©2020 NBN. All rights reserved – PREVIEW first 10 pages

ICS: 03.100.01

Geregistreerde Belgische norm

NBN EN ISO 22301

1e uitg., augustus 2014

Normklasse: Z 01

Maatschappelijke veiligheid - Managementsystemen voor bedrijfscontinuïteit - Eisen (ISO 22301:2012)

Sécurité sociétale - Systèmes de management de la continuité d'activité - Exigences (ISO 22301:2012)

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

Toelating tot publicatie: 22 augustus 2014

Deze Europese norm EN ISO 22301:2014 heeft de status van een Belgische norm.

Deze Europese norm bestaat in drie officiële versies (Duits, Engels, Frans).

standards for .be

Bureau voor Normalisatie - Jozef II-straat 40 - 1000 Brussel - België

Tel: +32 2 738 01 12 - Fax: +32 2 733 42 64 - E-mail: info@nbn.be - NBN Online: www.nbn.be

Bank 000-3255621-10 IBAN BE41 0003 2556 2110 BIC BPOTBEB1 BTW BE0880857592

© NBN 2014

Prijsgroep: 21

©2020 NBN. All rights reserved – PREVIEW first 10 pages

ICS: 03.100.01

norme belge enregistrée

NBN EN ISO 22301

1e éd., août 2014

Indice de classement: Z 01

Sécurité sociétale - Systèmes de management de la continuité d'activité - Exigences (ISO 22301:2012)

Maatschappelijke veiligheid - Managementsystemen voor bedrijfscontinuïteit - Eisen (ISO 22301:2012)

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

Autorisation de publication: 22 août 2014

La présente norme européenne EN ISO 22301:2014 a le statut d'une norme belge.

La présente norme européenne existe en trois versions officielles (allemand, anglais, français).

standards for .be

Bureau de Normalisation - rue Joseph II 40 - 1000 Bruxelles - Belgique
Tél: +32 2 738 01 12 - Fax: +32 2 733 42 64 - E-mail: info@nbn.be - NBN Online: www.nbn.be
Banque 000-3255621-10 IBAN BE41 0003 2556 2110 BIC BPOTBEB1 TVA BE0880857592

© NBN 2014

Prix: groupe 21

©2020 NBN. All rights reserved – PREVIEW first 10 pages

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO 22301

Juli 2014

ICS 03.100.01

Deutsche Fassung

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

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

Sécurité sociétale - Systèmes de management de la continuité d'activité - Exigences (ISO 22301:2012)

Diese Europäische Norm wurde vom CEN am 17. Juli 2014 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 Management-Zentrum des CEN-CENELEC 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, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, 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: Avenue Marnix 17, B-1000 Brüssel

© 2014 CEN Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den nationalen Mitgliedern von CEN vorbehalten.

Ref. Nr. EN ISO 22301:2014 D

©2020 NBN. All rights reserved – PREVIEW first 10 pages

EN ISO 22301:2014 (D)

Inhalt

Seite

©2020 NBN. All rights reserved – PREVIEW first 10 pages

©2020 NBN. All rights reserved – PREVIEW first 10 pages

EN ISO 22301:2014 (D)

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 22301:2014 durch das Technische Komitee CEN/TC 391 „Schutz und Sicherheit der Bürger“ übernommen, dessen Sekretariat vom NEN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Januar 2015, und etwaige entgegenstehende nationale Normen müssen bis Januar 2015 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN [und/oder CENELEC] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

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

Anerkennungsnotiz

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

©2020 NBN. All rights reserved – PREVIEW first 10 pages

0 Einleitung

0.1 Allgemeines

Diese Internationale Norm legt Anforderungen für die Erstellung und den Umgang mit einem effektiven Business Continuity Management System (BCMS) fest.

Ein BCMS betont die Bedeutung:

— des Verstehens der Bedürfnisse der Organisation sowie der Notwendigkeit der Einführung von Leitlinien und Zielsetzungen für das Business Continuity Management;

— des Einführens und Betreibens von Kontrollmechanismen und Maßnahmen für das Management der Gesamtfähigkeit einer Organisation, mit Zwischenfällen mit Betriebsunterbrechung umzugehen;

— des Überwachens und Überprüfens der Leistung und der Effektivität 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) Umsetzung und Betrieb,

   4) Leistungsbewertung,

   5) Managementüberprüfung, und

   6) Verbesserung;

d) Dokumentation zur Bereitstellung auditierbarer Nachweise; und

e) jeden Prozess des Business Continuity Managements, der für die Organisation bedeutsam 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 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.

©2020 NBN. All rights reserved – PREVIEW first 10 pages

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.

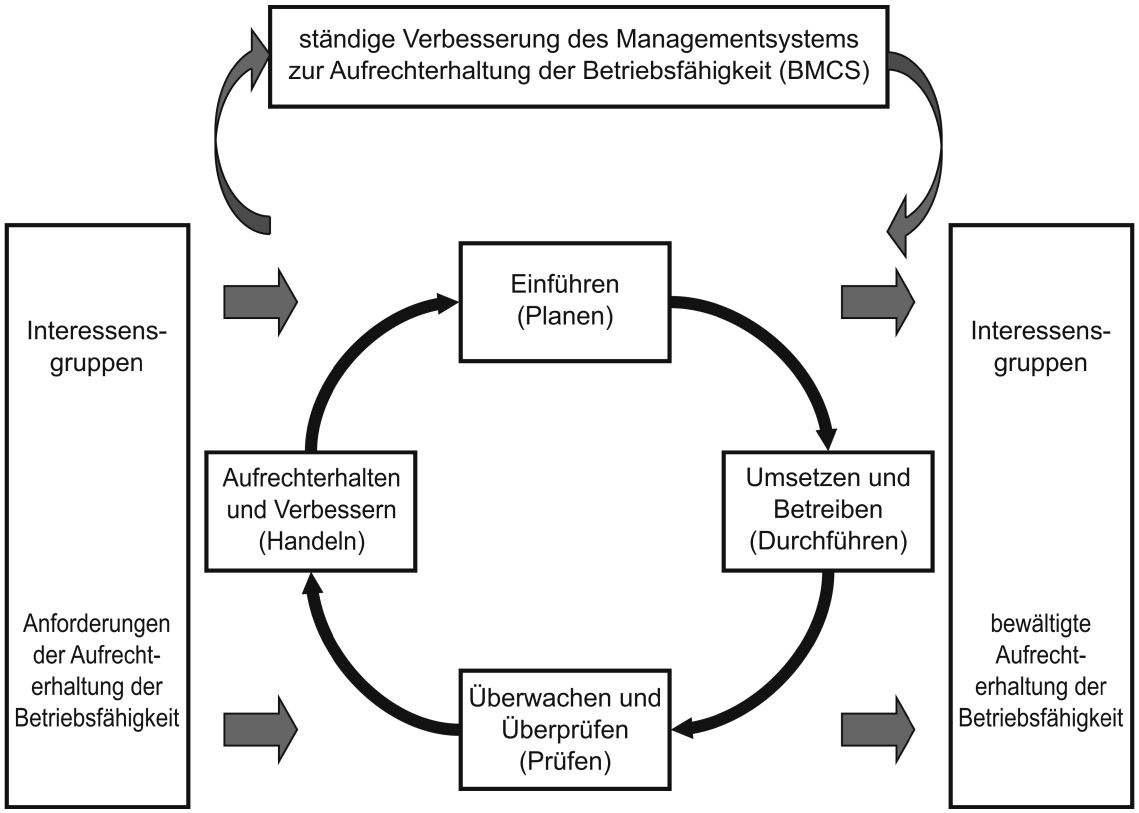

Bild 1 — An die BCMS-Prozesse angepasstes PDCA-Modell

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 Managementüberprüfung sowie Neufassung des Anwendungsbereichs des BCMS sowie der Leitlinien und Zielsetzungen .

©2020 NBN. All rights reserved – PREVIEW first 10 pages

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 Business Impact Analyse (BIA) abgeleitet sind.

ANMERKUNG Die Anforderungen der Business Impact Analyse 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 Zwischenfalls mit Betriebsunterbrechung.

— Abschnitt 9 ist Bestandteil des Elements „Prüfen“. Er fasst die Anforderungen zusammen, die zum Messen der Leitung des Business Contiunity Managements 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 Abweichung vom BCMS und reagiert auf diese durch Korrekturmaßnahmen.

©2020 NBN. All rights reserved – PREVIEW first 10 pages

1 Anwendungsbereich

Diese Internationale Norm zum Business Continuity Management 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 Zwischenfälle mit Betriebsunterbrechung 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 dieser Internationalen Norm 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.

Diese Internationale Norm beabsichtigt keine Einheitlichkeit im Aufbau eines Business Continuity Management Systems (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, Umsetzen, Aufrechterhalten und Verbessern eines BMCS;

b) Sicherstellen der Übereinstimmung mit den erklärten Leitlinien zur Aufrechterhaltung der Betriebsfähigkeit;

c) Darstellen der Übereinstimmung gegenüber anderen;

d) Zertifizierung/Registrierung ihres BMCS durch eine amtlich zugelassene Zertifizierungsstelle einer Drittpartei; oder

e) Erstellung einer Selbsterklärung zur Feststellung der Übereinstimmung mit 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.