbessern) Zyklus an (en: Plan-Do-Check-Act, PDCA), um das BCMS einer Organisation umzusetzen und aufrechtzuerhalten sowie dessen Effektivität ständig zu verbessern.

Dies stellt ein bestimmtes Ausmaß an Übereinstimmung mit anderen Normen zu Managementsystemen, wie z. B. ISO 9001, ISO 14001, ISO/IEC 20000-1, ISO/IEC 27001 und ISO 28000 sicher und unterstützt dadurch die einheitliche und integrierte Umsetzung und den Betrieb mit ähnlichen Managementsystemen.

In Übereinstimmung mit dem PDCA-Zyklus behandeln Abschnitt 4 bis Abschnitt 10 die folgenden Bestandteile:

- Abschnitt 4 führt die Anforderungen ein, die notwendig sind, um den Kontext des BCMS, der für die Organisation gilt, sowie Bedürfnisse, Anforderungen und den Anwendungsbereich festzulegen.

EN ISO 22301:2019 (D)

- Abschnitt 5 fasst die Anforderungen zusammen, die für die Rolle der obersten Leitung innerhalb des BCMS gelten, und wie die Führung ihre Erwartungen gegenüber der Organisation durch eine Erklärung zur Politik ausdrückt.
- Abschnitt 6 beschreibt Anforderungen für die Einführung strategischer Zielsetzungen und Leitsätze für das BCMS als Ganzes.
- Abschnitt 7 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 die geforderte dokumentierte Information erfasst, gelenkt, erhalten und aufbewahrt wird.
- Abschnitt 8 legt die Anforderungen an die Aufrechterhaltung der Betriebsfähigkeit fest, bestimmt den Umgang mit diesen und entwickelt Verfahren für die Leitung einer Organisation während einer Störung.
- Abschnitt 9 fasst die Anforderungen zusammen, die zum Messen der Leistung der Betriebsfähigkeit sowie der Übereinstimmung des BCMS mit diesem Dokument sowie zur Durchführung einer Managementbewertung erforderlich sind.
- Abschnitt 10 identifiziert die Abweichung vom BCMS und reagiert auf diese durch fortlaufende Verbesserungen und Korrekturmaßnahmen.

0.5^{N1)} Inhalte dieses Dokuments

Dieses Dokument entspricht den Anforderungen von ISO an Managementsystemnormen. Diese Anforderungen schließen eine Grundstruktur, ein einheitlicher Basistext und gemeinsame Benennungen und Basisdefinitionen ein, 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 gebracht oder in diese integriert werden können.

Dieses Dokument enthält Anforderungen, die von einer Organisation zur Verwirklichung 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 eine externe Partei; oder
- Erlangen einer Zertifizierung/Registrierung ihres BCMS durch eine externe Organisation.

Abschnitte 1 bis 3 in diesem Dokument legen den Anwendungsbereich, die normativen Verweisungen und Begriffe fest, die für die Verwendung dieses Dokuments gelten. Abschnitte 4 bis 10 enthalten die Anforderungen, die zur Beurteilung der Konformität mit diesem Dokument verwendet werden.

N1) Nationale Fußnote: Die Nummerierung entspricht der ISO-Originalfassung.

In diesem Dokument werden die folgenden Verbformen verwendet:

- a) „muss“ gibt eine Anforderung an;
- b) „sollte“ gibt eine Empfehlung an;
- c) „darf“ gibt eine Zulässigkeit an;
- d) „kann“ gibt eine Möglichkeit oder ein Vermögen an.

Als „ANMERKUNG“ gekennzeichnete Informationen dienen als Anleitung zum Verständnis oder zur Erläuterung der zugehörigen Anforderung. Als „Anmerkung zu Begriff“ gekennzeichnete Informationen im Abschnitt 3 dienen der zusätzlichen Erläuterung zur Ergänzung der terminologischen Daten und können Festlegungen im Zusammenhang mit der Verwendung eines Begriffs enthalten.

EN ISO 22301:2019 (D)**1 Anwendungsbereich**

Dieses Dokument legt Anforderungen fest, um ein Managementsystem zu verwirklichen, aufrechtzuerhalten und 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 in diesem Dokument aufgeführten Anforderungen 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 verwirklichen, aufrechterhalten und verbessern wollen;
- b) eine Übereinstimmung mit der erklärten Politik zur Aufrechterhaltung der Betriebsfähigkeit sicherstellen wollen;
- c) die Fähigkeit benötigen, die Belieferung mit Produkten und Dienstleistungen mit einer akzeptablen, zuvor festgelegten Kapazität während einer Störung fortzusetzen;
- d) anstreben, ihre Resilienz durch die effektive Anwendung des BCMS zu verbessern.

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

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO 22300, *Security and resilience — Vocabulary*

3 Begriffe

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

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

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

ANMERKUNG Die nachfolgend aufgeführten Begriffe ersetzen die in ISO 22300:2018 genannten.

3.1**Tätigkeit**

Satz von einer oder mehreren Aufgaben mit einem definierten Ergebnis

[QUELLE: ISO 22300:2018, 3.1, modifiziert — die Definition wurde ersetzt und das Beispiel gelöscht.]