Uitvoering van – en normenstelsels voor– een audit op een business continuity plan

Ernst J. Oud

De complexiteit van bedrijfsprocessen en bovenal de afhankelijkheid van de ondersteunende productiemiddelen zoals ICT is dermate groot dat vooraf nadenken over de te nemen acties ten tijde van crisis absoluut te prefereren is boven te moeten improviseren als het moment daar is. In dit artikel wordt aangegeven welke stappen moeten worden doorlopen om een continuïteitsplan en de ondersteunende voorzieningen in te richten om daaruit de voor een auditor relevante auditobjecten af te leiden.

Inleiding

In de nacht van zaterdag op zondag 13 februari 2005 werd in het centrum van Madrid door brand het 32-verdiepingen hoge Windsor kantoorgebouw verwoest. In tegenstelling tot berichten in de media dat het gebouw leegstond, werd bij de brand het hoofdkantoor van Deloitte in Spanje, gehuisvest op de onderste twintig verdiepingen van het gebouw, totaal vernietigd. Meer dan tweeduizend medewerkers verloren daarbij hun werkplek, communicatiemiddelen, dossiers en informatiesystemen. Een aantal brandweerlieden raakte bij de brand gewond. De brand was de grootste in de geschiedenis van de Spaanse hoofdstad.
Direct na de brand werd door Deloitte het continuïteitsplan geactiveerd en kwam het crisisteam in actie. Enkele uren na de brand communiceerde het crisisteam de voortgang van de operatie aan de pers en vooral de voortzetting van de activiteiten aan haar klanten.
Kort voor de brand was een back-up gemaakt waardoor alle informatie nog voorhanden was. Op maandagmorgen 14 februari kon een groot aantal medewerkers elders of thuis weer aan de slag. In Madrid heerste maandagochtend 14 februari chaos; het Windsor gebouw staat boven Madrids grootste metrostation. Vanwege de brand was dit metrostation afgesloten met een verkeerschaos als gevolg.

Het bovenstaande recente voorbeeld maakt duidelijk hoe snel een organisatie haar normale bedrijfsvoering kan verliezen en hoe belangrijk juist handelen op dat moment is. De complexiteit van bedrijfsprocessen en bovenal de afhankelijkheid van de ondersteunende productiemiddelen zoals ICT is dermate groot dat vooraf nadenken over de te nemen acties ten tijde van crisis absoluut te prefereren is boven te moeten improviseren als het moment daar is. Hoe groot die afhankelijkheid is werd geschetst in de recente ICT-barometer van Ernst&Young, waarin maar liefst driekwart van de ondervraagden aangeeft dat hun organisatie in sterke mate afhankelijk is van ICT en een kwart zelfs volledig afhankelijk is hiervan.

Daar waar ICT voor een aantal organisaties nog ondersteunend is, is de afhankelijkheid van productiemiddelen zoals machines in fabrieken waarschijnlijk nog groter. Het vooraf plannen van de continuïteit van de organisatie ten tijde van een calamiteit wordt continuïteitsplanning genoemd. Om het bedrijfsbrede en integrale karakter te onderstrepen, wordt de laatste jaren van *business*

Ernst J. Oud, senior manager bij Deloitte Enterprise Risk Services, adviseert organisaties met vraagstukken op het gebied van business continuity. Eind dit jaar verschijnt bij Academic Service van zijn hand de ‘Praktijkgids Business Continuity Management’.
Ernst is lid van de NEN normcommissie 381027 en van het Centraal College van Deskundigen – Informatiebeveiliging. Beide spelen een belangrijke rol bij de Code voor Informatiebeveiliging in Nederland. Daarnaast is hij docent bij NEN en kerndocent van de module ‘Continuïteit van de informatievoorziening’ in de masters opleiding informatiebeveiliging van de TIAS Business School.

continuity planning of business continuity *management* (BCM) gesproken. In PAS56, de *'Guide to Business Continuity Management'* van het British Standards Institute wordt het begrip BCM gedefinieerd als een 'holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities'.

Als deel van BCM wordt het *plannen* van continuïteit beschouwd. Business Continuity Planning (BCP) omvat het vooraf plannen en voorbereiden in een aantal stappen. De stappen bestaan uit het identificeren van potentieel verlies, het formuleren en implementeren van continuïteitstrategieën en het ontwikkelen van een continuïteitsplan welke de voortzetting ten tijde van een calamiteit garandeert binnen van te voren vastgelegde uitgangspunten. BCP levert een continuïteitsplan bestaande uit een gedocumenteerde set procedures en informatie voor het handelen ten tijde van de calamiteit. Om het continuïteitsplan uit te voeren ten tijde van de calamiteit zal naast het plan ook een groot aantal voorzieningen aanwezig moeten zijn zoals reserve ICT-faciliteiten, productiemiddelen en gebouwen.

In dit artikel wordt aangegeven welke stappen moeten worden doorlopen om een continuïteitsplan en de ondersteunende voorzieningen in te richten om daaruit de voor een auditor relevante auditobjecten af te leiden. Uiteraard kan een auditor ook gevraagd worden een oordeel te vormen over het proces waarin een continuïteitsplan tot stand komt.

Gevolgen van recente regelgeving voor de beoordeling van continuïteit

De IT-auditor zal steeds vaker een oordeel moeten vormen over de continuïteit van de geautomatiseerde gegevensverwerking. Immers, de Code Tabaksblat noemt expliciet – zij het niet dwingend – dat het verslag van de externe accountant met betrekking tot de werking van de interne risicobeheersings- en controlesystemen in zou kunnen gaan op verbeterpunten, geconstateerde leemten en opmerkingen over bedreigingen en risico's voor de vennootschap, inclusief de betrouwbaarheid en *continuïteit* van de geautomatiseerde gegevensverwerking. In sectie 404 van de Sarbanes-Oxley Act wordt de externe accountant opgedragen bij de jaarrekeningcontrole een oordeel uit te spreken over de door de bestuurders uitgevoerde beoordeling van de effectiviteit van de interne beheersing en procedures voor financiële rapportage.

Duidelijk mag zijn dat een organisatie zonder continuïteitsvoorziening, welke getroffen wordt door een ernstige calamiteit, niet in staat zal zijn op een effectieve wijze interne beheersing uit te voeren over haar bedrijfsprocessen, dus ook niet over de financiële processen. Financiële chaos is dan veelal het resultaat, vaak leidend tot faillissement.

De finale versie van de PCAOB auditing standard 2, *'An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements'* geeft invulling aan de in SOx gestelde eisen ten behoeve van de auditor. In appendix C staat een niet mis te verstane uitspraak:
'… management's plans that could potentially affect financial reporting in future periods are not controls. For example, a company's business continuity or contingency planning has no effect on the company's current abilities to initiate, authorize, record, process, or report financial data. Therefore, a company's business continuity or contingency planning is not part of internal control over financial reporting.'

Duidelijke taal; omdat business continuity planning gaat over het zeker stellen van de continuïteit in de toekomst, hoeft de externe auditor hierover geen oordeel te geven over de afgelopen periode.
De PCAOB auditing standard beschrijft echter ook dat *'.. controls over financial reporting may be preventive controls … that have the objective of preventing errors from occurring in the first place that could result in a misstatement of the financial statements'*. In deze context is de inrichting van een continuïteitsvoorziening een preventieve maatregel om te zorgen dat bij een calamiteit de beheersing van de financiële processen op orde blijft.

Dat die beheersing ook bij een calamiteit cruciaal is, wordt in sectie 409 van SOx onderkend. Daarin wordt verplicht dat de onderneming materiële veranderingen in de financiële situatie of in de bedrijfsvoering snel en tijdig aan het publiek meldt. Wordt een onderneming getroffen door een calamiteit welke de ICT treft, dan zal het niet eenvoudig zijn om tijdig de volgens sectie 409 verplichte informatie te verstrekken.
Of in SOx-oordelen daadwerkelijk continuïteitsplanning een belangrijk aandachtspunt wordt, staat in het vakgebied dus nog ter discussie [ZA2005] [SM2005].

Belangrijker is dat voor IT-governance in het algemeen het belang van (ICT-) continuïteitsplanning niet ter discussie staat. Voor een groot deel nog best-practice, maar IT-governance begint langzamerhand genormeerd te raken.

Zo heeft Standards Australia in AS 8015–2005 *'Corporate governance of information and communication technology'* wereldwijd het initiatief genomen tot de eerste norm voor IT-governance. Deze standaard legt vast dat IT-governance onder andere zekerheid geeft over continuïteit en dat de bestuurders sturing moeten geven aan de bescherming van gegevens tegen verlies en misbruik in overeenstemming met de vereisten uit ISO 17799. Voor de IT-auditor geeft deze standaard richting voor het adviseren, informeren en ondersteunen van de bestuurder.

Normenstelsels

Hoewel continuïteitsplanning al vrij snel na de brede toepassing van informatietechnologie aandacht kreeg – zo werd in Nederland al in 1981 het Computer Uitwijk Centrum in Lelystad opgericht – zijn er geen wereldwijd aanvaarde normen voor.

Vrijwel elke best-practice voor security management bevat echter een framework, standards en policies voor continuïteitsplanning. Een beperkte opsomming:

- ISO 17799 beschrijft in hoofdstuk 11 het proces continuïteitsmanagement, de aspecten van de risicoanalyse, (de inhoud van) het continuïteitsplan, het raamwerk daarvoor en het testen en onderhouden ervan. In totaal worden in dat hoofdstuk 133 best-practices opgesomd.
- CobiT control objective DS4 *'Ensure Continuous Service'* beschrijft op hoog niveau een dertiental doelstellingen welke een organisatie moet uitvoeren om de continuïteit van ICT-voorzieningen te waarborgen. Deze doelstellingen zijn uitgewerkt in 59 Control Practices.
- De eerder genoemde Publicly Available Standard 56 uit 2003 formaliseert de best-practices van het Britse Business Continuity Institute. PAS56 beschrijft het BCM-proces, de relaties met alle relevante bedrijfsprocessen (zoals HRM, ICT, facility management en dergelijke) en bevat een groot aantal best-practices ingedeeld in vijf processtappen.
- HB221:2003 *'Handbook Business Continuity Management'* van Standards Australia, bevat een definitie van BCM en bespreekt de evolutie van de focus op ICT naar een breed planningsgereedschap voor strategische en business planning. Het bevat een BCM-raamwerk toepasbaar voor elke organisatie.
- In de Verenigde Staten wordt veel gebruikgemaakt van de SANS-publicatie *'Disaster Recovery and Business Continuity Step-by-Step'* en van NIST Publication 800-34 *'Contingency Planning Guide for Information Technology Systems'*. Beide beschrijven de stappen om te komen tot een ICT-continuïteitsplan.
- Concreet maar beperkt tot ICT en enigszins verouderd (daterend uit 1989) is NIVRA-geschrift 53 *'Kwaliteitsoordelen over informatievoorziening'* waarin in bijlage 2.14 in totaal 97 normen op vier niveaus inclusief wegingsfactoren voor back-up, recovery, uitwijk en beschikbaarheid worden opgesomd.
- British Standard 15000 bevat de formele normstelling (specification) voor het ITIL Service Delivery proces Service Continuity Management. Het bevat slechts dertien doelstellingen.

Naast de openbare normstelsels gebruiken diverse aanbieders eigen methodieken waarbij de Disaster Recovery Methodology van Getronics de in Nederland meest bekende is.
Als voorbeeld worden in de volgende paragraaf CobiT DS4 en de bijbehorende control practices en ISO 17799 gebruikt. De verwachting is dat IT-auditors hiermee het meest worden geconfronteerd. Ook is voor CobiT in de Audit Guidelines omschreven hoe een audit op CobiT en dus ook op DS4 moet (kan) worden uitgevoerd.

Beschrijving van het BCM-proces

Business Continuity Management bestaat altijd uit drie fasen. In de eerste fase wordt een continuïteitsvoorziening ontworpen op basis van risico's, kenmerken van de bedrijfsprocessen, wettelijke verplichtingen en andere te voorziene eisen. In de tweede fase wordt de continuïteitsvoorziening ingericht en initieel getest. In de derde fase wordt de continuïteitsvoorziening onderhouden door een link naar change management, door audits, testen en dergelijke.
CobiT DS4 bevat slechts een rudimentaire beschrijving van het BCM-proces. Globaal kan de volgende indeling van de dertien control objectives worden gemaakt:

Fase 1: ontwerpen van de continuïteitsvoorziening

- IT Continuity Framework
  (ISO 17799 hoofdstuk 11.1.4)
- IT Continuity Plan Strategy and Philosophy
  (ISO 17799 hoofdstuk 11.1.1)
- Critical IT Resources
  (ISO 17799 hoofdstuk 11.1.2)
- Minimising IT Continuity Requirements

Fase 2: bouwen van de continuïteitsvoorziening

- Back-up Site and Hardware
- Off-site Back-up Storage
- User Department Alternative Processing
  Back-up Procedures
- IT Continuity Plan Contents
  (ISO 17799 hoofdstuk 11.1.3)
- IT Continuity Plan Distribution

Fase 3: onderhouden van de continuïteitsvoorziening
- Maintaining the IT Continuity Plan (ISO 17799 hoofdstuk 11.1.5)
- Testing the IT Continuity Plan
- IT Continuity Plan Training

(De dertiende DS4 Control Objective *'Wrap-up Procedures'* is hier weggelaten. Deze betreft handelen en leren na de calamiteit met als doel procesverbetering.)

Door deze indeling ontstaat een beeld hoe het BCM-proces moet worden ingericht en worden ook de auditobjecten duidelijk. Volgens CobiT DS4 moet er een raamwerk zijn, een continuïteitsstrategie en moeten de kritieke IT-componenten in kaart zijn gebracht, zodat de eisen, gesteld aan continuïteit, kunnen worden geminimaliseerd. De continuïteitsvoorziening bestaat dan uit een back-up locatie, systemen en dataopslag en er moeten – eventueel alternatieve – procedures zijn om de verwerking voort te zetten. De inhoud van het continuïteitsplan en de distributie ervan blijkt belangrijk te zijn en het plan moet worden getest, onderhouden en getraind.

Hieronder worden de delen van het proces besproken vanuit het gezichtsveld van de auditor.

Auditobjecten en onderzoeksvragen

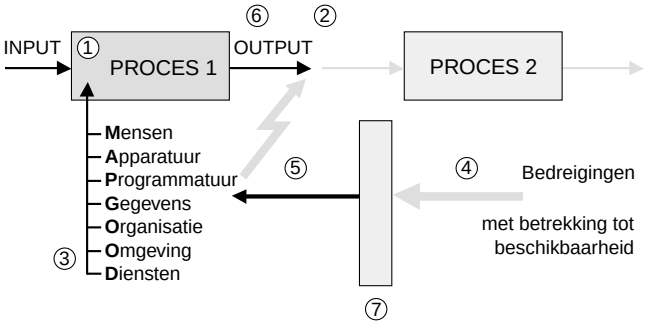
Business Continuity Management, Business Continuity Planning en Disaster Recovery Planning; de vele namen voor het vakgebied geven al aan dat het cruciaal is voor een auditor om de reikwijdte van het te toetsen object duidelijk vast te leggen. De IT-auditor zal veelal worden geconfronteerd met een uitwijkplan voor de ICT-voorzieningen als deel van een overkoepelend business continuity plan. De reikwijdte van het overkoepelende continuïteitsplan is vrijwel zeker breder dan alleen ICT; vaak is daarin ook uitwijk van werkplekken en van andere productiemiddelen opgenomen.

De volgende onderzoeksvragen kunnen worden gekoppeld aan de hierboven genoemde fasen van het BCM-proces:
1. Heeft de organisatie de uitgangspunten voor de continuïteitsvoorziening juist bepaald (opzet)?
2. Zijn de uitgangspunten op de juiste wijze vertaald naar technische voorzieningen, procedures en organisatorische aanpassingen (bestaan)?
3. Is de continuïteitsvoorziening getest en aantoonbaar functioneel; is het zeker dat de continuïteitsvoorziening bij een calamiteit zal werken (werking)?
4. Wordt de continuïteitsvoorziening juist onderhouden (werking)?

Bepalen van de uitgangspunten, opzet van de continuïteitsvoorziening

Bij een calamiteit zal de organisatie moeten zorgdragen dat zij overleeft. Dit betekent dat de schade die op dat moment wordt opgelopen niet boven een van te voren vastgestelde waarde mag komen. De materiële schade aan gebouwen en installaties is vrijwel altijd verzekerd.
De bedrijfsschade door uitval is soms te verzekeren, maar met een som geld is het bedrijfsproces niet gered.
Overleven betekent de primaire processen voortzetten en voorkomen dat chaos ontstaat. Van te voren, als uitgangspunten voor de continuïteitsvoorziening, zal duidelijk moeten zijn:
- wat de maximaal toelaatbare uitvalsduur (MTU) is van de diverse bedrijfsprocessen;
- hoe de bedrijfsprocessen (input, output) aan elkaar gerelateerd zijn (om te bepalen hoe stilval en schade in een proces leiden tot schade in andere processen);
- wat het maximale dataverlies (MDV) zal mogen zijn. Dit vormt een belangrijk uitgangspunt voor het back-up proces;
- wat de minimale mens- en productiecapaciteit ten tijde van een calamiteit moet zijn;
- welk aantal werkplekken, PC's, telefoons, kantoormeubelen en dergelijke nodig zal zijn ten tijde van een calamiteit.

De business impact analyse (BIA) vormt het gereedschap waarmee de organisatie antwoord op deze vragen dient te krijgen. In een business impact analyse moeten ter zake kundigen (veelal proceseigenaren) consensus bereiken over de vraag welke bedrijfsprocessen kritisch zijn door de gevolgen van stilstand te vertalen naar financieel verlies. Vragen voor de auditor zijn dan: Zijn de juiste functies/personen bij de analyse betrokken geweest?
Is consensus bereikt over de bovenstaande vragen?
Is de gevolgschade juist bepaald? Is de analyse bedrijfsdekkend geweest? Zijn alle materiële processen besproken? Zijn de MTU en het MDV duidelijk bepaald?
Is rapportage van de BIA voorhanden en is deze betrouwbaar? Sluiten MTU/MDV aan bij de eisen van klanten (in SLA's bijvoorbeeld) en/of bij de eisen van wet- en regelgevers?
Na de business impact analyse kan een risicoanalyse (zie *de EDP-Auditor* 2004 nrs. 3 en 4) duidelijk maken welke specifieke risico's de organisatie loopt.
In figuur 1 worden de stappen van de BIA en risicoanalyse grafisch weergegeven.
Uiteraard heeft de organisatie maatregelen getroffen waardoor een aantal risico's niet meer zal kunnen optreden.
Een QuickScan kan duidelijk maken welke preventieve en repressieve maatregelen al getroffen zijn. Vraag is hierbij



Figuur 1. De stappen tijdens het ontwerp

of *alle* mogelijke bedreigingen onderzocht zijn, of de kansen van optreden juist geschat zijn en of de gevolgschaden duidelijk gekwantificeerd zijn.

Specifieke BIA- en risicoanalysegereedschappen voor business continuity planning zijn schaars. Voor ICT-schadeontwikkeling kunnen de impact guidelines en dreigingen uit CRAMM worden gebruikt. Relevant is dat de auditor zeker stelt dat het door de organisatie gebruikte gereedschap tot betrouwbare resultaten heeft geleid. In de nummers 3 en 4 van de jaargang 2004 van *de EDP-Auditor* wordt de risicoanalyse nader beschreven.
De bepaling van de uitgangspunten voor de continuïteitsvoorziening dient zijn beslag te krijgen in een strategische keuze voor de uiteindelijke oplossing waarbij kosten en baten moeten worden gewogen. Bij lage MTU en MDV (minuten, uren) zal veelal standby reserveapparatuur noodzakelijk zijn waarin de productieomgeving wordt gespiegeld (data en/of processing).

Heeft de organisatie meerdere uren of dagen om bij een calamiteit de continuïteitsvoorziening aan te spreken, dan kan een commerciële uitwijkaanbieder de oplossing zijn. Altijd dient de afweging te worden gemaakt of de organisatie zelf de voorziening zal bouwen en onderhouden of dat zij dit uitbesteedt. Beide keuzes hebben specifieke voor- en nadelen.
Een voorbeeld casus. Een serviceorganisatie met een hoofdkantoor, waarin meer dan tweeduizend medewerkers werkzaam, heeft een zeer complexe ICT-infrastructuur en tijdskritische processen welke 24 uur per dag operationeel moeten zijn. Zij heeft externe uitwijk voor een klein deel van de informatiesystemen ingericht. Enerzijds bleek deze externe uitwijk tijdens testen niet altijd goed te werken en anderzijds was duidelijk dat zonder werkplekken en toegang tot het hoofdkantoor uitwijk niet zinvol zou zijn.
De onderzoeksvraag was of deze organisatie met een niet-acceptabele kans getroffen zou kunnen worden door een dermate grote calamiteit dat het gehele hoofdkantoor niet meer beschikbaar zou zijn. In een groot aantal interviews met proceseigenaren werd het schadeverloop bepaald waardoor duidelijk werd dat voor een klein deel van de processen de MTU maximaal één dag bedraagt. De overige processen mogen maximaal twee dagen tot één week stilvallen.
Op grond van de benodigde werkplekken, specifieke componenten in de processen zoals een call center, en de MTU bleek al snel dat externe uitwijk geen zekerheid kon bieden. Een uitgebreide dreigingenanalyse toonde aan dat de restrisico's rond het hoofdkantoor zodanig waren dat de kans op totaal verlies van het totale hoofdkantoor verwaarloosbaar klein zou zijn. Het complex is dermate uitgestrekt, de brandbeveiliging en noodvoorzieningen zodanig dat alles in ogenschouw nemend de inrichting van een interne uitwijkvoorziening de beste strategie werd. In de dreigingenanalyse zijn zelfs terroristische aanslagen beschouwd, is rekening gehouden met aanwezigheid van munitie uit de Tweede Wereldoorlog in de bodem, met blokkades en met transport van gevaarlijke stoffen langs het pand. Geen van de uitgebreide lijst risico's werd onaanvaardbaar geacht.

Vertalen van de uitgangspunten, audit naar bestaan van de continuïteitsvoorziening

Als de uitgangspunten waaraan de continuïteitsvoorziening moet voldoen duidelijk zijn, kunnen deze worden vertaald naar de juiste mix van technische voorzieningen, procedures en organisatorische inbedding. Hierbij zijn vele keuzes mogelijk waarbij de auditor kan worden gevraagd een oordeel te vormen of de gekozen combinatie voldoet aan de uitgangspunten.
Bij ICT-uitwijk spelen de gegevens altijd een cruciale rol. Zonder toegankelijke, herstelbare veiligheidskopieën zal het bedrijfsproces niet te herstellen zijn. Een sluitende

back-up en herstelprocedure zijn noodzakelijk.
Ten tijde van een calamiteit moet 'handelen' voorop staan en komt 'denken' op de tweede plaats. Een draaiboek met daarin duidelijk omschreven acties moet voorhanden zijn. Hierin moet worden uitgegaan van een worst-case situatie waarin anderen dan de normaal opgestelde medewerkers de acties moeten uitvoeren. De slapende organisatie beschreven in het draaiboek draait rond teams, teamleiders, teamleden en coördinatoren. Het draaiboek wordt gebouwd in een tekstverwerker met ondersteuning van flowchart tools. Figuur 2 toont een dergelijke flowchart (in DRM Toolkit van Getronics).
De onderzoeksvragen van de auditor richten zich op de betrouwbaarheid van de ingerichte technische voorzieningen en op de inhoud van het draaiboek. De eerste vormt in feite een normale IT-audit, de tweede is specifieker. Ook hiervoor bestaan echter geen duidelijke normen. Stelregel is dat het handboek voldoende en juist detail bevat om door relatief onbekenden begrepen en uitgevoerd te worden. Een draaiboek voor het activeren en in gebruik nemen van de continuïteitsvoorziening is in feite een procedure, een procesbeschrijving.
Bijzonder is hierin het tijdskritische aspect, de uitvoering door mogelijkerwijs met de materie onbekende personen en de veelheid van acties en de synchronisatie tussen die acties. In essentie blijft een dergelijk draaiboek echter een normale procesbeschrijving. Auditors kunnen dus voor het vormen van een oordeel over de kwaliteit (in opzet) van het draaiboek te rade gaan bij de literatuur voor procesbeheersing en procesbeschrijving. Die literatuur leert dat een procedure ingaat op:

- Doelstellingen
- Onderwerp
- Reikwijdte
- Wat moet er gebeuren
- Wie moet het doen
- Wanneer gebeurt het
- Waar gebeurt het
- Hoe moet het worden gedaan
- Welke middelen zijn noodzakelijk
- Welke documenten zijn gerelateerd
- Hoe moeten die documenten worden beheerst en vastgelegd

De minimale inhoud van een draaiboek
(bron: ITIL Service Delivery) is dan als volgt:

1. Document Control
1.1 Document distribution
1.2 Document revision
1.3 Document approval

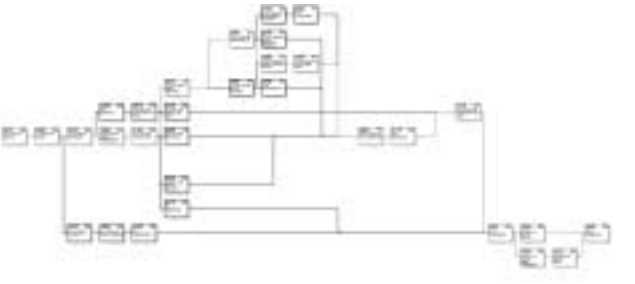
2. Supporting Information
2.1 Introduction
2.1 Recovery strategy
2.1 Invocation
2.1 General guidance
2.1 Dependencies
2.1 Recovery team
2.1 Recovery team checklist

3. Recovery Procedures

Hoofdstuk 2 bevat de achtergrondinformatie en hoofdstuk 3 de specifieke procedures voor elk uitwijkteam en teamlid. Vooral het activeren van het draaiboek moet goed omschreven staan. Wie besluit daartoe? En wat is de escalatieprocedure?

Werking van de continuïteitsvoorziening

Het beoordelen van de *werking* van de continuïteitsvoorziening is vrijwel onmogelijk! Gezien het inherente karakter van de continuïteitsvoorziening zal er geen evidence zijn dat de voorziening bij een calamiteit zal functioneren omdat immers de calamiteit nog niet opgetreden is. Wel zijn uitwijktesten mogelijk waarbij de voorziening (deels) geactiveerd wordt. Soms is een organisatie bereid tot een zogenaamde sloepenrol waarbij de calamiteit tot in detail nagespeeld wordt. De verstoring in het bedrijfsproces – dan bijna gelijk aan die bij de werkelijke calamiteit – zal door de organisatie echter niet snel geaccepteerd worden. Een sloepenrol is een zeldzaamheid.



Figuur 2. Een uitwijkdraaiboek
(afdruk uit DRM Toolkit van Getronics)

De auditor zal het dus moeten doen met verslagen van de gehouden oefeningen zoals uitwijktesten en droogtesten (waarbij het draaiboek in discussie tussen de betrokken personen besproken wordt).
In ieder geval is duidelijk dat om de continuïteitsvoorziening te laten werken een aantal aandachtspunten gelden. Regelmatig moet de continuïteitsvoorziening worden getest. Dit betekent dat de technische voorzienin-

gen zoals noodstroomaggregaten volgens de voorschriften van de leverancier worden getest en onderhouden.
Deze overeenkomst is als elke andere control door een auditor te toetsen.
Het draaiboek moet zoals hierboven beschreven in een sloepenrol, in deeltesten of door middel van droogtesten regelmatig worden geoefend. Verslagen van de testen vormen de evidence voor de auditor.
Belangrijkste aandachtspunten zijn de benoeming van verantwoordelijkheid voor continuïteit – de aanstelling van een coördinator of bijvoorbeeld een business continuity manager – en de inrichting van een link tussen het change management proces en de continuïteitsvoorziening.
Elke verandering in ICT-infrastructuur, personele bezetting, bedrijfsproces of anderszins moet worden beoordeeld op de gevolgen voor de continuïteitsvoorziening. Op deze wijze wordt de verandering ook doorgevoerd in de continuïteitsvoorziening en leidt een grote verandering als deel van de acceptatietest ook tot een test van de wijziging in de continuïteitsvoorziening.
De auditor dient de kwaliteit van de beheersing van het change management proces te beoordelen. Worden changes beoordeeld op impact op de continuïteit? Wordt aantoonbaar de verandering ook doorgevoerd in de continuïteitsvoorziening (techniek, draaiboek en organisatie)? Wordt bij een grote verandering ook de continuïteitsvoorziening direct getest? Is bij de beoordeling de voor BCM/BCP verantwoordelijke betrokken?

Valkuilen

Voor een IT-auditor is de grootste valkuil bij het vormen van een oordeel over de betrouwbaarheid van de continuïteitsvoorziening het feit dat er vrijwel nooit enige evidence zal zijn over de *werking* van deze voorziening.
De gehele inrichting van de continuïteitsvoorziening is gebaseerd op aannames van het management van de organisatie met betrekking tot dreigingen, kansen en gevolgschades. Alleen als deze aannames volledig gedocumenteerd zijn zal de auditor een oordeel kunnen geven over de opzet van de continuïteitsvoorziening of over het proces dat tot de inrichting van de continuïteitsvoorziening geleid heeft. Door het ontbreken van gedetailleerde normenkaders hiervoor moet de auditor met de auditee samen een norm vaststellen; de verwachtingen van de opdrachtgever moeten hierbij goed worden beheerst.

Literatuur

[COBIT] *CobiT Audit Guidelines, CobiT Control Objectives, CobiT Control Practices*, www.isaca.org

[CORP04] *Corporate Governance of Information and Communication Technology*, AS 815-2004, www.standards.com.au

[HARD] Hardjono R.J.M. Bakker, *Management van processen*, Kluwer, ISBN 90-14-09607-0

[ISACA] *e-Commerce Security Business Continuity Planning*, www.isaca.org

[ISO00] ISO/IEC (2000), *Code of practice for information security management*, ISO/IEC 17799:2000, www.iso.ch.

[ITIL] *ITIL Best Practice for Service Delivery,* www.exin.nl, ISBN 0-11-330017-4

[JORD] Jordan, J., H. Zellenrath en R. Verzuu, *Guide to Business Continuity Planning*, www.cpa.nl

[NIST] *Contingency Planning Guide for Information Technology Systems*, NIST Special Publication 800-34, www.nist.gov

[NIVR89] Nivra geschrift 53 (1989), *Kwaliteitsoordelen over Informatievoorziening*, www.nivra.nl

[PAS03] PAS56 (2003),*Guide to Business Continuity Management*, www.bsi-global.com

[SMIT05] Smith, R. (2005), *Sarbanes-Oxley Act and IT: Why There is No 'I' in 'SOx Team'*, www.dmreview.com/editorial/dmreview/print_action.cfm?articleId=1011206.

[WEIL04] Weil, S., S. Northcutt en M.T. Edmead (2004), *Disaster Recovery and Business Continuity Step-by-Step*, SANS Institute, ISBN 0-9743727-5-7.

[ZAWA05] Zawada, B. (2005), *Taking the Wind Out of the BCM Sails,* www.disaster-resource.com/articles/04p_044.shtml.