bcm+ ISO 22301 MAATSCHAPPELIJKE VEILIGHEID

VEREISTEN VOOR EEN GECERTIFICEERD BUSINESS CONTINUITY MANAGEMENT SYSTEEM (BCMS)

Gert Kogenhop is directeur van bcm+, een bedrijf dat is gespecialiseerd in training, consultancy en implementatie van Business Continuity Management Systemen conform de norm BS 25999 en ISO 22301. Gert heeft een financieel-economische achtergrond en is onder andere werkzaam geweest als Regional Finance Director Northern Europe bij DELL inc. en is een gecertificeerd trainer op het gebied van leidinggeven. Gert is bereikbaar via www.bcmplus.nl of per e-mail: gk@bcmplus.nl

Sinds november 2007 is BS 25999-2:2007 de enige certificeerbare norm voor Business Continuity Management (BCM). Na publicatie van ISO 22301:2012 (Societal security – Business continuity management systems – Requirements) op 15 mei jl. is daar verandering in gekomen. De norm van het British Standards Institution (BSI) zal per 1 november 2012 worden ingetrokken ter faveure van de in 163 landen geaccepteerde ISO norm. Tot die datum is het mogelijk een certificering conform BS 25999 af te ronden. Ook daarna zal een soepele overgang naar de ISO norm worden bewerkstelligd in samenwerking met BSI tot medio 2014.

Wat is BCM volgens ISO 22301?

De definitie wijkt niet substantieel af van de Britse versie, die tot op de dag van vandaag werd gebruikt, en wordt hierin omschreven als: "holistisch managementproces dat potentiële gevaren voor een organisatie identificeert en tot welke gevolgen deze gevaren mogelijk kunnen leiden met betrekking tot de operationele activiteiten. Het schept een kader voor het opbouwen van organisatorische weerstand en veerkracht, leidend tot een effectieve reactie welke de belangen van betrokkenen, reputatie, merk en waarde creërende activiteiten veiligstelt". Met holistisch wordt in dit kader het geheel en de onderlinge samenhang bedoeld, van zowel de organisatie zelf als de directe omgeving, zowel fysiek als de (logistieke en organisatorische) keten met afhankelijkheden beide kanten op. Hier zit tevens het grote verschil met bijvoorbeeld BCM binnen ISO/IEC 27001. Het gaat om de totale organisatie en meer.

Is ISO 22301 anders dan BS 25999?

Als gekeken wordt naar de inhoud van de nieuwe ISO norm wijkt deze technisch gezien niet echt af van de BSI-norm. Enkele definities van gebruikte termen zijn toegevoegd of gewijzigd, terwijl ook enkele zijn verdwenen. Dit laatste omdat deze niet worden toegepast in de ISO-norm of omdat de invulling vrij wordt gelaten. Zaken als het beleidsplan, de feitelijke continuïteitsplannen, de Bedrijfs Impact Analyse (BIA) en Risico Beoordeling (RB), de reactiestructuur en organisatie van het controleren, beoordelen, herzien, onderhouden en continu verbeteren van het managementsysteem zijn enigszins aangescherpt en veranderd op detailniveau, maar leiden zeker niet tot substantiële veranderingen en inspanningen tijdens een eventuele conversie.

De structuur van ISO 22301 is wezenlijk anders dan die van de BS 25999.

Het zes-stappenplan is niet meer terug te vinden, echter de Plan-Do-Check-Act (PDCA) cyclus wel. De grootste wijzigingen zijn vooral terug te vinden op de volgende gebieden:

- Systeembeheer (management);
- Betrokkenheid van het bestuur van de organisatie (top management);
- Communicatie voor, tijdens en na een ernstig incident (disruptive incident).

De nadruk ligt duidelijk op het vaststellen van de doelstellingen van het BCMS (fig. 1). Het meten en controleren van de prestaties, voortgang en gerealiseerde resultaten is een veel belangrijker onderdeel in deze norm. Het vastleggen van de verwachtingen van het bestuur van de organisatie heeft een prominente positie. Meer aandacht wordt geschonken aan de planning en voorbereiding van de inzet van mensen en middelen benodigd voor het zo optimaal mogelijk waarborgen van de bedrijfscontinuïteit. Meer dan voorheen geldt: "Voorbereiding is 90% van het resultaat".

De structuur van ISO 22301 is wezenlijk anders dan die van de BS 25999

Het feit dat de bestuurders van de organisatie volledig betrokken dienen te zijn bij het begrijpen en vaststellen van de benodigdheden (requirements), het bepalen van de doelstellingen en het meten van de resultaten, zal zeker leiden tot een eerdere en betere acceptatie van BCM als wezenlijk onderdeel van "Good Governance", maatschappelijk verantwoord ondernemen.

De inhoud en aanpak conform ISO 22301

Plan

Conform de PDCA cyclus (fig. 2) wordt gestart met de Plan (vaststellen) fase. In deze fase wordt allereerst aandacht besteed aan "context van de organisatie". Zaken met betrekking tot onder andere de activiteiten van de organisatie, functies, producten, diensten, samenwerkingsverbanden, logistieke keten en de relaties met belanghebbenden worden vastgelegd. Dit alles in relatie tot de mogelijke gevolgen van een ernstig incident. In de internationale norm spreekt men overigens nu over "interested parties" en niet meer over "stakeholders". Voorts dient er in het beleidsplan een volledige afstemming te zijn met de missie, visie en doelstellingen van de organisatie en het gewenste risicoprofiel (risk appetite). Tevens dient er rekening te worden gehouden met de behoefte en verwachtingen van de relevante (externe) belanghebbenden en eventueel van toepassing zijnde wet- en regelgeving. Zoals al eerder aangegeven wordt binnen de ISO norm de nadruk duidelijk gelegd op de betrokkenheid (commitment) van het bestuur van de organisatie. Binnen het onderdeel "Leiderschap" wordt hier vorm aan gegeven middels het verantwoordelijk stellen van de bestuurders voor onder andere het:

- vaststellen van het beleidsplan;
- zorg dragen voor het linken van het BCMS aan de strategische richting;
- integreren van het BCMS in alle processen;
  - beschikbaar stellen van de benodigde mensen en middelen;
  - vaststellen van de rollen, verantwoordelijkheden en bevoegdheden van betrokkenen;
  - sturen en ondersteunen van continue verbeteringsinitiatieven;
- communiceren van voortgang en resultaat.

De bestuurders dienen, zoals gesteld, de strategische doelstellingen van het BCMS vast te stellen alsmede de grondbeginselen. Deze bestaan uit het definiëren van de minimale prestatieniveaus met betrekking tot het leveren van producten en/of diensten en bedrijfsactiviteiten, op een dusdanig niveau dat het behalen van de doelstellingen van de organisatie wordt gegarandeerd. Dit alles dient meetbaar te zijn, rekening houdend met betrokken belanghebbenden, en gecontroleerd en bijgestuurd te worden, indien van toepassing.

Als laatste onderdeel binnen de Plan fase dienst men zaken vast te leggen met betrekking tot de uitvoering en ondersteuning. Het gaat hier om de dagelijkse gang van zaken, het zeker stellen dat de juiste mensen en middelen voor elke taak worden ingezet. Onder andere het beschikken over gekwalificeerde mensen met voldoende kennis, vaardigheden en ervaring. Daarna de juiste ondersteuning in de vorm van eventueel mensen van buiten de organisatie, specialisten. Het is van het grootste belang dat iedereen binnen de organisatie beseft wat het belang is van een goed functionerend BCMS en dat men zich bewust is van mogelijke gevolgen bij niet, onvoldoende of zelfs verkeerd reageren (awareness). Belangrijk is zeker in dit geval de communicatie aangaande in eerste instantie het implementatieproces en vervolgens het beheren van het BCMS. Dit alles als vanzelfsprekend ondersteund door een informatiesysteem (document management system) dat een waterdicht "audit trail" garandeert.

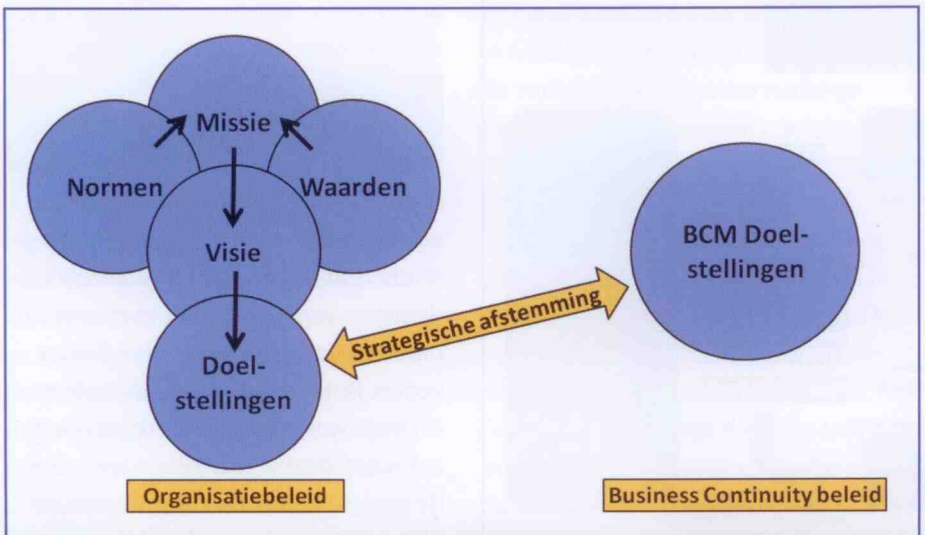
> Binnen de ISO-norm ligt de nadruk duidelijk op de betrokkenheid van het bestuur

Do

De executie van het BCMS is de Do (implementeren en uitvoeren) fase. Dit bevat onder andere de vaststelling van de:

- Bedrijfs Impact Analyse (BIA);
- Risico Beoordeling (RB);
- Business Continuity strategie;
- Business Continuity procedures (BCP);
- test- en oefenprocessen.

Het is van het grootste belang dat continu wordt beoordeeld of de activiteiten in dit kader in lijn liggen met de algemene richting waarin de organisatie zich beweegt. Tevens de wensen en eisen van belanghebbenden, inclusief eventueel van toepassing zijnde wet- en regelgeving. Bij het bepalen van de strategie is het een voorwaarde te kiezen voor haalbare oplossingen, ook al klinkt dat zo logisch en vanzelfsprekend. Afstemming binnen de organisatie, de mensen op de werkvloer, is van doorslaggevend belang bij het implementeren van een (mogelijk/hopelijk) succesvol BCMS. Men dient in



Figuur 1: Strategische afstemming ISO 22301