Noodprocedures en de noodzaak van testen.

Lezing tijdens het NGN Congres - 1998

Ernst J. Oud
Getronics Business Continuity BV

Email: e.j.oud@getronics.nl

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.

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!**

Denk in dit verband eens aan de luchtvaartmaatschappij PANAM waarvoor de ramp bij Lockerbie het einde betekende. Ook is bekend dat meer dan de helft van de bedrijven getroffen door een brand binnen drie maanden na de calamiteit niet meer bestaat.

Concreet cijfermateriaal laat zien dat de kans op een calamiteit die de bedrijfsvoering bedreigd niet zo klein is als we wellicht denken.

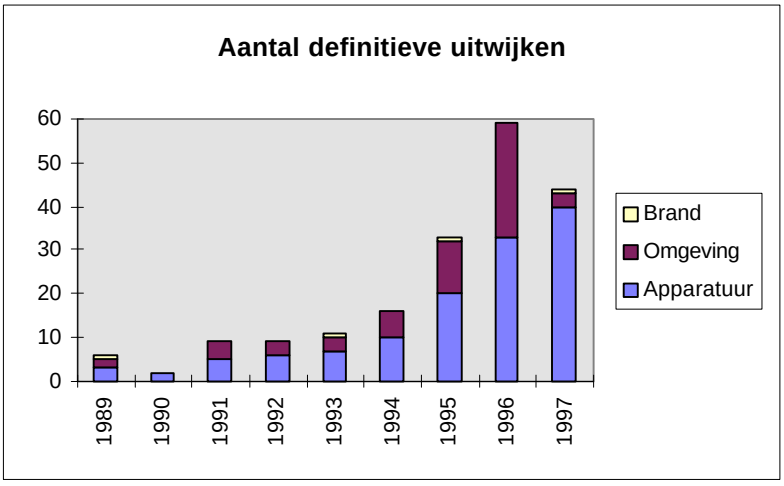


Figure 1 : Uitwijkmeldingen 1989-1997 bij CUC[1], Lelystad

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.

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

Maar wat dan wel te doen als je bedrijfsprocessen stilvallen?

Even terug naar de basis. Een organisatie die haar continuïteit wil zekerstellen doet er verstandig aan een integraal beleid m.b.t. informatiebeveiliging te voeren.

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

Continuïteitsplanning in de zin van planning tegen een eventuele calamiteit is namelijk nimmer een op zichzelf staand aandachtspunt.

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 met 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 (Fenit) 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 een essentiële en fundamentele maatregel is.

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.

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:

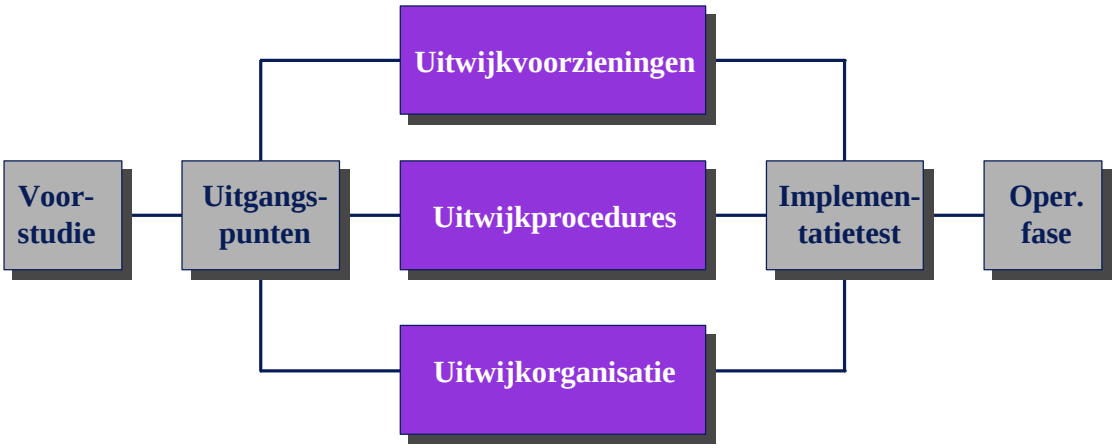


Figure 2 : Disaster Recovery Methodology™

Bij deze methode (te volgen van links naar rechts) wordt de 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 de juiste risico’s weggenomen of tot een acceptabel niveau beperkt kunnen worden voor deze kritieke bedrijfsprocessen.

Een risiso-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.

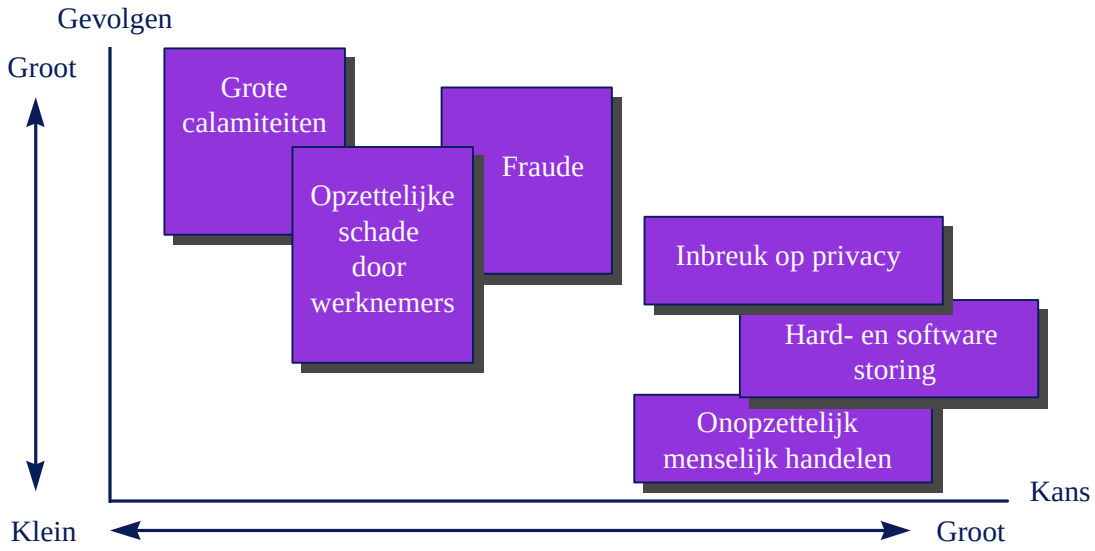


Figure 3 : Kwalitatieve risico-analyse

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			●	

Figure 4 : De resultaten van een kwalitatieve analyse

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

Welke methode, kwalitatief of kwantitatief 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 1 uur mogen stil liggen. De bepaling van de juiste uitgangspunten is 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 richt je de maatregelen, procedures en de organisatie in.

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 de machines e.d. die de organisatie wellicht gebruikt!

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 organisatie.

Een aantal van de ontwikkelen plannen:

- **Calamiteitenplan** → **Escalatieplan**
  → **Uitwijkdraaiboek**
- **Ontruimingsplan**
- **Aanvalsplan**
- **Veiligheidsplan**

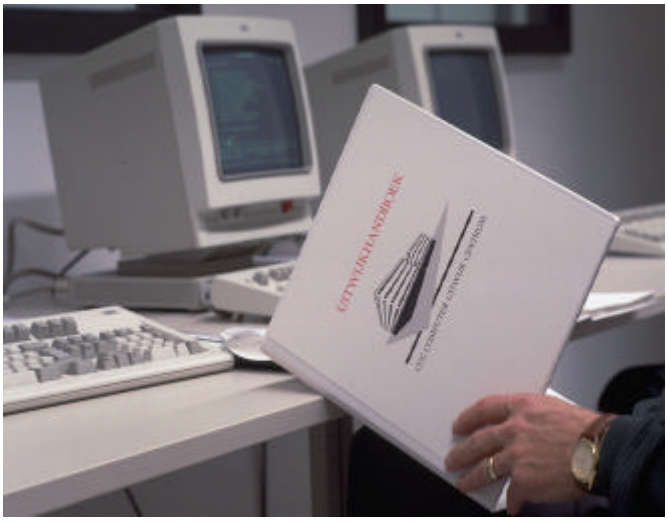


Figure 5 : Een uitwijkdraaiboek - de kern van een uitwijkplan

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:

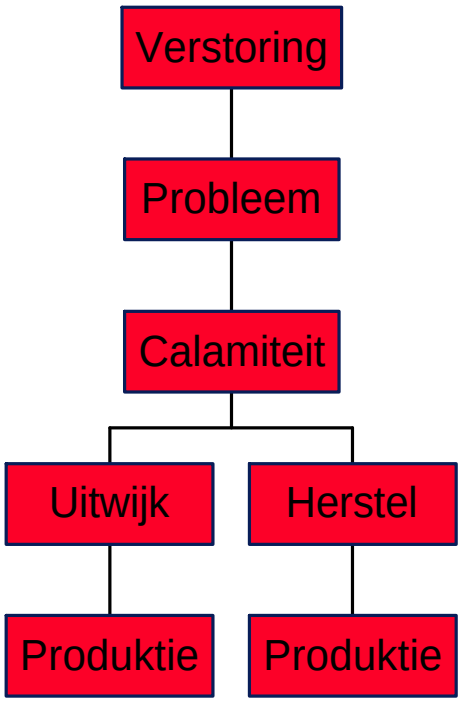


Figure 6 : Een voorbeeld escalatieprocedure

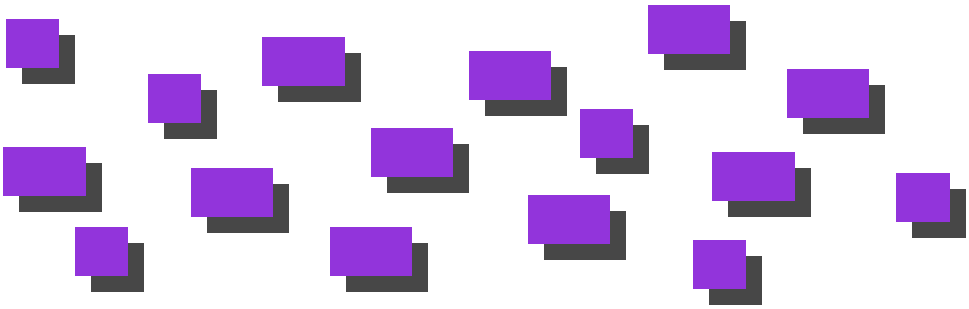
Het is bijzonder belangrijk om het traject van verstoring tot calamiteitenbesluit formeel vast te leggen. Het komt herhaaldelijk voor dat gesleuteld wordt aan een probleem wat een futiliteit leek maar na een bepaalde tijd betekent dat de bedrijfsprocessen gevaar lopen;
bedenk dat probleemoplossers vrijwel altijd denken het probleem snel opgelost te hebben.

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.

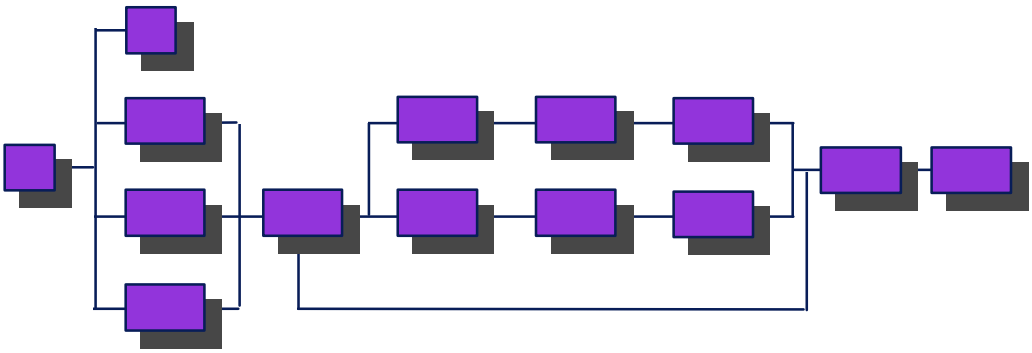
Uitwijkdraaiboek

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. Je krijgt dan een groot aantal activiteiten:



En die moet je dan rangschikken tot een netwerkschema:



Als elke stap beschreven is dan kun je ook alle doorlooptijden van de activiteiten afzonderlijk opnemen en weet je dus precies hoe lang dit proces in totaal gaat duren; kom je boven de maximale tijd uit (de MTU) dan moet je activiteiten parallel gaan laten lopen of anderszins versnellingen aanbrengen.

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:

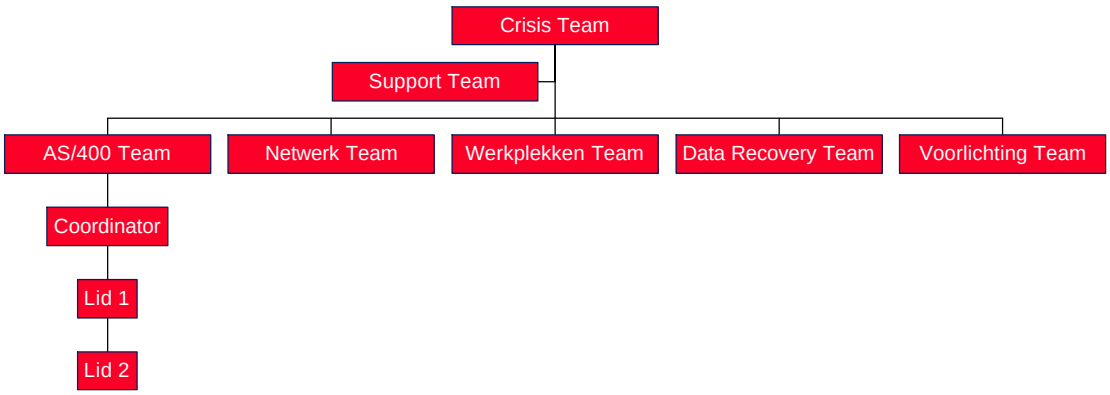


Figure 7 : Een voorbeeld calamiteitenorganisatie

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. Blijkt dit niet het geval dan moet het plan aangepast worden.

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 continuïteitsvoorziening vergt echter continue aandacht en dient minimaal jaarlijks getest te worden. Mogelijke testen zijn droogtesten (walkthroughs) en audits. Schrijf van te voren een testplan zodat vastgesteld zijn:

- **Doelstellingen**
- **Procedures**
- **Uitwijkvoorzieningen**
- **Evaluatie**
- **Terugkoppeling aan management**

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.

In de operationele fase moet zeker gesteld worden (bijvoorbeeld door koppelingen met beheersmethodes zoals ITIL change management) dat een verandering in de organisatie of haar middelen verwerkt wordt in het continuïteitsplan. Een continuïteitsplan vergt continue aandacht; een verouderd plan is net zo slecht als geen plan.

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

Tot slot een aantal nuttige links op internet:

- **Wetgeving**

Arbo wet	**http://www.industriebond.fnv.nl/vgwm/arbowet.html**
Wet Bescherming Persoonsgegevens	**http://www.minjust.nl/c_actual/persber/pb247.htm**
Wet Computercriminaliteit II	**http://www.minjust.nl/c_actual/persber/pb230.htm**

- **Calamiteitenplanning**

Contingency Planning Magazine	**http://www.contingencyplanning.com/index.cfm**
Disaster Recovery Journal	**http://www.drj.com**
Getronics Business Continuity	**http://www.getronics.nl/cuc**
Nationaal Centrum voor Preventie	**http://www.ncpreventie.nl/**
Software voor calamiteitenplannen	**http://www.rothstein.com/data1197/tng050.htm**
Survive!	**http://www.survive.com/**

- **Informatiebeveiliging**

Risico Analyse Tools	**http://www-08.nist.gov/training/risktool.txt**
IB bij de overheid	**http://www.minbiza.nl/acib/**
Nederlands Normalisatie Instituut	**http://www.nni.nl/**
