



NEN-EN-ISO 22301 (nl)

Maatschappelijke veiligheid – Managementsystemen voor bedrijfscontinuïteit (business continuity management systems) – Eisen

ICS 03.100.01

Augustus 2014

Nederlandse norm

NEN-EN-ISO 22301

(nl)

Maatschappelijke veiligheid -
Managementsystemen voor bedrijfscontinuïteit
(business continuity management systems) -
Eisen (ISO 22301:2012 (Cor.2012-06),IDT)

Societal security - Business continuity
management systems - Requirements
(ISO 22301:2012 (Cor.2012-06),IDT)

Dit document bevat de vertaling in het Nederlands van de Europese norm EN ISO 22301:2014. De Europese norm EN ISO 22301:2014 heeft de status van Nederlandse norm.

Normcommissie 342 223 "Maatschappelijke Veiligheid"



THIS PUBLICATION IS COPYRIGHT PROTECTED

DEZE PUBLICATIE IS AUTEURSRECHTELIJK BESCHERMD

Apart from exceptions provided by the law, nothing from this publication may be duplicated and/or published by means of photocopy, microfilm, storage in computer files or otherwise, which also applies to full or partial processing, without the written consent of the Royal Netherlands Standardization Institute.

The Royal Netherlands Standardization Institute shall, with the exclusion of any other beneficiary, collect payments owed by third parties for duplication and/or act in and out of law, where this authority is not transferred or falls by right to the Reproduction Rights Foundation.

Auteursrecht voorbehouden. Behoudens uitzondering door de wet gesteld mag zonder schriftelijke toestemming van het Koninklijk Nederlands Normalisatie-instituut niets uit deze uitgave worden verveelvoudigd en/of openbaar gemaakt door middel van fotokopie, microfilm, opslag in computerbestanden of anderszins, hetgeen ook van toepassing is op gehele of gedeeltelijke bewerking.

Het Koninklijk Nederlands Normalisatie-instituut is met uitsluiting van ieder ander gerechtigd de door derden verschuldigde vergoedingen voor verveelvoudiging te innen en/of daartoe in en buiten rechte op te treden, voor zover deze bevoegdheid niet is overgedragen c.q. rechtens toekomt aan de Stichting Reprorecht.

Although the utmost care has been taken with this publication, errors and omissions cannot be entirely excluded. The Royal Netherlands Standardization Institute and/or the members of the committees therefore accept no liability, not even for direct or indirect damage, occurring due to or in relation with the application of publications issued by the Royal Netherlands Standardization Institute.

Hoewel bij deze uitgave de uiterste zorg is nagestreefd, kunnen fouten en onvolledigheden niet geheel worden uitgesloten. Het Koninklijk Nederlands Normalisatie-instituut en/of de leden van de commissies aanvaarden derhalve geen enkele aansprakelijkheid, ook niet voor directe of indirecte schade, ontstaan door of verband houdend met toepassing van door het Koninklijk Nederlands Normalisatie-instituut gepubliceerde uitgaven.

ICS 03.100.01

Nederlandstalige versie

Maatschappelijke veiligheid – Managementsystemen voor bedrijfscontinuïteit (business continuity management systems) – Eisen (ISO 22301:2012)

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)

Deze norm is de Nederlandstalige versie van de Europese norm EN ISO 22301:2014. Hij is vertaald door NEN. Hij heeft dezelfde status als de officiële versies.

Deze Europese norm is door CEN aangenomen op 17 juli 2014.

CEN-leden zijn verplicht zich te houden aan het huishoudelijk reglement van CEN-CENELEC, waarin is vastgelegd onder welke voorwaarden aan deze Europese norm, zonder veranderingen, de status van nationale norm moet worden gegeven. Bijgewerkte lijsten van en bibliografische gegevens betreffende zulke nationale normen kunnen op aanvraag worden verkregen bij het managementcentrum van CEN-CENELEC en bij elk CEN-lid.

Deze Europese norm bestaat in drie officiële versies (Duits, Engels en Frans). Een versie in een andere taal die onder verantwoordelijkheid van een CEN-lid in zijn landstaal is gemaakt en die is aangemeld bij het managementcentrum van CEN-CENELEC, heeft dezelfde status als de officiële versies.

Leden van CEN zijn de nationale normalisatieorganisaties van België, Bulgarije, Cyprus, Denemarken, Duitsland, Estland, Finland, Frankrijk, Griekenland, Hongarije, Ierland, IJsland, Italië, Kroatië, Letland, Litouwen, Luxemburg, Macedonië, Malta, Nederland, Noorwegen, Oostenrijk, Polen, Portugal, Roemenië, Slovenië, Slowakije, Spanje, Tsjechië, Turkije, het Verenigd Koninkrijk, Zweden en Zwitserland.

CEN

Europees Comité voor Normalisatie

Europäisches Komitee für Normung

European Committee for Standardization

Comité Européen de Normalisation

Managementcentrum CEN-CENELEC: Marnixlaan 17, B-1000 Brussel

(blanco)

Inhoud

Voorwoord	6
ISO-voorwoord	6
0 Inleiding	7
0.1 Algemeen	7
0.2 Het Plan-Do-Check-Act (PDCA)-model	7
0.3 Componenten van het PDCA-model in deze internationale norm	9
1 Onderwerp en toepassingsgebied¹⁾	10
2 Normatieve verwijzingen	10
3 Termen en definities	11
4 Context van de organisatie	18
4.1 Inzicht in de organisatie en haar context	18
4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden	19
4.3 Het toepassingsgebied van het BCMS vaststellen	19
4.4 Managementsysteem voor bedrijfscontinuïteit.....	20
5 Leiderschap	20
5.1 Leiderschap en betrokkenheid	20
5.2 Betrokkenheid van de directie	20
5.3 Beleid	21
5.4 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie	22
6 Planning	22
6.1 Acties om risico's en kansen op te pakken	22
6.2 Doelstellingen voor bedrijfscontinuïteit en de planning om ze te bereiken	22
7 Ondersteuning	23
7.1 Middelen.....	23
7.2 Competentie	23
7.3 Bewustzijn	23
7.4 Communicatie	24
7.5 Gedocumenteerde informatie.....	24
8 Uitvoering	25
8.1 Operationele planning en beheersing	25
8.2 Bedrijfsimpactanalyse en risicobeoordeling.....	26
8.3 Strategie voor bedrijfscontinuïteit.....	27
8.4 Vaststellen en implementeren van procedures voor bedrijfscontinuïteit.....	28
8.5 Oefening en testen	30
9 Evaluatie van de prestaties	31
9.1 Monitoren, meten, analyseren en evalueren.....	31
9.2 Interne audit	32
9.3 Directiebeoordeling	33
10 Verbetering	34
10.1 Afwijkingen en corrigerende maatregelen.....	34
10.2 Continue verbetering	35
Bibliografie	36

Voorwoord

De tekst van ISO 22301:2012 is opgesteld door Technische Commissie ISO/TC 223, "Societal security" van de Internationale Organisatie voor Standaardisatie (ISO) en is overgenomen als EN ISO 22301:2014 door Technische Commissie CEN/TC 391 "Societal and Citizen Security", waarvan het secretariaat wordt gevoerd door NEN.

Aan deze Europese norm moet uiterlijk in januari 2015 de status van nationale norm worden gegeven, door publicatie van een identieke tekst of door bekrachtiging, en strijdige nationale normen moeten uiterlijk in januari 2015 worden ingetrokken.

Er wordt gewezen op de mogelijkheid dat sommige elementen van dit document onderwerp zijn van patentrechten. CEN (en/of CENELEC) is niet verantwoordelijk voor identificatie van dergelijke patentrechten.

Dit document is opgesteld onder een door de Europese Commissie en de Europese Vrijhandelsassociatie aan CEN verleend mandaat en steunt fundamentele eisen van de richtlijn(en) van de EU.

Volgens het huishoudelijk reglement van CEN-CENELEC zijn de normalisatieorganisaties van de volgende landen verplicht deze Europese norm in te voeren: België, Bulgarije, Cyprus, Denemarken, Duitsland, Estland, Finland, Frankrijk, Griekenland, Hongarije, Ierland, IJsland, Italië, Kroatië, Letland, Litouwen, Luxemburg, Macedonië, Malta, Nederland, Noorwegen, Oostenrijk, Polen, Portugal, Roemenië, Slovenië, Slowakije, Spanje, Tsjechië, Turkije, het Verenigd Koninkrijk, Zweden en Zwitserland.

Verklaring van bekrachtiging

De tekst van ISO 22301:2012 is zonder wijzigingen door CEN als EN ISO 22301:2014 aanvaard.

ISO-voorwoord

ISO (International Organization for Standardization) is een wereldwijde federatie van nationale normalisatie-instituten (de ISO-leden). Het voorbereidingswerk voor internationale normen wordt doorgaans uitgevoerd door de technische commissies van ISO. Elk lid dat interesse heeft in een onderwerp waarvoor een technische commissie is samengesteld, heeft recht op vertegenwoordiging in deze commissie. Ook internationale organisaties, zowel overheidsinstanties als niet-gouvernementele organisaties, nemen in samenwerking met ISO deel aan deze werkzaamheden. ISO werkt nauw samen met de International Electrotechnical Commission (IEC) inzake alle elektrotechnische normalisatie.

Internationale normen worden opgesteld overeenkomstig de voorschriften die in de ISO/IEC-richtlijnen deel 2 zijn opgenomen.

De voornaamste taak van de technische commissies is de voorbereiding van internationale normen. Ontwerpversies van internationale normen die zijn aangenomen door de technische commissies, worden ter stemming voorgelegd aan de leden. Publicatie als internationale norm vereist goedkeuring van ten minste 75 % van de stemmen die zijn uitgebracht door deelnemende leden.

Er wordt gewezen op de mogelijkheid dat sommige elementen van dit document onderwerp kunnen zijn van patentrechten. ISO is niet verantwoordelijk voor identificatie van dergelijke patentrechten.

ISO 22301 werd opgesteld door Technische Commissie ISO/TC 223, *Societal security*.

Deze gecorrigeerde versie van ISO 22301:2012 omvat de volgende correcties:

- de eerste opsomming van 6.1 is gewijzigd van een genummerde naar een ongenummerde opsomming;
- er zijn puntkomma's toegevoegd aan het einde van de ingangen van de opsommingen in 7.5.3 en 8.3.2;
- ingangen [19] en [20] van de bibliografie, die in de eerste versie waren samengevoegd, zijn gescheiden;
- op diverse plaatsen is de lettergrootte aangepast.

0 Inleiding

0.1 Algemeen

Deze internationale norm specificeert eisen voor inrichting en beheer van een doeltreffend managementsysteem voor bedrijfscontinuïteit ('Business Continuity Management System', BCMS).

Een BCMS benadrukt het belang van

- het onderkennen van de behoeften van de organisatie en de noodzaak om beleid en doelstellingen voor bedrijfscontinuïteitsmanagement vast te stellen,
- het implementeren en uitvoeren van beheersmaatregelen die ervoor zorgen dat een organisatie het vermogen heeft om verstorende incidenten te managen,
- monitoren en beoordelen van de prestaties en de doeltreffendheid van het BCMS, en
- continue verbetering gebaseerd op objectieve meting.

Net als elk ander managementsysteem bestaat een BCMS uit de volgende hoofdcomponenten:

- a) beleid;
- b) mensen met gedefinieerde verantwoordelijkheden;
- c) managementprocessen met betrekking tot:
 - 1) beleid,
 - 2) planning,
 - 3) implementatie en uitvoering,
 - 4) prestatiebeoordeling,
 - 5) directiebeoordeling, en
 - 6) verbetering;
- d) documentatie waarmee auditeerbaar bewijsmateriaal wordt geleverd; en
- e) de processen voor bedrijfscontinuïteitsmanagement (BCM) die relevant zijn voor de organisatie.

Bedrijfscontinuïteit draagt bij aan een veerkrachtiger maatschappij. De bredere gemeenschap en de invloed van de omgeving op de organisatie, en daarmee andere organisaties, moeten wellicht in het herstelproces worden betrokken.

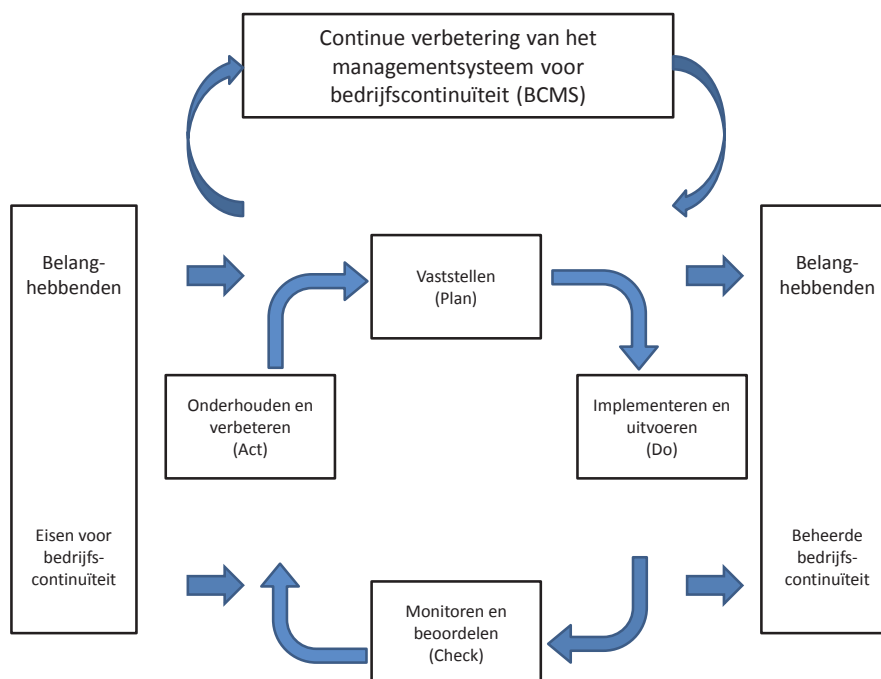
0.2 Het Plan-Do-Check-Act (PDCA)-model

Deze internationale norm past het Plan-Do-Check-Act (PDCA)-model toe voor het plannen, inrichten, implementeren, uitvoeren, monitoren, beoordelen, onderhouden en continu verbeteren van de doeltreffendheid van het BCMS van de organisatie.

Dit zorgt voor een mate van compatibiliteit met andere normen voor managementsystemen, zoals ISO 9001 *Kwaliteitsmanagementsystemen*, ISO 14001 *Milieumanagementsystemen*, ISO/IEC 27001 *Managementsystemen voor informatiebeveiliging*, ISO/IEC 20000-1 *Informatietechnologie – Service management*, en ISO 28000 *Specificatie voor veiligheidsmanagementsystemen voor de logistieke keten*,

waardoor consistente en geïntegreerde implementatie en uitvoering met gerelateerde managementsystemen wordt ondersteund.

Figuur 1 laat zien hoe een BCMS als input de eisen van de belanghebbenden voor bedrijfscontinuïteitsmanagement neemt en, door middel van de benodigde handelingen en processen, als uitkomsten continuïteit levert (d.w.z. beheerde bedrijfscontinuïteit) die aan deze eisen voldoet.



Figuur 1 — PDCA-model toegepast op BCMS-processen

Tabel 1 — Verklaring van het PDCA-model

Plan (Vaststellen)	Beleid, doelstellingen, taakstellingen, beheersmaatregelen, processen en procedures voor bedrijfscontinuïteit vaststellen die relevant zijn om de bedrijfscontinuïteit te verbeteren, teneinde resultaten te leveren die overeenstemmen met het algehele beleid en de doelstellingen van de organisatie.
Do (Implementeren en uitvoeren)	Beleid, beheersmaatregelen, processen en procedures voor bedrijfscontinuïteit implementeren en uitvoeren.
Check (Monitoren en beoordelen)	De prestaties ten opzichte van beleid en doelstellingen voor bedrijfscontinuïteit monitoren en beoordelen, de resultaten ter beoordeling aan het management rapporteren, en geaccordeerde maatregelen voor herstel en verbetering vaststellen.
Act (Onderhouden en verbeteren)	Het BCMS onderhouden en verbeteren door corrigerende maatregelen te nemen, op basis van de resultaten van de directiebeoordeling en herbeoordeling van het toepassingsgebied van het BCMS en tevens van het beleid en de doelstellingen voor bedrijfscontinuïteit.