# Borging en onderhoud van continuïteitsmaatregelen

Drs. R. van Petegem en ir. A.T. Wijsman RE MBCI

**Het regelen van bedrijfscontinuïteit houdt niet op bij de afronding van een bedrijfscontinuïteitsplan (BCP). Er moet ook een managementproces worden ingericht, waarmee wordt geborgd dat het BCP en alle technische en organisatorische voorzieningen worden onderhouden en ook periodiek worden getest. Zonder onderhoud verliest een BCP snel zijn waarde. Juist dit onderhoud blijkt in de praktijk voor veel organisaties een knelpunt te zijn. In dit artikel wordt een aantal factoren benoemd die helpen bij het inrichten van een managementproces voor continuïteit (BCM) waarbij daadwerkelijk onderhoud wordt uitgevoerd.**

## Inleiding

Het treffen van maatregelen voor het borgen van de continuïteit van bedrijfsprocessen is altijd van belang geweest. Vroeg of laat ontstaat binnen elke organisatie wel een aanleiding om op dit gebied een en ander te gaan regelen. De aanleiding kan bijvoorbeeld zijn: het bezoek van een toezichthouder, een klacht van een klant, een incident binnen het bedrijf of een gebeurtenis in de omgeving. Voorbeelden van zulke gebeurtenissen zijn de overstroming in New Orleans en (dreigende) aanslagen zoals in de Verenigde Staten, Spanje en het Verenigd Koninkrijk.

De echte beweegredenen om de continuïteit te waarborgen verschillen van organisatie tot organisatie, maar desgevraagd worden in de praktijk van KPMG één of meer van de volgende argumenten genoemd:

- het voldoen aan wet- en regelgeving, het 'afschudden' van toezichthouders;
- het voldoen aan verwachtingen van en afspraken met afnemers;
- bescherming van de cashflow ('als de schoorsteen niet rookt, dan wordt er niets verdiend');
- bescherming van de reputatie door het voorkomen van negatieve publiciteit;
- bescherming van de belangen van aandeelhouders (aandelenkoers);
- maatschappelijke verantwoordelijkheid;
- bescherming van de belangen van medewerkers;
- het voorkomen van schadeclaims;
- het voorkomen van vertraging bij de ontwikkeling en introductie van nieuwe producten;
- en ten slotte wordt steeds vaker onderkend dat continuïteitsmanagement zelfs kan worden ingezet voor het behalen van concurrentievoordeel, in het bijzonder door de leverbetrouwbaarheid van concurrenten te overtreffen.

*Drs. R. van Petegem*
is adviseur bij KPMG IT Advisory. Hij is betrokken bij dienstverlening op het gebied van risico- en continuïteitsmanagement en IT-sourcing. Hij houdt zich momenteel onder meer bezig met advisering betreffende de uitvoering van informatiebeveiligingsbeleid.

vanpetegem.reinier@kpmg.nl

*Ir. A.T. Wijsman RE MBCI*
is manager bij KPMG IT Advisory en is medeverantwoordelijk voor de dienstverlening van KPMG op het gebied van business continuity management. Hij heeft uitgebreide ervaring met risico- en continuïteitsmanagement en met organisatorische en beheeraspecten van informatiebeveiliging.

wijsman.antoine@kpmg.nl

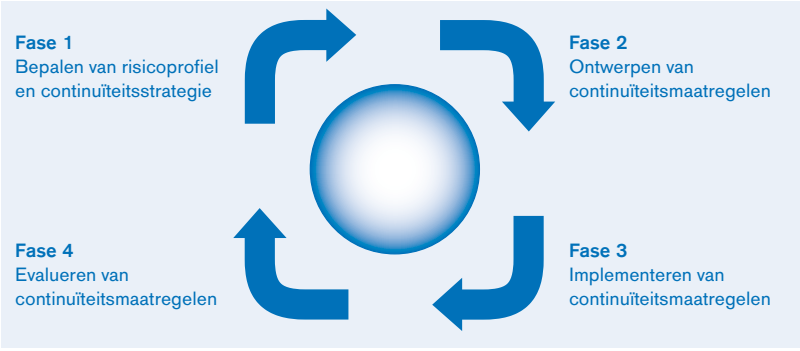
Als naar aanleiding van een interne of externe gebeurtenis een organisatie daadwerkelijk een project voor het borgen van de bedrijfscontinuïteit initieert, is het van belang dat opdrachtgever en projectgroep verder kijken dan de doelstelling om een bedrijfscontinuïteitsplan (BCP) op te leveren. Een BCP is samen met geïmplementeerde technische voorzieningen vaak wel één van de meest tastbare resultaten van een dergelijk project, maar het is eigenlijk pas geslaagd als ook het bijbehorende managementproces – business continuity management (BCM) – duurzaam is ingericht (een voorbeeld van zo'n proces is weergegeven in figuur 1). BCM zorgt ervoor dat de opgeleverde voorzieningen ook daadwerkelijk worden onderhouden en getest. De praktijk wijst echter uit dat structureel onderhoud van de procedures en voorzieningen bij veel organisaties een aandachtspunt is. Organisatorische en technische veranderingen volgen elkaar in een dusdanig hoog tempo op, dat een BCP snel kan verouderen. Ter illustratie, velen herkennen ongetwijfeld de situatie dat een collega na een periode van afwezigheid over tal van ontwikkelingen en nieuwe werkwijzen moet worden bijgepraat.

Dat het bovengenoemde aandachtspunt precies de grote uitdaging van veel organisaties is, blijkt uit een onderzoek dat KPMG in 2006 heeft uitgevoerd ([KPMG06]). Van de deelnemende organisaties:

- gaf 36% van de organisaties met een BCP toe dat dit BCP een jaar of langer niet was geactualiseerd;
- gaf 40% aan dat niet met het BCP wordt geoefend.

De conclusie die hieruit werd getrokken, luidde dan ook dat continuïteit op papier vaak wel is geregeld, maar dat het meestal niet zeker is of continuïteitsvoorzieningen in de praktijk ook goed werken.

In dit artikel wordt ingegaan op de uitdaging om een managementproces voor continuïteit in te richten. Aan de orde komt een aantal succesfactoren voor een situatie waarin continuïteitsvoorzieningen daadwerkelijk worden onderhouden en getest.




Figuur 1. Het BCM-proces volgens de KPMG BCM Methodologie.

## De koppeling van BCM met bedrijfsactiviteiten en/of IT-beheeractiviteiten

Managers zien informatiebeveiliging nog te vaak als een opzichzelfstaand fenomeen en niet als een integraal onderdeel van de bedrijfsvoering ([Over05]). Hierdoor is informatiebeveiliging onvoldoende geïntegreerd in de werkprocessen. Deze integratie is helaas over het algemeen ook onvoldoende voor BCM-processen. Om dit te voorkomen is het van belang dat het hoger management de verantwoordelijkheid neemt voor BCM en dat de IT-manager en de IT-organisatie volgend zijn ([Debe04]).

Wat is het gevolg als het hoger management onvoldoende zijn verantwoordelijkheid neemt voor BCM? Organisaties ervaren in dat geval pas bij het simuleren of optreden van calamiteiten dat BCP's niet volledig en/of juist zijn. BCP's, een resultaat van BCM, zijn de plannen die in werking treden in het geval van een calamiteit. Doordat het oefenen met BCP's vaak niet plaatsvindt ([KPMG06]), is het hoger management zich vaak niet eens bewust van onvolledigheid en/of onjuistheid van BCP's. Hierdoor bestaat het risico van ongewenste (langdurige) uitval van bedrijfsprocessen in geval van het optreden van calamiteiten. Dit probleem is op te vangen door het invoeren van twee maatregelen, namelijk het periodiek uitvoeren van BCP-tests en het inrichten van een onderhoudsproces voor alle onderdelen van een BCP.

Om periodiek kwalitatief goede tests te kunnen uitvoeren is het van belang dat in de periode tussen het plaatsvinden van de tests onderhoud op BCP's plaatsvindt als onderdeel van de reguliere bedrijfsprocessen. Met deze benadering realiseert de organisatie een beleid dat zowel reactief als proactief is. Het onderhoud moet onder andere gericht zijn op het continu vastleggen en onderhouden van de afhankelijkheden die bestaan tussen en binnen de ketens van (IT-)componenten die samen een bedrijfsproces of IT-dienst vormen (zie kader 1 voor een uitleg over ketenafhankelijkheden).

Waarom is het belangrijk dat deze afhankelijkheden duidelijk in kaart worden gebracht en gehouden? De prioriteit van de directie van een bedrijf wordt meestal bepaald op het niveau van bedrijfsprocessen. Op directieniveau wordt vastgesteld wat de kritieke bedrijfsprocessen zijn. Deze processen dienen in geval van een calamiteit binnen een vastgestelde tijd weer in productie te zijn. Om dit effectief te kunnen uitvoeren is het van belang dat inzichtelijk is van welke componenten de bedrijfsprocessen afhankelijk zijn. Op basis daarvan kan het bedrijf investeren in de juiste BCM-oplossingen die leiden tot BCP's die het bedrijf periodiek test.

Een organisatie kan niet zonder bedrijfsprocessen. Om deze bedrijfsprocessen te laten functioneren is een aantal middelen nodig, waaronder applicaties, mensen, procedures, grond- en hulpstoffen, etc. Deze middelen zijn op hun beurt weer afhankelijk van een aantal andere middelen. Applicaties bijvoorbeeld zijn voor hun functioneren weer afhankelijk van onder meer het netwerk, servers en andere applicaties.
Een voorbeeld: het bedrijfsproces inkoop heeft voor zijn dagelijkse werkzaamheden SAP nodig. SAP is beschikbaar via een cliënt die afhankelijk is van de beschikbaarheid van onder andere een applicatieserver en databaseserver van de organisatie. De applicatie- en databaseserver kunnen afhankelijk zijn van een licentie. Om de inkooporders te versturen vanuit SAP naar de leveranciers is tevens een externe koppeling, voor het uitwisselen van inkoopbestanden, met de leverancier noodzakelijk. Dit voorbeeld illustreert een aantal kritische componenten die van elkaar afhankelijk zijn en die samen als keten noodzakelijk zijn voor een inkoopproces.

Kader 1. Ketenafhankelijkheden.

Tabel 1 toont een mogelijke indeling van de componenten die van belang kunnen zijn voor een bedrijfsproces. Tussen deze componenten bestaan afhankelijkheden. Voorbeelden hiervan zijn applicaties die onderling afhankelijk zijn, zoals een klantensysteem of een relatiebeheersysteem dat klantgegevens verstrekt aan andere applicaties. Diezelfde applicaties kunnen op hun beurt bijvoorbeeld afhankelijk zijn van gegevensverzamelingen of koppelingen (interfaces) met derden.

Een organisatie met een tiental applicaties zal niet heel veel moeite hebben met het opstellen van een afhankelijkhedenschema. Veel middelgrote en grote organisaties hebben een applicatielandschap met meer dan honderd applicaties en een veelvoud aan afhankelijkheden (relaties) met bijvoorbeeld andere applicaties, databases, servers, (externe) koppelingen, organisatieonderdelen en bedrijfsprocessen. Deze afhankelijkheden kunnen tevens bestaan tussen en binnen ketens van bedrijfsprocessen.

Hoe gaan organisaties hier over het algemeen mee om? Soms beschikken organisaties over een schema waarin de initiële situatie van afhankelijkheden is vastgelegd. In de praktijk is de ervaring dat dergelijke schema's niet onderhouden worden en afhankelijk van de organisatie al na een half jaar of eerder verouderd zijn. De oorzaak is maar al te vaak dat niemand verantwoordelijk is of de verantwoordelijkheid neemt voor het vastleggen en onderhouden van deze afhankelijkheden. Een deel van de oplossing kan zijn om het onderhoud duidelijk te beleggen in de organisatie. Daarmee is een oplossing echter nog niet geïmplementeerd. Het risico bestaat namelijk nog steeds dat de BCP's niet tijdig zijn aangepast doordat wijzigingen in bijvoorbeeld de organisatie, de bedrijfsprocessen of het applicatielandschap niet tijdig zijn gemeld.

| Componenten | Relatieschema's |
|---|---|
| 1 Applicaties | 1 Applicaties - applicaties |
| 2 Gegevensverzamelingen | 2 Applicaties - gegevensverzamelingen |
| 3 IT-infrastructuur | 3 Gegevensverzamelingen - IT-infrastructuur |
| 4 Koppelingen & verbindingen | 4 Applicaties - IT-infrastructuur |
| 5 Organisatie | 5 Applicaties - koppelingen |
| 6 Bedrijfsprocessen | 6 Applicaties - organisatie |
| | 7 Applicaties - bedrijfsprocessen |

Tabel 1. Voorbeeld van een afhankelijkhedenschema.

Een bekend ITIL-proces waarmee organisaties dit kunnen ondervangen, is configuration management. Dit proces is niet een opzichzelfstaand proces maar moet gekoppeld zijn aan change management en release management (definities in kader 3), zodanig dat tijdens het uitvoeren van een wijziging die wijziging direct wordt verwerkt in een CMDB. Het configuration-managementproces moet daarbij zodanig zijn ingericht dat van alle componenten die van belang zijn voor de continuïteit van de organisatie, de relaties zijn vastgelegd.

Een Business Continuity Plan (BCP) beschrijft onder andere ([BSI03]):
- de scope van het BCP;
- doelstellingen van het BCP, zoals hersteltijden en toegestane hoeveelheid dataverlies in uren of dagen;
- eigenaar van het BCP;
- noodzakelijke organisatiestructuur – inclusief taken, bevoegdheden en verantwoordelijkheden – in het geval van een calamiteit. Voorbeelden zijn het crisisteam en de uitwijkteams;
- uitwijkprocessen, zoals het melden van een calamiteit, het creëren van een oplossing voor een calamiteit en het herstellen van de gevolgen van de calamiteit.

Kader 2. Business Continuity Plan.

*Configuration Management Database (CMDB)*: de administratie van de configuratie-items, namelijk ieder productiemiddel waarvan het bestaan en de versie geregistreerd worden inclusief de daaruit resulterende diensten.

*Change management*: het gecontroleerd begeleiden van wijzigingsverzoeken zodanig dat storingen als gevolg van wijzigingen uitgevoerd op configuratie-items beperkt blijven.

*Release management*: proces voor het waarborgen van de kwaliteit van de productieomgeving door gebruik te maken van formele procedures en controles bij het implementeren van nieuwe versies.

Kader 3. Toelichting beheerprocessen ([ITSM04]).

Voor de effectiviteit van een dergelijk proces is het van groot belang dat taken, bevoegdheden en verantwoordelijkheden, zoals beschreven in het vervolg van dit artikel, zijn vastgelegd en dat personeel hierop wordt afgerekend. Een voorbeeld: een uitgevoerde wijziging mag worden afgesloten als 'voltooid', nadat de change manager heeft vastgesteld dat:

- de wijziging succesvol is uitgevoerd;
- de wijziging is vastgelegd, inclusief een evaluatie van de wijziging (lessons learned e.d.);
- het resultaat van de wijziging is verwerkt in de CMDB;
- het resultaat van de wijziging is verwerkt in de BCP's.

Een dergelijke wijziging kan bijvoorbeeld een release van een nieuwe applicatie zijn, een wijziging in de organisatie met gevolgen voor de samenstelling van crisisteams of een wijziging in de infrastructuur.

De change manager is ervoor verantwoordelijk dat uiteindelijk alle changes kunnen worden afgesloten. Hiervoor heeft hij de bevoegdheid om bijvoorbeeld de configuration manager erop aan te spreken dat het verwerken van de changes in de CMDB en de BCP's ook daadwerkelijk plaatsvindt.

Om zekerheid te verkrijgen over de werking van het configuration-managementproces is het van belang dat organisaties periodiek steekproefsgewijs de inhoud van de CMDB verifiëren.

**De lezerskring van het BCM-beleid blijft niet zelden beperkt tot de auditors en/of de consultants**

Het inrichten van het configuration-managementproces kan een organisatie, naast een effectiever BCM-proces, velerlei voordelen opleveren, zoals:

- efficiënter incident en problem management, doordat de helpdesk en de tweedelijnsorganisatie sneller inzicht hebben in de configuratie;
- efficiënter change management, indien afhankelijkheden tussen componenten in de CMDB inzichtelijk zijn;
- effectiever licentiemanagement.

### De inbedding van BCM in de organisatie

Voor een effectief BCM-proces is het van belang dat de verantwoordelijkheden voor continuïteit op de juiste plaats zijn belegd. Belangrijker nog is echter dat deze verantwoordelijkheden ook daadwerkelijk worden genomen. Het komt in de praktijk vaak voor dat business continuity of informatiebeveiligingsfunctionarissen eigenhandig een business continuity beleid opstellen waarin de verantwoordelijkheden geheel of grotendeels 'volgens het boekje' worden beschreven:

- De directie is eindverantwoordelijk voor BCM, bekrachtigt het BCM-beleid, accordeert de continuïteitsstrategie en stelt een passend budget ter beschikking.
- De proceseigenaren uit de *business* zijn verantwoordelijk voor de continuïteit van hun eigen proces. Zij leveren input voor business-impactanalyses en risicoanalyses die onder hun verantwoordelijkheid worden uitgevoerd en stellen de continuïteitseisen vast, waaronder de maximale uitvalsduur en het maximale gegevensverlies. Deze proceseigenaren zijn tevens verantwoordelijk voor het actueel houden van hun eigen business continuity plan (of hun deel van het bedrijfsbrede business continuity plan).
- De IT-afdeling is verantwoordelijk voor het inrichten en onderhouden van de continuïteitsmaatregelen ten aanzien van de IT-voorzieningen. De IT-afdeling conformeert zich hierbij aan de eisen van de proceseigenaren uit de business.
- De business continuity functionaris (vaak business continuity manager, business continuity officer of business continuity coördinator genoemd) is verantwoordelijk voor het gevraagd en ongevraagd inhoudelijk adviseren van proceseigenaren en directie over BCM. Verder coördineert hij/zij activiteiten uit het BCM-proces, organiseert hij/zij afstemming op dit gebied tussen bedrijfsonderdelen en ontwikkelt hij/zij templates en tools voor BCM-activiteiten en documentatie. Deze rol wordt vaak vervuld door een (informatie)beveiligingsfunctionaris.
- De interne en/of externe auditor is verantwoordelijk voor onafhankelijke beoordeling van en rapportage over de opzet, het bestaan en de werking van BCM-maatregelen. De auditor rapporteert aan de eindverantwoordelijke, zijnde de directie of Raad van Bestuur.

Helaas krijgt het bovengenoemde beleidsdocument van de directie om diverse redenen niet altijd de aandacht en/of bekrachtiging die het verdient. Daarnaast komt het niet zelden voor dat de lezerskring van het BCM-beleid niet veel verder strekt dan de auditors en/of de consultants die worden ingehuurd om een BCP op te stellen. Hoe kunnen we ervoor zorgen dat de verantwoordelijkheden ten aanzien van BCM echt worden genomen? Hieronder volgen drie succesfactoren:

- Ten eerste is essentieel dat de eindverantwoordelijke (directie of Raad van Bestuur) het belang van BCM expliciet erkent. Hierdoor wordt automatisch op alle niveaus over het onderwerp gesproken. Deze gesprekken genereren weer de nodige awareness bij het lijnmanagement, waaruit vervolgens actie voortkomt. Bij dit punt moet worden opgemerkt dat erkenning van het belang van BCM door het topmanagement niet eenvoudig kan worden afgedwongen. Dit vereist een zorgvuldig proces waarbij timing, het hebben van de juiste argumenten, het kiezen van de juiste vorm en overtuigingskracht sleutelfactoren zijn.

• Ten tweede kan het opnemen van de BCM-prestatie in een balanced scorecard of ander soort dashboard, en uiteindelijk in de beoordeling van een proceseigenaar bevorderlijk werken. Het mag kinderachtig lijken, maar in de praktijk blijkt dat zaken aandacht krijgen als ze direct van invloed zijn op een beoordeling.
• Ten derde moeten medewerkers kunnen 'scoren' met het onderwerp BCM. Indien bijvoorbeeld een uitwijktest succesvol is verlopen, mag dit niet ongemerkt aan de rest van de organisatie voorbijgaan. Er moet dus de nodige interne en eventueel ook externe publiciteit aan worden gegeven, waarbij de betrokken afdelingen en/of medewerkers bij naam worden genoemd.

### Outsourcing van BCM-activiteiten

Bijna alle activiteiten op het gebied van continuïteit kunnen aan een externe partij worden uitbesteed. In drukke perioden is de verleiding groot om zoveel mogelijk van deze taken uit te besteden. De stelregel waarop men zich daarbij doorgaans baseert is dat alleen de zaken waarmee een bedrijf zich echt van de concurrentie onderscheidt binnenshuis moeten worden uitgevoerd, zodat het concurrentievoordeel beschermd blijft. Omdat de meeste bedrijven zich niet in de eerste plaats van concurrenten willen onderscheiden op het vlak van continuïteit, bestaat het risico dat te veel wordt uitbesteed. Vanuit de praktijk kunnen de volgende vuistregels ten aanzien van het al dan niet uitbesteden van continuïteitsgerelateerde activiteiten worden gegeven.

**Niet uitbesteden:**
• Het is niet verstandig om business continuity *management*-taken of regiefuncties uit te besteden, tenzij dit op zeer tijdelijke basis is. De verantwoordelijkheid voor het beheer van continuïteit hoort thuis bij het lijnmanagement. Uitbesteding hiervan kan de betrokkenheid van het lijnmanagement bij BCM negatief beïnvloeden. Bovendien geeft een lijnmanager hiermee ongewild het signaal af dat dit een minder belangrijk en/of interessant aspect van de bedrijfsvoering is.
• *Permanente* ondersteuning bij coördinatie en/of praktische uitvoering van het BCM-beleid op detacheringsbasis. Het verdient voorkeur de kennis die hiervoor benodigd is in huis te hebben en te houden. Zelf de coördinatie voeren betekent vaak ook een betere integratie in de overige bedrijfsprocessen.
• Het inhoudelijke onderhoud van BCP's. Eigen medewerkers zijn over het algemeen beter op de hoogte van de veranderingen in organisatie en infrastructuur dan externe medewerkers. De interne medewerkers zullen in een crisissituatie met het BCP moeten werken. Tevens bevordert het periodiek en proactief bezig zijn met onderhoud de kennis van en betrokkenheid bij het BCP.

**Wél uitbesteden:**
• Het oplossen van specialistische vraagstukken die zich zelden manifesteren;
• het leveren van templates voor business-impactanalyses, risicoanalyses, BCP's;
• het faciliteren van het onderhoud van BCP's;
• het leveren van software voor het opstellen en/of onderhouden van BCP's;
• *tijdelijke* ondersteuning bij coördinatie en/of praktische uitvoering van het BCM-beleid op detacheringsbasis;
• het verzorgen van cursussen of workshops op het gebied van continuïteit, mits deze kennis niet binnen de eigen organisatie beschikbaar is;
• het uitvoeren van onafhankelijke audits;
• het leveren van onafhankelijke adviesdiensten.

### Samenvatting

Business continuity management is meer dan het opstellen van een bedrijfscontinuïteitsplan (BCP). Organisaties moeten ook een managementproces voor continuïteit inrichten. Hiermee wordt continu onderhoud van de documentatie en voorzieningen geborgd. In dit artikel is een aantal factoren genoemd die helpen bij het inrichten van een managementproces voor continuïteit (BCM) waarbij daadwerkelijk onderhoud wordt uitgevoerd. Ten eerste is van belang dat de BCM-processen worden geïntegreerd in de bedrijfsactiviteiten en (IT-)beheeractiviteiten. Enerzijds om zorg te dragen dat organisaties afhankelijkheden tussen en binnen de ketens zodanig vastleggen dat kritieke bedrijfsprocessen altijd hersteld kunnen worden. Anderzijds om BCP's zodanig te onderhouden dat zij in geval van calamiteiten altijd effectief ingezet kunnen worden.

**De verantwoordelijkheid voor het beheer van continuïteit hoort thuis bij het lijnmanagement**

Ten tweede moet BCM goed in de organisatie worden ingebed. Dit is niet alleen een kwestie van het formeel in een beleid vaststellen van verantwoordelijkheden. De eindverantwoordelijke (directie of Raad van Bestuur) moet het BCM-beleid ook expliciet erkennen en liefst zelf actief uitdragen, zodat het belang ervan op alle niveaus in de organisatie wordt ingezien. Verder kan het opnemen van BCM-aspecten in de individuele beoordeling van lijnmanagers de prioriteitstelling beïnvloeden en daarmee de daadwerkelijke realisatie van BCM-doelstellingen bevorderen.

Ten derde werkt het goed en stimulerend als binnen de organisatie ruime aandacht wordt besteed aan successen op dit gebied, en de betrokkenen voor hun prestaties worden beloond.

Ten slotte moet een organisatie zorgvuldige keuzen maken met betrekking tot het al dan niet uitbesteden van BCM-gerelateerde activiteiten. Factoren die hierbij een rol spelen zijn het behoud en beheer van relevante kennis, het behouden van betrokkenheid bij het BCM-proces en de procedures in het BCP.

## Literatuur

[BSI03] British Standards Institution, *PAS 56:2003, Guide to Business Continuity Management*, 2003.

[Debe04] Drs. S. Debets MBA MSIT en dr. D. Leegwater, *Continuïteitseisen veranderen verantwoordelijkheid IT-manager*, Automatisering Gids maart 2006.

[KPMG06] *Onderzoek Informatiebeveiliging; Zes belangrijke signalen uit de praktijk*, KPMG Information Risk Management, 2006.

[Over05] Dr. ir. P.L. Overbeek RE, prof. dr. E.E.O. Roos Lindgreen RE en dr. M.E.M. Spruit, *Informatie-beveiliging onder controle?*, Compact 2005/1.

[ITSM04] *IT Service Management, een introductie*, V4.0, januari 2004. ISBN 90-806713-2-0.