# BCM PocketBook

*Louise Knegtel*

BCM ACADEMY
Business Continuity & Crisis Management Institute

ISBN-10: 90-810553-1-3
ISBN-13: 978-90-810553-1-4



*Vormgeving:* MGO-studio, Maarssen
*Illustraties:* Monique Giling
*Drukwerk:* Drukkerij Damen, Werkendam

# Inhoudsopgave



*Voorwoord* 7

*1. Inleiding tot BCM* 9
Risico's 10
De scope van BCM 13
BCM in een exponentieel veranderende omgeving 15

*2. Het BCM Proces* 23
BCM als holistisch proces 25
BCM als iteratief proces 27
De niveaus binnen het proces 28
Beleid 31
Risico Inventarisatie 35
Business Impact Analyse 41
Business Case & Benefit Logic 45
Stelsel van Maatregelen 47
Testen & onderhoud 57

*3. BCM in de praktijk* 61
De Koninklijke weg 63
Een pragmatische aanpak 65
Inrichtingsniveaus 69
Business as Unusual 71
PAS 56 75
Relatie met andere vakgebieden 77
Kritische succesfactoren 81
Tot slot 83

*4. Modellen en sjablonen* 85

*5. Begrippenlijst* 101

*6. Referenties, Literatuurlijst* 105

*Over de auteur* 107

*When planning for business continuity, remember Noah started building the ark before it began to rain.*

# Voorwoord

Risico's die de continuïteit van een organisatie bedreigen zijn divers van aard en nemen exponentieel in omvang toe. Traditionele rampen, zoals natuurrampen, brand en diefstal hebben naar waarschijnlijkheid van optreden plaatsgemaakt voor andere dimensies van bedreiging. In de 21e eeuw zijn het criminaliteit, fysiek en cyber terrorisme, bestuurlijke crises, sabotage, diefstal of verlies van informatie en lekken binnen organisaties die in de media breed worden uitgemeten. Ongeacht de aard en oorzaak van de verstoring of crisis, de gevolgen hebben grote impact en kunnen voor de organisatie desastreus van aard zijn. Het belang van Business Continuity Management is dan ook evident.

Dit 'BCM PocketBook' is een pragmatische gids voor Business Continuity Management: het geheel aan activiteiten dat erop is gericht de continuïteit van een organisatie te waarborgen. Het is een samenvatting van theoretische achtergronden, praktijkervaringen en best practices. Het 'BCM PocketBook' stelt u in staat van BCM een werkzaam proces te maken, waarbij de praktische toepassing leidend is. De theorie rondom BCM biedt aanvullend inzicht om optimale invulling voor de eigen organisatie mogelijk te maken.

Voor een ieder die het belang van continuïteit binnen een organisatie onderkent, biedt het 'BCM PocketBook' inzicht in een ogenschijnlijk complexe materie. Het is een inleiding op het vakgebied en het maakt het mogelijk prioriteiten te stellen en met de uitvoering van BCM op een praktische wijze aan te vangen.

In hoofdstuk 1 wordt de context van BCM in kaart gebracht. Het theoretisch kader en het ideaalproces worden beschreven in hoofdstuk 2. In hoofdstuk 3 wordt vervolgens geschetst hoe het proces in de praktijk wordt toegepast en aan welke randvoorwaarden in de organisatie dient te worden voldaan.

*"Next week there can't be a crisis.*

*My schedule is already full."*

*Henry Kissinger while Secretary of State*

# 1. Inleiding tot BCM



Bij een crisis verandert de wereld in chaos. De vertrouwde omgeving die we denken te kennen, verandert direct in een vreemde en mogelijk vijandige wereld. Het is 'ieder voor zich'. Het model van hoe de dagelijkse praktijk werkt, de business as usual, functioneert niet meer. Routines, gewoontes en procedures zijn er eenvoudig niet meer. Als daardoor communicatielijnen veranderen maakt hiërarchie uit bittere noodzaak plaats voor kennis en inzicht en is samenwerking essentieel.

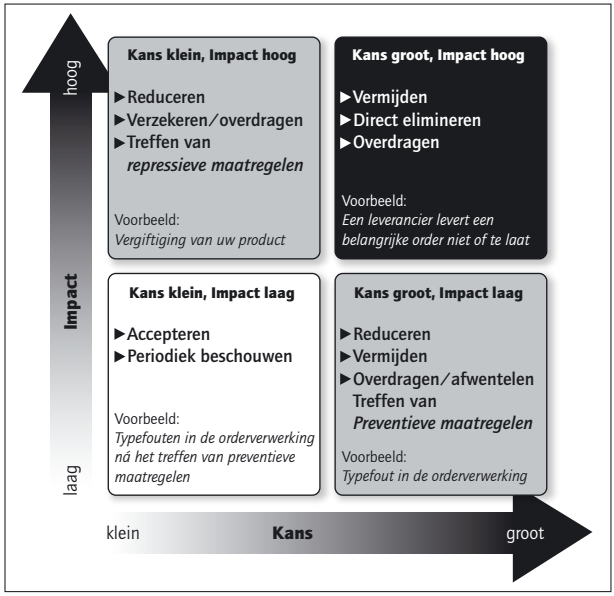
Business Continuity Management (BCM) heeft tot doel de continuïteit van het bedrijfsproces en het voortbestaan van de organisatie te waarborgen. Het biedt een Stelsel van Maatregelen om de kritische bedrijfsprocessen van een organisatie onder crisisomstandigheden voort te zetten en het kapitaal van die organisatie, waaronder de reputatie, te beschermen.

Het product van Business Continuity Management bestaat uit werkbare en toepasbare maatregelen, welke zowel preventief als repressief werkzaam zijn. In preventieve zin hebben maatregelen tot doel te voorkómen dat zich situaties voordoen die de continuïteit van de organisatie kunnen aantasten. En indien een risico manifest is geworden, zorgen repressieve maatregelen ervoor dat de gevolgschade beperkt blijft tot een acceptabel niveau.

## Risico's

Iedere organisatie is gericht op continuïteit; ondernemen is synoniem aan risico's nemen. Met het nemen van risico's, zoals het ontwikkelen van nieuwe producten of het betreden van nieuwe markten, onderscheidt men zich immers van de concurrentie. Het spanningsveld tussen deze twee uitersten (continuïteit versus risico's) wordt door 'risicomanagement' beheerst. Wanneer risicomanagement niet expliciet in de organisatie is benoemd, zal dit proces zich impliciet, tijdens het besluitvormingsproces, voltrekken.

De typen van risico's die zich binnen een organisatie kunnen manifesteren, zijn in te delen naar de factoren 'kans van optreden' en 'mate van impact':




*Risicomatrix*

***Kans klein, Impact laag***

Risico's die een lage kans van optreden kennen en weinig impact tot gevolg hebben, leiden niet direct tot het treffen van maatregelen.

***Kans groot, Impact hoog***

Risico's met een grote kans van optreden en relatief veel schade tot gevolg, worden direct als vanzelfsprekend geëlimineerd. Dit kan worden gerealiseerd door het terugbrengen van de factoren kans of impact of het overdragen van het risico. Wanneer zich onverhoopt toch risico's van deze aard voordoen, spreekt men in managementjargon van het 'blussen van brandjes'.

***Kans groot, Impact laag***

Voor de risico's die zich vaker voordoen, maar een beperkte gevolgschade hebben, treft men preventieve maatregelen. Dit zijn de risico's waar organisaties vaker mee worden geconfronteerd en welke tot risicobewustzijn leiden.

***Kans klein, Impact hoog***

Dit is niet het geval voor de laatste categorie risico's die een kleine kans van optreden kennen, de calamiteitenrisico's. Hoewel deze bij het manifest worden tot grote gevolgschade leiden, zijn het vaak deze risico's waarvan men zich niet bewust is.

*"If we want things to stay as they are,*
*things will have to change."*

*Giuseppe di Lampedusa (1896-1957)*

## De scope van BCM

BCM gaat de gehele organisatie aan. De prestatie van een organisatie wordt immers gevormd door de som van alle bedrijfsprocessen. Het geheel aan activiteiten van het BCM proces gaat dan ook over alle bedrijfsprocessen heen en de activiteiten die op het garanderen van continuïteit zijn gericht, vinden organisatiebreed plaats. Wellicht zijn er binnen de organisatie al versnipperd een groot aantal activiteiten op het gebied van BCM aanwezig. De waarde hiervan is echter relatief. Zolang activiteiten gefragmenteerd plaatsvinden en niet zijn geïntegreerd, door gebrek aan coördinatie, afstemming en business alignment, wordt er aan het primaire en beoogde doel van die activiteiten voorbijgegaan en gaat het beoogde effect daarvan volledig teniet.

BCM is voor iédere organisatie essentieel. Er is geen organisatie zonder achilleshiel en dus is iedere organisatie kwetsbaar voor bedreigingen. Als die achilleshiel van een organisatie wordt geraakt, is er altijd sprake van een crisis. Een crisis kan echter ook een minder uitgesproken verschijningsvorm kennen. Als ergens 'rook' wordt geconstateerd, kunnen de media daar 'vuur' van maken; zelfs als de rook al is opgetrokken.

Als de achilleshiel wordt geraakt, maakt de beheersbare, veilige en voorspelbare wereld plaats voor machteloosheid en angst. Deze belevenis gaat de verwerkingscapaciteit van (het management in) de business as usual te boven. Maar de scope van BCM gaat verder dan het overleven van een calamiteit. De inspanning die wordt geleverd om in detail naar de organisatie te kijken, levert voordelen op uit onverwachte hoek. Zo bieden preventieve maatregelen die de organisatie treft na het uitvoeren van een risico inventarisatie, veelal maximaal rendement met een minimum aan investering. Het zijn kleine aanpassingen met een verbluffend rendement.

Bovendien kan BCM een bijdrage leveren aan verbeteringen in kritische bedrijfsactiviteiten en -processen door het inzichtelijk maken van knelpunten daarbinnen. Wanneer moet worden beschouwd hoe een activiteit na een calamiteit doorgang kan vinden, kan blijken dat de dagelijkse uitvoering van die activiteit zo onlogisch is, dat dit ondoenbaar is. 'Process improvement' is dan een randvoorwaardelijke en kritische succesfactor om de continuïteit binnen dat proces mogelijk te maken.

*"He that will not apply new remedies must expect new evils."*

*Bacon (1561-1626)*

## BCM in een exponentieel veranderende omgeving

Veranderingen zijn uitdagingen en brengen mogelijkheden met zich mee. Een nieuw product, een nieuwe markt. Nieuwe bedrijfsprocessen, nieuwe activa. Nieuwe kansen, nieuwe mogelijkheden, een nieuwe aanpak. Veranderingen brengen onvermijdelijk risico's met zich mee. Elke stap kan de organisatie verder brengen, maar ook ten val. Maar ook niet veranderen leidt tot een verhoogd risico! Doordat de wereld om de organisatie heen beweegt, kan zij zelf, hoewel in stilstand, onder de voet gelopen worden. Stilstand is achteruitgang en kan leiden tot het einde van de onderneming. Voet zetten op nieuwe bodem kan leiden tot nieuwe risico's.

In onze exponentieel veranderende wereld, zal continu de vinger aan de pols moeten worden gehouden om levensvatbaarheid en continuïteit te kunnen waarborgen. In dit hoofdstuk schetsen we enkele actuele en relevante maatschappelijke bewegingen die direct of indirect invloed hebben op de heersende risicoperceptie en het risicoprofiel binnen de organisatie.

***Belevingseconomie***

De huidige consument of klant wil méér dan alleen een product. Deze is bijna schizofreen, eist uitersten en is steeds op zoek naar optimalisatie van genot, gemak en gewin. De organisatie is het podium voor het invullen van deze belevingen. Of daar nu wel of niet bewust invulling aan wordt gegeven, het oordeel van de consument of klant is essentieel. 'Verlies van reputatie' wordt door organisaties dan ook als één van de grootste risico's beschouwd. Reputatie komt te voet en gaat te paard.

***Collaborative merchandising en marketing***

Philips en Douwe Egberts creëerden gezamenlijk de Senseo. Het bleek een 'geslaagd huwelijk'.

In lijn met de vraag naar 'beleving' zoeken organisaties naar samenwerkingsvormen die aan de gevraagde uniciteit kunnen voldoen. Dergelijke verbanden bieden kansen, maar tegelijk enorme risico's. Binnen samenwerking kan eigenbelang tot misbruik leiden. Opportunistisch gedrag kan zich manifesteren in de vorm van misbruik en/of diefstal van kennis. Bij het (in meer of mindere mate) verbinden van het lot aan een derde

partij, loopt de organisatie bovendien het risico de dupe te worden van eventuele reputatieschade aan de ander.

***Ketenintegratie en ketenomkering***

Voortdurend trachten organisaties schakels uit de keten in de bedrijfsvoering te integeren om kostenreductie of omzetverhoging te realiseren. Binnen de keten worden informatiesystemen in toenemende mate aan elkaar gekoppeld en er worden overeenkomsten gesloten waarmee de organisatie meer bevoegdheden krijgt om een leverancier of afnemer rechtstreeks aan te sturen.

Ketenomkering is de verandering van een aanbodgericht naar een vraaggericht model. Anders gezegd worden markten steeds meer gedreven door de vraag en minder door het aanbod. Deze ontwikkeling komt tegemoet aan de behoefte van klanten om op de juiste plaats, in de juiste hoeveelheid en voor de juiste prijs, het juiste product, met de juiste beleving aangeboden te krijgen.

Doordat het aanbod toeneemt en door sterk verbeterde informatievoorziening, hebben klanten steeds beter inzicht en overzicht. Vooral internet en het toegenomen belang van andere media hebben aan deze verbeterde informatievoorziening bijgedragen. Als voorbeeld hiervoor staat de Belastingdienst model. De Belastingdienst vult inmiddels het teruggaveformulier voor haar klanten in. Deze hoeft slechts afwijkingen hierop aan te geven.

***Nieuw 'e'-business modellen***

Was het al dodelijk een klant te verliezen aan een te lange telefonische wachttijd, het verwachtingspatroon van online klanten ligt vele malen hoger. Deze klant eist 24 uur per dag, 7 dagen per week online antwoord te krijgen op zijn vraag. De uitdaging is gelegen in het realiseren van een beschikbaarheidsgraad die aansluit op de behoefte van die klant. Vooruitlopend op de trends in het komende decennium, waarin 'screenagers' domineren, wordt het invullen van die behoefte essentieel. De bijhorende niveaus van beveiliging zullen tot nog grotere uitdagingen leiden.

***Globalisering***

Globalisering is de toename van het aantal verbindingen tussen samenlevingen in de wereld en de uitingen daarvan. Gebeurtenissen, beslissingen en activiteiten in één deel van de wereld hebben daardoor belangrijke gevolgen voor individuen en gemeenschappen in een ander deel van de wereld. Deze trend manifesteert zich op alle domeinen van het maatschappelijke en culturele leven: economie en financiën, technologie, cultuur, politiek, mentaliteit (Ricardo Petrella; auteur van het boek "Grenzen aan de concurrentie").

***Communicatie***

Nieuwe media hebben de informatievoorziening (mede via de pers) volledig ontsloten. Van een organisatie wordt inmiddels volledige transparantie geëist, zowel door leveranciers, afnemers, aandeelhouders, milieuorganisaties en overige stakeholders. De aard en wijze waarmee de organisatie informatie, gevraagd en ongevraagd, beschikbaar stelt en de wijze waarop berichtgeving wordt vormgegeven, is in toenemende mate van kritisch belang.

***Outsourcing & Offshoring***

Organisaties gaan over tot outsourcing om zich te kunnen concentreren op de kern van hun business. Offshoring van ondersteunende processen zoals ICT, vindt doorgaans plaats voor reductie van de kosten of verhoging van de efficiency. Wanneer die processen, zoals dat vaak het geval is bij ICT, een kritisch ondersteunende functie hebben voor het primaire proces, dient het continuïteitsaspect zorgvuldig te worden bezien. Dit wordt echter structureel genegeerd.

Het blijft niet bij het uitbesteden van ICT. Steeds vaker worden ook primaire processen, zoals het call center, uitbesteed. Op dat moment doen zich onmiddellijk nieuwe risico's voor. Op welke wijze is de informatiebeveiliging geregeld? Heeft de partner voorzien in een continuïteitsplan? Welke reputatieschade kan worden opgelopen als de derde negatief in het nieuws komt? De kwaliteit van het uitbestede proces blijft te allen tijde de eigen verantwoordelijkheid. Om dit te garanderen zijn sluitende en bindende overeenkomsten essentieel, ook met betrekking tot de vereiste service levels ten tijde van een calamiteit. Business Continuity Management vervult hierin een sleutelrol. BCM betreft immers de gehele organisatie en

gaat over alle bedrijfsprocessen heen, zij het uitbesteed of niet. Er dienen eisen te worden gesteld aan de wijze waarop de partner heeft voorzien in het eigen Business Continuity Management. Het moet mogelijk worden gemaakt om de eigen continuïteitsvoorzieningen te testen. Kortom, maak afspraken over de business as unusual (business as NOT usual) en volg deze afspraken expliciet op.

Elke vorm van het 'niet in eigen huis of eigen beheer' uitvoeren van primaire processen, vereist een andere afspraak en een andere benadering, door cultuurverschillen, tijdsverschillen, miscommunicatie, interpretatieverschillen en onbegrip. Voer lokaal een degelijke risicoanalyse uit op de omgeving, de infrastructuur, huisvesting, cultuur en management; gerelateerd aan de eisen die het proces aan de organisatie stelt.

In het komende decennium zullen nieuwe varianten van offshoring en outsourcing worden ontwikkeld. Nieuwe begrippen daarbij zijn nearshoring, inshoring en rightshoring.

***Wet- en Regelgeving***

Er is wet- en regelgeving rondom BCM, zij het beperkt. In Nederland biedt dat enerzijds meer vrijheid om BCM zo in te richten als gewenst, maar anderzijds leidt dat tot onzekerheden. BCM wordt indirect voorgeschreven. Het is dan lastig te (laten) bepalen wanneer maatregelen van voldoende kwaliteit zijn. Management en directies worden echter wel aansprakelijk gesteld bij het ontbreken of niet hanteren van continuïteitsplannen.

De Wet Bescherming Persoonsgegevens, actuele Corporate Governance codes, regelgeving door de DNB, maar ook Best Practices in ICT (zoals ITIL en de Code voor Informatiebeveiliging) leiden tot toenemende verplichtingen. Ook niet -beursgenoteerde ondernemingen, overheden en NGO's zullen in de toekomst aan dergelijke verplichtingen moeten voldoen.

***Wet Bescherming Persoonsgegevens (WBP), 2001***

Artikel 13 eist dat "de verantwoordelijke, passende technische en organisatorische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligings-

niveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen."

De WBP geeft geen expliciete richtlijnen voor BCM. Het beschermen tegen verlies zou al bereikt kunnen worden door ICT technische maatregelen als back up en recovery. De WBP betreft echter uitsluitend persoonsgegevens. Alle andere gegevens die belangrijk zijn voor de organisatie blijven buiten beschouwing.

***Sarbanes-Oxley (SOx) Act, 2004***

Amerikaanse wetgeving voor beursgenoteerde bedrijven legt regels op teneinde deugdelijk ondernemingsbestuur af te dwingen. Bijzonder aan de wetgeving is het feit dat voor een hoofddirectie gevangenisstraf en geldboetes dreigen wanneer zij niet aan deze voorwaarden van deugdelijk ondernemingsbestuur voldoen. In dit kader wordt in 2006 voor het eerst in Nederland, door het OM een gevangenisstraf geëist voor de voormalige bestuurders van Ahold.

In artikel 404 worden regels gesteld voor de interne controle en de financiële rapportage. Het management wordt verplicht om jaarlijks expliciet een uitspraak te doen over de betrouwbaarheid van de interne controles die in de onderneming gehanteerd worden. De CEO en CFO moeten een verklaring afleggen dat alle controles waterdicht zijn en de accountant moet naast zijn gebruikelijke taak op het gebied van de financiële verslaglegging, een expliciete verklaring toevoegen omtrent het akkoord zijn met de uitspraken van de CFO en de CEO.

***De Code Tabaksblat***

De Code Tabaksblat is een zogenaamd 'principle based system' (in tegenstelling tot het 'rule based system' van SOx). Deze aanbeveling is wettelijk geïmplementeerd door op grond van artikel 2:391, lid 4, BW via algemene maatregel van bestuur, de Nederlandse corporate governance code aan te wijzen als gedragscode, waaraan beursgenoteerde vennootschappen in hun jaarverslag moeten refereren en waarbij deze vennootschappen moeten aangeven in hoeverre zij de codevoorschriften naleven. Deze wettelijke bepaling geldt vanaf boekjaar 2004. Voordeel van een 'principle

based system' is dat principes een stuk moeilijker zijn te omzeilen dan regels. Nadeel is dat het systeem geen 'tanden' heeft. De code bevat enkele expliciete verwijzingen naar continuïteit: "Het bestuur en de raad van commissarissen hebben een integrale verantwoordelijkheid voor de afweging van deze belangen, doorgaans gericht op de continuïteit van de onderneming." (preambule)

***Toetsingskader Business Continuity Planning (BCP) van De Nederlandse Bank***

Vooruitlopend op de 'High-level principles for business continuity' dat in december 2005 door het Basel Committee is uitgegeven, stelde DNB eind 2004 het toetsingskader BCP op. Deze is tot stand gekomen in samenwerking en overleg met de instellingen van de financiële kerninfrastructuur. Het BCP-toetsingskader is een aanbeveling aan de financiële kerninfrastructuur van het betalings- en effectenverkeer in Nederland en biedt een aantal BCP-principes die richtsnoer zijn voor de deelnemers van de kerninfrastructuur van het betalings- en effectenverkeer, teneinde het niveau van business continuity planning (BCP) en crisismanagement (CMT) van de sector te verhogen. De normen bieden een kader dat ook buiten de financiële sector onverkort hanteerbaar is.

*De 10 normen voor BCM uit het toetsingskader van DNB:*

1. Iedere instelling moet een door de directie en seniormanagement goedgekeurd Business Continuity Plan hebben waarin de strategie, doeleinden en kritische bedrijfsprocessen zijn bepaald en waar inadequate continuïteitsmaatregelen staan beschreven. In alle gevallen dient uiteraard de veiligheid van mensen voorop te staan. Het plan dient minstens een keer per jaar te worden geactualiseerd.
2. Elke instelling dient een risicoanalyse te hebben gemaakt van mogelijke calamiteiten en de impact op essentiële systemen en processen.
3. In het business continuity plan dient zichtbaar te worden gemaakt op welke wijze rekening wordt gehouden met de menselijke factor. Zonder mensen is voortzetting van business activiteiten of ICT processen onmogelijk.
4. Iedere instelling dient over een crisisorganisatie te beschikken om in geval van nood handelend te kunnen optreden. Deze wordt aangestuurd door de directie en seniormanagement.
5. Elke instelling heeft een analyse gemaakt over de afhankelijkheid van basisvoorzieningen als elektriciteit, telecom en water. Instellingen zijn dikwijls afhankelijk van een veelheid van externe providers waardoor single points of failure kunnen bestaan.
6. De essentiële bedrijfsprocessen en systemen dienen bij een calamiteit zo vlug mogelijk te worden hervat.
7. Elke instelling dient te kunnen uitwijken naar een ander centrum dat, afhankelijk van het risicoprofiel, op voldoende afstand ligt van de hoofdsite.
8. Uitwijk van procedures en systemen moet regelmatig worden getest.
9. Iedere instelling dient een communicatieplan te hebben waarmee alle belanghebbenden zo adequaat mogelijk kunnen worden geïnformeerd.
10. Er dient voor de sector als geheel een business continuity plan te worden gemaakt. Dit is een gezamenlijke verantwoordelijkheid van de kerninfrastructuur waarbij DNB het voortouw heeft.

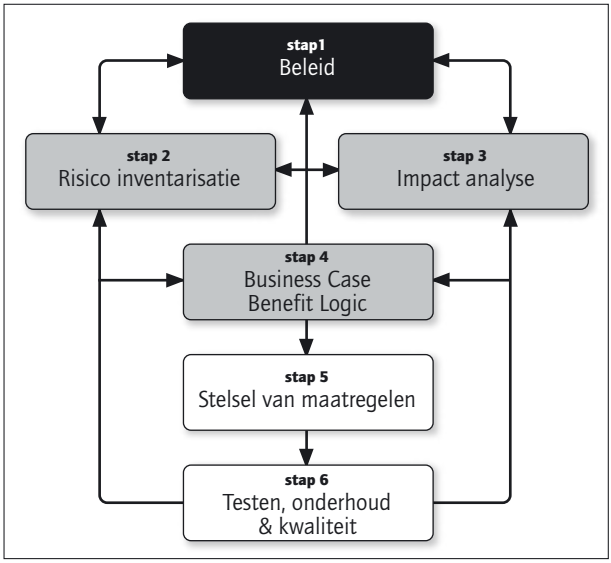
*Be not afraid of going slowly;*
*be only afraid of standing still.*

*Chinese Proverb*

# 2. Het BCM Proces

In dit hoofdstuk wordt een gestructureerde aanpak beschreven voor de implementatie en werking van BCM als proces binnen de organisatie. Deze aanpak voorziet in een theoretisch kader. Handreikingen voor de praktische invulling en beschrijving van de randvoorwaarden waaraan de organisatie moet voldoen, volgen in hoofdstuk 3.

Er is geen Nederlandse standaard beschikbaar voor de inrichting van BCM. Wel worden standaards geaccepteerd zoals PAS56 in Engeland en HB221 in Australië. Als ideaal-proces wordt hier onderstaand generiek model geïntroduceerd dat is gebaseerd op de Nederlandse best-practices en in lijn is met standaards zoals gehanteerd door the BCI en vastgelegd in PAS56:




*Overzicht van het BCM proces*

*Het BCM proces bestaat uit zes stappen en start met het BCM Beleid (stap 1). Hier wordt in eerste instantie globaal vastgesteld wie zich met het proces gaat bezighouden en op welke organisatieonderdelen het proces betrekking heeft.*

*Vervolgens wordt er een risico inventarisatie uitgevoerd. In de Business Impact Analyse wordt bepaald welke gevolgschade er optreedt als processen komen stil te liggen wanneer een calamiteitenrisico manifest wordt (Stap 2 & 3). Met de Business Case en Benefit Logic (Stap 4) worden de resultaten hiervan teruggekoppeld, waarna het beleid nader wordt vormgegeven. Nu kan immers worden besloten, welke maatregelen, voor welke risico's, tegen welke kosten en in welke context moeten worden geïmplementeerd. Hierna kunnen de maatregelen worden ingevoerd (stap 5), getest en worden onderhouden (stap 6). De resultaten van het testen en onderhouden zijn steeds weer input voor nieuwe analyses en beleidsvorming.*

Voordat wordt ingegaan op de details van de verschillende processtappen, wordt de aard van het proces nader beschreven. Door de specifieke eigenschappen daarvan wordt het BCM proces namelijk vaak als ingewikkeld beschouwd.

## BCM als holistisch proces

Business Continuity Management wordt vaak als een holistisch proces beschreven. Holistisch komt van het Griekse woord 'Holos', wat 'heel' betekent. 'Heel' heeft in dit geval betrekking op de organisatie. Het waarborgen van de continuïteit gaat immers de gehéle organisatie aan en gaat over álle bedrijfsprocessen heen. Bovendien kunnen activiteiten die op het garanderen van continuïteit zijn gericht op verschillende plaatsen in de organisatie plaatsvinden. Subprocessen als informatiebeveiliging, insurance management, security management, regelgeving, P&O of ICT uitwijk worden door de systematische, integrale en in onderlinge samenhang uitgevoerde aanpak van BCM geïntegreerd. Het is deze aanpak waar de waardeschepping van Business Continuity Management door wordt gecreëerd.

Doordat continuïteit als holistisch proces de hele organisatie aangaat, wordt BCM vaak onterecht als ingewikkelde materie beschouwd. Deze perceptie wordt nog eens versterkt doordat de invoering van BCM vraagt om een verandering in houding van de medewerkers die een rol spelen in het proces. Deze verandering gaat het gedrag, waarden en normen, risicohouding en risicoperceptie aan. Dit vraagt een fundamentele verandering. Door niet in eerste instantie een te hoog gespannen verwachtingspatroon te creëren wordt een realistisch groeipad gevolgd.

*"Fouten hebben en die niet verbeteren,*

*dat is pas fouten hebben."*

*Confucius (551 - 479 v.C.)*

## BCM als iteratief proces

Een realistisch groeipad betekent dat niet verwacht mag worden dat er direct een compleet ingevoerd BCM proces zal zijn. Het 'leren' denken vanuit een ander kader, vanuit een ondenkbare situatie ('business as unusual') kost tijd. De praktijk leert dat organisaties, gaandeweg de inrichting van het proces, leren om buiten de heersende referentiekaders van de business as usual te denken.

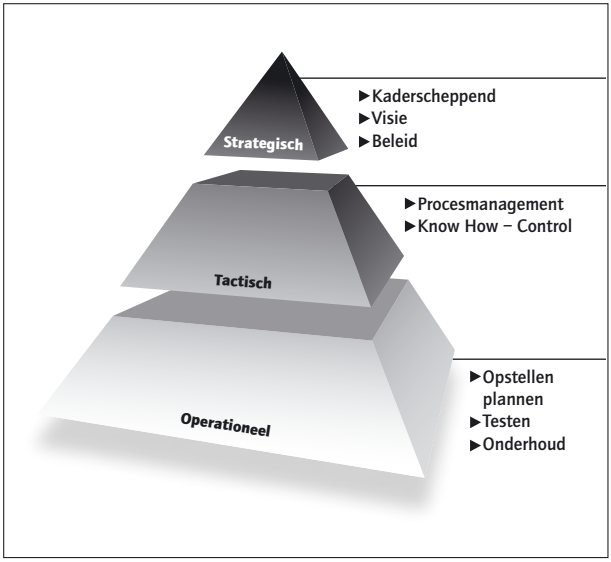
Zo kan een business unit in eerste instantie weliswaar input willen leveren voor de Business Impact Analyse ("welke gevolgschade ontstaat als ons proces wordt verstoord?"), maar nog niet de noodzaak zien zelf een continuïteitsplan voor het proces op te stellen. Wellicht zien zij uitsluitend de noodzaak voor een ICT uitwijkplan. Zou deze Business Unit echter worden betrokken in de uitwijktest voor ICT, dan wordt zij geconfronteerd met verlies van data en reconstructie van gegevens. Zo wordt het inzichtelijk dat ook voor het proces maatregelen moeten worden getroffen. Doordat nu, weliswaar later maar nog niet té laat, ook procesuitwijk bespreekbaar wordt, wordt het totaalresultaat beter.

Naast een holistisch proces, is het proces BCM dan ook een iteratief proces. De definitie van iteratie is herhaling. Een iteratief proces wil dat zeggen dat de activiteiten zich herhalen, zich vernieuwen en steeds opnieuw worden uitgevoerd. Hierbij wordt in opvolgende stappen naar een steeds beter resultaat toegewerkt. Dit resultaat krijgt steeds meer detail en diepgang en er wordt continu geleerd van voorgaande iteraties/stappen.

Geen van de processtappen kan compleet worden overgeslagen. Een stap kan echter wel worden geminimaliseerd indien daar bewust voor wordt gekozen en de motivatie volstaat. Zo kan de processtap 'Risico inventarisatie' niet worden overgeslagen, maar wel tot de volgende iteratie tot een minimum worden teruggebracht. Bijvoorbeeld door in eerste instantie slechts een beperkt aantal risico's of processen te beschouwen.

## De niveaus binnen het proces

Het BCM proces is een secundair proces, met een primaire functie, dat wordt uitgevoerd op verschillende niveaus in de organisatie.




*BCM proces in niveaus*

***Strategisch niveau***

Het beleid rondom BCM wordt op strategisch niveau vastgesteld. De scope van het proces wordt bepaald, de positionering van het proces geformaliseerd en de organisatorische verankering van BCM mogelijk gemaakt. Vervolgens worden er beslissingen genomen ten aanzien van de eisen aan de continuïteit van de bedrijfsprocessen. Een vereiste is dat binnen de strategie en beleidsbepaling proactief met continuïteitsaspecten wordt omgegaan. Op strategisch niveau ligt het eigenaarschap van het proces en de eindverantwoordelijkheid voor het resultaat.

***Tactisch niveau***

De besluitvorming die op strategisch niveau heeft plaatsgevonden, vormt op tactisch niveau het kader voor de inrichting en het management van

het BCM proces. Hier vindt de regie plaats over organisatiebrede activiteiten gerelateerd aan continuïteit. Voorbeelden van taken en verantwoordelijkheden op tactisch niveau zijn:

- Aansluiting realiseren op branche- of ondernemingsspecifieke wet- en regelgeving.
- Formuleren van de richtlijnen en normen waaraan het proces dient te voldoen.
- Het uitvoeren van analyses op het gebied van risico en impact op nieuwe en bestaande processen.
- Het ontwikkelen en borgen van het kennis- en ervaringsniveau binnen de organisatie.
- Op basis van het procesmodel dat op strategisch niveau is bepaald, worden de koppelvlakken tussen processen die een relatie kennen met continuïteit beschreven.
- Het beheren en beheersen van de overeengekomen SLA's met aanbieders van continuïteitsdiensten.

***Operationeel niveau***

Aan het proces dat op tactisch niveau is ingericht, wordt op operationeel niveau organisatiebreed uitvoering gegeven. De taken en verantwoordelijkheden omvatten:

- Het uitvoering geven aan het opstellen en onderhouden van het Stelsel van Maatregelen.
- Het uitvoeren van continuïteitstesten.
- Borgen van de vastgestelde serviceniveaus.

Het resultaat van de activiteiten op operationeel niveau, waaronder de testresultaten van het Stelsel van Maatregelen, vormen input voor tussentijdse analyse op tactisch niveau. Afhankelijk van de uitkomsten van die analyse kan er op strategisch niveau nieuwe besluitvorming of gewijzigd beleid tot stand komen. Hierdoor vindt de eerder genoemde iteratieve proceswerking plaats.

In de volgende paragrafen wordt het proces stap voor stap beschreven. Daarbij wordt gerefereerd naar modellen en sjablonen die in Hoofdstuk 4 zijn opgenomen.

*"Een gladiator maakt zijn plan*

*in de arena (te laat)."*

*Seneca 4vC-65nC,*

*Romeins schrijver en moralist*

## Beleid

Business Continuity Management Beleid komt helaas vaak reactief tot stand. Dat wil zeggen dat er op basis van incidenten en voorvallen gereageerd wordt. Proactief BCM beleid, als verzameling van doelen die op korte of langere termijn gerealiseerd moeten worden, geeft de organisatie richting, stabiliteit en samenhang.

Te vaak wordt er enthousiast begonnen met het realiseren van maatregelen, terwijl daar geen of onvoldoende beleidsmatig onderbouwde rechtvaardiging voor is. Dat kan tot gevolg hebben dat er uiteindelijk geen geld, tijd en dus geen commitment meer is om die maatregelen te onderhouden. Kapitaalvernietiging is het gevolg.

Elke implementatie van het BCM proces start met de vormgeving van Beleid. Doel van het BCM beleid is dat het strategisch management zich uitspreekt over en committeert aan de wijze waarop, hoe en waarmee de continuïteit van de organisatie wordt veiliggesteld. De positie van het proces wordt hier vastgesteld, overeenkomstig de cultuur, visie en missie van de organisatie en de aard van de 'industry'. De volgende aspecten worden ondermeer geadresseerd:

- *Rollen en verantwoordelijkheden*
  Binnen het management wordt een portefeuillehouder van het proces aangewezen. Er wordt een organisatievorm bepaald om aan het beleid uitvoering te geven (bijvoorbeeld in projectvorm) en de resources worden hieraan toegekend.

- *Scope van het proces*
  De organisatie(onder)delen of bedrijfsprocessen die binnen het risicobeschouwingsgebied vallen, worden vastgesteld. Er wordt bepaald welke typen van maatregelen binnen het werkgebied BCM vallen en welke worden uitgesloten.

- *Inrichting van het proces*
  Aan specifiek wenselijke aspecten van de invoering van BCM wordt prioriteit gegeven. Van reeds bestaande initiatieven binnen de organisatie wordt besloten of deze binnen het verantwoordelijkheidsgebied van BCM