Nieuwe norm voor Business Continuity Management in het Nederlands beschikbaar

Uw bedrijfscontinuïteit: belangrijker dan ooit

Afgelopen november is de nieuwe editie van ISO 22301 *'Security and resilience - Business continuity management systems – Requirements'* gepubliceerd. Tegelijkertijd is deze ISO-norm als Europese norm aanvaard en daarom ook automatisch als Nederlandse norm geïmplementeerd. In februari is de Nederlandstalige versie verschenen van NEN-EN-ISO 22301 *'Veiligheid en veerkracht - Managementsystemen voor bedrijfscontinuïteit - Eisen'*. In dit artikel wordt ingegaan op het belang en de inhoud van deze norm.

Door Dick Hortensius, consultant managementsystemen NEN

Er zijn elke week wel voorbeelden in het nieuws met problemen op het gebied van bedrijfscontinuïteit. Dat kan heel kleinschalig zijn, zoals een juwelier in het plaatselijke winkelcentrum die een paar dagen dicht is omdat de voorpui eruit ligt vanwege een ramkraak of de buurtsuper die tijdelijk moet sluiten vanwege een gesprongen waterleiding. Het kan ook grootschalig zijn en heel veel mensen treffen. Denk aan de problemen met de aanvoer van kerosine op Schiphol, waardoor veel vluchten moesten worden geannuleerd. Of de universiteit van Maastricht die werd platgelegd na gijzeling met *ransomware*. En heel actueel natuurlijk de uitbraak van het Corona-virus, waardoor wereldwijd leveringsproblemen zijn ontstaan. In alle gevallen is het voor de getroffen bedrijven van groot belang de verstoring zo snel mogelijk te verhelpen en tegelijkertijd – of zo snel mogelijk daarna – weer in de situatie van 'business as usual' te komen. Of in elk geval klanten en andere belanghebbenden op een minimaal acceptabel niveau te kunnen bedienen.

Daarover gaat het bij *business continuity management*: ervoor zorgen dat tijdens een verstoring producten en diensten kunnen worden geleverd op een vooraf vastgesteld niveau wat betreft capaciteit en tijdigheid. Waar rampenbestrijding en crisismanagement zich vooral richten op het verhelpen van de verstoring/calamiteit en het mitigeren van de directe effecten ervan op mens en omgeving, richt bedrijfscontinuïteitsmanagement zich op het tijdens en na de verstoring voortzetten van de essentiële bedrijfsactiviteiten. Dat is letterlijk van levensbelang voor een organisatie, want je kunt heel goed zijn verzekerd tegen schade door brand of wateroverlast, maar dat wil niet zeggen dat je klanten vanzelf weer terugkomen als je ze een tijdje nee hebt moeten verkopen.

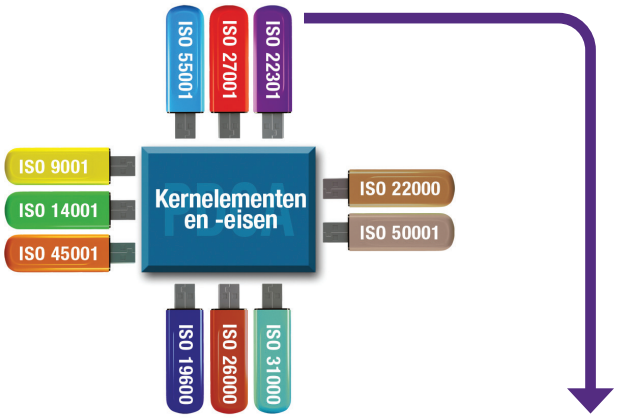
Aantoonbare borging BCM

Bedrijfscontinuïteit is dus van groot belang voor de organisatie zelf, maar vandaag de dag ook voor haar klanten en belanghebbenden. Denk aan een ziekenhuis waar stroomuitval of overstroming fatale gevolgen kan hebben voor patiënten of lang van tevoren geplande operaties in de war kan sturen. Voor een supermarktketen is het een groot probleem als door storing bij een leverancier de schappen met verse zuivel een paar dagen leeg blijven. Of het ontstaan van tekorten aan radiologische medicijnen, door het langdurig stilvallen van een reactor. Doordat in leveringsketens steeds meer 'just in time' wordt gewerkt en door de toenemende logistieke complexiteit van onze maatschappij is bedrijfscontinuïteit een essentieel facet van goede en verantwoorde bedrijfsvoering geworden. Steeds vaker worden daarvoor in de leveringsketen waarborgen in de vorm van certificaten vereist. Logisch dus dat ISO 22301 deel uitmaakt van de ISO-portfolio van managementsysteemnormen.

ISO 22301 en de HLS

De eerste editie van ISO 22301 verscheen in 2012. Het was toen een van de eerste managementsysteemnormen op basis van de *High Level Structure* (HLS). Uiteraard wordt de HLS ook in de 2019-editie weer toegepast. Daarmee behoort ISO 22301 tot de familie van normen die op basis van de HLS via het plug-in model met elkaar verbonden zijn en eenvoudig geïntegreerd zijn toe te passen. In de Nederlandstalige versie komt dat tot uiting en in de geelmarkering van de HLS-tekst (zie figuur 1).

De norm is ontwikkeld onder verantwoordelijkheid van ISO/TC 292 *'Security and resilience'* door TC 292/WG 2 *'Continuity and organizational resilience'*. De Nederlandse inbreng daarbij wordt geleverd door de Nederlandse



NEN-EN-ISO 22301:2019

c) rekening houden met van toepassing zijnde eisen (zie 4.1 en 4.2);

d) worden gemonitord;

e) worden gecommuniceerd;

f) passend bij de situatie worden geactualiseerd.

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

6.2.2 Doelstellingen voor bedrijfscontinuïteit bepalen

Bij het opstellen van planningen voor het bereiken van de doelstellingen voor bedrijfscontinuïteit moet de organisatie vaststellen:

a) wat er zal worden gedaan;

b) welke middelen er nodig zijn;

c) wie er verantwoordelijk is;

d) wanneer het zal zijn voltooid;

e) hoe de resultaten zullen worden geëvalueerd.

6.3 Wijzigingen van het managementsysteem voor bedrijfscontinuïteit plannen

Indien de organisatie vaststelt dat er behoefte is aan wijzigingen in het BCMS, waaronder de wijzigingen die zijn geïdentificeerd in hoofdstuk 10, moeten de wijzigingen op geplande wijze worden uitgevoerd.

De organisatie moet in overweging nemen:

a) het doel van de wijzigingen en de mogelijke gevolgen ervan;

b) de integriteit van het BCMS;

c) de beschikbaarheid van middelen;

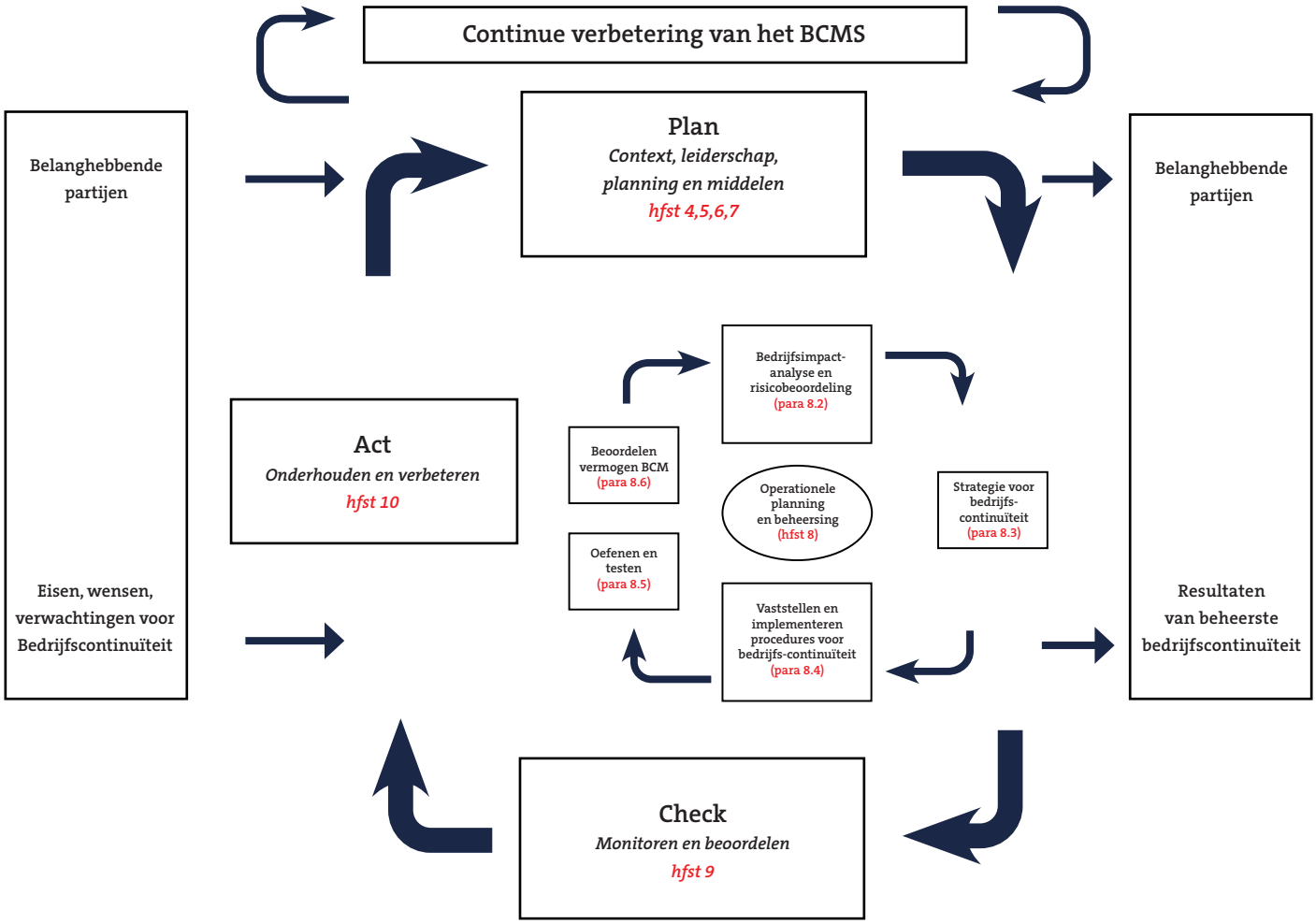
d) de toewijzing of hernieuwde toewijzing van verantwoordelijkheden en bevoegdheden.

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.

Figuur 1: ISO 22301 als deel van de samenhangende ISO-normen voor managementsystemen.



Figuur 2: Overzicht ISO 22301. Verwijzingen in rood naar hoofdstukken en paragrafen in ISO 22301. Dit overzicht is gebaseerd op een figuur uit ISO 22313:2020.

normcommissie 'BCM en crisismanagement' onder voorzitterschap van Gert Kogenhop, (hon.) MBCI en directeur van BCM+. Nederland was actief betrokken bij de ontwikkeling van ISO 22301 en vertegenwoordigd bij de reeks van vergaderingen van de ISO-werkgroep in 2018 en 2019.

ISO 22301 is de belangrijkste norm in een reeks normen en richtlijnen voor BCM: zie het kader.

Integratie BCM in bedrijfsvoering

Het managementsysteem voor bedrijfscontinuïteit (BCMS) is dus gebaseerd op dezelfde principes als bijvoorbeeld kwaliteitsmanagement (ISO 9001) en informatiebeveiliging (ISO 27001). Dat is handig, want bedrijfscontinuïteit is ook belangrijk voor het behoud van tevreden klanten en veel bedrijfsstoringen hebben te maken met uitval van IT. Logisch dus om al deze essentiële facetten van de bedrijfsvoering geïntegreerd te beheersen. Het managementsysteemjasje rond business continuity management in ISO 22301 is de HLS en de operationele BCM-activiteiten zijn beschreven in hoofdstuk 8 van de norm (zie figuur 2). De belangrijkste stappen daarin zijn:

1 Uitvoeren van de bedrijfsimpactanalyse (BIA) en risicobeoordeling.
Hierbij gaat het erom dat een organisatie vaststelt wat de impact is van verstoringen op de activiteiten die zorgen voor de belangrijkste producten en diensten voor klanten. Deze analyse wordt gebruikt om zogenoemde geprioriteerde activiteiten te bepalen waarvoor (herstel van) de continuïteit cruciaal is omdat die grote impact hebben op de dienstverlening van de organisatie en dus op haar stakeholders. De risicobeoordeling moet inzicht geven in de risico's op verstoringen van de geprioriteerde activiteiten en welke daarvan met voorrang moeten worden aangepakt.

2 Bepalen van strategieën en oplossingen voor bedrijfscontinuïteit.
Op basis van de BIA en risicobeoordeling moet de organisatie bepalen op welke manier:
- geprioriteerde activiteiten worden beschermd tegen (de impact van en kans op) verstoringen;
- deze activiteiten worden voortgezet, hervat en hersteld als zich een verstoring voordoet;
- er wordt gereageerd op de gevolgen van verstoringen en deze zoveel mogelijk worden beperkt; en
- wat er allemaal nodig is aan middelen

(mensen, faciliteiten, informatie, financiën, ICT) om dit voor elkaar te krijgen.

3 Vaststellen van plannen en procedures voor bedrijfscontinuïteit en de implementatie daarvan.
De vastgestelde strategieën en oplossingen moeten worden vertaald naar een goede organisatiestructuur, aanpak van communicatie, concrete plannen en procedures voor bedrijfscontinuïteit.

4 Oefenprogramma en periodieke beoordeling van het vermogen van de organisatie op het gebied van bedrijfscontinuïteit.
De plannen en procedures moeten regelmatig worden geoefend en op basis van de bevindingen daarbij worden aangepast. Dit, en de ervaringen bij een daadwerkelijke verstoring, moet de organisatie ook gebruiken om te beoordelen hoe adequaat zij is toegerust om bedrijfscontinuïteit te managen.

Eigenlijk is dit dus een PDCA voor bedrijfscontinuïteitsmanagement binnen het managementsysteem, zoals weergegeven in figuur 2. Hiermee wordt duidelijk dat BCM een specifieke aanpak vraagt, maar wel moet worden ingebed in het managementsysteem van de organisatie en goed moet worden afgestemd met andere disciplines, zoals risicomanagement, crisismanagement en kwaliteitsmanagement.

Toepassing van ISO 22301

ISO 22301 geeft beknopt de eisen voor een BCMS, op basis waarvan een organisatie een certificaat kan behalen. Volgens het jaarlijkse ISO Survey zouden eind 2018 in Nederland 37 certificaten zijn verleend die in totaal 158 locaties beslaan. Gezien het toenemende belang van aantoonbaar bedrijfscontinuïteitsmanagement, is de verwachting dat dit aantal certificaten de komende jaren zal stijgen. Daarnaast zullen veel bedrijven de eisen in ISO 22301 gebruiken om bedrijfscontinuïteit te borgen in hun kwaliteitsmanagementsysteem.

Richtlijnen voor de toepassing van ISO 22301 worden gegeven in ISO 22313, waarvan begin dit jaar een nieuwe editie is verschenen, die ook in het Nederlands is vertaald. **Q**

Voor meer informatie over ISO 22301 kunt u contact opnemen met Dick Hortensius, e-mail: dick.hortensius@nen.nl

Andere richtlijnen voor BCM

ISO 22313:2020 Security and resilience - Business continuity management systems - Guidance on the use of ISO 22301 (Nederlandse vertaling in voorbereiding).

ISO/TS 22317:2015 Societal security - Business continuity management systems - Guidelines for business impact analysis (BIA) (in herziening).

ISO/TS 22318:2015 Societal security - Business continuity management systems - Guidelines for supply chain continuity (in herziening).

ISO/TS 22330:2018 Security and resilience - Business continuity management systems - Guidelines for people aspects of business continuity.

ISO/TS 22331:2018 Security and resilience - Business continuity management systems - Guidelines for business continuity strategy.

ISO/TS 22332 Security and resilience - Business continuity management systems – Guidance for developing business continuity plans and procedures (in ontwikkeling).