De uitdaging bij Business Continuity Management

Drs. P.J. Mancham RE RA, drs. J.P. Hoogstra RE en R.A.L. Velthoen

Voor de IT-auditor is het een uitdaging om niet door het management als lastig te worden ervaren wanneer het gaat om Business Continuity Management-vraagstukken. De kunst is juist om over te komen als de professional waar het management niet omheen kan als het gaat om het mitigeren van risico's met betrekking tot Business Continuity Management. In dit artikel wordt ingegaan op de wijze waarop een IT-auditor in een Business Continuity-traject zich kan richten op de risico's en welke methodieken en hulpmiddelen hij hiervoor tot zijn beschikking heeft.

Inleiding

Ruim tweeënhalf jaar na de aanslagen in Amerika, anderhalf jaar na de brand bij de Universiteit Twente in Enschede en de bommeldingen bij IKEA zou men verwachten dat veel organisaties hun Business Continuity Management (BCM) op orde zouden hebben. Voor de IT-auditors zou dit dan betekenen dat zij het erg druk hebben gehad met het beoordelen van continuïteitsplannen en/of het adviseren over de continuïteitsmaatregelen. Integendeel. De meeste organisaties hebben nog steeds niet geïnventariseerd of de Business Continuity afdoende is geregeld, laat staan afdoende maatregelen zijn getroffen! 'Ach, de kans op een bommelding of een grote brand is erg klein', luidt vaak de reactie van het management. Het lijkt een logische reactie. Maar wordt er tegelijkertijd ook stilgestaan bij de gevolgen van stroomstoringen, de afhankelijkheid van telefonie en e-mail tijdens kantooruren, de afhankelijkheid van bepaalde fysieke brondocumenten en de gevolgen van een brand in een deel van een gebouw? Dit soort relatief 'onschuldige' risico's worden in de praktijk onderschat.

Voor de IT-auditor vormt dit nou juist de uitdaging. Hoe zorg je ervoor dat het management je niet lastig en erg theoretisch vindt, maar ziet als een professional die hem kan ondersteunen bij het managen van de belangrijkste restrisico's rondom Business Continuity. Immers, elke organisatie heeft maatregelen getroffen om de continuïteit te waarborgen en risico's af te dekken, al is het alleen maar het maken van back-ups van data of het archiveren van brondocumenten. Het is niet reëel om te veronderstellen dat je alle risico's kunt afdekken. Er is altijd sprake van bepaalde restrisico's die moeten worden geaccepteerd door het management. Dit houdt voor de IT-auditor in dat door het focussen op de restrisico's met betrekking tot Business Continuity, hij een waar-

Drs. P.J. Mancham RE RA
is werkzaam als senior manager bij KPMG Information Risk Management in De Meern. Hij heeft ruime IT-audit- en IT-advieservaring op het gebied van IT risk management, IT-projecten en IT-beheersing, waaronder Business Continuity Management. Als adviseur en auditor is hij betrokken geweest bij diverse complexe Business Continuity Management-opdrachten.

mancham.prem@kpmg.nl

Drs. J.P. Hoogstra RE
is werkzaam als consultant bij KPMG Information Risk Management in Arnhem. Hij heeft ruime IT-audit- en IT-adviesvaardigheden onder andere op het gebied van pakketselectie, IT-projecten en Business Continuity Planning. Zo is hij betrokken geweest bij het opstellen van een Business Continuity Plan bij een bank en het beoordelen van de getroffen maatregelen voor het waarborgen van de continuïteit bij een kredietinstelling.

hoogstra.jan@kpmg.nl

R.A.L. Velthoen
is werkzaam als interne IT-auditor bij de Universiteit Twente. Hij is als IT-auditor betrokken bij de meeste ICT-projecten van de UT. Voor zijn functie als IT-auditor heeft hij gewerkt in zowel de gebruikersorganisatie als de automatiseringsorganisatie. Hierdoor is hij in staat ICT-issues goed te plaatsen binnen het geheel.

R.A.L.Velthoen@utwente.nl

devolle bijdrage kan leveren aan de ICT Governance binnen een organisatie.

In dit artikel wordt ingegaan op de wijze waarop een IT-auditor in een Business Continuity-traject zich kan richten op de (rest)risico's en welke methodieken en hulpmiddelen hij hiervoor tot zijn beschikking heeft.

De 'harde' feiten en het belang van BCM

Hierna volgen enkele cijfers uit een internationaal gehouden BCM-onderzoek om het belang van Business Continuity Management te benadrukken ([KPMG03]):
- 81% van de organisaties in het onderzoek heeft te maken gehad met stroomonderbrekingen.
- 61% heeft te maken gehad met telecommunicatiestoringen.
- 53% van de organisaties die in het bezit zijn van een Business Continuity Plan, heeft aangegeven het plan ook daadwerkelijk te hebben gebruikt bij een storing.
- 23% heeft een Corporate Governance-programma voor Business Continuity Management.

Het is evident dat Business Continuity Management belangrijk is voor veel organisaties. De waarde ervan blijkt pas achteraf, zoals bij de Universiteit Twente (zie kader 1). De conclusie mag echter niet worden getrokken dat zonder een adequaat Business Continuity Management-programma de bedrijfscontinuïteit in geval van een calamiteit of ernstige storing niet is gewaarborgd. In voorkomende gevallen worden door het management maatregelen genomen om de schade zoveel mogelijk te beperken. De vraag is dan alleen of de schade niet minder had kunnen zijn als er een Business Continuity-programma was opgezet en ingevoerd. In dergelijke gevallen blijkt hoe cruciaal het managen van de 'schaarse' tijd en de beschikbare mensen en middelen is vanaf het moment dat een ernstige storing zich voordoet tot aan het moment dat er weer sprake is van 'business as usual'.

Business Continuity Management en Business Continuity Plan

In de praktijk worden de begrippen met betrekking tot Business Continuity Management vaak door elkaar gehaald en is de betekenis ervan onduidelijk. Regelmatig wordt IT-auditors gevraagd hoe men zou kunnen ondersteunen bij het opstellen van een Business Continuity Plan. Maar na een verkennend gesprek met de opdrachtgever blijkt het dan vaak te gaan om een Disaster Recovery Plan.

Ten behoeve van een eenduidig begrip van Business Continuity Management hanteren wij het in figuur 1 weergegeven fasenmodel van KPMG.

In het KPMG BCM-model worden drie focusgebieden onderscheiden:
- Strategic Use;
- Availability;
- Recoverability.

Uitslaande brand bewijst waarde calamiteitenplan

Op 20 november 2002 woedde in het UT-computercentrum een brand, waarbij onder meer het computernetwerk en een deel van de faculteit Toegepaste Wiskunde in vlammen opging. De Universiteit zette meteen het calamiteitenplan in werking. Het plan leidde onder andere tot het activeren van een crisisteam op UT-niveau, alsmede een afzonderlijk crisisteam voor de centrale IT-voorzieningen.

De totale schade van de brand is opgelopen tot tientallen miljoenen euro's. Tot de verloren IT-voorzieningen behoorden onder meer de netwerkvoorzieningen, computersystemen, helpdeskvoorzieningen, telefooncentrale en diverse werkplekvoorzieningen.

De internetaansluiting was binnen twee dagen hersteld. Centrale productiesystemen waren na ongeveer één week en administratieve informatiesystemen na vier weken bijgewerkt tot de datum van vlak voor de brand. Doordat de salarisadministratie was uitbesteed, liep de UT op dat punt geen risico.

Lessons learned:
De brand heeft in ieder geval aangetoond dat een tweede ICT-ruimte, die op dat moment in aanbouw was, noodzakelijk is. Het bewaren van de back-ups in een ander gebouw bleek achteraf ook een goede zaak. Een ander punt was de beschikbaarheid van werkplekken voor de beheerders in een ander gebouw. De brand was ook aanleiding om de back-upprocedure aan te scherpen. Belangrijkste les was het spreiden van de risico's, onder andere door een tweede ICT-ruimte, redundante systemen en netwerkcomponenten.

De rol van de interne IT-auditor na de brand was het houden van regelmatig contact met de relevante organisatieonderdelen, het evalueren van en het volgen van verbeteracties. De focus lag op het bewaken van de continuïteit van de belangrijkste bedrijfsprocessen om de restrisico's te beperken.

R.A.L. Velthoen, intern IT-auditor Universiteit Twente

Kader 1. Universiteit Twente.

ITIL
Volgens ITIL worden binnen Business Continuity Management 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.

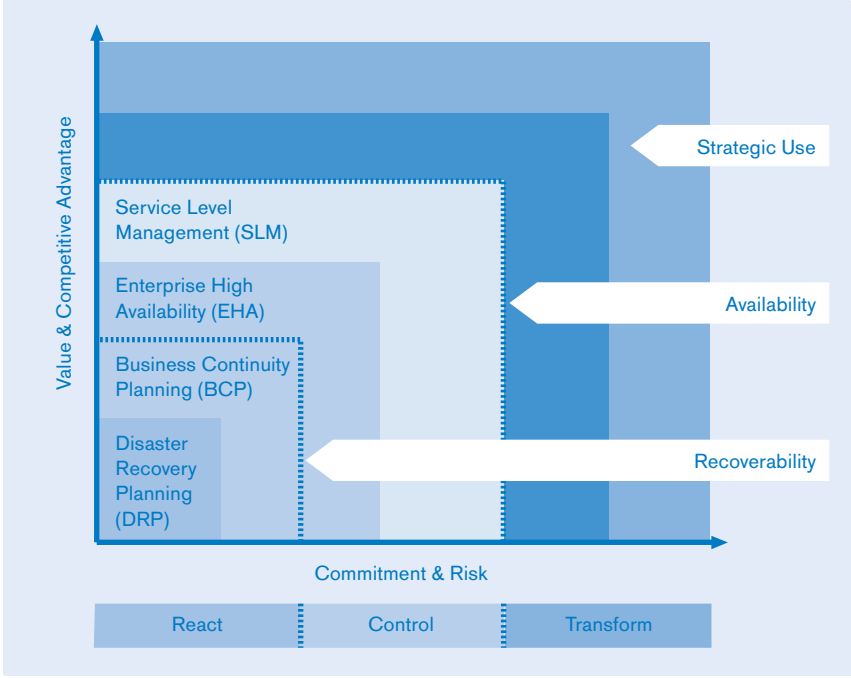
Fase 3 Implementatie
• Opstellen van een project om businesscontinuïteit te bereiken.
• Implementeren van faciliteiten en maatregelen zoals bepaald in de BCM-strategie.
• Ontwikkelen van de benodigde business recovery-plannen en -procedures.
• Testen van de getroffen maatregelen en business recovery-planning.

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 2. ITIL en BCM.

Een organisatie bevindt zich altijd in één van deze focusgebieden.

Strategic Use
Als een organisatie zich in dit focusgebied bevindt is er daadwerkelijk sprake van Business Continuity Management in de ruime betekenis van het woord. Binnen de bedrijfskolom worden afspraken gemaakt over Business



Figuur 1. Business Continuity Management-fasen (KPMG).

Continuity Management en het proactief voorkomen van problemen/calamiteiten. Een organisatie is met name gericht op het beheersen van risico's en de beschikbaarheid van informatie voor de uiteindelijke gebruiker/klant.

Availability
In het focusgebied Availability richt een organisatie zich op het continu beschikbaar zijn voor haar directe klanten. Er worden proactief maatregelen getroffen om te voorkomen dat er sprake is van discontinuïteit. Dit gebeurt bijvoorbeeld door het afsluiten van contracten en Service Level Agreements met leveranciers.

Recoverability
Veel organisaties bevinden zich in dit focusgebied. Hierin zijn de activiteiten van de organisatie erop gericht bij calamiteiten zo spoedig mogelijk weer te functioneren. Hierbij kan gedacht worden aan het maken van back-ups. De nadruk ligt op het adequaat reageren op calamiteiten en/of ernstige storingen en/of het herstel van de operationele dienstverlening. Een Business Continuity Plan beschrijft de verantwoordelijkheden en te ondernemen activiteiten bij een calamiteit zodat gestructureerd gereageerd wordt op calamiteiten.

Aangezien veel organisaties zich momenteel vooral nog richten op Recoverability, zullen we in de volgende paragrafen met name de methodieken, technieken en tools uitwerken die in dit focusgebied van belang kunnen zijn.

Code voor Informatiebeveiliging, BS7799
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 3. BS7799 en Continuïteitsmanagement.

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 4. CobIT en Continuïteit.

BCM-methoden en -technieken voor een IT-auditor

Momenteel ontbreekt het aan een algemeen aanvaarde aanpak en normenstelsel(s) voor Business Continuity Management. Wel wordt er door beroepsorganisaties als de NOREA en ISACA gewerkt aan standaarden voor BCM.

Daarnaast zijn er momenteel wel verschillende normenkaders waarin het onderwerp wordt behandeld en waarvan de IT-auditor gebruik kan maken, zoals ITIL, Code voor Informatiebeveiliging (BS7799) en CobIT. Het valt een oplettende lezer op dat in deze algemene normenkaders de terminologie van BCM en BCP door elkaar wordt gebruikt. Zo spreekt ITIL van Business Continuity Management, terwijl feitelijk Business Continuity Planning wordt bedoeld (zie de kaders 2 t/m 4). Wat verder opvalt is dat deze drie standaarden uitgaan van een benadering waarbij ICT erg belangrijk is. Uiteraard is dit een goede benadering, maar het is ook noodzakelijk aandacht te schenken aan zaken zoals de afhankelijkheid van fysieke documenten en de afhankelijkheid van bepaalde personen en organisaties.

KPMG BCM-aanpak

Binnen KPMG wordt gebruikgemaakt van een internationaal ontwikkelde BCM-aanpak (zie figuur 2). Deze aanpak wordt gekenmerkt door een cyclische benadering waarbij de nadruk continu ligt op het managen van de Business Continuity-restrisico's. Tevens is de aanpak zodanig uniform opgezet dat hij kan worden gebruikt in alle focusgebieden zoals onderkend in figuur 1.

In de BCM-aanpak worden de volgende fasen onderscheiden:
1. risicoanalyse;
2. ontwikkelen en/of aanpassen van de Business Continuity-strategie/Plan;
3. implementeren van noodzakelijke wijzigingen;
4. borging van de Business Continuity.

Deze fasen worden per laag in het Business Continuity Management-model (figuur 1) doorlopen. Afhankelijk van de focus zal de nadruk steeds op een ander gebied liggen. Bij Recoverability ligt de nadruk op het Business Continuity Plan (fase 2).

Voor een nadere toelichting van deze aanpak is hierna een globale uitwerking opgenomen van een Business Continuity Plan-traject (= tweede laag binnen Business Continuity Management, zie figuur 1).

Fase 1. Risicoanalyse
De risicoanalyse bestaat uit de volgende twee subfasen:
- Business Process Analyse;
- Business Continuity Impact Analyse.

Business Process Analyse
In deze fase worden op basis van het bedrijfsprocesmodel de kritische bedrijfsprocessen bepaald. Kritisch in dit kader wil zeggen dat het bedrijfsproces ook na een ernstige storing en/of calamiteit gecontinueerd moet worden.

Per kritisch bedrijfsproces worden (wordt) samen met de proceseigenaren:
- de business recovery requirements bepaald om inzicht te krijgen in de maximaal acceptabele uitvaltijden (= service- en hersteleisen), daarbij rekening houdend met eventuele wettelijke eisen die gelden voor bewaartermijnen en voor registraties;
- het maximaal acceptabele gegevensverlies bepaald om inzicht te krijgen in het maximale dataverlies;
- de benodigde minimale voorzieningen bepaald om in geval van storingen en dergelijke verder te kunnen werken, zoals documenten, applicaties, telefonie, aantal werkplekken en personen.

Business Continuity Impact Analyse
Op basis van de resultaten van de uitgevoerde procesanalyse wordt vervolgens een Business Continuity Impact Analyse uitgevoerd om inzicht te krijgen in de huidige continuïteitsrisico's per organisatieonderdeel of locatie en per vastgesteld kritisch bedrijfsproces.

Op basis van de vastgestelde business recovery requirements en eisen met betrekking tot het maximaal acceptabele gegevensverlies worden per organisatieonderdeel of locatie en per onderkend bedrijfsproces de getroffen continuïteitsmaatregelen, zoals contracten met leveranciers, back-upvoorzieningen, (ICT-)uitwijkvoorzieningen en telecommunicatievoorzieningen, in kaart gebracht en beoordeeld. Na deze evaluatie worden de restrisico's (en de impact op de bedrijfsvoering bij het optreden van een bedreiging) bepaald. Voor deze subfase zijn tools aanwezig voor vastlegging en registratie. Deze tools worden in de volgende paragraaf besproken.

Figuur 2. BCM-aanpak (KPMG).

Fase 2. Ontwikkelen en/of aanpassen van de Business Continuity-strategie/Plan
In deze fase worden de uitgangspunten en de te hanteren strategie bepaald en vastgesteld voor de Business Continuity. De uitgangspunten worden mede bepaald op basis van de resultaten uit de Business Continuity Impact Analyse en het door de organisatie gevoerde risicomanagementbeleid.

Op basis van de uitgangspunten en het risicomanagementbeleid van de organisatie wordt het Business Continuity Plan ontwikkeld of aangepast. Dit plan bestaat uit een aantal kernelementen, zoals doelstelling, uitgangspunten, belangrijke beslissingen, verantwoordelijkheden, teamstructuren, checklists en uitgewerkte maatregelen om verstoringen te verhelpen, en diverse bijlagen zoals een telefoonlijst.

Fase 3. Implementeren van noodzakelijke wijzigingen
Op basis van het vastgestelde Business Continuity Plan en de vastgestelde nog aanwezige (rest)risico's die niet wenselijk zijn voor de organisatie, worden zo nodig aanvullende continuïteitsmaatregelen getroffen. Er wordt onderscheid gemaakt tussen preventieve maatregelen en repressieve maatregelen. Een aanvullende preventieve maatregel kan het aanpassen van de fysieke toegangsbeveiliging van het rekencentrum zijn. Een aanvullende repressieve maatregel kan zijn het regelen van interne en/of externe uitwijklocaties.

Fase 4. Borging van de Business Continuity
In deze fase worden functionarissen die een rol vervullen binnen het Business Continuity Management getraind op basis van de afspraken en procedures zoals intern overeengekomen.

Tevens worden in deze fase procedures uitgewerkt en/of aangepast voor het actueel houden van de afspraken en het periodiek monitoren van de restrisico's. Een belangrijk onderdeel van deze fase is het regelmatig testen van de aanwezige procedures en maatregelen.

Samenvattend is het mogelijk met deze benadering gestructureerd en systematisch aandacht te schenken aan zowel de organisatorische ('zachte controls') als de technische kanten ('harde controls') van Business Continuity Planning.

Alleen maar 'een kunstje uitoefenen met een set tools' is niet aan de orde

De tools van de IT-auditor

In de praktijk blijkt dat kennis en ervaring onontbeerlijk zijn bij Business Continuity-trajecten, omdat deze trajecten per definitie situatieafhankelijk en organisatiespecifiek zijn. Hier geldt niet 'een kunstje uitoefenen met een set tools'. Desalniettemin zijn tools 'handig' voor de IT-auditor om structuur aan te brengen in zijn werk.

De rol van een IT-auditor kan zowel adviserend als beoordelend zijn. Per rol wordt in deze paragraaf aangegeven welke tools de IT-auditor tot zijn beschikking heeft. Doel is zeker niet om volledigheid na te streven, maar inzicht te geven in de mogelijkheden.

De IT-auditor in een adviserende rol

In zijn adviserende rol heeft de IT-auditor de beschikking over een aantal tools en hulpmiddelen. Per onderkende fase zoals in de vorige paragraaf beschreven, wordt een aantal tools nader toegelicht.

Risicoanalyse
Er zijn tools op de markt beschikbaar voor het documenteren van een Business Impact Analyse. Met deze tools vindt een vastlegging plaats van de bedrijfsprocessen, continuïteitsrisico's, beschikbaarheidseisen en continuïteitsvoorzieningen. Met behulp van deze vastlegging kunnen dan risico's grafisch in kaart worden gebracht door per proces en/of systeem de beschikbaarheid en mogelijke uitvalsduur weer te geven. Sommige tools maken het mogelijk geautomatiseerd een volledig BCP te produceren. Een voorbeeld van zo'n tool is 'BIA Professional' van Strohl. Ten slotte zijn er nog vrij in de markt (via internet) verkrijgbare tools gebouwd in Microsoft Excel of Microsoft Access.

Ontwikkelen en/of aanpassen van de Business Continuity-strategie/Plan
Ook voor de ontwikkeling van een Business Continuity-strategie en de vastlegging in een plan zijn diverse tools aanwezig:
- Strohl beschikt bijvoorbeeld over 'Living Disaster Recovery Planning System'. Dit systeem bevat een soort template voor een BCP. In samenwerking met het systeem 'BIA Professional' van Strohl en de te maken keuzen in de organisatie over welke strategie te volgen, kan een BCP worden gegenereerd.
- 'Business Protector Professional' van Business Protection Systems International.

Ook zijn er eenvoudige tools op de markt die eveneens een BCP kunnen genereren, zoals de hiervoor genoemde tools in Microsoft Access. Voor de organisaties die minder geautomatiseerd een BCP willen opstellen, zijn diverse templates op het internet aanwezig aan de hand waarvan een BCP kan worden opgesteld.

Implementeren van noodzakelijke wijzigingen
Het implementeren van noodzakelijke wijzigingen is feitelijk een reguliere activiteit van de organisatie. In deze activiteit kunnen systemen worden ontwikkeld of aangeschaft en geïmplementeerd. Vaak zijn ook het aanpassen of opstellen van procedures en documentatie van belang. De tools die de IT-auditor hiervoor kan gebruiken, zijn vaak afkomstig uit andere vakgebieden zoals systeemontwikkeling en pakketselectie. Voor bijvoorbeeld het selecteren van een leverancier en/of hardware en software zijn diverse methodieken van pakketselectie en daarbijbehorende vragenlijsten en aandachtspuntenlijsten voorhanden.

Borging van de Business Continuity
Een belangrijk onderdeel van de borging van de Business Continuity is het maken van afspraken en het testen van de getroffen maatregelen en procedures zoals uitwijk en noodplan. Aangezien dit veelal organisatorische zaken zijn, is het niet verwonderlijk dat hier vrijwel geen tools voor aanwezig zijn.

De IT-auditor in een beoordelende rol

Hoewel de NOREA bezig is met het opstellen van standaard-normenkaders als nadere uitwerking van het Studierapport 3 'Raamwerk voor de ontwikkeling van normenstelsels en standaarden', is er momenteel geen algemeen aanvaard normenkader voor het beoordelen van BCM-projecten en/of -producten. Een IT-auditor zal daarom samen met zijn opdrachtgever een normenkader op moeten stellen. Een aantal algemeen aanvaarde referentiekaders kan daarvoor als input worden genomen, zoals besproken in de paragraaf BCM-methoden en -technieken. Ook op het internet zijn diverse checklists beschikbaar voor het uitvoeren van een audit op de getroffen continuïteitsmaatregelen.

De IT-auditor zal altijd goed moeten nagaan of bepaalde checklists voldoende normen bevatten om te gebruiken als toetsingskader. De IT-auditor zal afhankelijk van de situatie en onderzoeksvraag eventueel aanvullende normen moeten formuleren en afstemmen met zijn opdrachtgever.

Binnen KPMG wordt gebruikgemaakt van een BCP Quick Scan, waarmee met behulp van een aantal normen de stand van zaken bij een organisatie in kaart wordt gebracht. In deze BCP Quick Scan worden de volgende gebieden onderscheiden: Business Continuity Organization, Business Focus, Recovery Strategy en Data Loss Strategy. Uit het tool wordt onder meer een statusoverzicht gegenereerd (zie figuur 3).

In het gebied waar een organisatie in het licht- of donkerblauw (0-7) scoort, zijn nog risico's aanwezig. In het gepresenteerde voorbeeld zijn met name nog risico's aanwezig op het gebied van de Business Continuity Organization en de Business Focus. Dit betekent dat de organisatie vooral aandacht dient te schenken aan het verbeteren van de organisatorische aspecten met betrekking tot Business Continuity Planning (o.a. people management, rollen en verantwoordelijkheden, informatie over contactpersonen, kritische bedrijfsprocessen).

Conclusie

In dit artikel is ingegaan op de wijze waarop een IT-auditor in een Business Continuity-traject zich kan richten op de (rest)risico's en welke methodieken en hulpmiddelen hij hiervoor tot zijn beschikking heeft. Door te kiezen voor een heldere aanpak met daarbijbehorende definitie kan de IT-auditor een waardevolle bijdrage leveren bij Business Continuity-trajecten. We hebben tevens geconstateerd dat er (nog) geen algemeen aanvaarde methoden en technieken voor dit soort trajecten zijn voor een IT-auditor. Wel zijn er diverse hulpmiddelen beschikbaar waarvan gebruik kan worden gemaakt.

Door beroepsorganisaties als NOREA en ISACA worden momenteel algemene normenkaders uitgewerkt voor Business Continuity Management. Zolang deze normen niet voorhanden zijn zal de IT-auditor het moeten doen met 'gangbare' methoden en technieken. Maar het belangrijkste bij Business Continuity-trajecten zijn niet zozeer de tools voor de IT-auditor, maar zijn eigen kennis en kunde om vanuit een risk management-benadering efficiënt en effectief te focussen op de restrisico's. De vraag is nu of iedere IT-auditor klaar is om de uitdaging van het management aan te nemen.

Literatuur en websites

Business Continuity Management Methodology, voorjaar 2002.

Business Continuity Planning Methodology, voorjaar 2002.

CobIT, Control Objects Information Technology.

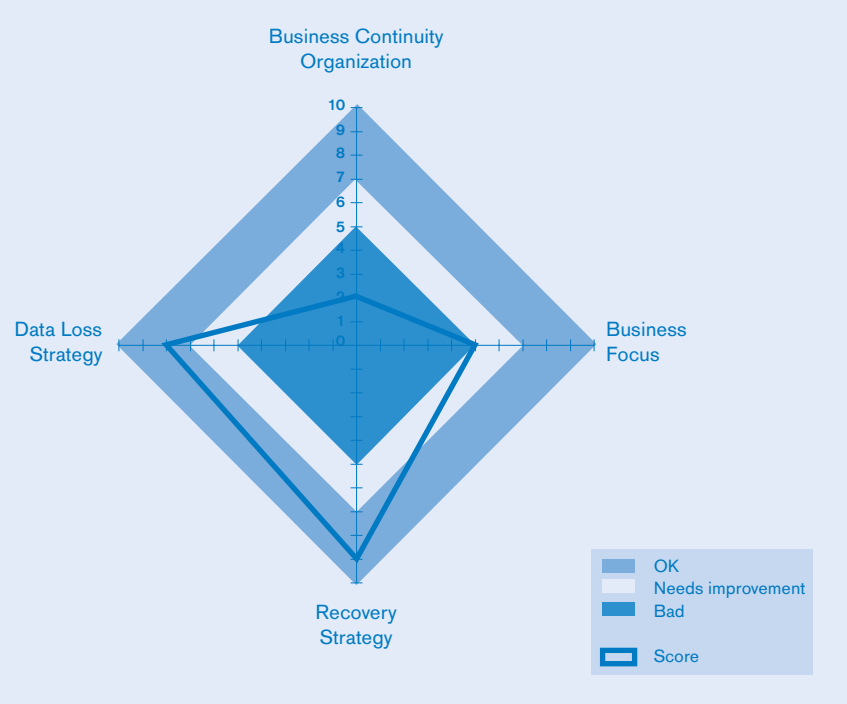
Code voor Informatiebeveiliging, ISO 17799/BS7799.

ITIL, IT Infrastructure Library *Continuïteitsmanagement*.

KPMG Business Continuity Benchmarking Study, *A review of factors influencing Business Continuity*, 31 October 2003.

www.businessprotection.com

www.strohl.com/BCP/default.asp



Figuur 3. Score BCP Quick Scan.