

HIGH LEVEL STRUCTURE



Dit document mag slechts op een stand-alone PC worden geïnstalleerd. Gebruik op een netwerk is alleen toegestaan als een aanvullende licentieovereenkomst voor netwerkgebruik met NEN is afgesloten.
This document may only be used on a stand-alone PC. Use in a network is only permitted when a supplementary license agreement for use in a network with NEN has been concluded.

NEN-EN-ISO 22301 (nl)

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

ICS 03.100.01

Augustus 2014



Normalisatie: de wereld op één lijn.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 4-7-2016 15:27:28

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)

ICS 03.100.01
augustus 2014

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.



© 2016 Koninklijk Nederlands Normalisatie-instituut
Postbus 5059, 2600 GB Delft
Telefoon (015) 2 690 390

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

© 2014 CEN

Alle rechten van gebruik, in welke vorm en op welke wijze
dan ook, zijn voorbehouden aan CEN-leden.

Ref. nr. EN ISO 22301:2014 nl

(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.

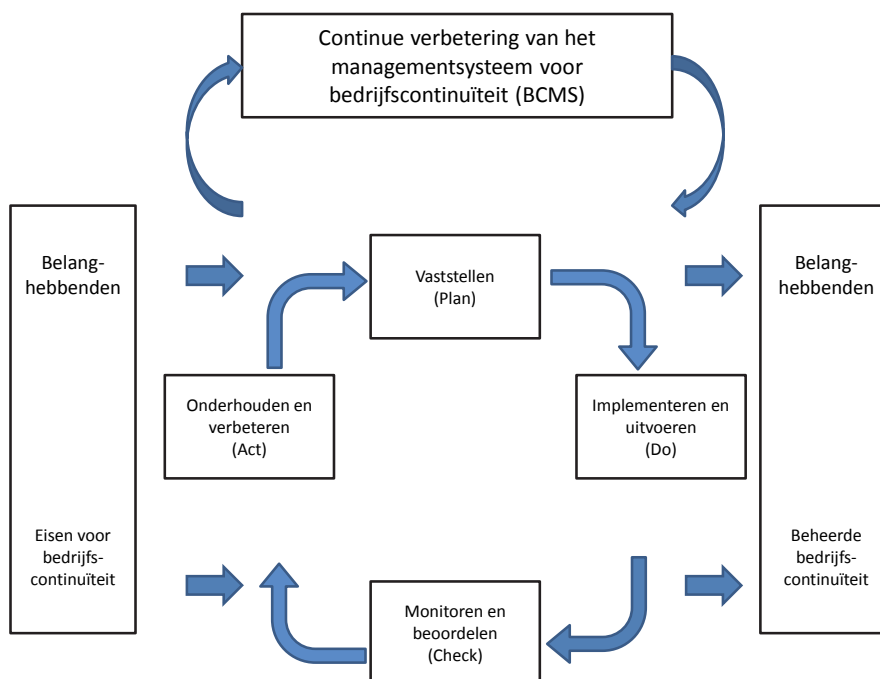
0.2 Het Plan-Do-Check-Act (PDCA)-model

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.

0.3 Componenten van het PDCA-model in deze internationale norm

In het PDCA-model zoals dat in tabel 1 is beschreven, omvatten hoofdstukken 4 t.m. 10 van deze internationale norm de volgende componenten.

- Hoofdstuk 4 behoort tot het onderdeel Plan. Hierin worden eisen beschreven die nodig zijn om de context van het BCMS vast te stellen zoals dat op de organisatie van toepassing is, evenals de behoeften, eisen en het toepassingsgebied ervan.
- Hoofdstuk 5 behoort tot het onderdeel Plan. Hierin worden de eisen samengevat die specifiek zijn voor de rol van de directie in het BCMS, en hoe het management haar verwachtingen aan de organisatie bekendmaakt door middel van een beleidsverklaring.
- Hoofdstuk 6 behoort tot het onderdeel Plan. Hierin worden eisen beschreven die betrekking hebben op het vaststellen van strategische doelstellingen en beginselen voor het BCMS als geheel. De inhoud van hoofdstuk 6 verschilt van het vaststellen van de mogelijkheden voor risicobeheersing op basis van risicobeoordeling, en van de doelstellingen voor herstel die zijn afgeleid van de bedrijfsimpactanalyse (BIA).

OPMERKING De eisen voor de bedrijfsimpactanalyse en voor het proces van risicobeoordeling worden beschreven in hoofdstuk 8.

- Hoofdstuk 7 behoort tot het onderdeel Plan. Dit ondersteunt BCMS-activiteiten die betrekking hebben op het vaststellen van competentie en communicatie, periodiek of naar behoefte, met belanghebbenden, waarbij de vereiste documentatie wordt opgesteld, beheerst, onderhouden en gearhiveerd.
- Hoofdstuk 8 behoort tot het onderdeel Do. Hierin zijn eisen voor bedrijfscontinuïteit vastgelegd, waarbij wordt beschreven hoe daaraan moet worden voldaan en welke procedures nodig zijn voor het beheersen van versturende incidenten.
- Hoofdstuk 9 behoort tot het onderdeel Check. Hierin wordt een overzicht gegeven van eisen die nodig zijn om de prestaties van het BCM te meten, en de mate vast te stellen waarin het BCMS voldoet aan deze internationale norm en aan de verwachtingen van het management beantwoordt, en het vraagt om feedback van het management over hun verwachtingen.
- Hoofdstuk 10 behoort tot het onderdeel Act. Dit betreft het vaststellen van en met corrigerende maatregelen reageren op afwijkingen in het BCMS.

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

1 Onderwerp en toepassingsgebied^{*)}

Deze internationale norm voor BCM specificeert eisen voor het plannen, inrichten, implementeren, uitvoeren, monitoren, beoordelen, onderhouden en continu verbeteren van een gedocumenteerd managementsysteem, ter bescherming tegen, verkleining van de kans op, voorbereiding op, reactie op en herstel van verstorende incidenten wanneer deze zich voordoen.

De eisen in deze internationale norm zijn algemeen en bedoeld om van toepassing te zijn voor alle organisaties, of delen daarvan, ongeacht type, omvang of aard van de organisatie. De mate waarin deze eisen van toepassing zijn, is afhankelijk van de complexiteit van de organisatie en van de omgeving waarin zij opereert.

Deze internationale norm heeft niet tot doel een uniforme structuur op te leggen voor een managementsysteem voor bedrijfscontinuïteit (BCMS), maar om een organisatie in staat te stellen een BCMS te ontwerpen dat op haar behoeften is afgestemd en dat voldoet aan de eisen van haar belanghebbenden. Deze behoeften worden gevormd door wettelijke, regelgevende, organisatie- en branchespecifieke eisen, producten en diensten, uitgevoerde processen, omvang en structuur van de organisatie en de eisen van haar belanghebbenden.

Deze internationale norm is van toepassing op organisaties van elk type en van elke omvang die:

- a) een BCMS willen inrichten, implementeren, onderhouden en verbeteren,
- b) naleving van het vastgestelde beleid voor bedrijfscontinuïteit willen bewerkstelligen,
- c) conformiteit aan anderen willen aantonen,
- d) certificatie/registratie van het BCMS door een geaccrediteerde certificatie-instelling willen verkrijgen, of
- e) zelf de naleving van deze internationale norm vast willen stellen en daarvan een eigen verklaring willen opstellen.

Deze internationale norm kan worden gebruikt om vast te stellen in hoeverre een organisatie in staat is te voldoen aan haar eigen behoeften en verplichtingen met betrekking tot bedrijfscontinuïteit.

2 Normatieve verwijzingen

Er zijn geen normatieve verwijzingen.

^{*)} Nederlandse voetnoot: Deze internationale norm voldoet aan de eisen van ISO voor managementsysteemnormen. Deze eisen omvatten een gemeenschappelijke hoofdstructuur, identieke kerntekst en gemeenschappelijke termen met kerndefinities ten behoeve van gebruikers die meer ISO-managementsysteemnormen implementeren. Om de gebruikers van meerdere managementsysteemnormen van dienst te zijn, zijn in deze norm de gemeenschappelijke termen met kerndefinities en identieke kerntekst door een (kleur)markering onderscheiden van de aanvullende voor bedrijfscontinuïteitsmanagement specifieke tekst. De gele markering betreft de identieke kerntekst.

3 Termen en definities

Voor de toepassing van deze norm gelden de volgende termen en definities.

3.1

activiteit

proces of geheel van processen die door (of namens) een organisatie worden uitgevoerd en waarmee een of meer producten of diensten worden geproduceerd of ondersteund

VOORBEELD Dit omvat processen met betrekking tot financiële administratie, callcenters, IT, fabricage en distributie.

3.2

audit

systematisch, onafhankelijk en gedocumenteerd proces voor het verkrijgen van auditbewijsmateriaal, en het objectief beoordelen daarvan om vast te stellen in welke mate aan de auditcriteria is voldaan

OPMERKING 1 Een audit kan een interne audit (eerste partij) of een externe audit (tweede partij of derde partij) zijn, en het kan een gecombineerde audit zijn (waarbij twee of meer disciplines worden gecombineerd).

OPMERKING 2 'Auditbewijsmateriaal' en 'auditcriteria' zijn gedefinieerd in ISO 19011.

3.3

bedrijfscontinuïteit

vermogen van de organisatie om na een verstoring incident producten of diensten te blijven leveren op aanvaardbare, vooraf vastgestelde niveaus

[Bron: ISO 22300]

3.4

bedrijfscontinuïteitsmanagement

BCM

holistisch managementproces waarin mogelijke bedreigingen voor een organisatie worden geïdentificeerd en de mogelijke gevolgen voor de bedrijfsvoering als die bedreigingen zich werkelijk manifesteren, en dat een kader biedt om het weerstandsvermogen en de veerkracht van de organisatie te versterken, zodat de organisatie doeltreffend kan reageren om de belangen van belanghebbenden, reputatie, merk en waardecreërende activiteiten veilig te stellen

3.5

managementsysteem voor bedrijfscontinuïteit

BCMS

dat deel van het algehele managementsysteem waarmee de bedrijfscontinuïteit wordt ingericht, geïmplementeerd, uitgevoerd, gemonitord, beoordeeld, onderhouden en verbeterd

OPMERKING Het managementsysteem omvat organisatiestructuur, beleid, activiteitenplanning, verantwoordelijkheden, procedures, processen en middelen.

3.6

bedrijfscontinuïteitsplan

gedocumenteerde procedures die de organisatie richting geven om te reageren, te herstellen, activiteiten te hervatten en terug te keren naar een vooraf vastgesteld niveau van bedrijfsvoering na een verstoring

OPMERKING Doorgaans omvat dit middelen, diensten en activiteiten die nodig zijn om voor de continuïteit van kritische bedrijfsfuncties te zorgen.

3.7

bedrijfscontinuïteitsprogramma

doorlopend management- en besturingsproces dat door de directie wordt ondersteund en dat van passende middelen is voorzien om het bedrijfscontinuïteitsmanagement te implementeren en te onderhouden

3.8

bedrijfsimpactanalyse

proces voor het analyseren van activiteiten en van de mogelijke gevolgen van een verstoring in het bedrijfsproces voor deze activiteiten

[Bron: ISO 22300]

3.9

competentie

vermogen om kennis en vaardigheden toe te passen om beoogde resultaten te bereiken

3.10

conformiteit

het voldoen aan een eis

[Bron: ISO 22300]

3.11

continue verbetering

zich herhalende activiteit om prestaties te verbeteren

[Bron: ISO 22300]

3.12

correctie

maatregel om een waargenomen afwijking weg te nemen

[Bron: ISO 22300]

3.13

corrigerende maatregel

maatregel om de oorzaak van een afwijking weg te nemen en om herhaling te voorkomen

OPMERKING In geval van andere ongewenste uitkomsten is actie noodzakelijk om oorzaken te minimaliseren of weg te nemen en de gevolgen te verminderen of herhaling te voorkomen. Dergelijke acties vallen buiten het concept van 'corrigerende maatregel' zoals bedoeld in deze definitie.

[Bron: ISO 22300]

3.14

document

informatie en haar gegevensdrager

OPMERKING 1 De drager kan papier zijn, een magnetische, elektronische of optische computerschijf, een foto of originele opname, of een combinatie daarvan.

OPMERKING 2 Een verzameling documenten, zoals specificaties en registraties, wordt vaak aangeduid als 'documentatie'.

3.15

gedocumenteerde informatie

informatie die een organisatie moet beheren en onderhouden en het medium waarop deze informatie is vastgelegd

OPMERKING 1 Gedocumenteerde informatie kan bestaan in elk format en in elk medium, en afkomstig zijn van elke bron.

OPMERKING 2 Gedocumenteerde informatie kan betrekking hebben op:

— het managementsysteem, met inbegrip van gerelateerde processen;

— informatie die is ontwikkeld om de organisatie te laten functioneren (documentatie);

— bewijsmateriaal dat resultaten zijn behaald (registraties).

3.16

doeltreffendheid

mate waarin geplande activiteiten worden gerealiseerd en geplande resultaten worden behaald

[Bron: ISO 22300]

3.17

gebeurtenis

optreden van of wijziging in een bepaalde combinatie van omstandigheden

OPMERKING 1 Een gebeurtenis kan een of meer voorvallen omvatten en kan diverse oorzaken hebben.

OPMERKING 2 Een gebeurtenis kan bestaan uit iets dat niet plaatsvindt.

OPMERKING 3 Een gebeurtenis kan soms worden aangeduid als een 'incident' of 'ongeval'.

OPMERKING 4 Een gebeurtenis die geen gevolgen heeft, mag ook worden omschreven als een 'bijna-ongeluk' of 'incident' (Eng. 'near miss', 'incident', 'near hit', 'close call').

[Bron: ISO/IEC Guide 73]

3.18

oefening

proces om te trainen, te beoordelen, te oefenen en de prestaties van de organisatie te verbeteren

OPMERKING 1 Oefeningen kunnen worden gebruikt voor: het valideren van beleid, plannen, procedures, training, uitrusting en overeenkomsten tussen organisaties; het voorlichten en trainen van personeel in rollen en verantwoordelijkheden; het verbeteren van coördinatie en communicatie tussen organisaties; het identificeren van lacunes in middelen; het verbeteren van individuele prestaties; en voor het identificeren van kansen voor verbetering, en van beheerste gelegenheden voor improvisatie.

OPMERKING 2 Een test is een uniek en specifiek type oefening, dat een verwachting omvat van falen of slagen binnen het doel of de doelstellingen van de geplande oefening.

[Bron: ISO 22300]

3.19

incident

situatie die een verstoring, verlies, noodsituatie of crisis kan zijn of daartoe kan leiden

[Bron: ISO 22300]

3.20

infrastructuur

systeem van faciliteiten, uitrusting en diensten, benodigd voor het functioneren van een organisatie

3.21

belanghebbende

stakeholder

persoon of organisatie die een besluit of activiteit kan beïnvloeden, door een besluit of activiteit kan worden beïnvloed, of zichzelf beschouwt als beïnvloed door een besluit of activiteit

OPMERKING Dit kan een individu of een groep personen zijn die een belang heeft in elk mogelijk besluit of elke mogelijke activiteit van een organisatie.

3.22

interne audit

audit die door of namens de organisatie zelf wordt uitgevoerd ten behoeve van de directiebeoordeling en andere interne doeleinden en die de basis kan vormen van een eigen verklaring van conformiteit van de organisatie

OPMERKING In veel gevallen, vooral in kleinere organisaties, kan onafhankelijkheid van de auditor worden aangetoond door het ontbreken van verantwoordelijkheid voor de activiteit waarop de audit wordt uitgevoerd.

3.23

inwerkingstelling

verklaring dat de maatregelen voor bedrijfscontinuïteit van de organisatie in werking moeten worden gesteld om de belangrijkste producten of diensten te kunnen blijven leveren

3.24

managementsysteem

geheel van samenhangende of elkaar beïnvloedende elementen van een organisatie om een beleid en doelstellingen vast te stellen, alsmede de processen om die doelstellingen te bereiken

OPMERKING 1 Een managementsysteem kan betrekking hebben op een of meer disciplines.

OPMERKING 2 Tot de elementen van het systeem behoren de organisatiestructuur, rollen en verantwoordelijkheden, planning, uitvoering enz.

OPMERKING 3 Het toepassingsgebied van een managementsysteem kan de gehele organisatie omvatten, specifieke en geïdentificeerde functies van de organisatie, specifieke en geïdentificeerde onderdelen van de organisatie, of een of meer functies in een groep van organisaties.

3.25

maximaal aanvaardbare uitvalsduur

MAO ('maximum acceptable outage')

tijdsduur die verstrijkt totdat nadelige gevolgen, die zich kunnen voordoen als gevolg van het niet leveren van een product/dienst of het niet uitvoeren van een activiteit, onaanvaardbaar worden

OPMERKING Zie ook maximaal toelaatbare periode van verstoring.

3.26

maximaal toelaatbare periode van verstoring

MTPD ('maximum tolerable period of disruption')

tijdsduur die verstrijkt totdat nadelige gevolgen, die zich kunnen voordoen als gevolg van het niet leveren van een product/dienst of het niet uitvoeren van een activiteit, onaanvaardbaar worden ¹⁾

OPMERKING Zie ook maximaal aanvaardbare uitvalsduur.

3.27

meting

proces om een waarde vast te stellen

3.28

minimumdoelstelling voor bedrijfscontinuïteit

MBCO ('minimum business continuity objective')

minimumniveau van levering van diensten en/of producten dat aanvaardbaar is voor de organisatie om haar bedrijfsdoelstellingen tijdens een verstoring te kunnen behalen

1) Nederlandse voetnoot: deze definitie is de exacte vertaling van de brontekst, maar identiek aan die van 3.26 'maximaal toelaatbare periode van verstoring'. 'Maximaal aanvaardbare uitvalsduur' kan vermoedelijk gedefinieerd worden als 'tijdsduur waarbinnen een herstelactie in werking moet treden voordat de gevolgen van het niet leveren van een product/dienst of niet uitvoeren van activiteit, onaanvaardbaar worden'.

3.29

monitoring

het vaststellen van de status van een systeem, een proces of een activiteit

OPMERKING Om de status vast te stellen kan het nodig zijn om te controleren, toezicht te houden of kritisch te observeren.

3.30

overeenkomst voor wederzijdse hulpverlening

vooraf overeengekomen afspraak tussen twee of meer entiteiten om elkaar assistentie te verlenen

[Bron: ISO 22300]

3.31

afwijking

het niet voldoen aan een eis

[Bron: ISO 22300]

3.32

doelstelling

te behalen resultaat

OPMERKING 1 Een doelstelling kan strategisch, tactisch of operationeel zijn.

OPMERKING 2 Doelstellingen kunnen betrekking hebben op verschillende disciplines (zoals financiële, gezondheids- en veiligheids- en milieudoelen), en kunnen gelden op verschillende niveaus (zoals strategisch, organisatiebreed, project-, product- en procesniveau).

OPMERKING 3 Een doelstelling kan op verschillende manieren worden verwoord, bijv. als een beoogde uitkomst, een doel, een operationeel criterium, als een doelstelling voor maatschappelijke veiligheid ²⁾ of door het gebruik van andere bewoordingen met gelijke betekenis (bijv. oogmerk, bedoeling of taakstelling).

OPMERKING 4 In de context van normen voor managementsystemen voor maatschappelijke veiligheid worden doelstellingen voor maatschappelijke veiligheid vastgesteld door de organisatie, in overeenstemming met het beleid voor maatschappelijke veiligheid, om specifieke resultaten te behalen.

3.33

organisatie

persoon of groep van personen die zijn eigen functies heeft met verantwoordelijkheden, bevoegdheden en relaties om zijn doelstellingen te bereiken.

OPMERKING 1 Het begrip organisatie omvat maar is niet beperkt tot eenmanszaak, bedrijf, vennootschap, firma, onderneming, autoriteit, partnerschap, liefdadigheidsinstelling of genootschap, of een deel of combinatie daarvan, hetzij als rechtspersoon erkend of niet, publiek of privaat.

OPMERKING 2 Voor organisaties met meer dan één bedrijfs onderdeel kan een enkel bedrijfs onderdeel als een organisatie worden gedefinieerd.

3.34

uitbesteden (werkwoord)

een overeenkomst treffen waarbij een externe organisatie een deel van een functie of proces van de organisatie verricht

OPMERKING Een externe organisatie valt buiten de reikwijdte van het managementsysteem, hoewel de uitbestede functie of het uitbestede proces er wel binnen valt.

2) Nederlandse voetnoot: vermoedelijk is hier in plaats van 'maatschappelijke veiligheid' ('societal security') 'bedrijfscontinuïteit' ('business continuity') bedoeld, zoals in 3.48.

3.35

prestatie(s)

meetbaar resultaat

OPMERKING 1 Prestaties kunnen betrekking hebben op hetzij kwantitatieve hetzij kwalitatieve bevindingen.

OPMERKING 2 Prestaties kunnen betrekking hebben op het management van activiteiten, processen, producten (met inbegrip van diensten), systemen of organisaties.

3.36

prestatie-evaluatie

proces waarmee meetbare resultaten worden vastgesteld

3.37

personeel

mensen die voor en onder het gezag van de organisatie werken

OPMERKING Het concept van personeel omvat onder meer werknemers, tijdelijke medewerkers en uitzendkrachten.

3.38

beleid

bedoelingen en richting van een organisatie zoals formeel door de directie kenbaar gemaakt

3.39

procedure

gespecificeerde wijze van het uitvoeren van een activiteit of proces

3.40

proces

geheel van samenhangende of elkaar beïnvloedende activiteiten dat input omzet in output

3.41

producten en diensten

nuttige uitkomsten die door een organisatie aan haar klanten, ontvangers en belanghebbenden worden geleverd, bijvoorbeeld fabricaten, autoverzekeringen en wijkverpleging

3.42

geprioriteerde activiteiten

activiteiten waaraan prioriteit moet worden verleend na een incident, om de gevolgen ervan te beperken

OPMERKING Algemeen gebruikte termen waarmee activiteiten die hieronder vallen worden aangeduid, zijn bijvoorbeeld: kritisch, essentieel, onmisbaar, urgent en belangrijk.

[Bron: ISO 22300]

3.43

registratie

verklaring over bereikte resultaten of bewijs van uitgevoerde activiteiten

3.44

herstelpuntdoelstelling

RPO ('recovery point objective')

punt waarnaar informatie die door een activiteit wordt gebruikt moet worden hersteld, om het mogelijk te maken dat de activiteit bij hervatting weer kan worden uitgevoerd

OPMERKING Kan ook worden aangeduid als 'maximaal dataverlies'.

3.45**hersteltijddoelstelling****RTO ('recovery time objective')**

tijdsperiode na een incident waarbinnen

- productlevering of dienstverlening moet worden hervat, of
- activiteit moet worden hervat, of
- middelen hersteld moeten zijn

OPMERKING Voor producten, diensten en activiteiten moet de hersteltijddoelstelling korter zijn dan de tijd die verstrijkt totdat nadelige gevolgen, die zich voordoen omdat de producten/diensten niet worden geleverd of een activiteit niet wordt uitgevoerd, onaanvaardbaar worden.

3.46**eis**

behoefte of verwachting die kenbaar is gemaakt, vanzelfsprekend is of dwingend is voorgeschreven

OPMERKING 1 'Vanzelfsprekend' betekent dat het gebruikelijk of gangbaar is voor de organisatie en belanghebbenden om de desbetreffende behoefte of verwachting stilzwijgend mee te nemen.

OPMERKING 2 Een gespecificeerde eis is een eis die kenbaar wordt gemaakt, bijvoorbeeld in gedocumenteerde informatie.

3.47**middelen**

alle bedrijfsmiddelen (assets), personeel, vaardigheden, informatie, technologie (met inbegrip van installaties en uitrusting), gebouwen, voorraden en informatie (al dan niet elektronisch) die een organisatie beschikbaar moet hebben voor gebruik, indien nodig, om te kunnen functioneren en haar doelstellingen te behalen

3.48**risico**

effect van onzekerheid op het behalen van doelstellingen

OPMERKING 1 Een effect is een afwijking ten opzichte van de verwachting – positief of negatief.

OPMERKING 2 Doelstellingen kunnen worden gekenmerkt door verschillende aspecten (zoals financiële, gezondheids- en veiligheids- en milieudoelen) en kunnen betrekking hebben op verschillende niveaus (zoals strategisch, organisatiebreed, een project, product of proces). Een doelstelling kan op verschillende manieren worden verwoord, bijv. als een beoogde uitkomst, een doel, een operationeel criterium, als een doelstelling voor bedrijfscontinuïteit of door het gebruik van andere bewoordingen met gelijke betekenis (bijv. oogmerk, doel of taakstelling).

OPMERKING 3 Een risico wordt vaak gekarakteriseerd door verwijzingen naar potentiële gebeurtenissen (Guide 73, 3.5.1.3) en gevolgen (Guide 73, 3.6.1.3), of een combinatie daarvan.

OPMERKING 4 Een risico wordt vaak uitgedrukt als een combinatie van de gevolgen van een gebeurtenis (met inbegrip van wijzigingen in omstandigheden) en de bijbehorende waarschijnlijkheid (Guide 73, 3.6.1.1) dat de gebeurtenis zich voordoet.

OPMERKING 5 Onzekerheid is het geheel of gedeeltelijk ontbreken van informatie over, inzicht in of kennis van een gebeurtenis, de gevolgen daarvan of de waarschijnlijkheid dat deze zich voordoet.

OPMERKING 6 In de context van normen voor managementsystemen voor bedrijfscontinuïteit worden doelstellingen voor bedrijfscontinuïteit vastgesteld door de organisatie, in overeenstemming met het beleid voor bedrijfscontinuïteit, om specifieke resultaten te behalen. Wanneer de term risico en componenten van risicomanagement worden gebruikt, behoort dit te worden gerelateerd aan de doelstellingen van de organisatie die, onder meer, de doelstellingen voor bedrijfscontinuïteit omvatten zoals gespecificeerd in 6.2.

[Bron: ISO/IEC Guide 73]

3.49

risicobereidheid

omvang van en soort risico dat een organisatie wil nastreven of behouden

3.50

risicobeoordeling

gehele proces van risico-identificatie, risicoanalyse en risico-evaluatie

[Bron: ISO Guide 73]

3.51

risicomanagement

gecoördineerde activiteiten gericht op het sturen en beheersen van de organisatie met betrekking tot risico

[Bron: ISO Guide 73]

3.52

testen

procedure voor evaluatie; een manier om de aanwezigheid, kwaliteit of waarheid van iets vast te stellen

OPMERKING 1 Testen kan worden aangeduid als een 'trial'.

OPMERKING 2 Testen wordt vaak toegepast om plannen te ondersteunen.

[Bron: ISO 22300]

3.53

directie

persoon of groep van personen die een organisatie op het hoogste niveau bestuurt en beheert

OPMERKING 1 De directie heeft de macht om bevoegdheid te delegeren en de organisatie van middelen te voorzien.

OPMERKING 2 Indien het toepassingsgebied van het managementsysteem slechts een deel van een organisatie omvat, dan verwijst de directie naar degenen die dat gedeelte van de organisatie besturen en beheren.

3.54

verificatie

bevestiging, door levering van bewijs, dat aan de gespecificeerde eisen is voldaan

3.55

werkomgeving

geheel van omstandigheden waaronder werkzaamheden worden uitgevoerd

OPMERKING De omstandigheden omvatten fysieke, maatschappelijke, psychologische factoren en omgevingsfactoren (zoals temperatuur, waarderingssystemen, ergonomie en samenstelling van de lucht).

[Bron: ISO 22300]

4 Context van de organisatie

4.1 Inzicht in de organisatie en haar context

De organisatie moet externe en interne belangrijke punten (issues) vaststellen die relevant zijn voor haar doelstelling en die haar vermogen beïnvloeden om het (de) beoogde resulta(a)t(en) van haar BCMS te behalen.

Deze punten moeten in beschouwing worden genomen bij het vaststellen, implementeren en onderhouden van het BCMS van de organisatie.

De organisatie moet het volgende vaststellen en documenteren:

- a) haar activiteiten, functies, diensten, producten, samenwerkingen, logistieke ketens, relaties met belanghebbenden, en de mogelijke gevolgen van een verstorend incident;
- b) verbanden tussen het beleid voor bedrijfscontinuïteit en de organisatiedoelstellingen en ander beleid, met inbegrip van de algehele risicomanagementstrategie; en
- c) haar risicobereidheid.

Bij het vaststellen van de context moet de organisatie:

- 1) haar doelstellingen bepalen, met inbegrip van doelstellingen voor bedrijfscontinuïteit,
- 2) de externe en interne factoren bepalen die onzekerheid opleveren, welke aanleiding geven tot risico,
- 3) risicocriteria vaststellen waarbij rekening wordt gehouden met de risicobereidheid, en
- 4) het doel van het BCMS vaststellen.

4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden

4.2.1 Algemeen

Bij het inrichten van het BCMS moet de organisatie vaststellen:

- a) welke belanghebbenden relevant zijn voor het BCMS, en
- b) wat de eisen van deze belanghebbenden zijn (d.w.z. hun behoeften of verwachtingen die kenbaar zijn gemaakt, vanzelfsprekend zijn, of dwingend zijn voorgeschreven).

4.2.2 Eisen uit wet- en regelgeving

De organisatie moet (een) procedure(s) vaststellen, implementeren en onderhouden voor het identificeren van, toegang geven tot en beoordelen van de van toepassing zijnde eisen uit wet- en regelgeving die de organisatie onderschrijft, welke gerelateerd zijn aan de continuïteit van de bedrijfsvoering, producten en diensten, evenals aan de belangen van relevante belanghebbenden.

De organisatie moet ervoor zorgen dat bij het vaststellen, implementeren en onderhouden van het BCMS rekening wordt gehouden met deze van toepassing zijnde eisen uit wet- en regelgeving en andere eisen die de organisatie onderschrijft.

De organisatie moet deze informatie documenteren en actueel houden. Nieuwe of aangepaste eisen uit wet- en regelgeving en andere eisen moeten worden gecommuniceerd aan werknemers en andere belanghebbenden die met die eisen te maken hebben.

4.3 Het toepassingsgebied van het BCMS vaststellen

4.3.1 Algemeen

De organisatie moet de grenzen en toepasselijkheid van het BCMS bepalen om het toepassingsgebied ervan vast te stellen.

Bij het vaststellen van dit toepassingsgebied moet de organisatie

- de in 4.1 genoemde externe en interne onderwerpen overwegen,
- de in 4.2 genoemde eisen overwegen.

Het toepassingsgebied moet als gedocumenteerde informatie beschikbaar zijn.

4.3.2 Toepassingsgebied van het BCMS

De organisatie moet

- a) vaststellen welke delen van de organisatie in het BCMS moeten worden opgenomen,
- b) eisen voor het BCMS vaststellen, waarbij rekening wordt gehouden met de missie, doelen, interne en externe verplichtingen (met inbegrip van verplichtingen die betrekking hebben op belanghebbenden) van de organisatie, evenals wettelijke of andere verantwoordelijkheden,
- c) producten en diensten en alle daarmee samenhangende activiteiten identificeren binnen het toepassingsgebied van het BCMS,
- d) rekening houden met de behoeften en belangen van belanghebbenden, zoals klanten, investeerders, aandeelhouders, de logistieke keten, inbreng en behoeften, verwachtingen en belangen (voor zover van toepassing) van de maatschappij en/of de gemeenschap, en
- e) het toepassingsgebied van het BCMS definiëren in termen van en passend bij de omvang, aard en complexiteit van de organisatie.

Bij het vaststellen van het toepassingsgebied moet de organisatie uitsluitingen documenteren en toelichten; dergelijke uitsluitingen mogen geen negatieve invloed uitoefenen op het vermogen en de verantwoordelijkheid van de organisatie om bedrijfscontinuïteit te leveren en bedrijfsvoering te blijven uitvoeren die voldoen aan de eisen van het BCMS, zoals vastgesteld middels een bedrijfsimpactanalyse of een risicobeoordeling en van toepassing zijnde eisen uit wet- of regelgeving.

4.4 Managementsysteem voor bedrijfscontinuïteit

De organisatie moet een BCMS inrichten, implementeren, onderhouden en continu verbeteren, met inbegrip van de benodigde processen en hun interacties, in overeenstemming met de eisen van deze internationale norm.

5 Leiderschap

5.1 Leiderschap en betrokkenheid

Directieleden en andere relevante leidinggevende functies in alle lagen van de organisatie moeten leiderschap tonen met betrekking tot het BCMS.

VOORBEELD Leiderschap en betrokkenheid kunnen worden getoond door personeel te motiveren en in staat te stellen bij te dragen aan de doeltreffendheid van het BCMS.

5.2 Betrokkenheid van de directie

De directie moet leiderschap en betrokkenheid tonen met betrekking tot het BCMS door:

- te bewerkstelligen dat beleid en doelstellingen voor het BCMS worden vastgesteld en aansluiten bij de strategische richting van de organisatie;
- te bewerkstelligen dat de eisen van het BCMS in de bedrijfsprocessen van de organisatie worden geïntegreerd;
- te bewerkstelligen dat de voor het BCMS benodigde middelen beschikbaar zijn;

- het belang van doeltreffend bedrijfscontinuïteitsmanagement en van het voldoen aan de eisen van het BCMS te communiceren;
- te bewerkstelligen dat het BCMS zijn beoogde resulta(a)t(en) behaalt;
- mensen aan te sturen en te ondersteunen om een bijdrage te leveren aan de doeltreffendheid van het BCMS;
- continue verbetering te bevorderen, en
- andere relevante managementfuncties te ondersteunen om hun leiderschap en betrokkenheid te tonen binnen hun verantwoordelijkheidsgebieden.

OPMERKING 1 Verwijzing naar 'bedrijfs-' in deze internationale norm behoort ruim te worden geïnterpreteerd als de activiteiten die wezenlijk zijn gezien de doelen waarvoor de organisatie bestaat.

De directie moet bewijs kunnen leveren van haar betrokkenheid met betrekking tot het inrichten, implementeren, uitvoeren, monitoren, beoordelen, onderhouden en verbeteren van het BCMS door:

- beleid voor bedrijfscontinuïteit vast te stellen;
- te bewerkstelligen dat de BCMS-doelstellingen en -plannen worden vastgesteld;
- functies, verantwoordelijkheden en bekwaamheden vast te stellen voor bedrijfscontinuïteitsmanagement, en
- een of meer personen aan te wijzen die verantwoordelijk zijn voor het BCMS, met passende bevoegdheden en bekwaamheden om verantwoordingsplichtig te zijn voor het implementeren en onderhouden van het BCMS.

OPMERKING 2 Deze personen kunnen ook andere verantwoordelijkheden binnen de organisatie dragen.

De directie moet bewerkstelligen dat de verantwoordelijkheden en bevoegdheden voor relevante functies worden toegekend en gecommuniceerd binnen de organisatie door:

- de criteria vast te stellen voor de aanvaarding van risico's en aanvaardbare risiconiveaus;
- actief deel te nemen aan oefeningen en testen;
- te bewerkstelligen dat interne audits van het BCMS worden uitgevoerd;
- directiebeoordelingen van het BCMS uit te voeren, en
- haar verbintenis tot continue verbetering aan te tonen.

5.3 Beleid

De directie moet een beleid voor bedrijfscontinuïteit vaststellen dat

- a) passend is voor het doel van de organisatie;
- b) een kader biedt voor het vaststellen van doelstellingen voor bedrijfscontinuïteit;
- c) een verbintenis bevat om te voldoen aan van toepassing zijnde eisen;
- d) een verbintenis bevat tot continue verbetering van het BCMS.

Het BCMS-beleid moet:

- beschikbaar zijn als gedocumenteerde informatie;
- worden gecommuniceerd binnen de organisatie;
- beschikbaar zijn voor belanghebbenden, voor zover van toepassing;
- worden beoordeeld op voortdurende geschiktheid, met geplande tussenpozen en zodra zich significante wijzigingen voordoen.

De organisatie moet gedocumenteerde informatie handhaven over het beleid voor bedrijfscontinuïteit.

5.4 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie

De directie moet bewerkstelligen dat de verantwoordelijkheden en bevoegdheden voor relevante rollen worden toegekend en gecommuniceerd binnen de organisatie.

De directie moet de verantwoordelijkheid en bevoegdheid toekennen met betrekking tot:

- a) het bewerkstelligen dat het BCMS voldoet aan de eisen van deze internationale norm, en
- b) het rapporteren over de prestaties van het BCMS aan de directie.

6 Planning

6.1 Acties om risico's en kansen op te pakken

Bij het plannen voor het BCMS moet de organisatie de in 4.1 genoemde belangrijke punten (issues) en de in 4.2 genoemde eisen overwegen, en de risico's en kansen vaststellen die moeten worden opgepakt om:

- te bewerkstelligen dat het BCMS zijn beoogde resulta(a)t(en) behaalt;
- ongewenste effecten te voorkomen of te verminderen;
- continue verbetering te bereiken

De organisatie moet:

- a) acties plannen om deze risico's en kansen op te pakken;
- b) plannen op welke manier:
 - 1) de maatregelen in haar BCMS-processen worden geïntegreerd en geïmplementeerd (zie 8.1),
 - 2) de doeltreffendheid van deze maatregelen moet worden geëvalueerd (zie 9.1).

6.2 Doelstellingen voor bedrijfscontinuïteit en de planning om ze te bereiken

De directie moet ervoor zorgen dat de doelstellingen voor bedrijfscontinuïteit worden vastgesteld voor en gecommuniceerd naar relevante functies en niveaus binnen de organisatie.

De doelstellingen voor bedrijfscontinuïteit moeten:

- a) consistent zijn met het beleid voor bedrijfscontinuïteit;

- b) rekening houden met het minimumniveau van producten of diensten dat voor de organisatie aanvaardbaar is om haar doelstellingen te bereiken;
- c) meetbaar zijn;
- d) rekening houden met van toepassing zijnde eisen, en
- e) worden gemonitord en passend bij de situatie, worden geactualiseerd.

De organisatie moet gedocumenteerde informatie over de doelstellingen voor bedrijfscontinuïteit bewaren.

Om de doelstellingen voor bedrijfscontinuïteit te bereiken, moet de organisatie vaststellen

- wie er verantwoordelijk is;
- wat er zal worden gedaan;
- welke middelen er nodig zijn;
- wanneer het zal zijn voltooid, en
- hoe de resultaten zullen worden geëvalueerd.

7 Ondersteuning

7.1 Middelen

De organisatie moet de middelen vaststellen en beschikbaar stellen die nodig zijn voor het inrichten, implementeren, onderhouden en continu verbeteren van het BCMS.

7.2 Competentie

De organisatie moet

- a) de noodzakelijke competentie vaststellen van de perso(o)n(en) die onder haar gezag werkzaamheden verricht(en) die de prestaties van de organisatie beïnvloeden;
- b) bewerkstelligen dat deze personen competent zijn op basis van de juiste scholing, opleiding of ervaring;
- c) waar van toepassing, maatregelen nemen om de benodigde competentie te verwerven, en de doeltreffendheid van de genomen maatregelen evalueren, en
- d) geschikte gedocumenteerde informatie als bewijsmateriaal van competentie bewaren.

OPMERKING Geschikte maatregelen kunnen bijvoorbeeld zijn: het voorzien in training van, het begeleiden van, of het in een andere functie benoemen van mensen die al in dienst zijn; of het inhuren of contracteren van competente personen.

7.3 Bewustzijn

Personen die werkzaamheden verrichten onder het gezag van de organisatie, moeten zich bewust zijn van

- a) het beleid voor bedrijfscontinuïteit;
- b) hun bijdrage aan de doeltreffendheid van het BCMS, met inbegrip van de voordelen van verbeterde prestaties van het BCM;

- c) de implicaties van het niet voldoen aan de eisen van het BCMS, en
- d) hun eigen rol tijdens verstorende incidenten.

7.4 Communicatie

De organisatie moet de behoefte vaststellen aan interne en externe communicatie die relevant is voor het BCMS, waaronder

- a) waarover te communiceren;
- b) wanneer te communiceren;
- c) met wie te communiceren.

De organisatie moet (een) procedure(s) vaststellen, implementeren en onderhouden voor:

- interne communicatie tussen belanghebbenden en personeel binnen de organisatie;
- externe communicatie met klanten, partners, de plaatselijke gemeenschap en andere belanghebbenden, waaronder de media;
- het ontvangen, documenteren en reageren op communicatie van belanghebbenden;
- aanpassing en integratie van nationale of regionale adviessystemen voor bedreigingen of vergelijkbare systemen in haar (eigen) planning en operationeel gebruik, voor zover geschikt;
- het zorg dragen voor de beschikbaarheid van communicatiemiddelen tijdens een verstorend incident;
- het faciliteren van gestructureerde communicatie met relevante autoriteiten en het zorg dragen voor de interoperabiliteit van meerdere organisaties en werknemers die reageren (op verstorende incidenten), voor zover van toepassing, en
- het bedienen en testen van communicatievoorzieningen die bedoeld zijn voor gebruik tijdens verstoring van normale communicatievoorzieningen.

OPMERKING Nadere eisen voor communicatie als reactie op een incident zijn gespecificeerd in 8.4.3.

7.5 Gedocumenteerde informatie

7.5.1 Algemeen

Het BCMS van de organisatie moet het volgende omvatten:

- de gedocumenteerde informatie die deze internationale norm vereist, en
- door de organisatie als noodzakelijk voor de doeltreffendheid van het BCMS vastgestelde gedocumenteerde informatie.

OPMERKING De uitgebreidheid van gedocumenteerde informatie voor een BCMS kan van organisatie tot organisatie verschillen vanwege:

- de omvang van de organisatie en het type van haar activiteiten, processen, producten en diensten;
- de complexiteit van de processen en hun interacties, en
- de competentie van de mensen.

7.5.2 Creëren en actualiseren

Bij het creëren en actualiseren van gedocumenteerde informatie moet de organisatie zorgen voor een passend(e):

- a) identificatie en beschrijving (bijv. een titel, datum, auteur of referentienummer);
- b) format (bijv. taal, softwareversie, afbeeldingen) en media (bijv. papier, elektronisch), en beoordeling en goedkeuring van geschiktheid en toereikendheid.

7.5.3 Beheersing van gedocumenteerde informatie

Gedocumenteerde informatie zoals het BCMS en deze internationale norm vereisen, moet worden beheerst om te bewerkstelligen dat:

- a) de informatie beschikbaar is en geschikt is voor gebruik, waar en wanneer het nodig is;
- b) de informatie afdoend is beveiligd (bijv. tegen verlies van vertrouwelijkheid, tegen oneigenlijk gebruik en aantasting).

Voor het beheersen van gedocumenteerde informatie moet de organisatie, voor zover van toepassing, invulling geven aan de volgende activiteiten:

- distributie, toegang, het terugvinden alsmede het gebruik;
- opslag en behoud, waaronder behoud van leesbaarheid;
- beheersing van wijzigingen (bijv. versiebeheer);
- bewaring en vernietiging;
- het terugvinden alsmede het gebruik;
- behoud van leesbaarheid (d.w.z. duidelijk genoeg om te lezen), en
- preventie van onbedoeld gebruik van verouderde informatie.

Gedocumenteerde informatie van externe oorsprong die de organisatie nodig acht voor de planning en uitvoering van het BCMS, moet bij de situatie passend worden geïdentificeerd en worden beheerst.

Bij het vaststellen van de beheersing van gedocumenteerde informatie moet de organisatie bewerkstelligen dat de gedocumenteerde informatie afdoende is beveiligd (bijvoorbeeld beveiliging tegen corruptie, onbevoegde wijziging of verwijdering).

OPMERKING Toegang impliceert een besluit tot toestemming om de gedocumenteerde informatie in te zien, of tot toestemming en bevoegdheid om de gedocumenteerde informatie in te zien en te wijzigen enz.

8 Uitvoering

8.1 Operationele planning en beheersing

Om te voldoen aan de eisen en om de in 6.1 vastgestelde maatregelen te implementeren moet de organisatie de benodigde processen plannen, implementeren en beheersen, door:

- a) criteria voor de processen vast te stellen;
- b) procesbeheersing te implementeren in overeenstemming met de criteria, en

- c) gedocumenteerde informatie bij te houden in de omvang die nodig is om het vertrouwen te hebben dat de processen volgens planning zijn uitgevoerd.

De organisatie moet geplande wijzigingen beheersen en de consequenties van onbedoelde wijzigingen beoordelen, en zo nodig maatregelen treffen om nadelige effecten tegen te gaan.

De organisatie moet bewerkstelligen dat uitbestede processen worden beheerst.

8.2 Bedrijfsimpactanalyse en risicobeoordeling

8.2.1 Algemeen

De organisatie moet een formeel en gedocumenteerd proces voor bedrijfsimpactanalyse en risicobeoordeling vaststellen, implementeren en onderhouden:

- a) waarmee de context van de beoordeling wordt vastgesteld, criteria worden vastgesteld en de mogelijke gevolgen van een verstoring incident worden geëvalueerd;
- b) waarin rekening wordt gehouden met wettelijke en andere eisen die de organisatie onderschrijft;
- c) dat systematische analyse, prioriteitstelling van risicobehandeling en de daarmee samenhangende kosten omvat;
- d) waarin de vereiste output van de bedrijfsimpactanalyse en risicobeoordeling is vastgesteld, en
- e) waarin eisen worden gespecificeerd om deze informatie actueel en vertrouwelijk te houden.

OPMERKING Er zijn diverse methoden voor de bedrijfsimpactanalyse en risicobeoordeling beschikbaar, hetgeen de volgorde bepaalt waarmee bovenstaande punten worden uitgevoerd.

8.2.2 Bedrijfsimpactanalyse

De organisatie moet een formeel en gedocumenteerd evaluatieproces vaststellen, implementeren en onderhouden om prioriteiten, doelstellingen en taakstellingen voor continuïteit en herstel te bepalen. Dit proces moet een beoordeling omvatten van de gevolgen van verstoring van activiteiten die de producten en diensten van de organisatie ondersteunen.

De bedrijfsimpactanalyse moet het volgende omvatten:

- a) identificatie van activiteiten die de levering van producten en diensten ondersteunen;
- b) beoordeling van de gevolgen, na verloop van tijd, wanneer deze activiteiten niet worden uitgevoerd;
- c) het vaststellen van een geprioriteerd tijdschema voor hervatting van deze activiteiten, waarbij een aanvaardbaar minimumniveau wordt gespecificeerd en waarbij rekening wordt gehouden met het tijdbestek waarbinnen de gevolgen onaanvaardbaar worden als de activiteiten niet worden hervat; en
- d) het vaststellen van onderlinge verbanden en ondersteunende middelen voor deze activiteiten, met inbegrip van leveranciers, partners voor uitbesteding en andere relevante belanghebbenden.

8.2.3 Risicobeoordeling

De organisatie moet een formeel en gedocumenteerd proces voor risicobeoordeling vaststellen, implementeren en onderhouden om het risico van verstoring incidenten voor de organisatie systematisch te identificeren, te analyseren en te evalueren.

OPMERKING Dit proces kan worden opgezet in overeenstemming met ISO 31000.

De organisatie moet:

- a) risico's voor verstoring van de geprioriteerde activiteiten van de organisatie identificeren en van de processen, systemen, informatie, personeel, bedrijfsmiddelen (assets), partners voor uitbesteding en andere middelen die deze activiteiten ondersteunen,
- b) risico's systematisch analyseren,
- c) evalueren welke risico's die verband houden met verstoring behandeld moeten worden, en
- d) beheersmaatregelen identificeren die zijn afgestemd op de doelstellingen voor bedrijfscontinuïteit en die in overeenstemming zijn met de risicobereidheid van de organisatie.

OPMERKING De organisatie moet zich realiseren dat bepaalde financiële verplichtingen of verplichtingen van de overheid kunnen vereisen dat deze risico's op uiteenlopende detailniveaus worden gecommuniceerd. Bovendien kunnen bepaalde maatschappelijke behoeften ook publicatie van deze informatie vergen, op een passend detailniveau.

8.3 Strategie voor bedrijfscontinuïteit

8.3.1 Bepaling en selectie

De bepaling en selectie van een strategie moet worden gebaseerd op de output van de bedrijfsimpactanalyse en de risicobeoordeling.

De organisatie moet een geschikte strategie voor bedrijfscontinuïteit bepalen om:

- a) de geprioriteerde activiteiten te beschermen;
- b) geprioriteerde activiteiten tezamen met hun onderlinge verbanden en ondersteunende middelen te stabiliseren, voort te zetten, te hervatten en te herstellen, en
- c) gevolgen tegen te gaan, op gevolgen te reageren en deze te managen.

De bepaling van de strategie moet goedkeuring van geprioriteerde tijdschema's voor hervatting van de activiteiten omvatten.

De organisatie moet het vermogen tot bedrijfscontinuïteit van leveranciers evalueren.

8.3.2 Vaststelling van eisen voor middelen

De organisatie moet bepalen welke middelen worden vereist om de geselecteerde strategieën te implementeren. Dit omvat onder meer de volgende typen middelen:

- a) personeel;
- b) gegevens en informatie;
- c) gebouwen, werkomgeving en bijbehorende voorzieningen;
- d) faciliteiten, uitrusting en verbruiksmaterialen;
- e) systemen voor informatie en communicatietechnologie (ICT);
- f) transport;
- g) financiën, en
- h) partners en leveranciers.

8.3.3 Bescherming en beperking

Voor geïdentificeerde risico's die behandeling vereisen, moet de organisatie proactieve maatregelen overwegen die

- a) de waarschijnlijkheid van verstoring verminderen;
- b) de periode van verstoring verkorten, en
- c) de gevolgen van de verstoring voor belangrijke producten en diensten van de organisatie beperken.

De organisatie moet geschikte risicobeheersmaatregelen kiezen en implementeren, in overeenstemming met haar risicobereidheid.

8.4 Vaststellen en implementeren van procedures voor bedrijfscontinuïteit

8.4.1 Algemeen

De organisatie moet procedures voor bedrijfscontinuïteit vaststellen, implementeren en onderhouden om een verstorend incident te managen en de activiteiten voort te zetten, op basis van doelstellingen voor herstel die geïdentificeerd zijn in de bedrijfsimpactanalyse.

De organisatie moet procedures (met inbegrip van de nodige regelingen) documenteren om continuïteit van activiteiten en management van een verstorend incident te bewerkstelligen.

Deze procedures moeten:

- a) een geschikt protocol voor interne en externe communicatie vaststellen;
- b) specifiek zijn met betrekking tot de stappen die tijdens een verstoring onmiddellijk moeten worden genomen;
- c) flexibel zijn om te kunnen reageren op onverwachte bedreigingen en verandering van interne en externe omstandigheden;
- d) zich richten op de gevolgen van gebeurtenissen die de bedrijfsvoering kunnen verstoren;
- e) worden ontwikkeld op basis van vastgestelde aannames en een analyse van onderlinge verbanden, en
- f) doeltreffend zijn in het minimaliseren van gevolgen, door implementatie van geschikte strategieën voor mitigatie.

8.4.2 Structuur voor reactie op incidenten

De organisatie moet procedures en een managementstructuur vaststellen, documenteren en implementeren om op een verstorend incident te reageren, waarbij personeel wordt ingezet met de nodige verantwoordelijkheden, bevoegdheden en competenties om een incident te managen.

Deze reactiestructuur moet:

- a) drempelwaarden voor gevolgen identificeren die de initiëring van een formele reactie rechtvaardigen;
- b) de aard en omvang van een verstorend incident en de mogelijke gevolgen ervan beoordelen;
- c) activering van een geschikte reactie voor bedrijfscontinuïteit bewerkstelligen;
- d) processen en procedures omvatten voor activering, uitvoering, coördinatie en communicatie van deze reactie;

- e) kunnen beschikken over middelen om de processen en procedures om het managen van een verstorend incident te ondersteunen, teneinde de gevolgen ervan te minimaliseren, en
- f) communicatie omvatten met belanghebbenden en autoriteiten, evenals de media.

De organisatie moet een besluit nemen over externe communicatie over significante risico's en gevolgen en moet dit besluit documenteren. Daarbij moet aan bescherming tegen levensgevaar de hoogste prioriteit worden verleend en moet worden overlegd met relevante belanghebbenden. Als een besluit tot externe communicatie wordt genomen, moet de organisatie procedures vaststellen en implementeren voor deze externe communicatie, alarmmeldingen en waarschuwingen, ook naar de media, voor zover passend.

8.4.3 Waarschuwingen en communicatie

De organisatie moet procedures vaststellen, implementeren en onderhouden om:

- a) een incident te detecteren;
- b) een incident regelmatig te monitoren;
- c) interne communicatie binnen de organisatie te voeren en communicatie van belanghebbenden te ontvangen, te documenteren en daarop te reageren;
- d) communicatie van nationale of regionale adviesorganen te ontvangen, te documenteren en daarop te reageren;
- e) de beschikbaarheid van communicatiemiddelen tijdens een verstorend incident te bewerkstelligen;
- f) gestructureerde communicatie met hulpdiensten te faciliteren;
- g) essentiële informatie te registreren over het incident, de getroffen maatregelen en genomen besluiten; ook het volgende moet worden overwogen en voor zover van toepassing worden geïmplementeerd:
 - het waarschuwen van belanghebbenden die mogelijk gevolgen ondervinden van een daadwerkelijk of dreigend verstorend incident;
 - de interoperabiliteit waarborgen van meerdere organisaties en personeel die tegelijk reageren (op een verstorend incident);
 - het functioneren van een communicatiefaciliteit.

De communicatie- en waarschuwingsprocedures moeten regelmatig worden geoefend.

8.4.4 Bedrijfscontinuïteitsplannen

De organisatie moet gedocumenteerde procedures vaststellen om te reageren op een verstorend incident, waarbij wordt aangegeven hoe de activiteiten worden voortgezet of hervat binnen een vooraf vastgesteld tijdbestek. Dergelijke procedures moeten zijn afgestemd op de eisen van degenen die ze gebruiken.

Tezamen moeten deze bedrijfscontinuïteitsplannen het volgende omvatten:

- a) vastgestelde functies en verantwoordelijkheden voor personeel en teams met bevoegdheden tijdens en na een incident;
- b) een proces om de reactie in gang te zetten;
- c) gegevens om de directe gevolgen van een verstorend incident te managen, waarbij rekening wordt gehouden met:
 - 1) het welzijn van personen,

- 2) strategische, tactische en operationele opties om op de verstoring te reageren, en
- 3) preventie van verder verlies of uitval van geprioriteerde activiteiten;
- d) gegevens over de manier waarop en de omstandigheden waarin de organisatie communiceert met werknemers en hun familieleden, belanghebbenden en contactpersonen voor noodsituaties;
- e) hoe de organisatie haar geprioriteerde activiteiten binnen vooraf vastgestelde tijdbestekken voortzet of hervat;
- f) gegevens over de communicatie met de media na een incident; dit omvat
 - 1) een communicatiestrategie;
 - 2) bij voorkeur te gebruiken interface met de media;
 - 3) richtlijn of sjabloon om een verklaring aan de media op te stellen, en
 - 4) geschikte woordvoerders;
- g) een proces voor neerschaling wanneer het incident voorbij is.

Voor elk plan moet het volgende worden vastgesteld:

- doel en reikwijdte;
- doelstellingen;
- criteria en procedures voor activering;
- procedures voor implementatie;
- functies, verantwoordelijkheden en bevoegdheden;
- eisen en procedures voor communicatie;
- interne en externe onderlinge verbanden en interacties;
- vereiste middelen, en
- informatiestromen en documentatieprocessen.

8.4.5 Herstel

De organisatie moet beschikken over gedocumenteerde procedures om bedrijfsactiviteiten te herstellen en hervatten na de tijdelijke maatregelen die werden getroffen, ter ondersteuning van de eisen voor normale bedrijfsvoering na een incident.

8.5 Oefening en testen

De organisatie moet haar procedures voor bedrijfscontinuïteit oefenen en testen om te bewerkstelligen dat deze in overeenstemming zijn met de doelstellingen voor bedrijfscontinuïteit.

De organisatie moet oefeningen en beproevingen uitvoeren die:

- a) in overeenstemming zijn met de reikwijdte en doelstellingen van het BCMS;

- b) zijn gebaseerd op geschikte scenario's die zorgvuldig zijn gepland met duidelijk vastgestelde doelen en doelstellingen;
- c) na verloop van tijd tezamen het geheel van de regelingen voor bedrijfscontinuïteit valideren, waarbij relevante belanghebbenden worden betrokken;
- d) het risico van verstoring van de bedrijfsvoering minimaliseren;
- e) evaluatierapporten na oefeningen leveren waarin uitkomsten, aanbevelingen en maatregelen formeel zijn vastgelegd om verbeteringen te implementeren;
- f) worden beoordeeld in het kader van bevordering van continue verbetering, en
- g) worden uitgevoerd met geplande tussenpozen en na significante veranderingen in de organisatie of de omgeving waarin de organisatie actief is.

9 Evaluatie van de prestaties

9.1 Monitoren, meten, analyseren en evalueren

9.1.1 Algemeen

De organisatie moet vaststellen

- a) wat moet worden gemonitord en gemeten;
- b) welke methoden worden gebruikt voor het, voor zover van toepassing, monitoren, meten, analyseren en evalueren om geldige resultaten te bewerkstelligen;
- c) wanneer moet worden gemonitord en gemeten, en
- d) wanneer de resultaten van het monitoren en meten moeten worden geanalyseerd en geëvalueerd.

De organisatie moet geschikte gedocumenteerde informatie bewaren als bewijsmateriaal van de resultaten.

De organisatie moet de prestaties van het BCMS en de doeltreffendheid van het BCMS evalueren.

Bovendien moet de organisatie

- waar nodig maatregelen nemen om te reageren op ongunstige trends of resultaten voordat er een afwijking ontstaat, en
- relevante gedocumenteerde informatie als bewijsmateriaal van resultaten handhaven.

De procedures voor het monitoren van de prestaties moeten voorzien in:

- het vaststellen van prestatie-indicatoren passend bij de behoeften van de organisatie;
- het monitoren van de mate waarin beleid, doelstellingen en taakstellingen voor bedrijfscontinuïteit van de organisatie worden nageleefd en gehaald;
- het beoordelen van prestaties van processen, procedures en functies die de geprioriteerde activiteiten beschermen;
- het monitoren van naleving van deze internationale norm en de doelstellingen voor bedrijfscontinuïteit;
- het monitoren van aanwijzingen over ontoereikende prestaties van het BCMS in het verleden, en

— registratie van gegevens en resultaten van monitoring en meting, om het nemen van corrigerende maatregelen te vergemakkelijken.

OPMERKING Afwijkende prestaties omvatten bijvoorbeeld afwijkingen, 'near misses', vals alarm en daadwerkelijke incidenten.

9.1.2 Evaluatie van procedures voor bedrijfscontinuïteit

- a) De organisatie moet haar procedures en vermogens met betrekking tot bedrijfscontinuïteit evalueren, om de continue geschiktheid, toereikendheid en doeltreffendheid ervan te bewerkstelligen.
- b) Deze evaluaties moeten worden uitgevoerd in de vorm van periodieke beoordelingen, oefeningen, beproevingen, rapportage na incidenten en prestatie-evaluaties. Significante wijzigingen die hieruit voortvloeien, moeten tijdig in de procedure(s) worden verwerkt.
- c) De organisatie moet periodiek naleving evalueren van eisen uit wet- en regelgeving, branchespecifieke 'best practices' en naleving van eigen beleid en doelstellingen voor bedrijfscontinuïteit, en
- d) De organisatie moet met geplande tussenpozen en na significante wijzigingen evaluaties uitvoeren.

In geval van een verstorend incident dat tot activering van de procedures voor bedrijfscontinuïteit leidt, moet de organisatie na het incident een beoordeling uitvoeren en de resultaten registreren.

9.2 Interne audit

De organisatie moet met geplande tussenpozen interne audits uitvoeren om informatie te verkrijgen over of het BCMS:

a) overeenkomt met

- 1) de eigen eisen van de organisatie voor haar BCMS;
- 2) de eisen van deze internationale norm, en

b) doeltreffend is geïmplementeerd en onderhouden.

De organisatie moet:

- (een) auditprogramma('s) plannen, vaststellen, implementeren en onderhouden, met inbegrip van de frequentie, methoden, verantwoordelijkheden, planningseisen en rapportage. Het auditprogramma moet rekening houden met het belang van de betrokken processen en de resultaten van voorgaande audits;
- de auditcriteria voor en de reikwijdte van elke audit definiëren;
- auditoren selecteren en audits uitvoeren zodanig dat de objectiviteit en de onpartijdigheid van het auditproces worden bewerkstelligd;
- bewerkstelligen dat de resultaten van de audits worden gerapporteerd aan het relevante management, en
- gedocumenteerde informatie bijhouden als bewijsmateriaal van de implementatie van het auditprogramma en de auditresultaten.

Het auditprogramma, met inbegrip van eventuele schema's, moet zijn gebaseerd op de resultaten van risicobeoordeling van de activiteiten die de organisatie uitvoert, en op resultaten van eerdere audits. De auditprocedures moeten de reikwijdte, frequentie, methoden en competenties, evenals de verantwoordelijkheden en eisen voor het uitvoeren van audits en het rapporteren van de resultaten omvatten.

Het management dat verantwoordelijk is voor het gebied dat een audit ondergaat, moet bewerkstelligen dat, zonder onnodig uitstel, alle noodzakelijke correcties en corrigerende maatregelen worden getroffen om ontdekte afwijkingen en hun oorzaken weg te werken. Vervolgactiviteiten moeten bestaan uit de verificatie van de getroffen maatregelen en rapportage van de verificatieresultaten.

9.3 Directiebeoordeling

De directie moet met geplande tussenpozen het BCMS van de organisatie beoordelen om de continue geschiktheid, toereikendheid en doeltreffendheid te bewerkstelligen.

Bij de directiebeoordeling moet onder andere in overweging worden genomen

- a) de status van acties die zijn voortgekomen uit voorgaande directiebeoordelingen;
- b) wijzigingen in externe en interne belangrijke punten (issues) die relevant zijn voor het BCMS;
- c) informatie over de prestaties van bedrijfscontinuïteit, met inbegrip van trends in:
 - 1) afwijkingen en corrigerende maatregelen;
 - 2) resultaten van evaluatie van monitoren en meten, en
 - 3) auditresultaten;
- d) kansen voor continue verbetering.

Bij een directiebeoordeling behoren de prestaties van de organisatie in beschouwing te worden genomen, met inbegrip van:

- vervolgmaatregelen van vorige directiebeoordelingen;
- de noodzaak wijzigingen aan te brengen in het BCMS, met inbegrip van beleid en doelstellingen;
- kansen voor verbetering;
- resultaten van BCMS-audits en -beoordelingen, ook die van belangrijke leveranciers en partners, voor zover passend;
- technieken, producten of procedures die in de organisatie zouden kunnen worden gebruikt om de prestaties en doeltreffendheid van het BCMS te verbeteren;
- status van corrigerende maatregelen;
- resultaten van oefening en beproeving;
- risico's of onderwerpen die in de vorige risicobeoordeling niet afdoende zijn behandeld;
- eventuele wijzigingen die van invloed kunnen zijn op het BCMS, hetzij intern dan wel extern ten opzichte van het toepassingsgebied van het BCMS;
- toereikendheid van beleid;
- aanbevelingen ter verbetering;
- lessen die zijn geleerd en maatregelen die voortvloeien uit verstoringen incidenten, en
- nieuw opkomende erkende werkwijzen ('good practice') en richtlijnen.

De resultaten van de directiebeoordeling moeten beslissingen omvatten met betrekking tot kansen voor continue verbetering en de mogelijke noodzaak voor wijzigingen in het BCMS. Dit omvat het volgende:

- a) variaties in het toepassingsgebied van het BCMS;
- b) verbetering van de doeltreffendheid van het BCMS;
- c) het bijwerken van de risicobeoordeling, bedrijfsimpactanalyse, plannen voor bedrijfscontinuïteit en daarmee samenhangende procedures;
- d) aanpassing van procedures en beheersmaatregelen om te reageren op interne en externe gebeurtenissen die het BCMS kunnen beïnvloeden, met inbegrip van wijzigingen in de:
 - 1) zakelijke en operationele eisen,
 - 2) eisen voor risicobeperking en veiligheid,
 - 3) operationele omstandigheden en processen,
 - 4) eisen uit wet- en regelgeving,
 - 5) contractuele verplichtingen,
 - 6) risiconiveaus en/of criteria voor risicoaanvaarding,
 - 7) behoeften aan middelen,
 - 8) eisen voor financiering en budgettering; en
- e) hoe de doeltreffendheid van de beheersmaatregelen wordt gemeten.

De organisatie moet gedocumenteerde informatie bewaren als bewijsmateriaal van de resultaten van de directiebeoordeling.

De organisatie moet:

- de resultaten van de directiebeoordeling kenbaar maken aan relevante belanghebbenden, en
- geschikte maatregelen nemen die betrekking hebben op die resultaten.

10 Verbetering

10.1 Afwijkingen en corrigerende maatregelen

Wanneer zich een afwijking voordoet, moet de organisatie:

- a) de afwijking identificeren;
- b) op de afwijking reageren, en indien van toepassing
 - 1) maatregelen treffen om de afwijking te beheersen en te corrigeren, en
 - 2) de consequenties aanpakken.
- c) de noodzaak evalueren om maatregelen te treffen om de oorzaken van de afwijking weg te nemen, zodat de afwijking zich niet herhaalt of zich elders voordoet, door

- 1) de afwijking te beoordelen,
- 2) de oorzaken van de afwijking vast te stellen, en
- 3) vast te stellen of zich gelijksoortige afwijkingen voordoen of zouden kunnen voordoen,
- 4) de noodzaak van corrigerende maatregelen evalueren om ervoor te zorgen dat afwijkingen zich niet herhalen of zich elders voordoen,
- 5) de vereiste corrigerende maatregelen vaststellen en implementeren,
- 6) de doeltreffendheid van getroffen corrigerende maatregelen beoordelen en
- 7) zo nodig, wijzigingen aanbrengen in het BCMS.

d) de benodigde maatregelen implementeren;

e) de doeltreffendheid van getroffen corrigerende maatregelen beoordelen;

f) zo nodig, wijzigingen aanbrengen in het BCMS.

Corrigerende maatregelen moeten passend zijn voor de effecten van de opgetreden afwijkingen.

De organisatie moet gedocumenteerde informatie bijhouden als bewijs van:

- de aard van de afwijkingen en de vervolgens genomen maatregelen, en
- de resultaten van corrigerende maatregelen.

10.2 Continue verbetering

De organisatie moet continu de geschiktheid, toereikendheid of doeltreffendheid van het BCMS verbeteren.

OPMERKING De organisatie kan de processen van het BCMS, zoals evaluatie van leiderschap, planning en prestaties, gebruiken om verbeteringen te bewerkstelligen.

Bibliografie

- [1] ISO 9001, *Quality management systems – Requirements*
- [2] ISO 14001, *Environmental management systems – Requirements with guidance for use*
- [3] ISO 19011, *Guidelines for auditing management systems*
- [4] ISO/IEC 20000-1, *Information Technology – Service Management*
- [5] ISO 22300, *Societal security – Terminology*
- [6] ISO/PAS 22399, *Societal security – Guideline for incident preparedness and operational continuity management*
- [7] ISO/IEC 24762, *Information technology – Security techniques – Guidelines for Information and communications technology disaster recovery services*
- [8] ISO/IEC 27001, *Information Security Management Systems*
- [9] ISO/IEC 27031, *Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*
- [10] ISO 31000, *Risk management – Principles and Guidelines*
- [11] ISO/IEC 31010, *Risk management – Risk assessment techniques*
- [12] ISO/IEC Guide 73, *Risk management – Vocabulary*
- [13] BS 25999-1, *Business continuity management – Code of practice*, British Standards Institution (BSI)
- [14] BS 25999-2, *Business continuity management – Specification*, British Standards Institution (BSI)
- [15] SI 24001, *Security and continuity management systems – Requirements and guidance for use*, Standards Institution of Israel
- [16] NFPA 1600, *Standard on disaster/emergency management and business continuity programs*, National Fire Protection Association (USA)
- [17] *Business Continuity Plan Drafting Guideline*, Ministry of Economy, Trade and Industry (Japan), 2005
- [18] *Business Continuity Guideline*, Central Disaster Management Council, Cabinet Office, Government of Japan, 2005
- [19] ANSI/ASIS SPC.1, *Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use*
- [20] SS 540:2008, *Singapore Standard for Business Continuity Management*
- [21] ANSI/ASIS/BSI BCM.01, *Business Continuity Management Systems: Requirements with Guidance for Use*

Waarom betaalt u voor een norm?

Normen zijn afspraken voor en door de markt, zo ook deze norm. NEN begeleidt het gehele normalisatieproces. Van het bijeenbrengen van partijen, het maken en vastleggen van de afspraken en het bieden van hulp bij de toepassing van de normen. Om deze diensten te kunnen bekostigen betalen alle belanghebbende partijen die aan tafel zitten voor het normalisatieproces, en u als gebruiker voor normen en trainingen. NEN is een stichting en heeft geen winstoogmerk.

Wat is nu precies de toegevoegde waarde van normen?

Stelt u zich eens voor ... u wilt in het buitenland geld pinnen, maar uw bankpas past niet. Of uw nieuwe telefoon herkent uw simkaart niet. De samenstelling van de benzine over de grens is anders, waardoor u niet kunt tanken. Het dagelijks leven zou zonder goede afspraken over producten, processen en diensten een stuk complexer zijn.

Het maken en vastleggen van afspraken door belanghebbende partijen noemen we het normalisatieproces. Normalisatie had vanouds betrekking op techniek en producten. Nu worden steeds vaker normen voor diensten ontwikkeld. Zo zijn er afspraken op het gebied van gezondheidszorg, schuldhulpverlening, kennisintensieve dienstverlening, externe veiligheid en MVO.

Normen zorgen voor verbetering van producten, diensten en processen; qua veiligheid, gezondheid, efficiëntie, kwaliteit en duurzaamheid. Dit ziet u op de werkvloer, in de omgang met elkaar en in de samenleving als geheel. Organisaties die normalisatie onderdeel van hun strategie maken, vergroten hun professionaliteit, betrouwbaarheid en concurrentiekracht.

Wat doet NEN?

NEN ondersteunt in Nederland het normalisatieproces. Als een partij zich tot NEN richt met de vraag om een afspraak tot stand te brengen, gaan wij aan de slag. We onderzoeken in hoeverre normalisatie mogelijk is en er interesse voor bestaat. Wij nodigen vervolgens alle belanghebbende partijen uit om deel te nemen. Een breed draagvlak is een randvoorwaarde. De afspraken komen op basis van consensus tot stand en worden vastgelegd in een document. Dit is meestal een norm. Afspraken die in een NEN-norm zijn vastgelegd mogen niet conflicteren met andere geldige NEN-normen. NEN-normen vormen samen een coherent geheel. Een belanghebbende partij kan een producent, ondernemer, dienstverlener, gebruiker, maar ook de overheid of een consumenten- of onderzoeksorganisatie zijn.

De vraag is niet altijd om een norm te ontwikkelen. Vanuit de overheid komt regelmatig het verzoek om te onderzoeken of er binnen een bepaalde sector of op een bepaald terrein normalisatie mogelijk is. NEN doet dan onderzoek en start afhankelijk van de uitkomsten een project. Deelname staat open voor alle belanghebbende partijen. NEN beheert ruim 30.000 normen. Dit zijn de in Nederland aanvaarde internationale (ISO, IEC), Europese (EN) en nationale normen (NEN). In totaal zijn er ruim 800 normcommissies actief met in totaal bijna 5.000 normcommissieleden. Een goed beheer van de omvangrijke normencollectie en de afstemming tussen nationale, Europese en internationale normcommissies vereisen dan ook een zeer goede infrastructuur.

Betalen kleine organisaties net zoveel als grote organisaties?

Het uitgangspunt is dat alle partijen die deelnemen aan het normalisatieproces een evenredig deel betalen. De normcommissieleden kunnen onderling andere afspraken maken. Zo worden er wel eens afspraken gemaakt dat de grote partijen een groter deel betalen dan de kleinere bedrijven. De prijzen voor normen zijn voor iedereen gelijk. De kosten voor licenties zijn afhankelijk van de omvang van een organisatie en het aantal gebruikers.

Voordelen van normalisatie en normen

Gegarandeerde kwaliteit | Veiligheid geborgd | Bevordert duurzaamheid | Opschalen en vermarkten van nieuwe innovatieve producten | Meer (internationale) handelsmogelijkheden | Verhoogde effectiviteit en efficiëntie | Onderscheidend in de markt.

Voordelen van deelname

Invloed op de (internationale en Europese) afspraken | Als eerste op de hoogte van veranderingen | Netwerk; ook op Europees en internationaal niveau | Kennisvergroting.

NEN

Postbus 5059
2600 GB Delft

Vlinderweg 6
2623 AX Delft

T +31 (0)15 2 690 390
info@nen.nl

www.nen.nl