

## WHITEPAPER CONTINUÛTEITSPLANNING

---

# Wat als...?

*Continuïteitsplanning in het geval van een calamiteit kan kosteneffectief zijn als je uitgaat van bedrijfsprocessen*

Wat als... de IT ruimte onderstroomt met water of er is rookschade aan de servers door brand? De oplossing die het meest gekozen wordt voor continuïteitsplanning is een uitwijkvoorziening. Vaak blijkt deze zwaar te drukken op het exploitatiebudget van de IT-afdeling. De vraag is of dit geld niet beter besteed kan worden en of deze oplossing wel écht voldoet als het nodig is. De druk vanuit de markt is echter groot; zeer veel leveranciers van uitwijkdiensten verdienen een dikke boterham met de algemene trend tot calamiteitenplanning. Er is echter een slimmere manier om de continuïteit van een bedrijf te waarborgen bij calamiteiten. En tegen lagere kosten! Dat is de Innervate methode!



# a

De noodzaak van een goede continuïteitsplanning is evident: bij het optreden van een grotere calamiteit kan uw bedrijf jarenlang hinder en/of verlies van kostbare gegevens ondervinden. Het is nog maar de vraag of uw organisatie voldoende herstelt en uiteindelijk failliet gaat of niet. Het rekening houden met calamiteiten, oftewel continuïteitsplanning, wordt daarom door steeds meer bedrijven serieus genomen. Gedreven door een grotere bewustwording van risico's en de maatschappelijke trend om bewust en actief met potentiële dreigingen om te gaan motiveert directies en management om plannen te maken voor het continueren van de bedrijfsvoering, ook onder niet normale omstandigheden. Vaak ligt het initiatief daartoe bij brancheverenigingen of Overheid (zoals het Bank en Verzekeringswezen) maar even vaak ook bestaan er interne drijfveren. Een speciale rol is daarbij weggelegd voor de IT-afdelingen. Het continueren van IT-functies en -services bij calamiteiten vergt niet alleen een nauwkeurige analyse van de gehele IT-infrastructuur, maar meer nog van de relaties tussen IT en bedrijfsprocessen.

#### *Wat is een calamiteit?*

Over het begrip calamiteit bestaat veel verwarring. Vaak worden incidenten gelijkgesteld aan calamiteiten. Het belangrijkste verschil zit hem echter in de impact op de continuïteit van de bedrijfsvoering. Een calamiteit heeft een grote impact, dit in tegenstelling tot een incident. Een incident is vervelend en kost veel tijd en geld, maar de gevolgen zijn te overzien. De uitkomst is helder: dit kunnen we aan!

Bij calamiteiten is die uitkomst niet zeker. Als de vraag gesteld wordt: "overleven we dit wel als bedrijf?" dan kan er van een calamiteit gesproken worden. Voorbeelden van

incidenten zijn het uitvallen van een mailserver, het wegvallen van een belangrijke verbinding, het crashen van een harde schijf in een ERP-server. Voorbeelden van calamiteiten zijn een brand met rookschade naar alle servers, het onder water lopen van een IT ruimte.....Een Business Continuity Plan (BCP) heeft dit soort calamiteiten als onderwerp.

#### *Wat is een BCP?*

Een eenduidige betekenis van het begrip Business Continuity Plan bestaat niet. Veel bedrijven c.q. instellingen geven een eigen uitleg aan wat een BCP zou moeten bevatten en zelfs wat de doelstelling daarvan zou moeten zijn. In globale termen wordt met het opstellen van een BCP gepoogd op een gestructureerde wijze een plan te schetsen hoe de bedrijfsvoering kan worden gecontinueerd na het plaatsvinden van een calamiteit. M.a.w. in een BCP worden antwoorden gegeven op vragen als 'wat kan er mis gaan', 'welke schade kunnen we oplopen', 'wat kunnen we er tegen doen' en 'hoe moeten we dat doen?'. De scope kan daarbij variëren van alle bedrijfsmiddelen tot slechts een deel daarvan, bijvoorbeeld de IT-infrastructuur.

#### *BCP in meer delen*

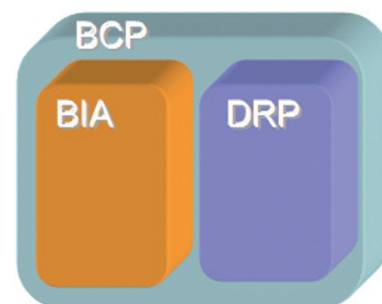
Een BCP bestaat grofweg uit twee onderdelen, de zogenaamde BIA en het DRP. In de Business Impact Analyse wordt bepaald wat de impact van een calamiteit op de bedrijfsprocessen is. Het deel waarin de recovery-scenario's beschreven worden heet Disaster Recovery Planning. M.a.w. in de BIA staat **wat** de schade is en in de DRP **hoe** die hersteld kan worden.

Het document waarin zowel BIA als DRP zijn samengevoegd tot één geheel, met daarbij zowel organisatorische als procesmatige maatregelen om calamiteiten aan te pakken wordt BCP genoemd.

*Verskillende aanpakken voor BIA*  
Omdat binnen de BIA zowel omvang als richting van het BCP bepaald wordt, is deze het meest cruciaal. In de praktijk worden verschillende benaderingswijzen gehanteerd voor het uitvoeren van een BIA:

1. Componentenmethode: hierbij ligt de focus op uitval van IT componenten zoals servers en netwerken.
2. Procesbenadering: hierbij wordt uitval van kritische bedrijfsprocessen als uitgangspunt genomen. Daarbij zijn twee invalshoeken mogelijk:
  - a. Worst-case methode: hierbij wordt uitgegaan van een grote calamiteit van *onbekende* aard, die grote schade aanricht.
  - b. Analytische methode: daarbij wordt met een grotere of kleinere granulariteit een analyse uitgevoerd op de impact die *specifieke* calamiteiten hebben op bedrijfsprocessen.

Het belangrijkste uitgangspunt voor een BIA dient te zijn dat er gestart wordt vanuit de bedrijfsprocessen, m.a.w. schade wordt gedefinieerd als schade aan *processen* en niet aan middelen of resources. Immers de kern van de bedrijfsvoering is het bedrijfsproces en niet de middelen.



Het nadeel van de componentenmethode is, dat de focus ligt op IT-middelen, waarvan *verondersteld* wordt dat deze essentieel zijn voor de bedrijfsvoering. De praktijk leert

dat dit alleen met enige zekerheid kan worden bepaald als de relaties tussen IT-middelen en bedrijfsprocessen in kaart worden gebracht. Indien dit niet gebeurt bestaat de kans dat er verkeerde veronderstellingen worden gedaan die leiden tot te dure, of erger, overbodige maatregelen. De beslissende factor hierbij is TIJD. Immers het maakt veel uit of een bepaald primair bedrijfsproces binnen enkele uren in gevaar komt bij wegvallen van resources of dat dat pas gebeurt

na enkele dagen of zelfs weken. Voorbeelden daarvan zijn belangrijk geachte enterprise-applicaties die bij uitval pas na dagen schade veroorzaken en eenvoudige resources, zoals bijvoorbeeld een faxlijn, die cruciaal blijkt en al na uren voor veel schade zorgt.

#### *Veelal Worst-case*

De meeste BIA methoden gaan uit van een worst-case scenario. Dat wil zeggen dat er op *voorhand* wordt uitgegaan van de noodzaak

van een uitwijklokatie voor de kritische bedrijfsprocessen. Dit betekent in de praktijk altijd kostbare maatregelen die een hoge belasting vormen voor voornamelijk IT-budgetten. Bovendien gaan deze methoden veelal voorbij aan preventie, d.w.z. het reduceren van impact op bedrijfsprocessen waardoor bij het daadwerkelijk optreden van een calamiteit wellicht geen uitwijk noodzakelijk is!

## De Innervate methode

De Innervate methode gaat uit van de procesbenadering, dat wil zeggen de bedrijfsprocessen (de business), zijn het uitgangspunt. Er wordt op een gestructureerde en beproefde wijze een analyse uitgevoerd op de relatie tussen bedrijfsprocessen en IT-middelen en de impact die calamiteiten daarop kunnen hebben.

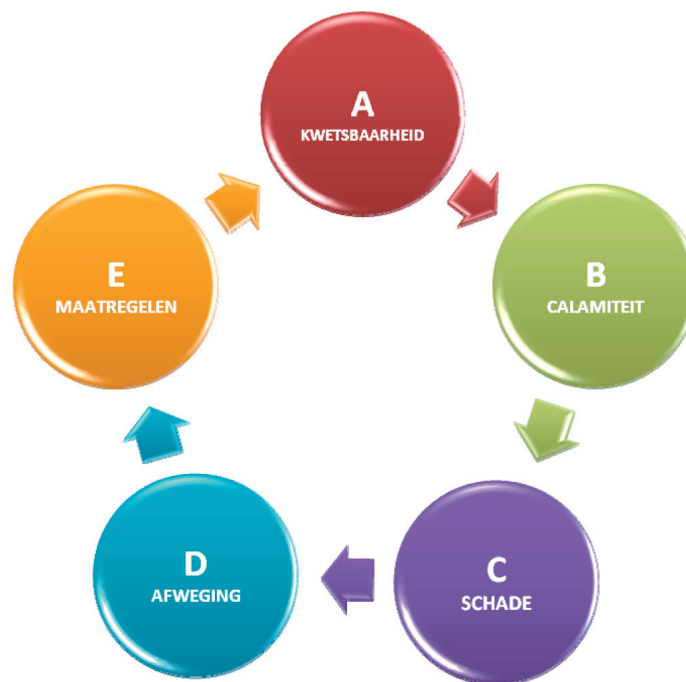
Dit heeft een aantal voordelen:

- het uitgangspunt is de steeds veranderende business;
- er worden gepaste maatregelen genomen voor die processen waarvoor het daadwerkelijk nodig is;
- er wordt geen geld en tijd verspild aan maatregelen voor gebeurtenissen met een verwaarloosbare impact op bedrijfsprocessen;
- er wordt gedurende het proces een perfect en onderhoudbaar inzicht verkregen in de relaties tussen bedrijfs-processen en IT-middelen.

#### Stappenplan

De kern van de Innervate methode is het opstellen van een BIA, waarbij de bedrijfsprocessen centraal staan. De scope is daarbij primair uitval, veroorzaakt door uitval van

IT middelen. In het kort komt deze aanpak neer op een itererende cyclus van vijf stappen:



- **Stap A.** Bepaal de kwetsbaarheid van bedrijfsprocessen
- **Stap B.** Bepaal welke calamiteiten kunnen plaatsvinden en met welke kans
- **Stap C.** Bepaal welke schade iedere calamiteit kan uitoefenen op de continuïteit van bedrijfsprocessen
- **Stap D.** Bepaal of de procesuitval ten gevolge hiervan groter is dan de kritische grens
- **Stap E.** Bepaal aan de hand van kosten van maatregelen en kans van voorkomen van een calamiteit of ingrijpen wenselijk is.

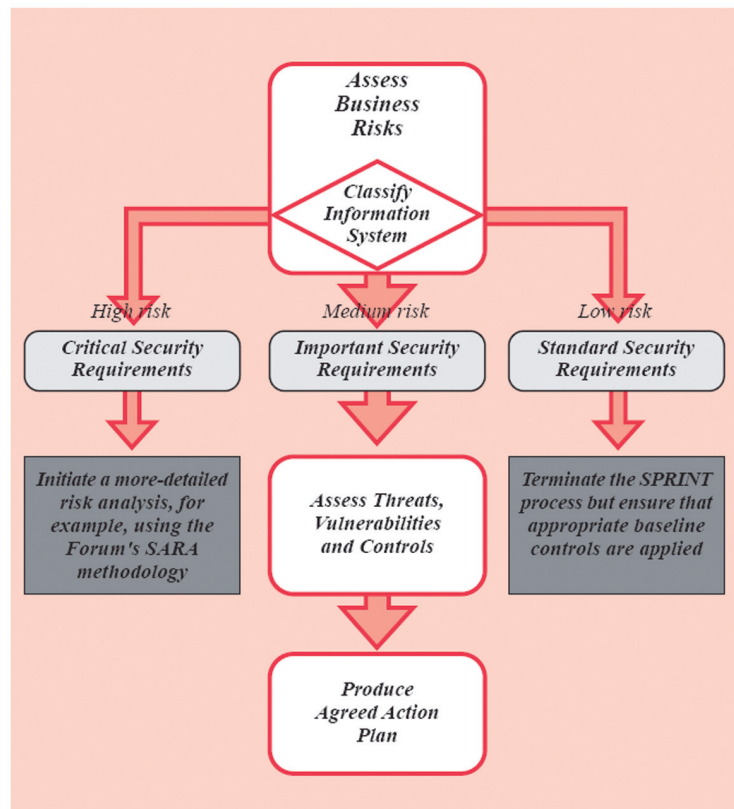
# STAP A: Bepaal de kwetsbaarheid van bedrijfsprocessen

Deze wordt bepaald aan de hand van het begrip SCHADE. Elke uitval van een proces veroorzaakt schade aan de bedrijfsvoering. Deze schade kan verschillende gedaanten hebben:

- Juridische schade: contractbreuk
- Sociale schade: o.a. technische werkloosheid van personeel
- Financiële schade: orderverliezen, daling van beurswaarde, renteverlies
- Reputatieschade.

De bepalende factor hierbij is de factor TIJD. Hoe langer een proces uitvalt, des te groter zal in het algemeen de schade zijn. De uitvaltijd waarbij onoverkomenlijke schade optreedt, d.w.z. schade waarvan een bedrijf zich niet meer kan herstellen, bepaalt de kwetsbaarheid van een bedrijfsproces. Deze tijd wordt Toegestane Uitval Tijd genoemd, oftewel T.U.T.

Het bepalen van deze TUT wordt gedaan middels een gestructureerde methodiek op basis van SPRINT. SPRINT is ontwikkeld



door het European Security Forum en staat voor Simplified Proces for Risk Identification. Deze methodiek biedt inzicht in de risico's die ontstaan bij uitval van een bedrijfsproces middels een specifieke onder-

vraging van managers. Hiertoe is door Innervate een webtool ontwikkeld die het mogelijk maakt deze methodiek snel en efficiënt toe te passen, zonder veel tijdverlies voor managers en verantwoordelijken.

# STAP B: Welke calamiteiten kunnen plaatsvinden en met welke kans?

Om actief te kunnen anticiperen op calamiteiten is het noodzakelijk voorspellingen te doen over de mate en wijze waarop calamiteiten zich kunnen voltrekken. Hiervoor wordt gebruik gemaakt van informatie die lage en hogere overheden bijhouden over calamiteiten en de kans daarop. Deze informatie is sterk plaatsgebonden. Het heeft bijvoorbeeld weinig zin om een analyse te doen van de impact van een overstrooming van een rivier als het bedrijf in kwestie zich 100 km van de dichtstbijzijnde rivier bevindt.

Als datzelfde bedrijf echter langs een druk bereden spoorverbinding ligt, waarover transporten naar een raffinaderij plaatsvinden dan heeft het zin te kijken naar de impact van een ontsporing van een wagon met brandbare Nafta.

Door een inventarisatie te doen van de specifieke ligging van vestigingen van een bedrijf en de calamiteiten die zich op die lokatie kunnen voordoen kan een lijst worden samengesteld met aannemelijke calamiteiten en de kans daarop.

Daarbij wordt gebruik gemaakt van o.a.:

- Ministerie van VROM: 'Leidraad Risico Inventarisatie – Overige Ramptypen' december 2006
- Ministerie BZK: Leidraad maat-ramp
- Verfijning naar klantspecifieke situatie:
  - Risicokaart Provincie
  - Rampencoördinatie Gemeente.

Deze calamiteitenlijst kan gebruikt worden als input voor de volgende fase.

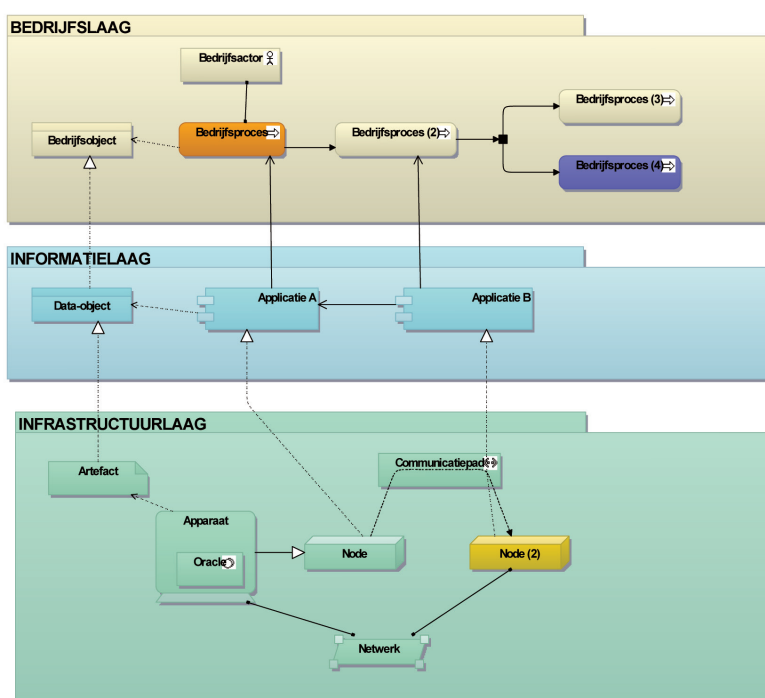
## Stap C. Bepaal welke schade iedere calamiteit kan veroorzaken

In verreweg de meeste gevallen heeft een calamiteit een impact op gebouwgebonden voorzieningen. D.w.z. dat schade wordt toegebracht aan *fysieke* resources. Binnen de context van deze whitepaper betekent dit schade aan IT-hardware/software- en verbindingen. Uitzonderingen hierop zijn bijvoorbeeld schade aan databestanden door criminele activiteiten zoals hacking en kwaadaardige malware.

Om de schade van een calamiteit op de gehele IT-omgeving te kunnen bepalen dient er een analyse te worden gemaakt van de keten IT hardware - software - bedrijfsprocessen.

Door te bepalen welke IT hardware schade ondervindt van een calamiteit kan via deze keten bepaald worden welke bedrijfsprocessen getroffen worden.

Indien bijvoorbeeld een calamiteit één zijde van een gebouw treft waar een VPN-verbinding binnenkomt die gebruikt wordt om orders door te sturen aan toeleveranciers,



dan is die zijde van het gebouw belangrijk voor het proces "Orderverwerking". Op deze wijze kan een betrouwbare link worden gelegd tussen calamiteiten en de invloed op processen.

Voor het bepalen van de keten IT hardware - software - bedrijfspro-

cessen wordt gebruik gemaakt van moderne tooling die op grafische wijze alle relevante relaties legt in een algemeen geaccepteerde universele taal. Analyses op deze ketens worden daardoor voor een groot deel geautomatiseerd.

## Stap D. Bepaal of de procesuitval ten gevolge van calamiteiten groter is dan de kritische grens

Nadat in de vorige fase de relatie bepaald is tussen calamiteiten en de invloed hiervan op bedrijfsprocessen, dient vervolgens bepaald te worden hoe *groot* deze invloed is. Dit gebeurt door de in Stap A bepaalde "Toegestane Uitval Tijd" van een proces te vergelijken met de tijd die nodig is om de schade als gevolg van de desbetreffende calamiteit te herstellen. Indien deze hersteltijd groter geschat wordt dan de TUT voor dat proces, dan betekent dit dat deze calamiteit een be-

dreiging vormt voor de bedrijfsvoering en dat maatregelen gewenst zijn.

Als voorbeeld kan de eerder genoemde VPN verbinding weer genomen worden. Indien het proces "Orderverwerking" maximaal acht uur mag uitvallen voordat de bedrijfsvoering in gevaar komt, dan dient de verbinding binnen deze acht uur weer hersteld te kunnen worden. Als dat niet mogelijk is, doordat bijvoorbeeld de provider

niet in staat is een glasvezelbreuk binnen deze tijd te herstellen, dan dient gezocht te worden naar alternatieven om deze hersteltijd wel te halen.

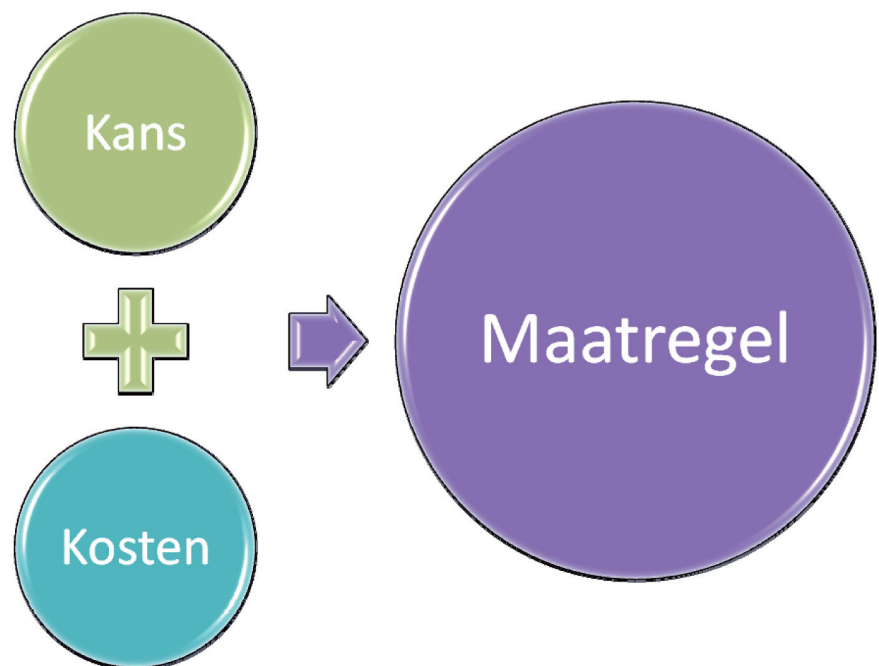
Indien echter anderzijds de hersteltijd van de verbinding wel binnen deze acht uur ligt, dan is hiermee duidelijk dat additionele maatregelen kunnen worden vermeden en dus Tijd en Geld kunnen worden bespaard.

## Stap E. Bepaal aan de hand van kosten van maatregelen en kans van voorkomen van een calamiteit of ingrijpen wenselijk is

In de vorige fase is bepaald welke combinaties van Calamiteiten en Processen in aanmerking komen voor maatregelen. In deze fase wordt bepaald of maatregelen daadwerkelijk worden uitgevoerd. Dit wordt gedaan aan de hand van een afweging tussen de kans van voorkomen van een calamiteit en de kosten van maatregelen die daar tegenover staan. Dit kan het beste worden toegelicht aan de hand van een voorbeeld:

Stel de hoofdvesting van een bedrijf ligt op een drukke vliegroute, met dagelijks tientallen vliegbewegingen. Dan is het neerstorten van een passagiersjet op of in de buurt van het hoofdgebouw, een calamiteit die in ogenschouw kan worden genomen. Stel verder dat de kans hierop door overheidsinstanties geschat wordt op éénmaal per tweehonderd jaar.

De directie kan dan op basis van deze kans, namelijk 0,5% per jaar, afgezet tegen de kosten van maatregelen, besluiten géén volledige uitwijk voor huisvesting en IT te organiseren. Met andere woorden de directie heeft het besluit genomen dit risico te accepteren en niet te in-



vesteren in maatregelen voor deze calamiteit zolang de hoofdlocatie op deze plek gevestigd is.

*De Innervate BIA-methodiek; een verantwoorde afweging*

Aan de hand van de hierboven uitgewerkte stappen en voorbeelden is getracht duidelijk te maken dat deze methodiek een zeer solide en goede onderbouwde BIA mogelijk maakt dat een groot aantal voordelen heeft. Door gebruik te ma-

ken van algemeen geaccepteerde methodieken, zoals SPRINT en Archimate zijn de resultaten toetsbaar en reproduceerbaar. Dit laatste is zeer belangrijk omdat een BCP geen éénmalig dood document is, maar op regelmatige basis dient te worden getoetst aan veranderende omstandigheden. Een toetsing-frequentie van eenmaal per één à twee jaar is zeker wenselijk.

# Waarom Innervate?

Vraagstukken op het vlak van continuïteitsplanning vragen een multidisciplinaire aanpak. De multidisciplinaire aanpak is een core competentie van Innervate.

Onze consultants zijn ervaren professionals die al jaren hun sporen verdiend hebben in de ICT. Ze maken gebruik van bewezen methodieken en een pragmatische aanpak, dat gepaard gaat met de kennis van en ervaring in hun vakgebied. Deze bundeling van kennis, expertise en het leveren van optimale oplossingen levert een hoog rendement van projecten op. Innervate is **SUCCESVOL ONAFHANKELIJK MULTIDISCIPLINAIR**

## De Innervate BCP toets

Daag onze consultants uit om uw Business Continuïty Planning vraagstuk te komen oplossen! Vraag aan één van onze professionals om de Innervate toets en de klantreferenties!

Kortom: bent u klaar voor continuïteitsplanning in uw organisatie?

- Geschikt
- Ongeschikt

## Nawoord

Deze whitepaper is opgesteld door Innervate, gebaseerd op haar project- en onderzoekservaring op het gebied van Informatie Management & Enterprise Architecture.

Copyright 2010 Innervate.  
[www.innervate.nl](http://www.innervate.nl)