Bestaande standaarden voor continuïteitsmanagement en PAS56

Ir. A.T. Wijsman RE MBCI

Nieuwe wet- en regelgeving is in het huidige tijdsgewricht een belangrijke *driver* voor continuïteitsmanagement. Duidelijk wordt vanuit de eisen dát bedrijfscontinuïteit moet worden geregeld. Minder duidelijk is hoe het moet worden geregeld en veel organisaties worstelen met de realisatie en vooral met de inbedding en borging van continuïteitsmanagement in de praktijk. Vanuit de invalshoek van informatietechnologie en vanuit de financiële sector zijn al geruime tijd richtlijnen beschikbaar. Sinds kort bestaat daarnaast de onafhankelijke PAS56-standaard, die specifiek ingaat op continuïteitsmanagement en een aantal sterke punten heeft ten opzichte van de al langer bestaande standaarden.

Inleiding

Organisaties worden de laatste jaren geconfronteerd met een grote hoeveelheid wet- en regelgeving op het gebied van corporate governance en risicobeheersing. Deze wet- en regelgeving is in het leven geroepen om risico's binnen individuele organisaties, binnen bedrijfstakken, markten en hele economieën te beheersen en het vertrouwen in ondernemingen en markten te bevorderen. Vertrouwen en risicobeheersing worden op macroniveau gezien als randvoorwaarden voor een duurzame economische groei en maatschappelijke stabiliteit. Ook op het niveau van individuele organisaties zijn vertrouwen en risicobeheersing van belang voor de bedrijfscontinuïteit.

In het eerste deel van dit artikel zal worden toegelicht hoe wet- en regelgeving in toenemende mate eisen stelt aan het continuïteitsmanagement bij organisaties. In het tweede gedeelte wordt een overzicht gegeven van beschikbare standaarden die als leidraad kunnen worden gebruikt bij het inrichten of beoordelen van een beheerproces voor bedrijfscontinuïteit. Er wordt stilgestaan bij de standaarden uit de wereld van de IT en informatiebeveiliging, en bij de nadelen die kleven aan een eenzijdige benadering van continuïteitsmanagement vanuit de IT-hoek. Ook wordt beschreven welke richtlijnen worden gebruikt in de financiële sector in Nederland. In dit tweede deel wordt tevens PAS56 geïntroduceerd, nader geanalyseerd en op bruikbaarheid beoordeeld. PAS56 is een opkomende standaard op het gebied van continuïteitsmanagement die steeds meer aan populariteit wint en voorziet in een behoefte.

Ir. A.T. Wijsman RE MBCI is als adviseur en auditor werkzaam bij KPMG Information Risk Management 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

Wet- en regelgeving

Organisaties – vooral de beursgenoteerde – hebben te maken met een toename van wet- en regelgeving op het gebied van corporate governance en risicomanagement. Continuïteit van de bedrijfsvoering is hiervan een belangrijke component. De wetten en regels die in dit kader de grootste impact hebben zijn:

- Sarbanes-Oxley Act (organisaties met een beursnotering in de Verenigde Staten);
- Code-Tabaksblat (organisaties met een beursnotering in Nederland);
- Basel II (banken);
- Regeling Organisatie en Beheersing (financiële sector in Nederland).

Hoewel continuïteitsmanagement een belangrijke rol speelt bij het voldoen aan deze wet- en regelgeving worden vanuit de wet- en regelgevende instanties in het algemeen weinig concrete en praktisch bruikbare richtsnoeren gegeven. Zo is over de Sarbanes-Oxley regelgeving bijvoorbeeld veel geschreven en gesproken, maar ontstaan nog veel vragen bij de vertaling van de regelgeving naar de praktijk ([Brou03]). Dit geldt ook voor Basel II ([Cart04], [Conn05]). Deze onduidelijkheid heeft overigens niet uitsluitend betrekking op continuïteitsmanagement maar ook op andere aandachtsgebieden die door deze regelgeving worden geraakt. Er bestaat in ieder geval behoefte aan een praktische standaard die organisaties helpt een proces voor continuïteitsmanagement in te richten en te beoordelen, onder andere om aan de nieuwe wet- en regelgeving te voldoen. Een aantal bekende standaarden voor continuïteitsmanagement wordt in het vervolg van dit artikel behandeld.

Standaarden vanuit de IT-wereld

In een eerdere uitgave van Compact is door Mancham, Hoogstra en Velthoen ([Manc04]) reeds een beknopte uitwerking gegeven van enkele beschikbare en algemeen aanvaarde kaders op het gebied van continuïteitsmanagement. Hun uitwerking van continuïteitsmanagement volgens ITIL, de Code voor Informatiebeveiliging en CobIT is opgenomen in de kaders 1 tot en met 3.

Vanuit de wet- en regelgevende instanties worden in het algemeen weinig concrete en praktisch bruikbare richtsnoeren gegeven

Door bovengenoemde auteurs is reeds opgemerkt ([Manc04]) dat in de Code voor Informatiebeveiliging, ITIL en CobIT is gekozen voor een benadering van continuïteitsmanagement waarin IT erg belangrijk is. Dit geldt met name voor CobIT, waarin het onderwerp continuïteit vrijwel uitsluitend op IT is gericht. Gegeven de oorsprong en gebruikersgroep van de genoemde standaarden is dit niet onbegrijpelijk. Het vakgebied is grotendeels in de IT-wereld tot ontwikkeling gekomen en speelt daar een grote en nog steeds groeiende rol. Organisaties worden steeds afhankelijker van IT en stellen steeds hogere eisen aan de beschikbaarheid daarvan, terwijl het door groeiende technische complexiteit steeds moeilijker wordt om aan de eisen te voldoen. Continuïteitsmanagement is daarom in veel organisaties – al dan niet als onderdeel van informatiebeveiliging – ondergebracht bij IT-afdelingen. Het

ITIL

Volgens ITIL worden binnen Business Continuity Management (BCM) de volgende drie kernelementen onderscheiden:

- Doel is het reduceren of het voorkomen van geïdentificeerde risico's (gebaseerd op het uitgangspunt dat voorkomen beter is dan genezen).
- In het geval dat een risico zich voordoet en een verstoring optreedt, dient er een planning te zijn voor de recovery van businessprocessen.
- Risico's dienen te worden ondergebracht bij third parties via bijvoorbeeld verzekering, uitbesteding, financieringsvorm, aansprakelijkheid.

De BCM-lifecycle volgens ITIL bestaat uit vier fasen:

Fase 1 Initiatie

- Formuleren van BCM-beleid.
- Integreren van BCM met het organisatorisch en technisch beleid.
- Opzetten BCM-organisatie.

Fase 2 Eisen en strategie

- Bepalen van businessimpact en risico's.
- Identificeren en evalueren van maatregelen om risico's te beheersen en recovery van businessprocessen.
- Opstellen van een kosteneffectieve BCM-strategie.

Fase 3 Implementatie

- Opstellen van een project om businesscontinuïteit te bereiken.
- Implementeren van faciliteiten en maatregelen zoals bepaald in de BCM-strategie.
- Ontwikkelen van de benodigde business recovery-plannen en -procedures.
- Testen van de getroffen maatregelen en business recovery-planning.

Fase 4 Operational Management

- Continu testen en monitoren van business continuity-strategie, -plannen en -procedures.
- Opzetten en uitvoeren van training en programma's voor bewustzijn van BCM.

Kader 1. ITIL en continuïteit ([Manc04]).

Code voor Informatiebeveiliging, ISO 17799

De Code voor Informatiebeveiliging kent de volgende elementen voor continuïteitsmanagement:

• *Aspecten van continuïteitsmanagement*
Doelstelling: het reageren op verstoringen van bedrijfsactiviteiten en het beschermen van de kritieke bedrijfsprocessen tegen de effecten van grote storingen of calamiteiten.

• *Het proces van continuïteitsmanagement*
Er moet een beheerst proces ingesteld zijn voor het ontwikkelen en handhaven van de bedrijfscontinuïteit in de gehele organisatie.

• *Bedrijfscontinuïteit en analyse van de mogelijke gevolgen*
Er moet een strategisch plan op basis van een passende risicoanalyse zijn ontwikkeld om de algehele benadering van bedrijfscontinuïteit te bepalen.

• *Het schrijven en invoeren van continuïteitsplannen*
Er moeten plannen worden ontwikkeld om de bedrijfsactiviteiten na een onderbreking of verstoring van kritieke bedrijfsprocessen in stand te houden of tijdig te herstellen.

• *Structuur van de continuïteitsplanning*
Er moet een consistente structuur voor bedrijfsplannen worden gehandhaafd om ervoor te zorgen dat alle plannen consistent zijn en om prioriteiten te stellen voor het uitvoeren van tests en onderhoud.

• *Testen, onderhouden en evalueren van continuïteitsplannen*
Continuïteitsplannen moeten regelmatig worden getest en door middel van regelmatige evaluaties worden geactualiseerd, om zeker te stellen dat ze up-to-date en effectief zijn.

Kader 2. ISO 17799 en continuïteit ([Manc04]).

CobIT

Binnen CobIT wordt het volgende over continuïteit genoemd:

• Het waarborgen van de beheersing van de continuïteit van de IT-processen wordt gerealiseerd door aan de eisen van de organisatie te voldoen. De beschikbaarheid van de IT-services dient met andere woorden aan de eisen van de organisatie te voldoen.

• Als een verstoring van de IT-processen zich voordoet, dient de impact op de business minimaal te zijn. Dit wordt bereikt door operationaliseren en testen van een IT-continuïteitsplan, dat in lijn ligt met het business continuïteitsplan dat aan de eisen van de gebruikersorganisatie voldoet.

• De volgende zaken dienen in het continuïteitsplan te worden benoemd:
– classificatie van kritische processen en resources;
– procedures;
– back-up en recovery;
– systematische en periodieke uitvoering van tests en aanbod van training;
– procesdefiniëring van monitoring en escalatie;
– interne en externe organisatorische verantwoordelijkheden;
– business continuïteitsplan, fallback planning en recovery planning;
– risicomanagementactiviteiten;
– analyse van knelpunten;
– problem management.

Kader 3. CobIT en continuïteit ([Manc04]).

is in die organisaties een uitdaging om invulling te geven aan business continuity management in brede zin. Dit komt enerzijds doordat afdelingen buiten de IT-afdeling – de gebruikersorganisatie – continuïteitsmanagement dan zien als iets technisch wat door de IT-afdeling wel wordt geregeld. Anderzijds voelt de IT-afdeling er doorgaans weinig voor om de operationele continuïteit van hele bedrijfsprocessen te gaan organiseren. Het gevolg is vaak dat uitsluitend IT-continuïteit wordt geregeld, en dat de algemene bedrijfscontinuïteit blijft liggen omdat niemand er de verantwoordelijkheid voor neemt.

Deze situatie is problematisch omdat ook veel niet-IT-middelen, zoals opgeleid en ervaren personeel, leveranciers, huisvesting en transportmiddelen, een kritieke rol spelen in veel bedrijfsprocessen. Dit pleit ervoor om de algemene verantwoordelijkheid voor continuïteitsmanagement buiten de IT-afdeling te beleggen.

Een andere ontwikkeling die hiervoor pleit is de opkomst van het organisatiebrede risicomanagement als antwoord op de eisen die onder andere de Sarbanes-Oxley Act en de Code-Tabaksblat stellen aan corporate governance. In de wereld van continuïteitsmanagement en risicomanagement is een discussie gaande over de positionering van de beide vakgebieden. Veel professionals zien continuïteitsmanagement als een onderdeel van risicomanagement, anderen beweren dat beide functies aan elkaar gerelateerd zijn maar naast elkaar bestaan, en er wordt ook betoogd dat risicomanagement vooral moet worden gezien als een functie van continuïteitsmanagement ([Crac04]). De twee vakgebieden vertonen in ieder geval veel overlap en het is daarom logisch ze – afhankelijk van de omvang van de organisatie – binnen één afdeling of bij één functionaris te beleggen.

Een stafafdeling buiten de IT-organisatie is daarvoor in het algemeen de meest geschikte plaats, vanwege de onafhankelijke positionering, overzicht over de organisatie en korte communicatielijnen met de raad van bestuur of directie.

Standaarden vanuit de financiële wereld

De financiële wereld speelt een maatschappelijk en economisch vitale rol en heeft daarom van oudsher te maken met veel regelgeving op het gebied van continuïteitsmanagement. Ook is het risicomanagement in deze sector relatief volwassen. Het Basel II-kapitaalakkoord, dat is opgesteld door de Bank of International Settlements (BIS), dwingt banken er onder andere toe om gegevens over hun operationele continuïteitsrisico's te verzamelen, te analyseren en te modelleren. In de bijbehorende Sound Practices for the Management and Supervision of Operational Risk wordt door de BIS op hoog niveau een aantal strikte eisen gesteld aan continuïteitsmaatregelen en -management ([Verh03], [BIS03]). In Nederland moeten de meeste financiële instellingen voldoen aan de Regeling Organisatie en Beheersing (ROB). De ROB is afkomstig van De Nederlandsche Bank (DNB) en vindt haar grondslag in de Wet toezicht kredietwezen (Wtk). De ROB heeft tot doel richtlijnen en aanbevelingen te geven voor de organisatie en beheersing van bedrijfsprocessen bij instellingen ([DNB04a]). Onderdeel hiervan vormen richtlijnen voor de beheersing van specifieke risicogebieden waaronder operationeel risico en informatietechnologie. Een aanvulling op de enigszins abstracte eisen uit de ROB is eind 2004 door DNB vastgelegd en gepubliceerd in het Toetsingskader business continuity planning betalings- en effectenverkeer. De concrete normen uit dit toetsingskader zijn van toepassing op organisaties die behoren tot de kerninfrastructuur van het Nederlandse betalings- en effectenverkeer en het kader komt overeen met de normen die internationaal in de sector gebruikelijk zijn ([DNB04b]). De tien normen uit het toetsingskader zijn samengevat in kader 4.

Bijzonder is de tiende norm, die bepaalt dat ook voor de integrale keten van organisaties uit de kerninfrastructuur van het betalings- en effectenverkeer de continuïteit moet worden geregeld. Dit is een kenmerk van volwassenheid op het gebied van continuïteitsmanagement en komt op dit moment in geen of weinig andere sectoren voor. Voldoen aan deze norm vereist nauwe samenwerking over organisatiegrenzen heen.

PAS56

Een relatief nieuwe standaard op het gebied van continuïteitsmanagement is PAS56[1]. PAS56 is in 2004 door de British Standards Institution (BSI) geïntroduceerd, maar heeft niet de formele status van British Standard die bijvoorbeeld de Code voor Informatiebeveiliging wel heeft. De standaard wordt echter steeds populairder en het ligt in de lijn der verwachtingen dat PAS56 op termijn wordt uitgeroepen tot een British Standard en/of een ISO-standaard. PAS56 is gebaseerd op een publicatie van Business Continuity Institute (BCI): *Business Continuity Management: Good Practice Guidelines,* 2002.

Bijzonder is de norm die bepaalt dat ook voor de integrale keten van organisaties de continuïteit moet worden geregeld

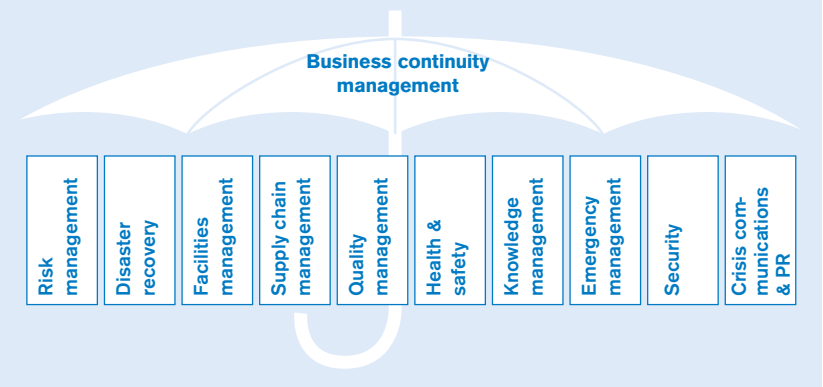
Toetsingskader business continuity planning betalings- en effectenverkeer

Het toetsingskader bevat samengevat de volgende tien normen:

1. Business continuity plan
   Iedere instelling moet een door de directie / het senior management goedgekeurd business continuity plan hebben.
2. Risicoanalyse
   Iedere instelling dient een risicoanalyse te hebben gemaakt van mogelijke calamiteiten en vooral de impact op essentiële systemen en processen.
3. Menselijke factor
   In het business continuity plan dient transparant te worden gemaakt op welke wijze in de plannen rekening is gehouden met de menselijke factor.
4. Crisisorganisatie
   Iedere instelling dient over een crisisorganisatie te beschikken.
5. Afhankelijkheidsanalyse
   Elke instelling dient een analyse te hebben in welke mate men afhankelijk is van basisvoorzieningen en externe providers en op welke wijze de uitwijk hiervoor is georganiseerd.
6. Hervatting essentiële processen
   De essentiële bedrijfsprocessen en systemen dienen zo vlug mogelijk te worden hervat (het huidige voorstel is binnen vier uur, op termijn in lijn met internationale normen binnen twee uur).
7. Uitwijk
   Elke instelling dient met haar essentiële systemen te kunnen uitwijken naar een ander centrum dat, afhankelijk van het risicoprofiel, op voldoende afstand ligt van de hoofdsite.
8. Uitwijktests
   Uitwijk van systemen en continuity- en contingency-procedures moeten regelmatig worden getest.
9. Communicatieplan
   Iedere instelling dient een communicatieplan te hebben voor communicatie in geval van een calamiteit.
10. Business continuity planning voor kerninfrastructuur als geheel
    Voor de kerninfrastructuur van het betalings- en effectenverkeer als geheel dient een business continuity strategie en plan te worden gemaakt. (DNB neemt hierin het voortouw en vervult een coördinerende rol.)

Kader 4. Toetsingskader business continuity planning van DNB (afgeleid uit [DNB04]).

1) PAS staat voor Publicly Available Specification.

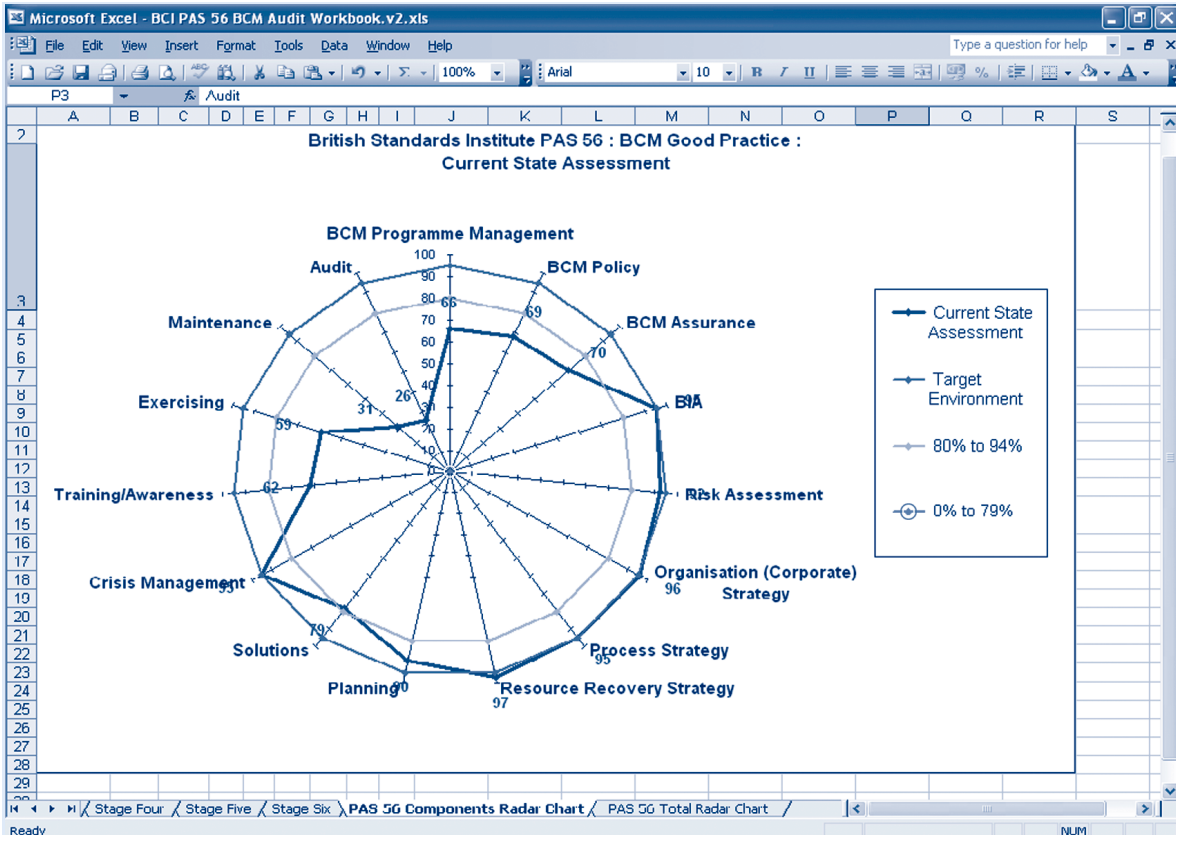


Figuur 1. BCM, het verenigende proces (uit: [BSI03]).

Net zoals de Code voor Informatiebeveiliging biedt PAS56 een raamwerk voor het opzetten van een managementsysteem en een verzameling van best practices. Een aantal gerenommeerde Britse organisaties is betrokken geweest bij de ontwikkeling van de standaard.

De PAS56-standaard heeft een combinatie van sterke punten die hem onderscheidt van de standaarden die eerder in dit artikel zijn behandeld:

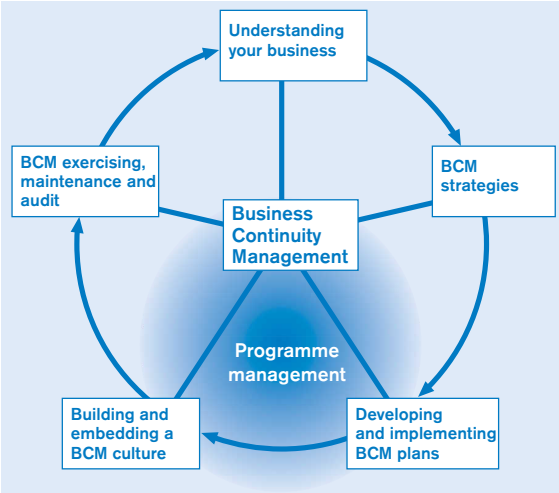
- De standaard is bedoeld voor zowel grote als kleine organisaties binnen alle sectoren.
- De standaard gaat uit van een holistische benadering en koppelt continuïteitsmanagement aan corporate governance en de hieronder genoemde gerelateerde aandachtsgebieden (zie ook figuur 1). Hiermee wordt tegemoetgekomen aan het eerder in dit artikel genoemde bezwaar dat kleeft aan de standaarden uit de IT-wereld en het beleggen van de verantwoordelijkheid en uitvoering van continuïteitsmanagement bij IT-afdelingen. De aandachtsgebieden zijn:
  - Risk management;
  - Disaster recovery;
  - Facilities management;
  - Supply chain management;
  - Quality management;
  - Health & safety;
  - Knowledge management;
  - Emergency management;
  - Security;
  - Crisis communications & PR.
- De standaard biedt een uitgebreid normenkader waartegen het continuïteitsmanagement binnen een organisatie kan worden getoetst. Hiervoor is een geautomatiseerd assessment tool beschikbaar, dat het onder andere mogelijk maakt om een benchmark met andere organisaties op te zetten (zie figuur 2) en de voortgang van implementatie meetbaar te maken.
- PAS56 wordt steeds populairder en heeft net zoals de Code voor Informatiebeveiliging de potentie om uit te groeien tot een internationaal algemeen geaccepteerde en bekende standaard. Een voordeel hiervan voor een organisatie die (liefst aantoonbaar) werkt volgens PAS56



Figuur 2. Het BCI PAS56 BCM Audit Workbook (bron: Business Continuity Institute, www.thebci.org).

is dat eenvoudig aan 'de buitenwereld' – leveranciers, afnemers, aandeelhouders, kredietverstrekkers, verzekeraars, etc. – kan worden uitgelegd dat het continuïteitsmanagement goed is ingericht. Een ander voordeel van een gemeenschappelijk kader voor continuïteitsmanagement is dat continuïteitsplannen en -voorzieningen over organisatiegrenzen heen gemakkelijker kunnen worden opgezet en onderhouden. Denk hierbij aan het eerder in dit artikel genoemde voorbeeld van de organisaties behorende tot de kerninfrastructuur van het Nederlandse betalings- en effectenverkeer, die gezamenlijk hun continuïteit moeten regelen. Het belang van bovengenoemde argumenten groeit mee met de waarneembare ontwikkeling naar meer ketenintegratie en outsourcing.

- PAS56 kiest voor een benadering met een levenscyclus. Hiermee wordt continuïteitsmanagement daadwerkelijk geborgd in een organisatie (zie figuur 3).



Figuur 3. De BCM-levenscyclus (uit: [BSI03]).

Conclusie

Veel wet- en regelgeving die de laatste jaren op organisaties afkomt stelt eisen op het gebied van continuïteitsmanagement. Deze eisen zijn echter grotendeels abstract en bij de toepassing in de praktijk rijzen veel vragen. Er bestaat dus behoefte aan concrete normen en praktische richtsnoeren voor de implementatie van de eisen. Vanuit de IT-wereld is een aantal algemeen aanvaarde standaarden beschikbaar die onder andere op bedrijfscontinuïteit ingaan. Deze standaarden zijn echter vooral gericht op continuïteit van informatietechnologie en zijn voornamelijk bij IT-afdelingen en IT-auditors in gebruik. Omdat bedrijfscontinuïteit veel breder is dan IT heeft het beleggen van de verantwoordelijkheid en uitvoering buiten het IT-domein de voorkeur. Een groot deel van de financiële organisaties in Nederland heeft te maken met de Regeling Organisatie en Beheersing en het meer concrete Toetsingskader business continuity planning betalings- en effectenverkeer van De Nederlandsche Bank. Een relatief nieuwe sectoronafhankelijke standaard die specifiek ingaat op bedrijfscontinuïteit en aan populariteit wint is PAS56. De standaard gaat uit van een holistische benadering en positioneert de discipline business continuity management duidelijk ten opzichte van gerelateerde disciplines, waaronder corporate governance, risk management, security, facilities en supply chain management. Daarnaast onderscheidt PAS56 zich van eerdergenoemde standaarden door de algemene toepasbaarheid en de uitgebreide ondersteuning bij het inrichten en beoordelen van een management-control-cyclus voor bedrijfscontinuïteit.

Literatuur

[BIS03] Bank for International Settlements, *Sound Practices for the Management and Supervision of Operational Risk,* February 2003.

[Brou03] Drs. P.P.M.G.G. Brouwers RE RA en drs. ing. A.M. Meuldijk RE, *SOX 404-implementatie in de praktijk: het process van 'trust me' naar 'prove me'*, Compact 2003/3.

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

[Cart04] Phil Carter, *PAS 56 – Defining a Standard; Phil Carter discusses the strengths and weaknesses of PAS56,* November 2004, www.continuitycentral.com.

[Conn05] Patrick Mc Connell, *Measuring Operational Risk Management Systems under Basel II,* 2005.

[Crac04] Andrew McCrackan, *Is Business Continuity a Subset of Risk Management?*, 2004, www.continuitycentral.com.

[DNB04a] De Nederlandsche Bank, *4201 Regeling Organisatie en Beheersing*, in: Handboek Wtk, januari 2004, www.dnb.nl.

[DNB04b] De Nederlandsche Bank, Nota *Toetsingskader business continuity planning betalings- en effectenverkeer,* 29 november 2004, www.dnb.nl.

[Manc04] Drs. P.J. Mancham RE RA, drs. J.P. Hoogstra RE en R.A.L. Velthoen, *De uitdaging bij Business Continuity Management,* Compact 2004/2.

De PAS56-standaard gaat uit van een holistische benadering en koppelt continuïteitsmanagement aan andere aandachtsgebieden