

DIN EN ISO 22301

ICS 03.100.01

Einsprüche bis 2014-04-21

Entwurf**Sicherheit und Schutz des Gemeinwesens –
Aufrechterhaltung der Betriebsfähigkeit –
Anforderungen (ISO 22301:2012);
Deutsche Fassung FprEN ISO 22301:2014**

Societal security –
Business continuity management systems –
Requirements (ISO 22301:2012);
German version FprEN ISO 22301:2014

Sécurité sociétale –
Gestion de la continuité des affaires –
Exigences (ISO 22301:2012);
Version allemande FprEN ISO 22301:2014

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2014-02-21 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

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

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

Gesamtumfang 36 Seiten

Normenausschuss Feuerwehrwesen (FNFW) im DIN

Nationales Vorwort

Der Text von ISO 22301:2012 wurde vom Technischen Komitee ISO/TC 223 „Societal Security“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO 22301:2012 durch das Technische Komitee CEN/TC 391 „Schutz und Sicherheit der Bürger“ ohne Änderungen übernommen, dessen Sekretariat vom NEN (Niederlande) gehalten wird.

Für die deutsche Mitarbeit ist das Gremium NA 031-05 FBR „Fachbereichsausschuss Sicherheit und Schutz des Gemeinwesens - SpA zu ISO/TC 223 Societal security“ im Normenausschuss Feuerwehrwesen (FNFW) im DIN verantwortlich.

Sicherheit und Schutz des Gemeinwesens — Aufrechterhaltung der Betriebsfähigkeit — Anforderungen (ISO 22301:2012)

Sécurité sociétale — Gestion de la continuité des affaires — Exigences (ISO 22301:2012)

Societal security — Business continuity management systems — Requirements (ISO 22301:2012)

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: einstufiges Annahmeverfahren
Dokument-Sprache: D

STD Version 2.5a

Inhalt

	Seite
Vorwort	4
0 Einleitung.....	5
0.1 Allgemeines	5
0.2 Das Planen-Durchführen-Prüfen-Handeln-Modell (PDCA-Modell)	5
0.3 Bestandteile des PDCA-Modells in dieser Internationalen Norm	7
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	8
4 Kontext der Organisation.....	16
4.1 Verstehen der Organisation und ihres Kontextes	16
4.2 Verstehen der Bedürfnisse und Erwartungen der Interessensgruppen	17
4.2.1 Allgemeines	17
4.2.2 Rechtliche und behördliche Anforderungen	17
4.3 Festlegung des Anwendungsbereichs des Managementsystems zur Aufrechterhaltung der Betriebsfähigkeit	17
4.3.1 Allgemeines	17
4.3.2 Anwendungsbereich des BCMS.....	17
4.4 Managementsystem zur Aufrechterhaltung der Betriebsfähigkeit.....	18
5 Führung	18
5.1 Führung und Selbstverpflichtung	18
5.2 Selbstverpflichtung der Leitung.....	18
5.3 Leitlinien	19
5.4 Funktionen, Verantwortlichkeiten und Befugnisse innerhalb der Organisation	20
6 Planung	20
6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten	20
6.2 Zielsetzungen zur Aufrechterhaltung der Betriebsfähigkeit und Pläne zur Zielerreichung	20
7 Unterstützung.....	21
7.1 Ressourcen	21
7.2 Kompetenz.....	21
7.3 Bewusstseinsbildung.....	21
7.4 Kommunikation	22
7.5 Dokumentation.....	22
7.5.1 Allgemeines	22
7.5.2 Erstellung und Aktualisierung.....	23
7.5.3 Dokumentationskontrolle	23
8 Betrieb.....	24
8.1 Ablaufplanung und Kontrolle	24
8.2 Analyse der Auswirkung auf die Betriebsfähigkeit und Risikobewertung	24
8.2.1 Allgemeines	24
8.2.2 Analyse der Auswirkung auf die Betriebsfähigkeit.....	24
8.2.3 Risikobewertung	25
8.3 Strategie zur Aufrechterhaltung der Betriebsfähigkeit.....	25
8.3.1 Festlegung und Auswahl	25
8.3.2 Ressourcenbedarf	25
8.3.3 Schutz und Schadensminderung.....	26

8.4	Einführung und Umsetzung von Maßnahmen zur Aufrechterhaltung der Betriebsfähigkeit.....	26
8.4.1	Allgemeines	26
8.4.2	Struktur zur Gefahrenabwehr.....	27
8.4.3	Warnung und Kommunikation	27
8.4.4	Pläne zur Aufrechterhaltung der Betriebsfähigkeit	28
8.4.5	Wiederherstellung	29
8.5	Übungen und Überprüfungen	29
9	Leistungsüberprüfung	29
9.1	Überwachung, Messung, Analyse und Bewertung.....	29
9.1.1	Allgemeines	29
9.1.2	Bewertung der Verfahren zur Aufrechterhaltung der Betriebsfähigkeit.....	30
9.2	Internes Audit	30
9.3	Überprüfung des Managements	31
10	Verbesserung.....	33
10.1	Nichtkonformität und Korrekturmaßnahmen	33
10.2	Ständige Verbesserung	33
	Literaturhinweise.....	34

Vorwort

Der Text von ISO 22301:2012 wurde vom Technischen Komitee ISO/TC 223 „Societal Security“ der Internationalen Organisation für Normung (ISO) erarbeitet und als FprEN ISO 22301:2014 durch das Technische Komitee CEN/TC 391 „Schutz und Sicherheit der Bürger“ übernommen, dessen Sekretariat vom NEN gehalten wird.

Dieses Dokument ist derzeit zum einstufigen Annahmeverfahren vorgelegt.

Anerkennungsnotiz

Der Text von ISO 22301:2012 wurde vom CEN als FprEN ISO 22301:2014 ohne irgendeine Abänderung genehmigt.

0 Einleitung

0.1 Allgemeines

Diese Internationale Norm legt Anforderungen für die Erstellung und den Umgang mit effektiven Managementsystemen zur Aufrechterhaltung der Betriebsfähigkeit (BCMS, en: business continuity management system) fest.

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 Einführens und Betreibens von Kontrollen und Maßnahmen für das Management der Gesamtfähigkeit einer Organisation, mit Vorfällen mit Betriebsunterbrechung umzugehen;
- des Überwachens und Überprüfens der Leistung und des Wirkungsgrads des BCMS; und
- einer ständigen Verbesserung auf Grundlage objektiver Messungen.

Ein BCMS hat, wie jedes andere Managementsystem, folgende zentrale Bestandteile:

- a) Leitlinien;
- b) Personen mit festgelegten Verantwortlichkeiten;
- c) Managementprozess in Bezug auf:
 - 1) Leitlinien,
 - 2) Planung,
 - 3) Implementierung und Betrieb,
 - 4) Leistungsbewertung,
 - 5) Bewertung des Managements, und
 - 6) Verbesserung;
- d) Dokumentation zur Bereitstellung auditierbarer Nachweise; und
- e) jeden Managementprozess zur Aufrechterhaltung der Betriebsfähigkeit, der für die Organisation relevant ist.

Die Aufrechterhaltung der Betriebsfähigkeit trägt zu einer widerstandsfähigeren Gesellschaft bei. Es kann erforderlich sein, die Gesellschaft im weiteren Sinne und den Einfluss des Organisationsumfeldes auf die Organisation (und daher auch anderer Organisationen) in den Wiederherstellungsprozess einzubeziehen.

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

Diese Internationale Norm 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 Wirkungsgrad 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 Implementierung und den Betrieb mit ähnlichen Managementsystemen.

Bild 1 stellt dar, wie ein BCMS Interessensgruppen und Anforderungen an eine Aufrechterhaltung der Betriebsfähigkeit als Eingaben verwendet und mittels der notwendigen Maßnahmen und Prozesse Kontinuitätsergebnisse (d. h. eine gelenkte Aufrechterhaltung der Betriebsfähigkeit) erzeugt, die diese Anforderungen erfüllen.

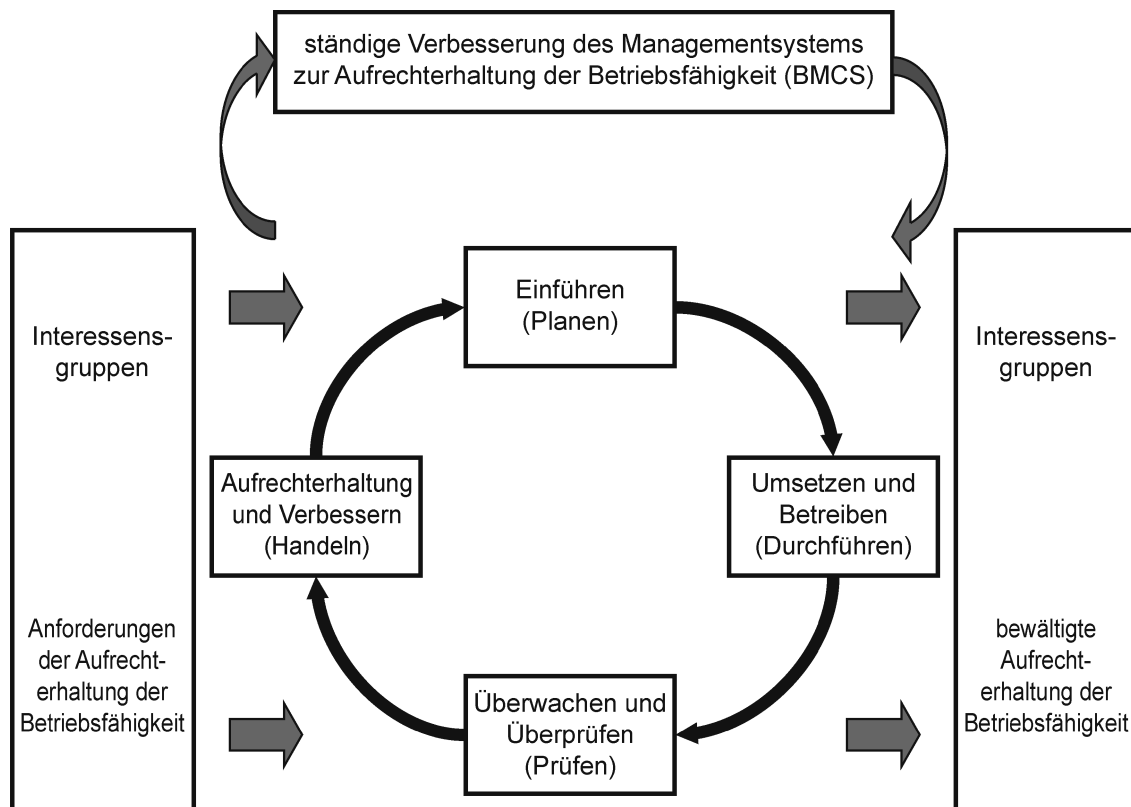


Bild 1 — An die BCMS-Prozesse angepasstes PDCA-Modell

Tabelle 1 — Erläuterungen zum PDCA-Modell

Planen (Einführen)	Einführen von Leitlinien, Zielsetzungen, Einzelziele, Kontrollen, Prozessen und Verfahren zur Aufrechterhaltung der Betriebsfähigkeit, die zur Verbesserung der Aufrechterhaltung der Betriebsfähigkeit relevant sind, und um Ergebnisse zu erzielen, die sich mit den übergeordneten Leitlinien und Zielsetzungen der Organisation in Übereinstimmung befinden.
Durchführen (Umsetzen und Ausführen)	Umsetzen und Ausführen der Leitlinien, Kontrollen, Prozesse und Verfahren.
Prüfen (Überwachen und Überprüfen)	Überwachen und Überprüfen der Leistung vor dem Hintergrund der Leitlinien und Zielsetzungen, Berichten der Ergebnisse an die Leitung zum Zwecke der Überprüfung, Festlegung und Autorisierung von Maßnahmen zur Korrektur und Verbesserung
Handeln (Aufrechterhalten und Verbessern)	Aufrechterhalten und Verbessern des BCMS durch die Ausführung von Korrekturmaßnahmen auf Grundlage der Ergebnisse der Überprüfung durch die Leitung sowie Neufassung des Anwendungsbereichs des BCMS sowie der Leitlinien und Zielsetzungen .

0.3 Bestandteile des PDCA-Modells in dieser Internationalen Norm

Innerhalb des PDCA-Modells, wie in Tabelle 1 ausgeführt, behandeln die Abschnitte 4 bis 10 dieser Internationalen Norm 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 des Leitungsgremiums innerhalb des BCMS gelten, und wie die Führung ihre Erwartungen gegenüber der Organisation durch eine Grundsatzerklärung 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. Der Inhalt von Abschnitt 6 unterscheidet sich von der Einführung von Behandlungsmöglichkeiten für Risiken, die aus der Risikobewertung stammen, sowie von den Zielsetzungen für die Wiederherstellung, die aus der Analyse der Auswirkung auf die Betriebsfähigkeit (BIA, en: business impact analysis) abgeleitet sind.

ANMERKUNG Die Anforderungen der Analyse der Auswirkung auf die Betriebsfähigkeit und des Prozesses der Risikobewertung sind ausführlich in Abschnitt 8 aufgeführt.

- Abschnitt 7 ist Bestandteil des Elements „Planen“. Er unterstützt BCMS-Abläufe, die sich auf die Festlegung von Kompetenz und die Kommunikation mit Interessensgruppen auf einer periodisch wiederkehrenden oder bedarfsorientierten Grundlage beziehen, während sie die geforderten Dokumente dokumentieren, 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 eines Vorfalles mit Betriebsunterbrechung.
- Abschnitt 9 ist Bestandteil des Elements „Prüfen“. Er fasst die Anforderungen zusammen, die zum Messen der Managementleistung zur Aufrechterhaltung der Betriebsfähigkeit sowie der Übereinstimmung des BCMS mit dieser Internationalen Norm und den Erwartungen der Leitung erforderlich sind, und strebt eine Rückmeldung der Leitung in Bezug auf Erwartungshaltungen an.
- Abschnitt 10 ist Bestandteil des Elements „Handeln“. Er identifiziert die Nichtkonformität des BCMS und reagiert auf diese durch Korrekturmaßnahmen.

1 Anwendungsbereich

Diese Internationale Norm zur Aufrechterhaltung der Betriebsfähigkeit legt Anforderungen fest, um ein dokumentiertes Managementsystem zu planen, einzuführen, umzusetzen, zu betreiben, zu überwachen, zu überprüfen, aufrechtzuerhalten und ständig zu verbessern, um sich gegen Vorfälle mit Betriebsunterbrechung zu schützen, die Wahrscheinlichkeit ihres Auftretens zu vermindern, sich auf diese vorzubereiten, auf diese zu reagieren und sich von diesen zu erholen, wenn sie auftreten.

Die Anforderungen dieser Internationalen Norm sind generischer 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.

Diese Internationale Norm beabsichtigt keine Einheitlichkeit im Aufbau eines Managementsystems zur Aufrechterhaltung der Betriebsfähigkeit (BCMS), setzt jedoch bei einer Organisation voraus, dass diese ein BCMS gestaltet, das ihren Bedürfnissen gerecht wird und die Anforderungen ihrer Interessensgruppen erfüllt. Diese Bedürfnisse werden durch rechtliche, behördliche, organisationstechnische und industrielle Anforderungen geprägt sowie durch Produkte und Dienstleistungen, eingesetzte Prozesse, Größe und Aufbau der Organisation und die Anforderungen ihrer Interessensgruppen.

Diese Internationale Norm gilt für sämtliche Arten und Größen von Organisationen, die Folgendes wollen:

- a) Einführen, Implementieren, Aufrechterhalten und Verbessern eines BMCS;
- b) Sicherstellen der Konformität mit den erklärten Leitlinien zur Aufrechterhaltung der Betriebsfähigkeit;
- c) Darstellen der Konformität gegenüber anderen;
- d) Zertifizierung/Registrierung ihres BMCS durch eine amtlich zugelassene Zertifizierungsstelle einer Drittpartei; oder
- e) Erstellung einer eigenen Konformitätsfeststellung oder einer eigenen Konformitätserklärung mithilfe dieser Internationalen Norm.

Dieses Dokument kann dazu genutzt werden, die Befähigung einer Organisation zur Erfüllung ihrer eigenen Kontinuitätsbedürfnisse und -verpflichtungen zu bewerten.

2 Normative Verweisungen

Die folgenden zitierten Dokumente, in Gänze oder in Teilen, 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).

Es gibt keine normativen Verweisungen.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1 Tätigkeit
Prozess oder Prozesse, ausgeführt von einer Organisation (oder für diese), die ein(e) oder mehrere Produkt(e) und Dienstleistung(en) erzeugt oder unterstützt

BEISPIEL Diese Prozesse umfassen Buchhaltungstätigkeiten, Call-Center, IT, Herstellung, Vertrieb.

3.2

Audit

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

ANMERKUNG 1 Ein Audit kann ein internes Audit (Erstparteien-Audit) oder ein externes Audit (Zweit- oder Drittparteien-Audit) sein und es kann ein kombiniertes Audit (Kombination zweier oder mehrerer Wissensgebiete) sein.

ANMERKUNG 2 „Auditnachweis“ und „Auditkriterium“ sind in ISO 19011 definiert.

3.3

Aufrechterhaltung der Betriebsfähigkeit

Fähigkeit einer Organisation, die Belieferung mit Produkten oder Dienstleistungen nach einem Vorfall mit Betriebsunterbrechung auf akzeptablen, zuvor festgelegten Niveaustufen fortzusetzen

[QUELLE: ISO 22300]

3.4

Management zur Aufrechterhaltung der Betriebsfähigkeit

ganzheitlicher Managementprozess, der potenzielle Bedrohungen für Organisationen und die Auswirkungen ermittelt, die diese Bedrohungen, falls sie umgesetzt werden, womöglich auf die Geschäftsabläufe haben und der ein Gerüst zum Aufbau der Belastbarkeit einer Organisation im Verbund mit der Fähigkeit einer effektiven Reaktion, die die Interessen ihrer zentralen Interessensgruppen, das Ansehen, die Marke und die wertschöpfenden Tätigkeiten sichert, bereitstellt

3.5

Managementsystem zur Aufrechterhaltung der Betriebsfähigkeit

BCMS

(en: Business Continuity Management System)

Teil des Gesamt-Managementsystems zur Einführung und Implementierung, den Betrieb sowie die Überwachung, Überprüfung, Verwaltung und Verbesserung der Aufrechterhaltung der Betriebsfähigkeit

ANMERKUNG Das Managementsystem umfasst den organisatorischen Aufbau, Leitlinien, Planungstätigkeiten, Verantwortlichkeiten, Verfahren, Prozesse und Ressourcen.

3.6

Plan zur Aufrechterhaltung der Betriebsfähigkeit

dokumentierte Verfahren, die eine Organisation dabei leiten, auf eine Störung zu reagieren, sich von dieser zu erholen, den Betrieb fortzusetzen und nach einer Störung eine zuvor festgelegte Betriebsstufe wiederherzustellen

ANMERKUNG Üblicherweise werden dadurch Ressourcen, Dienstleistungen und Tätigkeiten erfasst, die erforderlich sind, um die Aufrechterhaltung kritischer Geschäftsfunktionen sicherzustellen.

3.7

Programm zur Aufrechterhaltung der Betriebsfähigkeit

permanenter Management- und Steuerungsprozess, der durch das Leitungsgremium unterstützt und angemessen mit Ressourcen ausgestattet wird, um ein Management zur Aufrechterhaltung der Betriebsfähigkeit zu implementieren und aufrechtzuhalten

3.8

Analyse der Auswirkung auf die Betriebsfähigkeit

BIA

(en: Business Impact Analysis)

Prozess der Analyse der Tätigkeiten und des Einflusses, den die Störung des Betriebes auf diese haben kann

[QUELLE: ISO 22300]

3.9

Kompetenz

Fähigkeit, Wissen und Fertigkeiten anzuwenden, um angestrebte Ergebnisse zu erreichen