

White paper

Business Continuity Management (BCM) bij Gemeenten

Continuïteitsrisico's bij informatie-uitwisseling in keten verband.



**VERDONCK
KLOOSTER &
ASSOCIATES**

Stef Liethoff

Dick Leegwater

Oktober 2010

Managementsamenvatting.....	2
Aanleiding	4
Ronde tafel bijeenkomst en interviews	6
Situatieschets.....	7
Inventarisatie kritieke processen.....	8
Inventarisatie belangrijkste risico's met grote impact	10
Specifieke risico's bij ketensamenwerking	11
Aanpak BCM.....	12
Tips voor BCM in ketenverband.....	17
Kritieke succesfactoren.....	18
Bijlage 1 – Overzicht risico's uit de workshop.....	20

Managementsamenvatting

De overheid staat voor de uitdaging aan burgers en bedrijven een integraal dienstenaanbod te leveren. Om aan de daaraan gekoppelde eisen van efficiency en effectiviteit te kunnen voldoen is ketenmanagement (lees: ketensamenwerking) noodzakelijk. In het bijzonder vormen gemeenten daarin het voorportaal en staan daarbij voor de vraag hoe de continuïteit van de bedrijfsprocessen in de keten te beheersen (Business Continuity Management ofwel BCM in de keten) en te waarborgen.

De uitdaging van ketenmanagement is dat er meer relaties en afhankelijkheden ontstaan en deze relaties en afhankelijkheden ook steeds zichtbaarder worden; hierdoor is de impact groter als bijvoorbeeld het systeem niet beschikbare of onjuiste informatie bevat. Dit vereist extra aandacht om hiermee samenhangende risico's te beperken.

Op basis van interviews, een rondetafel bijeenkomst met een achttal uiteenlopende gemeenten en de praktijkervaring vanuit VKA en Infráccent is een beeld gevormd van de actuele status van BCM binnen de gemeente wereld.

Hierbij valt op dat vanuit het gemeentelijk bestuur en de politiek onvoldoende bewustwording is van de impact van politieke besluiten op de continuïteit van de dienstverlening met als gevolg dat juiste en tijdige informatie bij kritieke processen zoals rampenbestrijding ontbreekt en ook dat onvoldoende budget voor BCM beschikbaar wordt gesteld.

Een tweede belangrijke bevinding is dat bij BCM voornamelijk wordt gekeken naar uitwijkvoorzieningen op het gebied van ICT en maar heel weinig naar het voorkomen van continuïteitsrisico's (preventie) en naar een goede respons op het optreden van ernstige verstoringen (repressie) ten aanzien van de dienstverlening.

Daarbij speelt dat de positie van BCM vaak is (weg)gedelegeerd binnen ICT; de primaire gebruikers (aan de bedrijfsvoeringskant) binnen de gemeentelijke diensten zijn zich nog niet bewust van hun eigen verantwoordelijkheid

In de genoemde ronde tafel bijeenkomst is door de deelnemers een beeld geschetst van de kritieke ketengerelateerde bedrijfsvoeringsprocessen en vervolgens een top vijf risico's vastgesteld:

1. Computerruimte/ generieke ICT voorzieningen en netwerk zijn niet beschikbaar;
2. Stroomvoorziening faalt
3. Personeel is niet beschikbaar
4. Telefoon/ Internet niet beschikbaar (dus geen communicatie meer mogelijk)
5. Corrupte (onjuiste of onvolledige) gegevens

Om deze risico's het hoofd te kunnen bieden is essentieel dat een gemeente zich de volgende vragen stelt alvorens een aanpak voor het bepalen van de vereiste continuïteitsmaatregelen:

- Hoe kan voorkomen worden dat het BCM-traject traag en ineffectief wordt gerealiseerd?
- Hoe houden we het draagvlak in de hele organisatie hoog?
- Hoe kunnen we snel successen boeken en veerkracht vergroten?
- Hoe worden de schaarse middelen (geld en menskracht) zo effectief mogelijk ingezet?
- Hoe wordt voorkomen dat de keuzes rondom bedrijfscontinuïteit worden bepaald op basis van "RTO's" (Recovery Time Objectives, ofwel de maximale uitvalduur), die niet met de praktijk stroken?

Bij een traditionele BCM aanpak wordt een project- of programmaplan opgesteld, een business impact analyse (BIA) uitgevoerd en vervolgens een risicoanalyse opgesteld en dan moet het management een strategie vaststellen alvorens deze tot uitvoering wordt gebracht in de nodige plannen en procedures.

Praktijkervaring leert dat een dergelijke traditionele aanpak leidt tot BCM-trajecten die vaak vele maanden en soms meer dan een jaar duren alvorens de organisatie voldoende robuustheid en veerkracht heeft om een crisis het hoofd te kunnen bieden.

Een alternatieve aanpak, die bij diverse organisaties met succes is toegepast, is gebaseerd op het doorwerken van één of meerdere crisisscenario's en geeft inzicht in de feitelijke maximale uitvalduur. Is deze acceptabel voor het management en heeft de organisatie bovendien een goede reputatie dan is de uitgebreide traditionele BCM aanpak overbodig geworden

Aan het slot van deze white paper staat een aantal tips voor BCM in ketenverband onder de hoofdpunten:

1. Vergroot het ketenperspectief
2. Versterk de samenwerking in de keten
3. Verstevig de afspraken met leveranciers
4. Versterk de BCM cultuur en bewustwording
5. Breng crisismanagement op het hoogste niveau.

Tenslotte een drietal succesfactoren voor een succesvolle implementatie van BCM:

1. Niet meer BCM "plannen" dan noodzakelijk
2. De crisismanagers binnen de gemeentelijke organisaties dienen over het nodige improvisatie- en organisatietalent en de nodige flexibiliteit te beschikken gefundeerd op weten wat belangrijk is (prioriteiten), goede back-up/herstel faciliteiten en up-to-date contactgegevens
3. BCM betreft de gehele organisatie. Zorg daarom (continu) voor voldoende bewustwording van het belang van BCM.

Aanleiding

De overheid is op diverse beleidsterreinen actief. Diverse aanbieders, waaronder de Rijksoverheid, provincies, gemeenten, semi-overheidsinstellingen en diverse commerciële bedrijven, bieden binnen deze beleidsterreinen een grote verscheidenheid aan producten en diensten aan. Deze organisaties opereren veelal los van elkaar. De uitdaging voor de overheid is hoe beleid, uitvoering en informatievoorziening rond complexe probleemsituaties van burgers en bedrijven voldoende op elkaar kunnen worden afgestemd voor een effectieve en klantgerichte publieke dienstverlening. De oplossing hiervoor is om met de verschillende aanbieders een zogenaamde ketensamenwerking op te zetten om zo een integraal dienstenaanbod te kunnen leveren aan de klanten. Gemeenten vormen in de meeste gevallen het zogenaamde voorportaal voor deze ketensamenwerking en worden hierdoor ook in de positie gedwongen om over deze samenwerkingsverbanden regie te voeren aangezien zij ook aangesproken worden op de effectiviteit en de kwaliteit van de dienstverlening waaronder het borgen van de continuïteit.

Deze white paper geeft een antwoord op de vraag binnen de gemeentelijke overheid: *hoe kunnen we de continuïteit van de bedrijfsprocessen in de keten beheersen (Business Continuity Management ofwel BCM in de keten) en waarborgen?*

In onderstaand kader staat een aantal voorbeelden van continuïteitsproblemen waar gemeenten mee te maken hebben gehad.

Een grootschalige storing bij een gemeente van tussen de 150.000 en 200.000 inwoners is mogelijk het gevolg geweest van sabotage. Een extern consultantsbureau deed onderzoek naar de oorzaak van de storing, en al vrij snel werd duidelijk dat de storing niet door een defect aan de apparatuur veroorzaakt is. Volgens de consultants valt "moedwillig menselijk handelen" dan ook niet uit te sluiten. Omdat het hier mogelijk een strafbaar feit betreft wordt nu de politie ingeschakeld en zal de gemeente donderdag aangifte doen. Op 2 oktober 2007 werd de gemeente getroffen door een storing in de hardware van het computernetwerk. De SAN (Storage Area Network) is de opslagruimte voor alle bij de gemeente in gebruik zijnde netwerkschijven. In deze SAN heeft een defect aan de inhoudsopgave er voor gezorgd dat alle gebruikersdata, de applicatiedata en de applicaties zelf niet meer toegankelijk waren. Nadat al op donderdag weer contact mogelijk was tussen de gemeente en het publiek, duurde het tot maandag 8 oktober voordat de storing volledig was verholpen. Er worden echter nog steeds data vermist. Zo is bijvoorbeeld al het inkomende en uitgaande e-mailverkeer van 2 oktober, en alle productie die op die dag gedraaid is, verdwenen. (bron www.security.nl)

De volgende aspecten illustreren het belang van BCM in de ketenprocessen van de gemeenten:

- De gemeente ontwikkelt zich tot het voorportaal van de overheid:

- De gemeente biedt 1 loket naar burgers, bedrijven en instellingen
- De diensten worden aangeboden via meerdere kanalen (Internet e-mail, telefonie, post, balie) hetgeen de complexiteit sterk vergroot.
- De gemeente is verantwoordelijk voor de regionale coördinatie en samenwerking bij handhaving en rampenbestrijding
- De gemeenten moet voor het aanbieden van haar diensten aansluiten op de zogenaamde e-overheidsvoorzieningen zoals Digid, de landelijke basisregistraties, BSN, etc.
- De gemeente is verantwoordelijk voor de integratie van de dienstverlening waardoor burgers en bedrijven kunnen volstaan met één aanvraag voor een samengesteld product (evt. vanuit meerdere (semi-)overheidsorganisaties, bedrijven en instellingen.
- De uitdaging van ketenverwerking is dat er meer relaties en afhankelijkheden ontstaan en deze relaties en afhankelijkheden ook steeds zichtbaarder worden; hierdoor is de impact groter als bijvoorbeeld het systeem niet beschikbare of onjuiste informatie bevat. Dit vereist extra aandacht om hiermee samenhangende risico's te beperken.

Om een goed en eenduidig beeld te krijgen van de problematiek van BCM binnen gemeenten hebben wij input verzameld uit een aantal interviews met gemeenten en uit de hierna gehouden rondetafel bijeenkomst met diverse gemeenten. Daarnaast hebben we de nodige informatie opgedaan uit de diverse adviesopdrachten die we hebben uitgevoerd bij gemeenten en andere overheidsinstellingen.

Hieronder volgen de belangrijkste bevindingen met betrekking tot BCM bij gemeenten:

- Het GBA is cruciaal bij de coördinatie en samenwerking bij rampenbestrijding. De huidige opzet van het GBA is minder geschikt voor de informatievoorziening bij regionale rampenbestrijding.
- Er is onvoldoende bewustwording bij het gemeentelijk bestuur en de politiek. Men realiseert zich onvoldoende dat politieke besluiten directe impact hebben op BCM. Dit heeft tot gevolg dat er ook onvoldoende budget voor BCM wordt gereserveerd.
- Digitale informatie groeit explosief. Hierdoor ontstaan problemen met het waarborgen van de beschikbaarheid van de data, doordat er o.a. problemen zijn met de maken van een kopie (backup) en het herstellen (restore) van kritieke informatie.
- Communicatie naar de burgers en bedrijven is cruciaal bij rampenbestrijding. Uitval van het callcenter bij een ramp moet dus te aller tijde vermeden worden.
- Er is onvoldoende aandacht voor het beheer van gebruikersnamen, wachtwoorden en toegangsrechten in de ketenverwerking van informatie.
- Er is onvoldoende aandacht voor het belang van beschikbare, juiste en tijdige informatie bij rampenbestrijding. Bijvoorbeeld scenario's als:
 - Op het moment dat een ramp plaatsvindt, valt ook de ICT infrastructuur uit;

- Op het moment dat een ramp plaatsvindt, is het stadskantoor niet meer beschikbaar;
- Op het moment dat een ramp plaatsvindt, zijn er onvoldoende gekwalificeerde mensen beschikbaar door bijvoorbeeld een pandemie.
- Er is onvoldoende inzicht in het belang en de prioriteit van de bedrijfsprocessen:
 - Welke processen moeten als eerste worden hersteld;
 - Het belang van de GBA processen bij de handhaving.
- Er is onvoldoende aandacht voor het voorkomen van misbruik van gegevens (privacy).
- Het bestuur en de politiek realiseren zich onvoldoende dat er verkeerde beleidsbeslissingen kunnen worden genomen door onjuiste of onvolledige informatie als gevolg van een calamiteit.
- Positie van BCM is nu vaak (weg)gedelegeerd binnen ICT; De primaire gebruikers (aan de bedrijfsvoeringskant) binnen de gemeentelijke diensten zijn zich nog niet bewust van hun eigen verantwoordelijkheid.
- In de praktijk blijkt discontinuïteit toch op verrassende plaatsen te zitten. Men denkt vaak niet aan de eenvoudige zaken die mis kunnen gaan. De vraag is: hoe kunnen we dit voorkomen?

Ronde tafel bijeenkomst en interviews

De hiervoor beschreven problematiek geeft ons de aanleiding om eens wat dieper van gedachten te wisselen met gemeenten en hierbij ook de gemeenten de gelegenheid te geven om ervaringen met elkaar uit te wisselen. De vorm die we hiervoor hebben gekozen is een zogenaamde rondetafel bijeenkomst. Deze rondetafel bijeenkomst hebben wij voorbereid door een aantal deelnemers aan de rondetafel bijeenkomst te interviewen. De volgende gemeenten hebben hun medewerking verleend aan deze bijeenkomst in het kader van BCM: Rotterdam, Amsterdam, Eindhoven, Groningen, Gouda, Ede, Hogeveen, Aalsmeer/Uithoorn.

Op basis van de genoemde interviews, de rondetafel bijeenkomst en de praktijkervaring vanuit VKA en Infráccent hebben we een beeld gevormd van de actuele status van BCM binnen de gemeente wereld.

In het volgende hoofdstuk zullen wij dieper ingaan op de situatieschets van BCM binnen de gemeentelijke wereld. Om deze situatieschets in beeld te brengen hebben we de volgende stappen doorlopen:

- Inventarisatie van de kritieke processen binnen de gemeenten;
- Inventarisatie van de belangrijkste risico's (oorzaken) met grote impact;
- Bepalen prioriteiten.

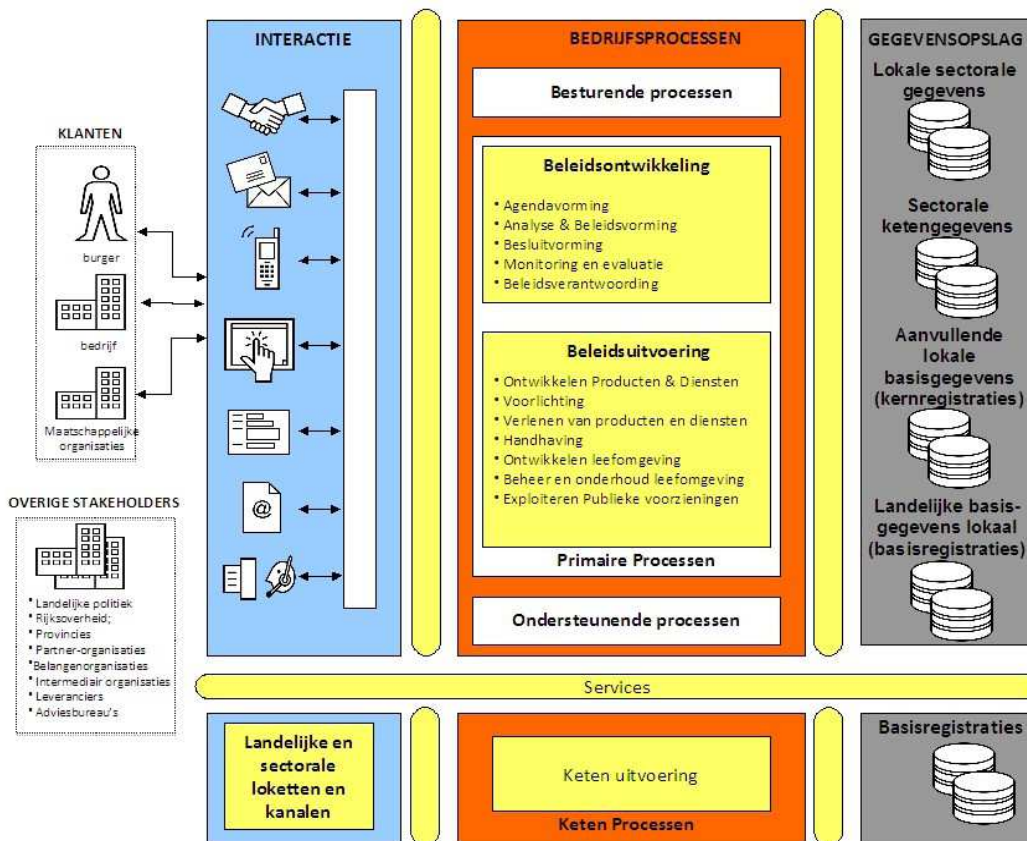
Aan de hand van de hiervoor genoemde stappen en de hierin gevoerde discussies is de situatieschets nader vorm gegeven.

Situatieschets

Zoals eerder vermeld vormen de gemeenten het voorportaal van de dienstverlening vanuit de overheid naar burgers en bedrijven. Als men naar de opzet van de dienstverlening kijkt, dan zien we dat deze bestaat uit de volgende lagen:

- Interactie: Vanuit deze laag vindt de communicatie plaats met de klanten en eventuele overige stakeholders. Deze communicatie vindt plaats over meerdere kanalen. Hierin zie je meteen de kern van de continuïteitsproblematiek, aangezien men deze kanalen te allen tijde beschikbaar moet houden en dat men de informatievoorziening en vastlegging van de informatie-uitwisseling over deze kanalen heen eenduidig moet houden.
- Bedrijfsprocessen: De bedrijfsprocessen kan men onderverdelen in besturende processen, primaire processen en ondersteunende processen.
- Gegevensopslag: De gemeente is verantwoordelijk voor de zogenaamde basisregistraties (o.a: persoonsgegevens, kadastrale gegevens, bedrijfsgegevens en topografische gegevens). Deze gegevens dienen eenmalig in de systemen te worden vastgelegd, op een wijze in overeenstemming met de richtlijnen van de rijksoverheid, waarmee toegankelijkheid, uitwisselbaarheid en actualiteit optimaal zijn.
- Services: Via zogenaamde services worden de hierboven beschreven componenten gekoppeld aan landelijke voorzieningen en ketenprocessen.

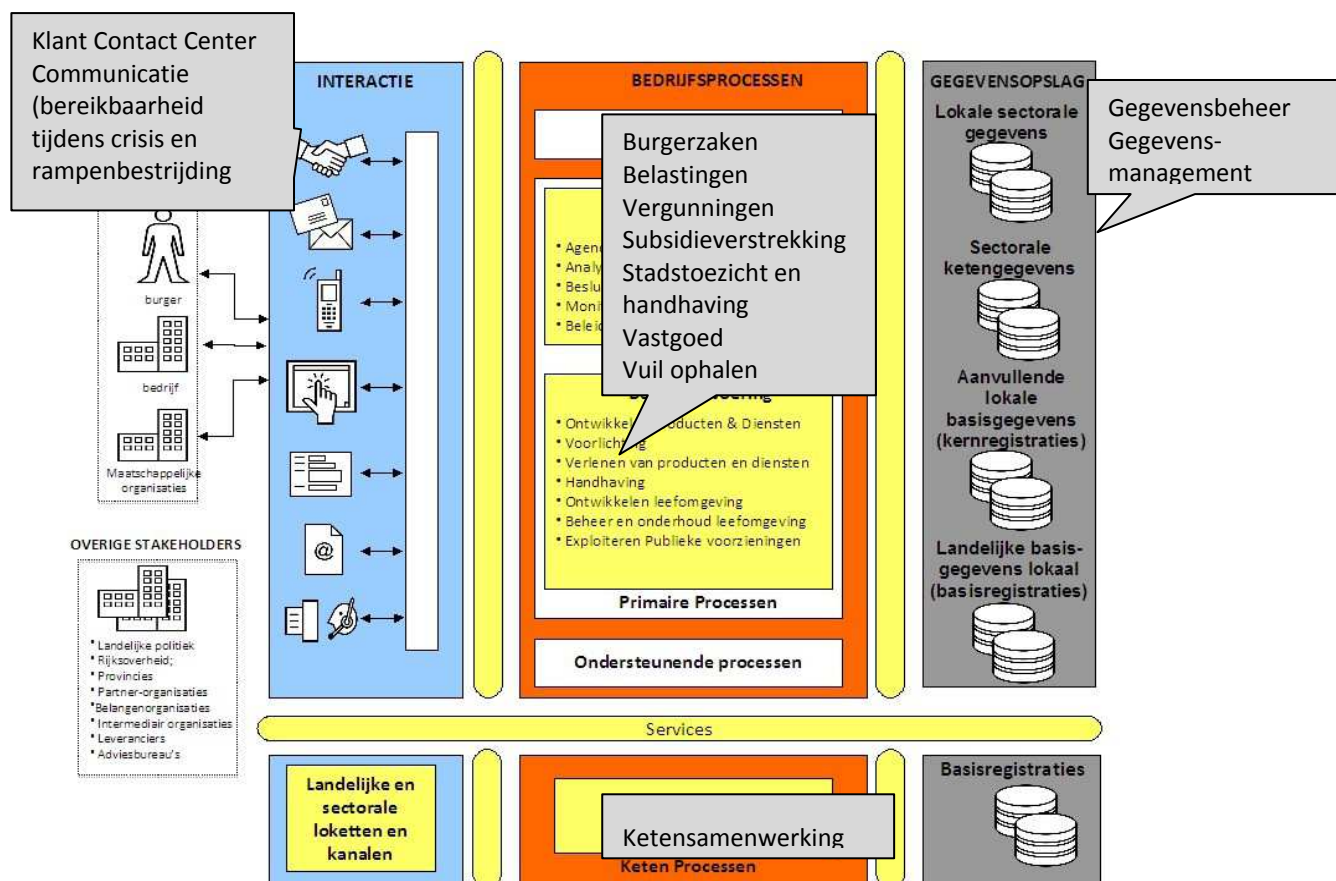
In het onderstaande plaatje zijn de hierboven beschreven lagen schematisch afgebeeld:



(Bron: GEMMA Thema's en Kernprincipes_ voor gemeentelijke proces- en informatiearchitectuur, 2009.03.30)

Inventarisatie kritieke processen

Het beheersen en verbeteren van processen is vaak terug te leiden tot het beheersen en reduceren van mogelijke risico's in deze processen. Tijdens de workshop in de rondetafel sessie hebben we de belangrijkste en meest kritieke processen en componenten geïnventariseerd. De focus van de discussie kwam te liggen op de risico's waarbij er imagoschade of juridische consequenties kunnen optreden. Het resultaat hiervan is weer geplot in het lagenmodel:



De belangrijkste bevindingen uit deze inventarisatie waren:

- Proces inventarisatie is een goed initiatief en vormt een goede basis voor de invoering van BCM in de organisatie. Echter in de praktijk blijkt dat bij uitval van een proces direct het probleem wordt neergelegd bij ICT. Of men gebruikt het verkeerde informatiesysteem of de gegevens in het informatiesysteem zijn niet juist. De oorzaak hiervan is dat men het informatiesysteem vaak niet goed gebruikt. Ook moet ICT ervoor zorgen dat indien de primaire systemen uitvallen deze binnen afzienbare tijd weer operationeel zijn of worden uitgeweken.
- Bij BCM wordt voornamelijk gekeken naar uitwijkvoorzieningen op het gebied van ICT en maar heel weinig naar het voorkomen van continuïteitsrisico's (preventie) en naar een goede respons op het optreden van ernstige verstoringen (repressie) ten aanzien van de dienstverlening..
- De eigenschappen, prioriteiten en betrouwbaarheidseisen van applicaties en de hiervan afhankelijke processen zijn niet in kaart gebracht.
- Burgerzaken wordt op regelmatige basis getoetst op de aanwezigheid van uitwijkvoorzieningen bijv. m.b.t. de GBA. Er wordt dus niet gekeken naar de volledige BCM aspecten.
- De ketenafhankelijkheid maakt het noodzakelijk dat men continuïteitsmaatregelen (soms extern) moet afdwingen.

- Risicobeheersing is voornamelijk gericht op het beperken van de imagoschade en het kunnen voldoen aan (externe) wet- en regelgeving'
- De positie van BCM is nu nog belegd binnen ICT; Primaire gebruikers en management zijn zich niet of onvoldoende bewust van hun verantwoordelijkheid op continuïteitsgebied.
- Het bepalen van de prioriteiten vindt plaats:
 - Of door externe triggers als wet- en regelgeving;
 - Of in combinatie met de lokale politieke ambitie/ imago.

Inventarisatie belangrijkste risico's met grote impact

In bijlage 1 zijn de risico's opgenomen die in de workshop zijn vastgesteld.

Uit deze lijst is door de deelnemers uit de workshop de top vijf risico's vastgesteld:

6. Computerruimte/ generieke ICT voorzieningen en netwerk zijn niet beschikbaar;
7. Stroomvoorziening faalt
8. Personeel is niet beschikbaar
9. Telefoon/ Internet niet beschikbaar (dus geen communicatie meer mogelijk)
10. Corrupte gegevens binnen het proces

De belangrijkste bevindingen uit deze risico-inventarisatie waren:

- Vanuit de business moet er input worden gegeven over het herstel van de voorzieningen. Wat is de maximaal toelaatbare uitvalduur en wat is het maximale dataverlies? Deze input is vaak niet bekend door het ontbreken van een risicoanalyse.
- IT- continuïteit wordt meer gedaan dan BCM. Er is onvoldoende bewustwording bij de bestuurlijke organisaties over het onderwerp. De algemene vraag is hoe krijgen we de bestuurlijke organisaties mee.
- De klassieke weg van BCM (op basis van de British Standard BS25999¹) duurt vaak veel te lang. Een pragmatische aanpak op basis van een realistisch scenario verdient de voorkeur (zie verderop in deze white paper).
- Men moet niet alleen focussen op de 'dramatische' incidenten met een zeer lage kans en met een hoge impact. Ook de lichtere incidenten zijn van belang. Deze komen relatief vaker voor (hogere kans) en bij elkaar opgeteld hebben deze incidenten ook een hoge impact.

Dit laatste punt leidt tot de vraag: "welke risico's als continuïteitsrisico's kunnen worden beschouwd?"

Van belang daarbij is dat er onderscheid wordt gemaakt tussen:

¹ Is verschenen in 2006/2007 en bestaat uit twee delen. Deel 1 is een praktijkcode met aanbevelingen en deel 2 bevat de specificaties/eisen van een Business Continuity Management Systeem (BCMS).

- **Crisiscontinuïteit** – dit is de meest ingrijpende vorm. Het te boven komen van een crisis is van levensbelang voor de gemeente, immers het imago c.q. het vertrouwen staat op het spel en zeker als door onvoldoende crisismanagement aanzienlijke schade voor de samenleving (menselijk leed, financiële schade door fraude of onzorgvuldig bestuur, economische schade, milieuschade) het gevolg is. Er zijn derhalve acties nodig om te overleven, de voor burgers en bedrijven onmisbare overheidsdienstverlening dan wel het geschonden imago c.q. vertrouwen voldoende te herstellen.
- **Operationele continuïteit** – min of meer business as usual; dat wil zeggen dat een operationeel continuïteitsprobleem een paar keer per jaar zou kunnen gebeuren. Als het printerpapier op is, is dat geen crisis waard. Vaak is in het gebouw nog ergens wel een doos, of anders is de kantoorboekhandel vlakbij. Als de auto met reisdocumenten in het kanaal terechtkomt is dat ernstig, maar in het algemeen geen ramp. De uitgifte van reisdocumenten stagneert, maar de gemeente zelf komt niet in gevaar.

Specifieke risico's bij ketensamenwerking

Voordat we ingaan op de specifieke risico's bij ketensamenwerking wordt een tweetal voorbeelden toegelicht van actuele samenwerkingsverbanden waar gemeenten bij betrokken zijn, dan wel de regievoerder zijn.

Bureau Keteninformatisering Werk en Inkomen (BKWI) die de samenwerking ondersteunt tussen gemeenten, CWI, UWV en de Sociale Verzekeringsbank (SVB). Het BKWI biedt voorzieningen waarmee deze organisaties hun gegevens op een efficiënte en betrouwbare manier met elkaar kunnen delen. Het BKWI beheert verder het maken van afspraken tussen de partners over de inhoud van de gegevens en de manier waarop die uitwisseling kan worden aangepakt.

Het Veiligheidshuis is een samenwerkingsverband, bestaande uit meerdere partners uit de straf- en zorgketen. Het bijzondere van het veiligheidshuisconcept is dat het geen eigenstandige organisatie is, maar zijn bestaansrecht moet bewijzen door de meerwaarde die de partners aan het Veiligheidshuis toekennen. De thema's die het Veiligheidshuis behandelt zijn casussen op het gebied van: veelplegers, risicojeugd, relationeel geweld, stedelijke problemen met accent op verslaving (gebiedsgerichte veiligheid). De werkzaamheden van het Veiligheidshuis concentreren zich rondom de behandeling en nazorg van een casus. Iedere partner heeft de beschikking over informatie over deze casus vanuit de eigen vakdiscipline van de partner. Een zorgverlener heeft zorggerelateerde informatie en het OM heeft informatie over het juridisch verleden van een casus. Iedere partner neemt zelf de beslissing in hoeverre informatie over een casus wordt gedeeld.

Zoals uit de hierboven beschreven voorbeelden blijkt, vereist ketensamenwerking intensieve informatie-uitwisseling tussen de partners. Deze uitwisseling van informatie is cruciaal voor een effectieve en efficiënte integrale aanpak, waarbij er veel meer informatie beschikbaar is over de probleemsituatie (zie casus veiligheidshuis). De ketenintegratie vormt daarbij het informatieknooppunt. De effectiviteit van de ketensamenwerking is dus afhankelijk van de beschikbaarheid en continuïteit van de informatie binnen dat knooppunt.

Binnen de ketensamenwerking worden de volgende risico's onderkend:

- De werking van de informatiesystemen is vaak onvoldoende, waardoor de informatie onjuist of onvolledig beschikbaar is;
- Het ontbreekt vaak ook aan concrete afspraken om de beschikbaarheid, de integriteit en de vertrouwelijkheid van de informatie te kunnen waarborgen;
- Vertegenwoordigers van de betrokken organisaties binnen de ketensamenwerking hebben geen of beperkte toegang tot de actuele informatie via de informatiesystemen bij de moederorganisatie.

In het voorgaande zijn de continuïteitsrisico's benoemd en is inzicht gegeven in de belangrijkste kritische componenten binnen de gemeente. Op basis van dit inzicht moeten de maatregelen worden gedefinieerd om de kans op een calamiteit te verminderen, dan wel de impact van de schade na optreden van een calamiteit zo klein mogelijk te houden. De aanpak hiervoor is beschreven in de volgende paragraaf.

Aanpak BCM

In deze paragraaf wordt allereerst kort ingegaan op de traditionele aanpak van BCM (gerelateerd aan de eerdere genoemde BS25999). Vervolgens wordt een alternatieve aanpak beschreven die naar onze mening veel beter aansluit bij de problematiek bij gemeenten. Met deze aanpak worden op pragmatische wijze snelle en concrete resultaten geboekt en wordt impliciet gewerkt aan het verhogen van de bewustwording over de continuïteitsproblematiek bij zowel het management als bij de betrokken medewerkers.

Voor beide aanpakken geldt dat voldaan moet zijn aan een aantal basisvoorwaarden om sowieso met BCM te starten.

Concreet houdt dit in dat op alle onderstaande vragen bevestigende moet kunnen geantwoord:

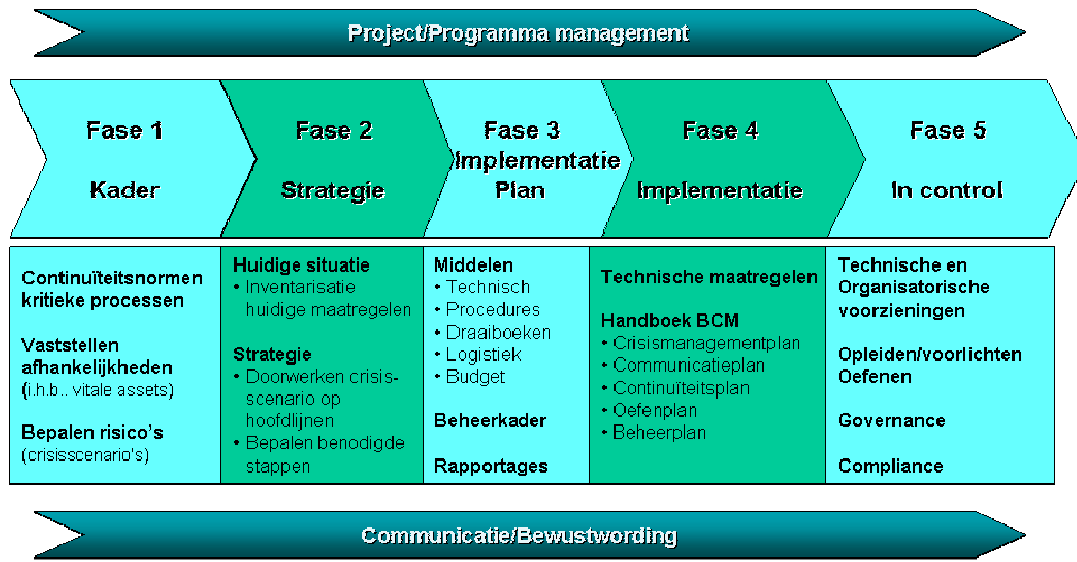
- Zijn er afdoende maatregelen tegen brand en bliksemschade getroffen?
- Zijn er afdoende maatregelen genomen in het kader van Informatiebeveiliging?
- Zijn de SPOF's zoveel mogelijk geëlimineerd? (Brenge voorzieningen aan in de architectuur)
- Zijn de afhankelijkheden geminimaliseerd van fysieke huisvesting ('het nieuwe

werken')?

- Zijn de maatregelen rondom de fysieke toegangsbeveiliging van de panden op orde?
- Is het personeel in het dagelijkse werk wel voldoende beschermd via Arbo-maatregelen?

Traditionele aanpak

De traditionele aanpak van BCM is gebaseerd op onderstaande stappen.



Figuur 2 BCM aanpak in 5 fasen

Deze stappen worden hieronder nader besproken.

1. In fase 1 (Kader) worden de kritieke processen en de omgevingsfactoren regelgeving, risico's en afhankelijkheden geïnventariseerd. Uitgaande van de impact van het falen van business c.q. dienstverlening (Business Impact Analysis oftewel BIA) worden continuïteitsnormen bepaald: de maximale uitvalduur van een proces en het maximale gegevensverlies. Eisen van klanten en 'de markt' alsmede van toezichthouders (compliance eisen) maken hier ook deel van uit. In deze fase worden tevens de vitale componenten oftewel kritieke assets bepaald waar de kritieke processen afhankelijk van zijn. Het bepalen van de risico's komt neer op het vaststellen welke crisisscenario's van belang zijn. Hierbij kan men denken aan het uitvallen van de telefonie, het niet kunnen beschikken over toegang tot het GBA bij een ramp in de Openbare Orde en veiligheid, het wegvallen van basisregistraties, geen toegang tot vitale databases zoals gevaarlijke stoffen, een pandemie of een 'worst case' scenario waarin het hele gebouw met alle voorzieningen door brand is verwoest.
2. In fase 2 (Strategie) wordt geïnventariseerd in hoeverre aan de continuïteitsnormen kan worden voldaan met het oog op de omgevingsfactoren en de huidige maatregelen. Het

is hiertoe van belang de crisisscenario's op hoofdlijnen door te werken dat wil zeggen de oplossingsrichting om de crisis te kunnen managen. De bijbehorende stappen worden bepaald, waarbij wordt aangeven hoe men deze wil uitvoeren. Dit leidt tot inzicht in de continuïteitskwetsbaarheden en in de maatregelen(opties) om deze kwetsbaarheden te reduceren dan wel op te heffen. Van belang is een duidelijke afweging te maken tussen preventieve maatregelen en repressieve maatregelen of bewust accepteren van een restrisico. Tegelijkertijd kan worden overwogen om al verbeteracties in gang te zetten (quick wins). In deze fase is het tevens van belang te bepalen hoe BCM governance en compliance moet worden ingericht.

3. In fase 3 (Implementatieplan) wordt de besluitvorming van fase 2 omgezet in implementatieplannen voor zowel de technische als organisatorische voorzieningen en bijbehorend beheerkader met de gewenste rapportages voor het management dan wel toezichthouders c.q. auditors.
4. In fase 4 (Implementatie) wordt het implementatieplan ten uitvoer gebracht en daarmee heeft de organisatie de beschikking over de noodzakelijke technische en organisatorische voorzieningen waaronder het handboek BCM met deelplannen voor crisismanagement, communicatie (extern en intern), continuïteit (c.q. noodoplossing) en oefenen alsmede een Beheerplan.
5. Eenmaal in fase 5 aangekomen is er sprake van BCM in Control: er is periodiek onderhoud met evaluaties van normen, risicoanalyses en plannen en er worden calamiteiten- en crisis oefeningen gehouden. Er is een continue proces van bewustwording, actualisering en geoefendheid gaande. Met andere woorden: er is een Business Continuity Management Systeem (BCMS).

Alternatieve aanpak

Waarom deze aanpak?

Praktijkervaring leert dat de traditionele aanpak leidt tot BCM-trajecten die vaak vele maanden en soms meer dan een jaar duren alvorens de organisatie voldoende robuustheid en veerkracht heeft om een crisis het hoofd te kunnen bieden.

Bij de traditionele aanpak wordt een project- of programmaplan opgesteld, een business impact analyse (BIA) uitgevoerd en vervolgens een risicoanalyse opgesteld en dan moet het management een strategie vaststellen alvorens deze tot uitvoering wordt gebracht in de nodige plannen en procedures.

Het wordt pas leuk als er wordt getest en geoefend, maar dan kan het draagvlak en de animo bij zowel het management als de betrokken medewerkers al behoorlijk zijn teruggelopen en kan er inmiddels een andere bedrijfssituatie zijn ontstaan of de benodigde aanpassingen op basis van de

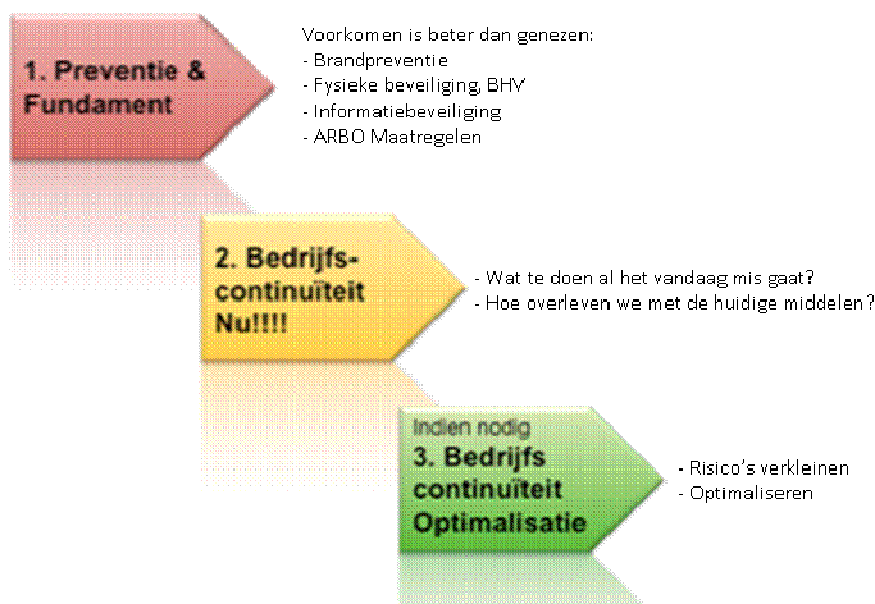
strategie zijn nog niet gerealiseerd.

Beschouw derhalve de volgende kritische vragen:

- Hoe kan voorkomen worden dat het BCM-traject traag en ineffectief wordt gerealiseerd?
- Hoe houden we het draagvlak in de hele organisatie hoog?
- Hoe kunnen we snel successen boeken en veerkracht vergroten?
- Hoe worden de schaarse middelen (geld en menskracht) zo effectief mogelijk ingezet?
- Hoe wordt voorkomen dat de keuzes rondom bedrijfscontinuïteit worden bepaald op basis van "RTO's" (Recovery Time Objectives), die niet met de praktijk stroken?

Een gereede kans dat de traditionele aanpak hier geen adequate oplossing biedt. Genoeg redenen dus om een andere weg te kiezen. Deze weg staat in figuur 3 en is veel meer gericht is op het omgekeerde van de traditionele aanpak, namelijk: begin met oefenen en stel op basis van de oefenresultaten vast of men voldoende bestand is tegen een crisis. Zo niet dan heeft men toch al enige ervaring met het managen van een crisis en zo ja dan kan een veel sneller BCM-traject worden doorlopen.

Meer effectieve aanpak BCM



Figuur 3 – Alternatieve aanpak BCM

In het kort bestaat de alternatieve aanpak uit drie stappen.

1. De eerste (Preventie & Fundament) is het nagaan of aan de bovengenoemde voorwaarden voor BCM is voldaan.
2. De tweede (Bedrijfscontinuïteit Nu!!!!) is de kern van de aanpak en wordt hieronder nader beschreven.

3. De derde (Bedrijfscontinuïteit Optimalisatie) is de traditionele aanpak, die alleen noodzakelijk is als de vorige stap onvoldoende resultaten oplevert.

Men voert bij de alternatieve aanpak als het ware een omgekeerde BIA uit zonder last te hebben van het toch vaak moeilijke traject om een goed beeld te krijgen van bijvoorbeeld de maximale uitvalduur of het maximale productieverlies van bijvoorbeeld gegevens. Verschillende c.q. wisselende personen geven verschillende schattingen en bovendien zijn schattingen van de impact van een calamiteit veeleer kwalitatief: "laag, midden of hoog".

'Bedrijfscontinuïteit Nu!!!' start met het doorwerken van één of meerdere crisisscenario's en geeft inzicht in de feitelijke maximale uitvalduur. Is deze acceptabel voor het management en heeft de organisatie bovendien een goede reputatie dan is de uitgebreide traditionele BCM aanpak (stap 3) overbodig.

Voorbeeldscenario's voor gemeenten zijn:

1. Het stadhuis is weg of voor langere tijd onbruikbaar
2. Het rekencentrum is weg of voor langere tijd onbruikbaar
3. Er is een langdurig tekort aan mensen bijvoorbeeld als gevolg van een pandemie

Voor alle duidelijkheid: de alternatieve aanpak is gericht op BCM, dus niet op bijvoorbeeld het vraagstuk welke uitwijkpolicy voor een rekencentrum optimaal is. In het laatste geval is het wel noodzakelijk een BIA uit te voeren en deze te vertalen naar continuïteitseisen voor de desbetreffende ICT-voorzieningen.

Doorwerken van de crisisscenario's houdt in: organiseer een leuke en vooral een effectieve droogzwem exercitie.

Vragen daarbij zijn:

- Wat is er mogelijk met de huidige middelen die de organisatie ter beschikking staan?
- Wie neemt tijdens de crisis vandaag de leiding? Wie neemt besluiten? Wie voert deze besluiten uit en hoe communiceren we met elkaar? En wie moeten we waarschuwen dat de productie stil ligt?
- Leg de antwoorden op deze vragen vast in een tweetal documenten ("Bedrijfscontinuïteitsplan" resp. "Crisismanagementplan". Maak tevens een structureel oefenplan.

Evaluatie:

- Zijn de gerealiseerde hersteltijden (Recovery Time Realisation!) acceptabel? Dan BCM traject klaar, ga anders een uitgebreid BCM traject in.

N.B. De vraag kan terecht worden gesteld of een auditor genoeg zal nemen met de alternatieve methode. Als deze methode echter leidt tot het duidelijk documenteren van de bevindingen c.q.

te nemen stappen betreffende crisismanagement, communicatiemanagement, continuïteitsmanagement en hoe deze 'in control' te houden, dan hoeft dit geen probleem te zijn.

Tips voor BCM in ketenverband

Voor het kunnen waarborgen van de continuïteit van het werken in ketenverband is een overzicht van de belangrijkste tips samengesteld:

6. Vergroot het ketenperspectief
 - Beschouw de keten niet alleen vanuit het oogpunt van kosten en/of dienstverlening, maar ook vanuit reductie van risico's en met name van continuïteitsrisico's. Let daarbij op kritieke paden in zowel de feitelijke dienstverlening (aan burgers en bedrijven) als de informatiestroom en op zwakke punten (bijvoorbeeld een single supplier).
 - Zorg voor een transparante keten niet alleen door te zorgen voor een betrouwbare informatievoorziening betreffende klantvraag en (diensten)leveringen, maar ook door risico's en reële crisisscenario's door de hele keten te communiceren.
 - Wees niet benauwd om re-engineering toe te passen door in de keten op de juiste posities ontkoppelpunten te creëren en intelligente capaciteitsplanning toe te passen waardoor op strategische posities additionele capaciteit (mensen, productie- en transportmiddelen) beschikbaar is.
 - Neem bij het inrichten van continuïteitsmaatregelen in de keten duurzaamheid mee als belangrijke enabler van kostenbesparing en imagoversterking
7. Versterk de samenwerking in de keten
 - Vorm samenwerkingsverbanden tussen gemeenten ten aanzien van BCM in de vorm van gemeenschappelijke noodvoorzieningen zoals een gezamenlijk uitwijkcentrum. Een ander voorbeeld is dat organisaties onderlinge afspraken maken om bijvoorbeeld bij een calamiteit elkaars printstraat (voor het printen van formulieren) te kunnen gebruiken.
 - Neem ook in ketenverband het aspect duurzaamheid mee in relatie tot BCM
8. Verstevig de afspraken met leveranciers
 - Ga geen outsourcingovereenkomst aan zonder een aantoonbaar kwalitatief continuïteitsplan van de andere partij.
 - Maak concrete afspraken met de leveranciers voor het geval zich een

calamiteit voordoet. Neem bijvoorbeeld een calamiteitenparagraaf op in de af te sluiten overeenkomsten met eventueel een aparte DAP (Dossier Afspraken Procedure).

9. Versterk de BCM cultuur en bewustwording
 - Schep een cultuur waarin BCM 'business as usual' wordt en in control is. Hierbij hoort periodiek updaten van continuïteitsnormen en het bijhouden van een lijst van de belangrijkste risico's, maar ook bijstellen van continuïteitsplannen en oefenen.
 - Zorg daarbij ook dat bij ontwikkeling van nieuwe producten of diensten de kwetsbaarheden met betrekking tot beschikbaarheid van onderdelen c.q. componenten en levertijden bekend zijn. Dit is vooral een issue bij outsourcing.
10. Breng crisismanagement op het hoogste niveau.
 - Zorg voor een adequaat waarschuwingsprotocol door de hele keten heen en voor snelle en betrouwbare communicatie met klanten, medewerkers en media. Oefen daar ook mee.
 - Organiseer een workshop met de belangrijkste ketenpartners om de alternatieve BCM methode toe te passen op een door alle partijen geaccepteerde crisissituatie

Kritieke succesfactoren

Deze white paper wordt afgesloten met het benoemen van een reeks kritieke succesfactoren (KSF's) voor een succesvolle implementatie van BCM. Dit betreft zowel intern als extern gerichte KSF's.

4. In het algemeen geldt de stelling: niet meer BCM "plannen" dan noodzakelijk. Randvoorwaarden, om in het geval van een crisis succesvol aan herstel van de continuïteit te kunnen werken (in eerste instantie veelal middels een noodoplossing), zijn:
 - De crisismanagers binnen de gemeentelijke organisaties dienen over het nodige improvisatie- en organisatietalent te beschikken;
 - Tegelijkertijd wordt aan de medewerkers maximale flexibiliteit gevraagd.
 - Binnen de gemeenten weet men wat belangrijk is (prioriteitenstelling);
 - Binnen de ICT infrastructuur beschikt men over goede back-up/herstel(restore) faciliteiten en redundantie heeft ingebouwd daar waar dat nodig is.

Men voorkomt hiermee "veel te dikke, boekenkastvullende" continuïteitsplannen.

5. De eis om laatstgenoemde te kunnen realiseren is dat men weet wat belangrijk is

(prioriteitenstelling), beschikt over goede back-up/restore faciliteiten en redundantie heeft ingebouwd daar waar dat nodig is.

6. Net zoals voor iedere andere investering zal ook voor BCM gelden dat de investering zakelijk onderbouwd moet zijn. Direct gevolg is dat er niet meer voorzieningen getroffen worden dan strikt noodzakelijk is.
7. Bij de zakelijke onderbouwing dient men de juiste afweging te maken tussen de 'verzekeringspremie' van BCM en de af te dekken continuïteitsrisico's. Met andere woorden zorg voor proportionele continuïteitsmaatregelen.
8. Bij de zakelijke onderbouwing dient niet alleen naar het investeringsplaatje te worden gekeken maar ook naar de operationele kosten waaronder de in het kader van duurzaamheid relevante energiekosten. De in het vorige punt vermelde flexibele respons strategie draagt hiertoe positief bij. Een energiezuinige (en CO2 arme) inrichting van een rekencentrum alsmede van de werkplekken is eveneens een belangrijk aspect. Behoedt u voor de valkuil dat concentratie van alle toepassingen in een shared service center altijd een gunstige duurzaamheidsfactor heeft. Het gaat uiteindelijk om de duurzaamheid in de gehele keten en inclusief mobiliteitskosten van het personeel.
9. Begin met de snelle weg conform de bovengeschetste alternatieve methode. Richt te allen tijde een kwaliteitscirkel op (Plan, Do, Check, Act in ("Deming")).
10. BCM betreft de gehele organisatie. Zorg daarom (continu) voor voldoende bewustwording van het belang van BCM. De leidinggevenden dienen het goede voorbeeld te geven. Organiseer oefeningen en zorg daarbij dat iedereen 'van harte' deelneemt.
11. Wees praktisch: zorg dat de belangrijkste telefoonnummers altijd voorhanden zijn ook al is de locatie niet meer bereikbaar of is de mobiele telefoon kwijtgeraakt. Zorg dat de belangrijkste documentatie, plannen en werkinstructies altijd beschikbaar zijn. Men komt vaak achter deze praktische tekortkomingen als men regelmatig oefent. Oefen ook als de meest ervaren mensen niet beschikbaar zijn!

Bijlage 1 – Overzicht risico's uit de workshop

Uit de workshop zijn de volgende risico's benoemd:

- Het niet beschikbaar zijn van personeel door bijvoorbeeld staking of ziekte;
- Men is teveel afhankelijk van de kennis van een enkel persoon (SPOF);
- Fraude;
- Het netwerk (infrastructuur) is niet beschikbaar;
- De generieke ICT voorzieningen zijn niet beschikbaar;
- Storingen aan hard- en software;
- Stroomvoorziening faalt;
- Calamiteit in computerruimte;
- Storing aan telefonie;
- Internetverbinding ligt eruit;
- Backup van gegevens niet beschikbaar;
- Gegevensstroom binnen de keten stagneert;
- Toegang van gegevens niet op orde na reorganisatie;
- Corrupte gegevens binnen proces;
- Autorisatiebeheer faalt;
- Geen continuïteitsvoorzieningen geregeld door bezuinigingen;
- Organisatie beschikt niet over een uitwijkstrategie;
- Politieke besluitvorming niet in lijn met beleid;
- Outsourcings - leverancier faalt.

Auteurs

Ing. Stef Liethoff is managing consultant bij Infráccent en is gespecialiseerd in informatiebeveiliging, risico management, identity & access management, PKI en in het beschrijven van ICT beveiligings-architecturen.

Dr. Dick Leegwater is management/executive consultant bij Verdonck, Klooster & Associates en gespecialiseerd in informatiebeveiliging, in procesmodellen ter beschrijving van bedrijfsprocessen in Business Continuity Management en duurzaamheid in ICT. Dick Leegwater is tevens als universitair docent verbonden aan de Erasmus Universiteit Rotterdam.