Continuïteitsplanning; meer dan ITIL Contingency Planning.

Uitgeschreven tekst van de lezing met dezelfde titel tijdens IT Beheer '98.

Ter publikatie in IT IMFormatie.

Ernst J. Oud
Getronics Business Continuity BV

Email: e.j.oud@getronics.nl

In dit artikel wordt aangegeven in welk kader continuïteitsplanning geplaatst dient te worden en welke methode gevolgd kan worden om een (ICT) continuïteitsplan te ontwikkelen. Tevens wordt aangegeven welke gereedschappen ontwikkeld zijn om het beheer van het ontwikkelde plan te koppelen aan ITIL Change Management.

Inleiding

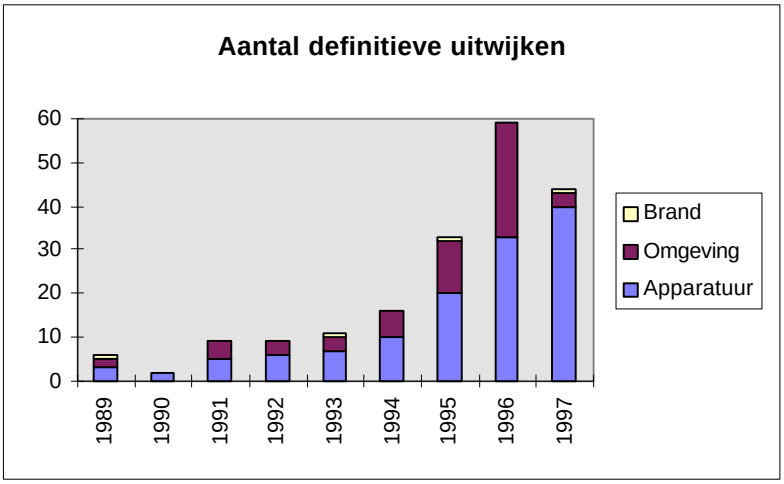
Ondernemingen zijn in steeds grotere mate afhankelijk geworden van informatie en communicatie technologie (ICT). Zelfs in die mate dat bij verstoringen in de ICT systemen de bedrijfsprocessen, en daardoor de organisatie, stil komen te liggen. Terugvallen op handmatig werken is veelal niet meer mogelijk of betekent een enorme terugval in de output van de organisatie.

Om een aantal gevolgen van een calamiteit te noemen:

- **Vitale informatie gaat verloren**
- **Financiële controle is niet meer mogelijk**
- **Informatie is niet meer beschikbaar**
- **Goederen en diensten kunnen niet geleverd worden**
- **Demotivatie bij medewerkers**
- **Chaos**
- **Fraude**
- **Faillissement!**

De schattingen geven aan dat meer dan de helft van de bedrijven getroffen door een verwoestende brand binnen drie maanden na de calamiteit niet meer bestaat. Ook bij kleinere calamiteiten kan toch de gevolgschade op langere termijn, denk bijvoorbeeld aan imago-schade, groot zijn.

Concreet cijfermateriaal (zie figuur 1) laat zien dat de kans op een calamiteit die de bedrijfsvoering bedreigt niet zo klein is als wellicht gedacht wordt.



Figuur 1 : Uitwijkmeldingen 1989-1997 bij CUC[1], Lelystad

Van de 1400 klanten die CUC in 1997 kende werden er ruim 40 geconfronteerd met een dermate grote calamiteit dat uitwijk naar Lelystad noodzakelijk werd, bijna 3% dus.

[1] Computer Uitwijk Centrum: vóór 5 oktober 1998 de bedrijfsnaam van Getronics Business Continuity

Zoals uit de grafiek blijkt is apparatuurstoring de grootste boosdoener. Dit geeft te denken want vrijwel elke afnemer van ICT heeft een service contract met de leverancier; klaarblijkelijk is dat niet de redding!

Bedrijfscontinuïteit - het kader

Maar wat dan wel te doen als de bedrijfsprocessen stilvallen? Hoe stelt een organisatie haar bedrijfscontinuïteit zeker?

Even terug naar de basis. Hierboven werden de gevolgen van een calamiteit geschetst vanuit het gezichtspunt van ICT. De trend is daarentegen om de gevolgen van calamiteiten veel meer te beschouwen vanuit de bedrijfsprocessen. *Disaster Recovery* zoals het vakgebied heet dat zich alleen bezighoudt met de opvang na een calamiteit, maakt plaats voor *Business Continuity Planning* waarbij ook preventieve en repressieve maatregelen en voorzieningen een grote rol spelen. Op dat moment wordt organisatiebreed risico management het kader en dienen alle disciplines, dus human resource management, asset management, finance management en information management in een continuïteitsplan meegenomen te worden.

Continuïteitsplanning in de brede zin van het woord is dus geen zaak alléén van juist IT beheer. Dat neemt niet weg dat, gezien de enorme afhankelijkheid van IT systemen bij vrijwel alle organisaties, IT beheer waarbij ook continuïteitsplanning meegenomen wordt, van levensbelang is.

Continuïteit onderdeel van informatiebeveiliging

Een organisatie die haar continuïteit vanuit het ICT gezichtspunt wil zeker stellen doet er verstandig aan een *integraal* beleid m.b.t. informatiebeveiliging te voeren. Continuïteitsplanning in de zin van planning tegen een eventuele calamiteit is namelijk nimmer een op zichzelf staand aandachtspunt. En continuïteitsplanning is dus meer dan het regelen van een uitwijkvoorziening.

Informatiebeveiliging dus. Wat is dat dan? Wel, een gangbare definitie is:

'Informatiebeveiliging is het geheel van preventieve-, repressieve- en herstel maatregelen alsmede procedures welke de beschikbaarheid, exclusiviteit en integriteit van alle vormen van informatie garanderen met als doel de continuïteit van de organisatie te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald, niveau te beperken.'

Kortom; informatiebeveiliging heeft te maken met garanties en waarborgen, met repressie, preventie én opvang en met procedures naast maatregelen.

Als informatiebeveiliging integraal aangepakt moet worden is het niet nodig het wiel opnieuw uit te vinden, er bestaan nl. een aantal standaards, zoals:

- **Code voor Informatiebeveiliging (BS 7799)**
- **Voorschrift Informatiebeveiliging Rijksdienst (VIR)**
- **Regeling Informatiebeveiliging Politie (RIP)**

Maar de organisatie kent natuurlijk ook branche voorschriften of de moedermaatschappij stelt eisen en uiteraard spreekt de wetgever een woordje mee in wetten zoals de Wet Persoonsregistraties, de Wet Computercriminaliteit en de ARBO wet.

De genoemde Code voor Informatiebeveiliging vormt een leidraad voor beleid en implementatie. De Code, uitgegeven door het Nederlands Normalisatie Instituut in Delft, omschrijft in totaal 109 te treffen maatregelen, waarvan er 10 essentieel en fundamenteel zijn; m.a.w. elke organisatie zou ze moeten implementeren.

De 10 essentiële en fundamentele maatregelen zijn als volgt de rangschikken:

Management

- **Toewijzing van verantwoordelijkheden voor informatiebeveiliging**
- **Naleving van de wetgeving inzake bescherming van persoonsgegevens**
- **Naleving van het beveiligingsbeleid**

Procedures

- **Het rapporteren van beveiligingsincidenten**
- **Het proces van continuïteitsplanning**
- **Beveiliging van bedrijfsdocumenten**

Maatregelen

- **Opleiding en training voor informatiebeveiliging**
- **Viruscontrole**
- **Voorkomen van het onrechtmatig kopiëren van programmatuur**
- **Beveiliging van bedrijfsdocumenten**

De Code voor Informatiebeveiliging erkent dus dat continuïteitsplanning (gezien de aard van de Code wordt daarmee dan de continuïteit van de ICT systemen bedoeld) een essentiële en fundamentele maatregel is.

Continuïteitsplanning

Wat is dat dan wel ‘continuïteitsplanning’?

Continuïteitsplanning is het van te voren zeker stellen dat de kritische bedrijfsprocessen binnen een bepaalde tijdsduur weer beschikbaar zijn na een (maximale) calamiteit.

De basis voor continuïteit is een continuïteitsplan waarin de onderneming van te voren vastlegt hoe zij haar continuïteit geregeld heeft. Dit roept de vraag op hoe een continuïteitsplan ontwikkeld wordt. De aanbeveling hier is om een in de praktijk bewezen methode te gebruiken en niet zonder meer over te gaan tot implementatie van maatregelen (zoals een uitwijkcontract!). Volg een stappenplan en denk eerst eens goed na over de te bereiken doelen.

ITIL Contingency Planning

Uiteraard is het zinvol in dit verband de ITIL module Contingency Planning daar waar mogelijk te gebruiken; zeker als de organisatie andere modules zoals Change Management, Problem Management en Helpdesk volgens de ITIL methodiek opgezet heeft. Echter, de huidige ITIL module Contingency Planning (aan een update wordt gewerkt) is slechts beperkt bruikbaar; aan de orde komen:

- **Het opzetten van een IT recovery plan**
- **De definities van begrippen zoals hot/cold sites**
- **Een voorbeeld inhoudsopgave recovery plan**
- **Een globale beschrijving van gereedschappen**

Veel belangrijker is daarentegen dat niet aan de orde komt:

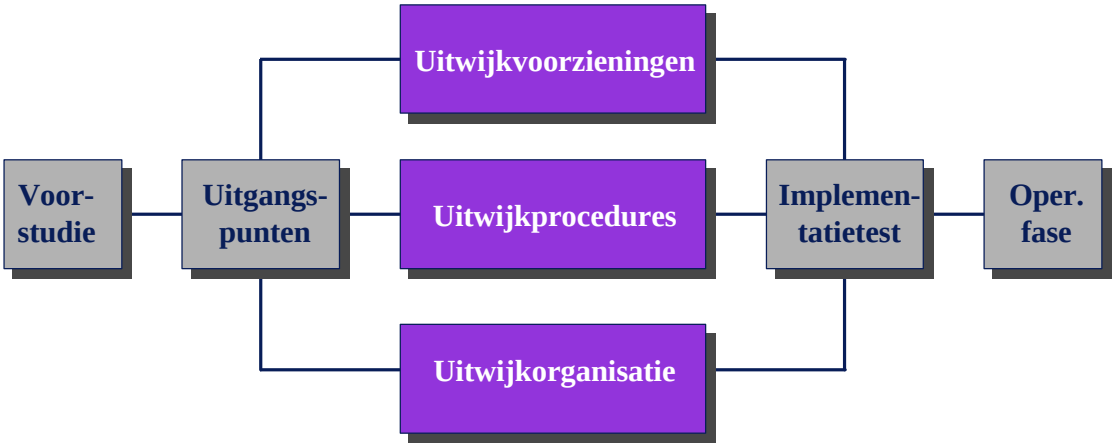
- **Het opzetten van recovery van bedrijfsprocessen**
- **Hoe en waarom een risico analyse uitgevoerd wordt**
- **Het bepalen van uitgangspunten waaraan recovery moet voldoen**

Maar meest belangrijke omissie is dat niet beschreven wordt hoe de koppelingen met andere ITIL processen tot stand gebracht moeten worden. We komen hier tegen het einde van dit artikel op terug.

De ITIL module Contingency Planning is dus niet volledig en geeft te weinig concrete informatie om een succesvol ICT continuïteitsplan te ontwikkelen en te onderhouden.

Disaster Recovery Methodology™

Een project methode voor de ontwikkeling van een continuïteitsplan, in gebruik bij honderden bedrijven in Europa, is bijvoorbeeld de Disaster Recovery Methodology™. Het stappenplan welke deze methode voorschrijft is als volgt:



Figuur 2 : Disaster Recovery Methodology™

Bij deze methode (te volgen van links naar rechts) wordt een operationele continuïteitsvoorziening (beschreven in het continuïteitsplan) bereikt door na een voorstudie na te denken over de uitgangspunten op basis waarvan voorzieningen, procedures en een organisatie ingericht worden. Na de implementatietest is de continuïteitsvoorziening dan uiteindelijk operationeel.

We lopen hierna de stappen kort eens langs.

Voorstudie

In de voorstudie wordt veelal een risico-analyse en eventueel een gevolgschade onderzoek uitgevoerd om de risico's voor de bedrijfsprocessen boven tafel te krijgen zodat later voor deze kritieke bedrijfsprocessen de juiste risico's weggenomen of tot een acceptabel niveau beperkt kunnen worden

Een risico-analyse kan op een aantal manieren plaatsvinden; de meest gangbare is de kwantitatieve methode waarbij de risico's voor het manifest worden van alle onderkende bedreigingen (het optreden van een calamiteit dus) voor de organisatie bepaald worden en deze dan te sommeren.

Bijvoorbeeld:

Schadeverwachting = Σ (risico x schade)

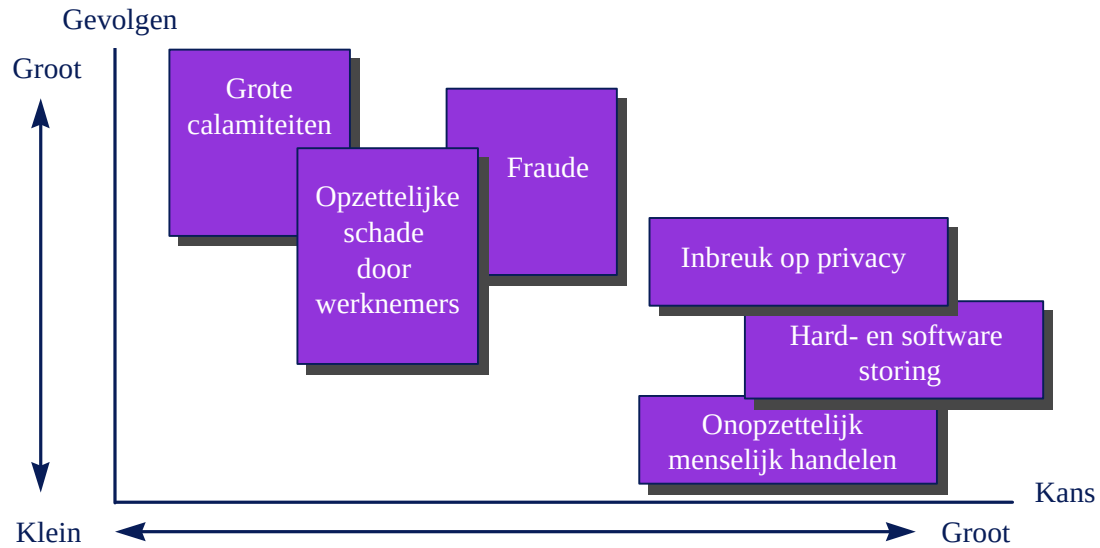
bv. kans op overstroming

eens per 1250 jaar, schade ƒ 10 miljoen : 1/1250 x 10.000.000 = 8.000

Dit alles geeft niet meer dan een indicatie, want:

> ***There are three kinds of lies; lies, damned lies and statistics.***
> **Benjamin Disraeli**

In de laatste jaren komt de kwalitatieve methode meer in zwang. Hierbij worden risico's niet meer in cijfers achter de komma bepaald maar worden klassen samengesteld en kan het management van een organisatie vervolgens keuzen maken welke klasse calamiteiten men wilt kunnen overleven.



Figuur 3 : Kwalitatieve risico-analyse

Deze methode levert meer ‘tastbare’ handvatten daar deze de bedrijfsprocessen bijvoorbeeld zo weergeeft:

UITVAL / BEDRIJFSPROCESSEN		EFFECTEN 1 d	2 d	1 wk	1 mnd
1. Proces 1	Input / Output	●			
2. Proces 2	Input / Output		●		
3. Proces 3	Input / Output			●	
4. Proces 4	Input / Output			●	

Figuur 4 : De resultaten van een kwalitatieve analyse

Het management van de onderneming ziet dan in een oogopslag welke processen de hoogste prioriteit in een continuïteitsplan dienen te krijgen.

Welke methode voor een risico-analyse de organisatie ook gebruikt, na de voorstudie zijn de bedrijfsprocessen geanalyseerd, zijn prioriteiten aangegeven en zijn de risico’s onderkend en kan men in principe de maatregelen kiezen (aan de hand van begrippen zoals ‘repressief’, ‘preventief’ en ‘opvang’). Bijvoorbeeld als volgt:

Actie	Voorbeeld maatregel
Niets doen (aanvaarden)	**-**
Preventie (voorkomen)	**Brand-/rookmelding, Toegangsbeveiliging**
Repressie (beperken)	**Brandblusinstallatie, Ontruimingsprocedures**
Verzekeren (afwentelen)	**Materiële gevolgschade polis afsluiten**
Continuïteit (opvangen)	**Computeruitwijk, Calamiteitenplannen**

Uitgangspunten

Na de voorstudie start de belangrijkste fase; het bepalen van de uitgangspunten. Wordt deze fase overgeslagen of onjuist doorlopen dan worden later de verkeerde continuïteitsvoorzieningen getroffen. Denk aan het gebruik van een UPS op een niet-kritisch systeem of een uitwijkvoorziening die pas na 24 uur operationeel is terwijl de processen niet meer dan 8 uur stil mogen liggen. De bepaling van de juiste uitgangspunten is dus cruciaal.

Een aantal mogelijke uitgangspunten waar de organisatie over na moet denken:

- **Maximaal Toelaatbare Uitvalsduur (MTU)**
- **Meest ernstige calamiteit**
- **Gewenste recentheid van bestanden (maximaal dataverlies)**
- **Prioriteit van bedrijfssystemen**
- **Aantal gewenste werkplekken**
- **Kwaliteitskenmerken (t.b.v. leveranciersselectie)**

Hiervan is de MTU weer de belangrijkste; hoe lang mogen de tijdens de voorstudie bepaalde kritische bedrijfsprocessen bij het optreden van een onderkend risico, maximaal stil komen te liggen. Met andere woorden; binnen welke tijd dient een continuïteitsvoorziening operationeel te zijn. Op basis van dit soort van te voren bepaalde kencijfers worden de maatregelen, procedures en de organisatie ingericht.

Voorzieningen

Voor het bepalen van de benodigde uitwijkvoorzieningen moet duidelijk worden welke mensen en middelen benodigd zijn voor de kritieke bedrijfsprocessen, denk bijvoorbeeld aan:

- **Externe opslag van backups**
- **Computersyste(e)m(en)**
- **Datacommunicatie**
- **Uitwijklocatie**
- **Telefonie/fax**
- **Werkplekken**
- **Dealingroom**
- **Mensen**
- **Call center**

En dit staatje noemt alleen de ICT produktiemiddelen; nog niet eens produktiemiddelen zoals machines e.d. die de organisatie wellicht gebruikt! Een dergelijke inventarisatie is absoluut noodzakelijk.

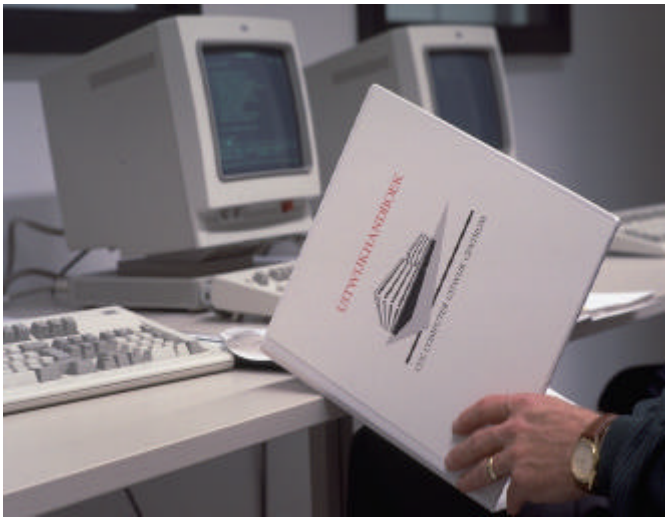
Procedures

Als we weten welke mensen en middelen van te voren geregeld moeten zijn om een continuïteitsvoorziening in te richten komt een zeer belangrijk aspect aan de orde; het ontwikkelen van de juiste procedures en het inrichten van de calamiteitenorganisatie.

Een aantal van de ontwikkelen plannen:

- **Calamiteitenplan**[2] → **Escalatieplan**
  → **Uitwijkdraaiboek**
- **Ontruimingsplan**
- **Aanvalsplan**
- **Veiligheidsplan**

[2] Merk op dat de term continuïteitsplan en calamiteitenplan hier door elkaar gebruikt worden; in feite is een continuïteitsplan breder; het calamiteitenplan beschrijft alleen hoe de continuïteit na een vooraf bepaalde maximale calamiteit zeker gesteld is.

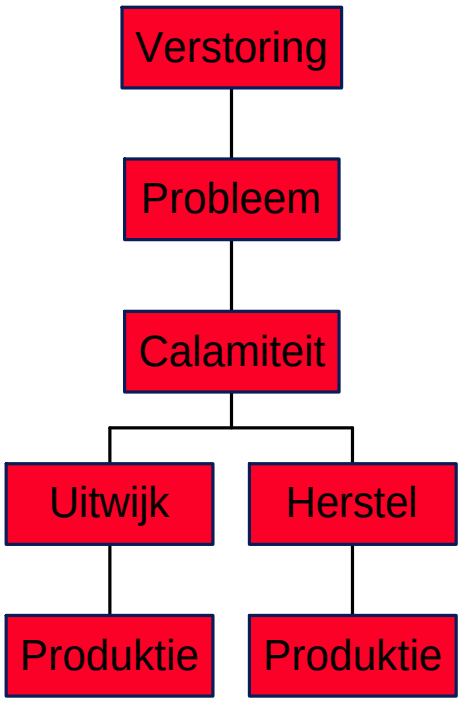


Figuur 5 : Een uitwijkdraaiboek - de kern van een uitwijkplan

Het calamiteitenplan bevat het escalatieplan en het uitwijkdraaiboek (beschrijft stap voor stap alle activiteiten die uitgevoerd moeten worden na een calamiteit om de continuïteitsvoorziening te activeren).

Escalatieplan

Het tevens zeer belangrijke escalatieplan beschrijft de stappen Probleemherkenning, Calamiteitenbesluit, Uitwijkbesluit en Produktiebesluit en de criteria daarvoor zoals de escalatietijden. Grafisch weergegeven ziet dat er bijvoorbeeld zo uit:



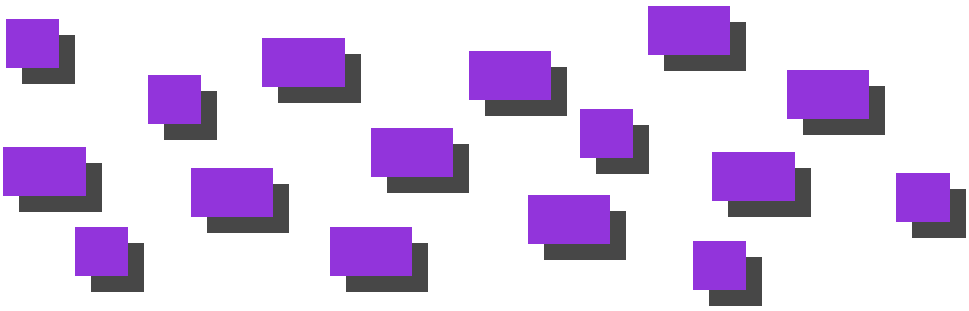
Figuur 6 : Een voorbeeld escalatieprocedure

Het is bijzonder belangrijk om het traject van verstoring tot calamiteitenbesluit formeel vast te leggen. Als bekend is dat de bedrijfsprocessen slechts 4 uur kunnen stil liggen moet bijvoorbeeld al een half uur na het optreden van een verstoring uitgeweken worden. Als dit niet bewaakt wordt via een formele escalatieprocedure dan blijft men wellicht te lang nadenken over herstel.

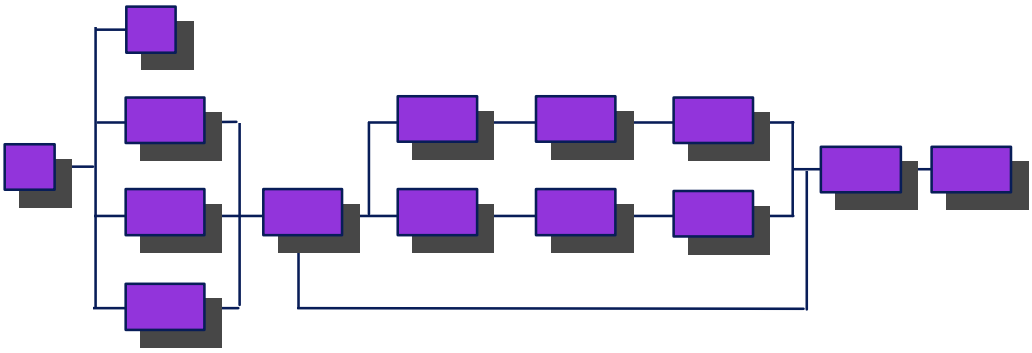
Uitwijkdraaiboek

Blijft nog over het cruciale uitwijkdraaiboek waarin alle acties in details beschreven om de continuïteitsvoorziening operationeel te maken. Denk aan het opbrengen van systemen, het restoren van de backup, het aansluiten van de apparatuur aan het netwerk, het herrouteren van netwerkverkeer etc. etc.

De beste manier voor het opstellen van een dergelijk draaiboek is middels brainstorm sessies alle activiteiten die uitgevoerd moeten worden boven tafel te krijgen. Alle disciplines binnen het bedrijf betrokken bij de uit te wijken processen moeten hierin betrokken worden. Men krijgt dan een groot aantal activiteiten:



En die moeten gerangschikt worden tot een netwerkschema:

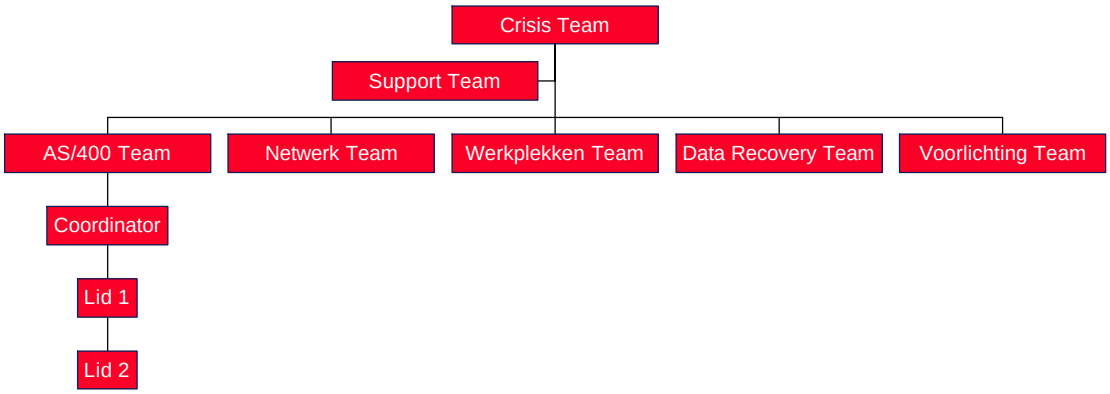


Als elke stap beschreven is dan kunnen ook alle doorlooptijden van de activiteiten afzonderlijk opgenomen worden en weet men dus precies hoe lang dit proces in totaal gaat duren; komt men boven de maximale tijd uit (de MTU) dan moeten activiteiten parallel gaan lopen of moeten anderszins versnellingen aangebracht worden.

Het bovenstaande is geen sinecure; men kan daarvoor het beste gebruik maken van een voor dit doel ontwikkeld tool zoals de DRM Toolkit.

Calamiteitenorganisatie

Op het moment van een calamiteit dienen de activiteiten zoals beschreven in het uitwijkdraaiboek uitgevoerd te worden volgens een strak schema. De daarvoor benodigde personen, veelal ingedeeld in teams, dienen in een ‘slapende’ organisatie (de normale organisatie van een bedrijf wordt vaak de lijnorganisatie genoemd) aanwezig te zijn, bijvoorbeeld als volgt:



Figuur 7 : Een voorbeeld calamiteitenorganisatie

De in de calamiteitenorganisatie aanwezige personen dienen een exemplaar van het uitwijkdraaiboek in hun bezit (liefst thuis!) te hebben en de inhoud er van te kennen.

Testen, testen, testen …

Zonder meer het allerbelangrijkste van het inrichten van een continuïteitsvoorziening op welke wijze dan ook is het uitvoeren van een implementatietest waarbij de getroffen voorzieningen, de procedures en de calamiteitenorganisatie getest worden om zeker te stellen dat aan de uitgangspunten wordt voldaan. Een niet getest plan kan net zo slecht zijn als geen plan. Een mogelijke implementatietest is de zgn. sloepenrol. Hierbij wordt het totale plan getest; soms zelfs door een calamiteit te ensceneren; ‘trek de stekker er maar uit’.

Operationele fase

Is met de implementatietest gebleken dat het plan ‘werkt’ dan gaat de operationele fase in. Een continuïteitsplan vergt echter continue aandacht; een verouderd plan is net zo slecht als geen plan. Ten behoeve van correctief onderhoud dient minimaal jaarlijks getest te worden. Mogelijke testen zijn droogtesten (walkthroughs) en audits. Schrijf van te voren een testplan zodat vastgesteld zijn:

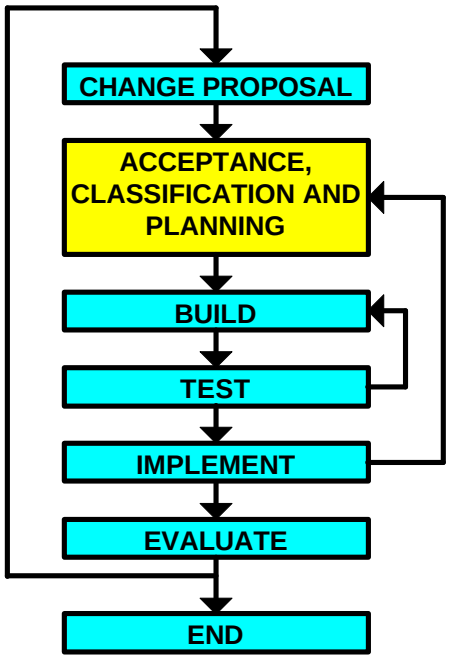
- **De doelstelling(en) - wat wil de test bewijzen?**
- **De procedure - hoe gaat de test uitgevoerd worden?**
- **De uitwijkvoorzieningen - wat gaat er getest worden?**
- **De evaluatie - wanneer, hoe en met wie worden de resultaten besproken?**

Zonder van te voren vast te leggen waar de test aan moet voldoen (de doelstellingen) is het resultaat van de test niet aan de verwachting te toetsen.

Links met ITIL Change Management

Preventief onderhoud is in te richten door koppelingen met beheersmethodes zoals ITIL Change Management zodat een verandering in de organisatie of haar middelen direct en juist verwerkt wordt in het continuïteitsplan.

Heeft de organisatie het ITIL Change Management proces ingericht (zie figuur 8) dan dient de stap waarbij een change geaccepteerd, geclassificeerd en gepland wordt, uitgebreid te worden (zie figuur 9).



Figuur 8 : ITIL Change Management proces

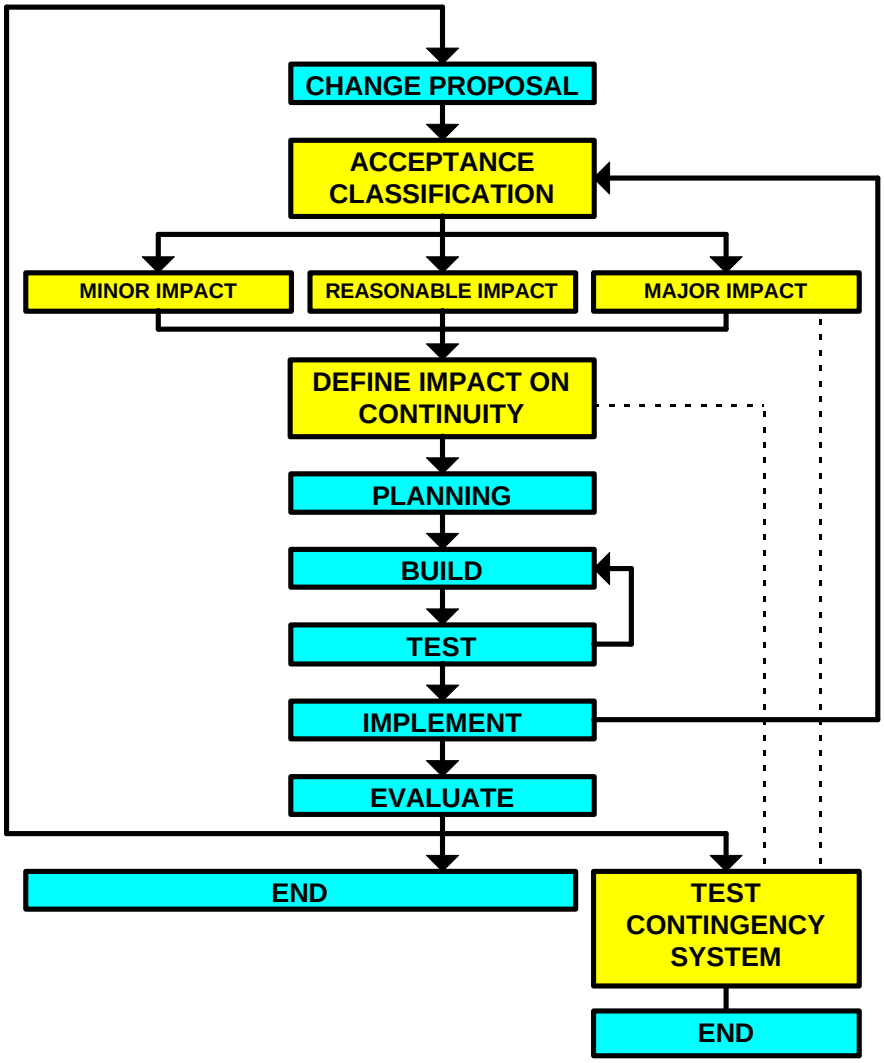
Toelichting bij figuur 9:

Zodra een change voorstel ontvangen is dient het voorstel geclassificeerd te worden. Classificatie omvat het vaststellen van de impact welke de verandering zal hebben op de organisatie, het budget, de personele invulling ***en of de continuïteit van de organisatie in gevaar komt door de voorgestelde change.***

Het aantal classificatie niveaus moet klein gehouden worden, wellicht in de trant van ‘lage impact’, ‘impact’ en ‘hoge impact’. ***Voor elk van deze classificaties moet ook de impact van de change op de continuïteit van de organisatie vastgesteld worden.***

Na classificatie moet het change voorstel geautoriseerd en ingepast worden in de planning van de uitstaande changes. Autorisatie m.b.t. continuïteit kan bijvoorbeeld zo ingericht worden dat *het management* changes autoriseert welke geclassificeerd zijn als ‘hoge impact’, dat *de change manager* autorisatie verleent voor changes met classificatie ‘lage impact’ en dat *het change overleg* (met als lid de contingency manager) alle changes met classificatie ‘impact’ autoriseert.

De contingency manager dient betrokken te zijn met het autorisatie proces zelf door het deelnemen in het change overleg of door direct te rapporteren of deel te nemen in het management team.



Figuur 9 : ITIL Change Management met ingerichte link naar Contingency Planning

Elke change met classificatie 'hoge impact' dient te leiden tot het volledig hertesten van het continuïteitsplan en de continuïteitsvoorziening.

De contingency manager moet volledige toegang hebben tot de configuratie management database zodat rapportages van alle uitstaande changes mogelijk zijn en dat de benodigde changes aan de continuïteitsvoorziening(en) en het continuïteitsplan vastgesteld, gepland en uitgevoerd kunnen worden.

Met de juiste projectmethode voor het bouwen van een continuïteitsplan en het inrichten van de continuïteitsvoorziening en organisatorische inbedding, bijvoorbeeld op basis van de ITIL processen, is het zonder meer mogelijk de continuïteit van de ICT processen zeker te stellen.

Bedenk : Een calamiteit is erg maar wordt pas een ramp als u niet voorbereid bent!

Geraadpleegde bronnen:

DRM Project Manual
Getronics Business Continuity BV
http://www.getronics.nl/gbc

Code voor Informatiebeveiliging
Nederlands Normalisatie Instituut
http://www.nni.nl

Operationeel beheer van Informatiesystemen
Kluwer Bedrijfsinformatie
Sander Koppens / Bas Meyberg
ISBN 90 267 1841 1

Het ABC tot IPW
ICT Management Pocket Guides
ten Hagen Stam uitgevers
ISBN 90 71694 98 4
http://www.quint.nl/index_uk.htm

ITIL Module Contingency Planning
Central Computer & Telecommunications Agency
http://www.ccta.org

COMPACT - Tijdschrift EDP Auditing
Themanummer 1998/5 - Informatiebeveiligingsbeleid
ten Hagen Stam uitgevers
ISSN 0920 1645

Informatie omtrent de auteur:

Ernst J. Oud is senior consultant bij Getronics Business Continuity. Op dit moment onderzoekt hij de uitwijk van de back-office van een dealingroom bij een grootbank. Tevens werkt hij in een internationale werkgroep aan het tot stand komen van de vernieuwde ITIL module Contingency Planning.