BS 25999-norm gericht op het beheersen van risico's die de continuïteit bedreigen

De kwaliteitsmanage bedrijfscontinuïteit

ISO 9001 (kwaliteit) en ISO 14001 (milieuzorg) zijn inmiddels bekende normen binnen Nederlandse organisaties. Er staat een nieuwe ISO-norm op stapel, ISO 22301, gebaseerd op de *British Standard* BS 25999. Deze standaard gaat over het beheersen van (externe) risico's die de continuïteit van de organisatie kunnen bedreigen. Als onderdeel van het kwaliteitssysteem van de organisatie zal dit de kwaliteitsmanager de mogelijkheid bieden om zich te ontwikkelen tot de *bewaker* van de continuïteit van de organisatie. Een op z'n minst gezegd 'interessant vooruitzicht'.

Door Gert Kogenhop

Commerciële-, productie- en operationele functies binnen de organisatie zijn voornamelijk bezig met het presteren en de executie van de plannen opgesteld door het management, terwijl de aandacht minder is gericht op bekende en onbekende risico's die het voortbestaan van de organisatie ernstig kunnen bedreigen. Het halen van de gestelde (financiele) doelstellingen staat bovenaan elke agenda. Business Continuity — in goed Nederlands *bedrijfscontinuïteit* — en dan natuurlijk iets specifieker het managen hiervan, verdient zeker een meer prominente plek in de organisatie dan momenteel vaak het geval is. Wanneer de continuïteit van de organisatie in gevaar komt als direct gevolg van een ernstig incident, komen clichés als: 'Hadden we maar…' naar voren. In Engeland is het al een wettelijke verplichting voor veel organisaties om te beschikken over een managementsysteem aangaande de waarborging van de continuïteit van de organisatie (Civil Contingencies Act 2004).

In november 2007 is Business Continuity Management (BCM) als nieuw fenomeen toegevoegd en wel in de vorm van de BS 25999-norm, geschreven door het British Standards Institution. Deze British Standard is direct opgepakt door de International Organization for Standardization (ISO) en zal naar verwachting eind 2011 leiden tot de publicatie van de norm ISO 22301. Maar… kunt en wilt u daar op wachten?

De kwaliteitsmanager (KAM, QA/QC) heeft, naast vakspecifieke normen en certificeringen, vaak ook het ISO 9001-kwaliteitssysteem en het ISO 14001-milieuzorgsysteem onder zijn of haar hoede. Over het algemeen zijn deze systemen zowel verguisd als gewaardeerd, mede daar men deze ervaart als 'opgelegd'. Het voldoen aan de eisen wordt helaas door velen niet gezien als toegevoegde waarde en de kwaliteitsmanager scoort met het *handhaven* van deze normen intern over het algemeen geen populariteitspunten. Hoe anders wordt dit wanneer de kwaliteitsmanager zich kan ontwikkelen tot de *bewaker* van de continuïteit van de organisatie.

> *'Business Continuity verdient zeker een meer prominente plek in de organisatie'*

Het opbouwen van weerstand en veerkracht

Bedrijfscontinuïteit kan worden omschreven als de strategische en tactische vaardigheid van een organisatie om te *plannen voor en te reageren op* incidenten met als direct gevolg disruptie (ernstige ontwrichting) van de organisatie. Doel is te waarborgen dat de organisatie operationeel op minimaal een van tevoren vastgelegd niveau functioneert. BCM dientengevolge is het complete management*proces* dat mogelijke gevaren met betrekking tot de continuïteit van de bedrijfsvoering identificeert en een kader schept voor het opbouwen van weerstand en veerkracht. Door effectief reageren worden de organisatiebelangen, de reputatie alsmede het merk bewaakt. Tevens wordt de executie van de waardecreërende activiteiten gewaarborgd.

In de wereld van de informatietechnologie is het managen van continuïteit dé nummer één prioriteit. Sterker nog, wij eisen van de IT-functie binnen onze organisatie minimaal 99,9% betrouwbaarheid en 'up-time'. Er mag niets gebeuren en als er iets gebeurt, moeten we zo snel mogelijk verder kunnen zonder al te veel vertraging en dataverlies. Het antwoord van de IT-functie op deze (terechte) eisen is dat er onder andere back-up procedures zijn ontwikkeld en dezelfde *realtime* data op verschillende plaatsen (in de wereld) beschikbaar is gemaakt. De afgelopen jaren is men zich gaan realiseren dat dit eigenlijk zou moeten gelden voor *alle* belangrijke functies binnen de organisatie.
Niet geheel verwonderlijk loopt Engeland daarin voorop. Het land heeft in korte tijd

r als bewaker van de

een groot aantal rampen en bijna-rampen te verwerken gekregen. Denk hierbij bijvoorbeeld aan de enorme brand bij Hemel Hempstead in december 2005 (Hertfordshire Oil Storage Terminal), de diverse overstromingen waar men mee te kampen heeft gehad, de terroristische aanslagen en de gevallen van gekke koeienziekte, vogelgriep en varkenspest. In het geval van de brand in Hemel Hempstead is uiteindelijk ongeveer 72% van de bedrijven op het aangrenzende bedrijventerrein als direct aanwijsbaar gevolg hiervan failliet gegaan. In de andere gevallen kunt u zich wellicht voorstellen dat er ernstige gevolgen voor uw organisatie kunnen ontstaan wanneer u zich in het getroffen gebied bevindt of wanneer uw belangrijkste klant(en) en/of leverancier(s) daar gevestigd zijn.

Dichter bij huis zijn daar ook genoeg voorbeelden van. De helikoptercrash in de Bommelerwaard enkele jaren geleden (dagenlang geen stroom); de dreiging van een pandemie (nu wél opeens aandacht voor een continuïteitsplan); het voor langere tijd uitvallen van mobiel telefoonverkeer (Vodafone, eind 2009), met als direct gevolg onder andere geen tramverkeer in de stad Utrecht en zeer recentelijk de extreme weersomstandigheden, waardoor vele werkzaamheden niet konden worden uitgevoerd. Denk echter ook aan de mogelijke gevolgen van een staking; het verdubbelen van de prijs van een belangrijke grondstof; het failliet gaan van nou juist die ene leverancier waarvoor (volgens uw inkoper) geen alternatief voorhanden is; die grote, trouwe relatie die niet meer voor uw organisatie kiest of de overheid, die door veranderende regelgeving een behoorlijke spaak in het wiel steekt. Onder de huidige economische omstandigheden zijn vele risico's veel dreigender geworden en beïnvloeden ze zowel kans als impact. Wanneer u dit zo leest zou u bijna bang worden en dat is wellicht terecht, zeker indien u niet goed voorbereid bent.

Een zes-stappen benadering

In Engeland is de overheid nauw betrokken geweest bij de totstandkoming van de norm BS 25999. Echter ook organisaties uit de verzekeringsbranche als AON en Marsh plus diverse andere commerciële partijen (Sainsbury's, Cable & Wireless, Siemens, Royal Bank of Scotland, KPMG en Deloitte) hebben meegewerkt aan de ontwikkeling van een *werkbare* norm. BS 25999 onderscheidt zich van andere normen omdat het *de gehele organisatie*, alle functies en activiteiten betrekt in het programma. De benadering bevat zes stappen, die uiteindelijk, indien gewenst, kunnen leiden tot certificering door bijvoorbeeld BSI of Lloyds RQA (geaccrediteerd door UKAS). De zes stappen zijn:

1. BCM Programma Management;
2. Begrijpen van de organisatie;
3. Vaststellen van de 'Continuïteit' strategie;
4. Ontwikkelen en implementeren van een BCM-actieplan;
5. Oefenen, onderhouden en herzien van de BCM-structuur en -inhoud; en
6. Onderdeel maken van de organisatiecultuur.

In de eerste stap wordt het Programma Management geregeld: het instellen van het projectteam en het vaststellen van het beleidsplan. Hierin worden o.a. zaken als de uitgangspunten, het doel, de aanpak, het toepassingsgebied, de betrokkenen en het mandaat opgenomen.

Vervolgens wordt in stap twee hieraan invulling gegeven. BS 25999 gaat uit van de voor de organisatie belangrijkste producten en/of diensten. Nadat deze zijn vastgesteld worden alle activiteiten tegen het licht gehouden (bij voorkeur middels het linken aan ISO 9001) en dié activiteiten geselecteerd, die een directe bijdrage leveren aan het tot stand komen van de belangrijkste producten en/of diensten middels een Business Impact Analyse (BIA). Deze activiteiten worden vervolgens geanalyseerd en beoordeeld op gevoeligheid voor een aantal vooraf vastgestelde risico's, waaronder bijvoorbeeld de eerder genoemde voorbeelden. Deze Risico Analyse (RA) is vergelijkbaar met de methodiek binnen ISO 14001. Alles moet beoordeeld worden: van mogelijke staking tot gefailleerde

leverancier, van wetswijziging tot brand en alles wat daar tussen zit. Het gaat hier om de kans en de mogelijke impact van het feit dat een risico een disruptie kan veroorzaken. Niet alle risico's kunnen worden uitgesloten, maar onderdeel van BS 25999 is wel degelijk ook risicomanagement. Hieronder wordt, enigszins kort door de bocht, verstaan: *'Het vermijden, voorkomen of wegnemen van het risico; indien niet mogelijk de kans verkleinen dat het risico een bedreiging wordt en tevens: indien het een bedreiging wordt deze zo klein en kortstondig mogelijk maken'*.

Verantwoordelijkheid bij de kwaliteitsmanager

Nu de 'gevaarlijke' combinatie van geïdentificeerde en gekwalificeerde risico's en de eerder vastgestelde activiteiten, die onze belangrijke producten en/of diensten ondersteunen, zijn bepaald, dienen de volgende mogelijkheden te worden overwogen:

1. Gaan we dit behandelen/afdekken in onze actieplannen (Treat)?
2. Accepteren we dit risico (Tolerate)?
3. Dragen we dit risico over aan derden middels uitbesteding (SLA) of in de vorm van een verzekering (Transfer)?
4. Moeten we deze activiteit beëindigen/opschorten/veranderen (Terminate)?

In de derde stap wordt besloten 'Wat te doen' en nog belangrijker en uitermate krachtig: 'Hoe kunnen we de weerstand en veerkracht van de organisatie verhogen?'. Het vinden van soms eenvoudige mogelijkheden om de kans en impact van een disruptie te verkleinen gedurende de implementatie van dit programma levert een enorme toegevoegde waarde. Het bijvoorbeeld tot de conclusie komen dat men enkele uitermate belangrijke medewerkers in de organisatie heeft rondlopen die specifieke kennis en vaardigheden bezitten, kan leiden tot de beslissing om de vastlegging van procedures en werkvoorschriften nóg strakker te organiseren en kan de implementatie van bijvoorbeeld 'succession planning', 'knowledge sharing' en/of 'job rotation' tot gevolg hebben. Een ander voorbeeld: het vaststellen van het feit dat we voor enkele belangrijke grondstoffen of diensten slechts één leverancier hebben en dat alternatieven nodig zijn, lijkt een open deur, maar is dat voor vele organisaties niet. Al deze activiteiten dienen te worden opgenomen in een separaat actie/verbeterplan met stappen, eigenaren en deadlines, indien nodig voorzien van een budget. Het beheren van het hier geproduceerde 'Weerstand en Veerkracht Plan' is een wezenlijk onderdeel van de suc-

cesvolle implementatie van BCM binnen de organisatie. De verantwoordelijkheid hiervan dient te liggen bij de kwaliteitsmanager, ondersteund door een ondubbelzinnig mandaat vanuit het management van de organisatie.

De invulling met betrekking tot 'Wat te doen?' wordt in een belangrijke mate bepaald door een aantal factoren. Welke activiteiten (met de juiste prioriteit) betreft het? En vervolgens: welke (en hoeveel) mensen en middelen zijn nodig? Verder is het van het grootste belang te weten wat de maximaal toelaatbare periode van de disruptie mag zijn: na welk moment in de tijd gemeten heeft doorgaan geen zin meer en kunnen we beter energie steken in andere zaken? De laatste factor is het minimale activiteitenniveau waarop we tijdelijk kunnen functioneren.

Het smeden van actieplannen

In stap vier worden de actieplannen gesmeed. Allereerst het Incident Management Plan (IMP). Dit is de gedocumenteerde set *procedures en informatie* die is ontwikkeld en samengesteld, met als doel deze in geval van een incident te gebruiken, om er zorg voor te dragen dat de juiste beslissingen worden genomen met betrekking tot mensen, middelen en organisatieactiviteiten:

- Confirm (vaststellen/bevestigen wat er exact aan de hand is);
- Control (zorg dat de situatie onder controle komt);
- Contain (zorg dat de situatie niet verslechtert/escaleert);
- Communicate (communiceer zorgvuldig m.b.t. het incident).

Vervolgens het Business Continuity Plan (BCP): de gedocumenteerde set *procedures en informatie* die is ontwikkeld en samengesteld met als doel deze in geval van een disruptie te gebruiken om het zodoende mogelijk te maken de belangrijke activiteiten van de organisatie te kunnen blijven uitoefenen op in ieder geval een van tevoren vastgelegd (minimaal) niveau.

Als derde actieplan is er het Business Recovery Plan (BRP). In het geval van een ernstige disruptie moet naast aan de continuïteit ook worden gewerkt aan het zo snel mogelijk terugkeren naar de 'normale situatie' van voor het incident. Dit kan het geval zijn wanneer nieuwe huisvesting moet worden gezocht of moet worden herbouwd als gevolg van bijvoorbeeld een brand, een explosie of natuurgeweld.

In de vijfde stap worden onder andere zaken vastgelegd met betrekking tot de oefeningen van de diverse plannen, het onderhoud van het systeem en de periodieke herziening. Voorts de zowel interne als externe 'audits'. Voor de kwaliteitsmanager betekent dit wederom een aanvullende taak in de vorm van integratie met de andere normen in het kwaliteitssysteem van de organisatie, maar ook bijvoorbeeld gecombineerde oefeningen (brand en BHV) en audits. Ook kruisbestuiving is mogelijk, wanneer je denkt aan de Risico Analyse binnen BS 25999 en ISO 14001.

Stap zes is de schil om het totale programma heen. BS 25999 moet onderdeel gaan uitmaken van de organisatiecultuur. Het aloude gezegde 'voorkomen is beter dan genezen' is hier zeker op z'n plaats. Ogen en oren open en meedenken op alle niveaus in de organisatie. Continuïteit is voor iedereen in de organisatie net zo belangrijk. Ook hier ligt een mooie taak voor de kwaliteitsmanager te wachten.

Verantwoordelijk voor waarborging continuïteit

Het is duidelijk voor welke organisaties BCM relevant is, namelijk *alle*; profit en non-profit, bij de overheid en in het bedrijfsleven. Geen enkele organisatie, *lees bestuurder*, mag zich onttrekken aan zijn of haar verantwoordelijkheid om al het mogelijke te doen aan de waarborging van de continuïteit van de organisatie. Tevens moeten we het belang voor onze '*stakeholders*' niet vergeten of onderschatten.

Veel bij de organisatie betrokken partijen zullen de inspanningen op dit gebied met vertrouwen en waardering ontvangen. Klanten, banken en verzekeraars, maar ook leveranciers en niet in de laatste plaats aandeelhouders en werknemers hebben baat bij een organisatie die er morgen ook nog is. Aandacht voor BCM is dan ook van wezenlijk belang.

Het laatste en zeker niet minst belangrijke aspect waarop gewezen moet worden is dat in geval van ernstige bedrijfsschade of erger (faillissement of bedrijfsbeëindiging) de aandeelhouders en/of andere betrokkenen met een belang, mogelijk de correctheid van de handelswijze van bestuurders tijdens de disruptie in twijfel kunnen trekken. 'Kennelijk onbehoorlijk bestuur' kan leiden tot individuele aansprakelijkheid van bestuurders op grond van bestuurdersaansprakelijkheid of zelfs onrechtmatige daad. Het mag duidelijk zijn dat wanneer de bestuurder kan aantonen dat BCM is geïmplementeerd en een correcte en zorgvuldige executie van de geproduceerde plannen heeft plaatsgevonden, men de kans op een succesvol verweer positief beïnvloedt.

'De kwaliteitsmanager kan als bewaker van het BCM-systeem een uiterst belangrijke rol gaan vervullen'

De kwaliteitsmanager kan als *bewaker* van het Business Continuity Management Systeem een uiterst belangrijke rol gaan vervullen en een interessante dimensie toevoegen aan het takenpakket.

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. Regelmatig worden lezingen gegeven, zoals onlangs voor het NNK en binnenkort bij de KwaliteitsKring Noord-Holland. Voor meer informatie kunt u terecht op www.bcmplus.nl of per e-mail: gk@bcmplus.nl.